EURÓPSKA ÚNIA

EURÓPSKY PARLAMENT **RADA**

V Bruseli 14. mája 2024
(OR. en)

2021/0106(COD) **PE-CONS 24/24**

TELECOM 54
JAI 238
COPEN 69
CYBER 37
DATAPROTECT 76
EJUSTICE 11
COSI 16
IXIM 49
ENFOPOL 63
RELEX 180
MI 151
COMPET 154
CODEC 412

LEGISLATÍVNE AKTY A INÉ PRÁVNE AKTY

Predmet:	NARIADENIE EURÓPSKEHO PARLAMENTU A RADY, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii)

NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2024/...

z …,

ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii)

(Text s významom pre EHP)

EURÓPSKY PARLAMENT A RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä na jej články 16 a 114,

so zreteľom na návrh Európskej komisie,

po postúpení návrhu legislatívneho aktu národným parlamentom,

so zreteľom na stanovisko Európskeho hospodárskeho a sociálneho výboru[1],

so zreteľom na stanovisko Európskej centrálnej banky[2],

so zreteľom na stanovisko Výboru regiónov[3],

konajúc v súlade s riadnym legislatívnym postupom[4],

---

1 Ú. v. EÚ C 517, 22.12.2021, s. 56.
2 Ú. v. EÚ C 115, 11.3.2022, s. 5.
3 Ú. v. EÚ C 97, 28.2.2022, s. 60.
4 Pozícia Európskeho parlamentu z 13. marca 2024 (zatiaľ neuverejnená v úradnom vestníku) a rozhodnutie Rady z ...

keďže:

(1) Účelom tohto nariadenia je zlepšiť fungovanie vnútorného trhu stanovením jednotného právneho rámca, najmä pokiaľ ide o vývoj, uvádzanie na trh, uvádzanie do prevádzky a používanie systémov umelej inteligencie (ďalej len „systémy AI“) v Únii v súlade s hodnotami Únie, podporovať zavádzanie dôveryhodnej umelej inteligencie (ďalej len „AI“ – artificial intelligence) sústredenej na človeka a zároveň zaistiť vysokú úroveň ochrany zdravia, bezpečnosti a základných práv zakotvených v Charte základných práv Európskej únie (ďalej len „charta“), vrátane ochrany demokracie, právneho štátu a životného prostredia, chrániť pred škodlivými účinkami systémov AI v Únii a podporovať inovácie. Týmto nariadením sa zabezpečuje voľný pohyb tovaru a služieb založených na AI cez hranice, čím sa členským štátom zabraňuje ukladať obmedzenia na vývoj, uvádzanie na trh a používanie systémov AI, pokiaľ to toto nariadenie výslovne nepovoľuje.

(2) Toto nariadenie by sa malo uplatňovať v súlade s hodnotami Únie zakotvenými v charte, čím sa uľahčí ochrana fyzických osôb, podnikov, demokracie, právneho štátu a životného prostredia a zároveň sa podporia inovácie a zamestnanosť a Únia sa stane lídrom v zavádzaní dôveryhodnej AI.

(3) Systémy AI možno ľahko nasadiť vo veľkej škále odvetví hospodárstva a mnohých oblastiach spoločnosti, a to aj cezhranične, a môžu ľahko obiehať po celej Únii. Niektoré členské štáty už zvažujú prijatie vnútroštátnych pravidiel na zabezpečenie toho, aby bola AI dôveryhodná a bezpečná a aby sa vyvíjala a používala v súlade s povinnosťami týkajúcimi sa základných práv. Rozdielne vnútroštátne pravidlá môžu viesť k fragmentácii vnútorného trhu a znížiť právnu istotu pre prevádzkovateľov, ktorí vyvíjajú, dovážajú alebo používajú systémy AI. Mala by sa preto zabezpečiť konzistentná a vysoká úroveň ochrany v celej Únii, aby sa dospelo k dôveryhodnej AI, pričom by sa malo zabrániť rozdielom, ktoré bránia voľnému obehu, inováciám, nasadzovaniu a zavádzaniu systémov AI a súvisiacich výrobkov a služieb v rámci vnútorného trhu, a to stanovením jednotných povinností pre prevádzkovateľov a zaručením jednotnej ochrany prevažujúcich dôvodov verejného záujmu a práv osôb na celom vnútornom trhu na základe článku 114 Zmluvy o fungovaní Európskej únie (ďalej len „ZFEÚ“). Pokiaľ toto nariadenie obsahuje osobitné pravidlá ochrany jednotlivcov pri spracúvaní osobných údajov týkajúce sa obmedzení používania systémov AI na diaľkovú biometrickú identifikáciu na účely presadzovania práva, používania systémov AI na posudzovanie rizík fyzických osôb na účely presadzovania práva a používania systémov AI s biometrickou kategorizáciou na účely presadzovania práva, je vhodné, pokiaľ ide o uvedené osobitné pravidlá, aby bol základom tohto nariadenia článok 16 ZFEÚ. Pokiaľ ide o tieto osobitné pravidlá a použitie článku 16 ZFEÚ, je vhodné konzultovať s Európskym výborom pre ochranu údajov.

(4) AI je rýchlo sa rozvíjajúca skupina technológií, ktorá prispieva k širokému spektru hospodárskych, environmentálnych a spoločenských prínosov vo všetkých odvetviach a spoločenských činnostiach. Zlepšením predpovedí, optimalizáciou operácií a prideľovania zdrojov a personalizáciou digitálnych riešení, ktoré sú k dispozícii jednotlivcom a organizáciám, môže využívanie AI poskytnúť podnikom kľúčové konkurenčné výhody a podporiť sociálne a environmentálne priaznivé výsledky, napríklad v oblasti zdravotnej starostlivosti, poľnohospodárstva, bezpečnosti potravín, vzdelávania a odbornej prípravy, médií, športu a kultúry, riadenia infraštruktúry, energetiky, dopravy a logistiky, verejných služieb, bezpečnosti, spravodlivosti, efektívneho využívania zdrojov a energie, monitorovania životného prostredia, zachovania a obnovy biodiverzity a ekosystémov a zmierňovania zmeny klímy a adaptácie na ňu.

(5) AI môže zároveň v závislosti od okolností týkajúcich sa jej konkrétnej aplikácie, použitia a úrovne technologického vývoja vytvárať riziká a ujmu pre verejné záujmy a základné práva, ktoré sú chránené právom Únie. Toto poškodzovanie môže byť hmotné aj nehmotné vrátane fyzickej, psychickej, spoločenskej alebo ekonomickej ujmy.

(6) Vzhľadom na veľký vplyv, ktorý AI môže mať na spoločnosť, a na potrebu budovať dôveru je nevyhnutné, aby sa AI a jej regulačný rámec rozvíjali v súlade s hodnotami Únie zakotvenými v článku 2 Zmluvy o Európskej únii (ďalej len „Zmluva o EÚ“), základnými právami a slobodami zakotvenými v zmluvách a podľa článku 6 Zmluvy o EÚ v charte. Nevyhnutnou podmienkou je, aby AI bola technológiou sústredenou na človeka. Mala by slúžiť ako nástroj pre ľudí s konečným cieľom zvyšovať ich blahobyt.

(7) S cieľom zabezpečiť jednotnú a vysokú úroveň ochrany verejných záujmov, pokiaľ ide o zdravie, bezpečnosť a základné práva, by sa mali stanoviť spoločné pravidlá pre vysokorizikové systémy AI. Tieto pravidlá by mali byť v súlade s chartou a mali by byť nediskriminačné a v súlade so záväzkami Únie v oblasti medzinárodného obchodu. Mali by zohľadňovať aj Európske vyhlásenie o digitálnych právach a zásadách v digitálnom desaťročí a etické usmernenia pre dôveryhodnú AI expertnej skupiny na vysokej úrovni pre umelú inteligenciu.

(8) Na podporu rozvoja, využívania a zavádzania AI na vnútornom trhu je preto potrebný právny rámec Únie, ktorým sa stanovujú harmonizované pravidlá v oblasti AI a ktorý zároveň spĺňa vysokú úroveň ochrany verejných záujmov, ako sú zdravie a bezpečnosť, a ochrany základných práv vrátane ochrany demokracie, právneho štátu a životného prostredia, ako sú uznané a chránené právom Únie. Na dosiahnutie tohto cieľa by sa mali stanoviť pravidlá upravujúce uvádzanie určitých systémov AI na trh, do prevádzky a ich používanie, čím sa zabezpečí hladké fungovanie vnútorného trhu a umožní sa, aby tieto systémy využívali zásadu voľného pohybu tovaru a služieb. Tieto pravidlá by mali byť jasné a spoľahlivé pri ochrane základných práv, mali by podporovať nové inovačné riešenia, byť nápomocné európskemu ekosystému verejných a súkromných aktérov vytvárajúcich systémy AI v súlade s hodnotami Únie a mali by uvoľňovať potenciál digitálnej transformácie vo všetkých regiónoch Únie. Stanovením uvedených pravidiel, ako aj opatrení na podporu inovácie s osobitným dôrazom na malé a stredné podniky (ďalej len „MSP“) vrátane startupov v tomto nariadení sa podporí cieľ presadzovať európsky prístup k AI sústredený na človeka a stať sa svetovým lídrom v rozvoji bezpečnej, dôveryhodnej a etickej AI, ako to vyjadrila Európska rada[5], a zabezpečí sa ochrana etických zásad, ako to osobitne požaduje Európsky parlament[6].

---

5 Európska rada, mimoriadne zasadnutie Európskej rady (1. a 2. októbra 2020) – závery, EUCO 13/20, 2020, s. 6.

6 Uznesenie Európskeho parlamentu z 20. októbra 2020 s odporúčaniami pre Komisiu k rámcu etických aspektov umelej inteligencie, robotiky a súvisiacich technológií, 2020/2012(INL).

(9) Harmonizované pravidlá uplatniteľné na uvádzanie vysokorizikových systémov AI na trh, do prevádzky a na ich používanie by sa mali stanoviť v súlade s nariadením Európskeho parlamentu a Rady (ES) č. 765/2008[7], rozhodnutím Európskeho parlamentu a Rady č. 768/2008/ES[8] a s nariadením Európskeho parlamentu a Rady (EÚ) 2019/1020[9] (ďalej len „nový legislatívny rámec“). Harmonizované pravidlá stanovené v tomto nariadení by sa mali uplatňovať vo všetkých odvetviach a v súlade s novým legislatívnym rámcom by nimi nemali byť dotknuté existujúce právne predpisy Únie, najmä pokiaľ ide o ochranu údajov, ochranu spotrebiteľa, základné práva, zamestnanosť, ochranu pracovníkov a bezpečnosť výrobkov, ktoré sa týmto nariadením dopĺňajú. V dôsledku toho všetky práva a prostriedky nápravy stanovené takýmto právom Únie pre spotrebiteľov a iné osoby, na ktoré môžu mať systémy AI negatívny vplyv, a to aj pokiaľ ide o náhradu možných škôd podľa smernice Rady 85/374/EHS[10], zostávajú nedotknuté a plne uplatniteľné.

---

7 Nariadenie Európskeho parlamentu a Rady (ES) č. 765/2008 z 9. júla 2008, ktorým sa stanovujú požiadavky akreditácie a ktorým sa zrušuje nariadenie (EHS) č. 339/93 (Ú. v. EÚ L 218, 13.8.2008, s. 30).

8 Rozhodnutie Európskeho parlamentu a Rady č. 768/2008/ES z 9. júla 2008 o spoločnom rámci na uvádzanie výrobkov na trh a o zrušení rozhodnutia 93/465/EHS (Ú. v. EÚ L 218, 13.8.2008, s. 82).

9 Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/1020 z 20. júna 2019 o dohľade nad trhom a súlade výrobkov a o zmene smernice 2004/42/ES a nariadení (ES) č. 765/2008 a (EÚ) č. 305/2011 (Ú. v. EÚ L 169, 25.6.2019, s. 1).

10 Smernica Rady 85/374/EHS z 25. júla 1985 o aproximácii zákonov, iných právnych predpisov a správnych opatrení členských štátov o zodpovednosti za chybné výrobky (Ú. v. ES L 210, 7.8.1985, s. 29).

Okrem toho by toto nariadenie v kontexte zamestnania a ochrany pracovníkov nemalo mať vplyv na právo Únie v oblasti sociálnej politiky a vnútroštátne pracovné právo, ktoré je v súlade s právom Únie, pokiaľ ide o podmienky zamestnávania a pracovné podmienky vrátane ochrany zdravia a bezpečnosti pri práci a vzťahu medzi zamestnávateľmi a pracovníkmi. Týmto nariadením by nemalo byť dotknuté ani vykonávanie základných práv uznaných v členských štátoch a na úrovni Únie vrátane práva na štrajk alebo slobody štrajkovať alebo prijímať iné opatrenia, na ktoré sa vzťahujú osobitné systémy odvetvových vzťahov v členských štátoch, ako aj práva rokovať o kolektívnych dohodách, uzatvárať a presadzovať ich alebo prijímať kolektívne opatrenia v súlade s vnútroštátnym právom. Týmto nariadením by nemali byť dotknuté ustanovenia zamerané na zlepšenie pracovných podmienok v oblasti práce pre platformy stanovené v smernici Európskeho parlamentu a Rady o zlepšení pracovných podmienok v oblasti práce pre platformy. Okrem toho je cieľom tohto nariadenia posilniť účinnosť takýchto existujúcich práv a prostriedkov nápravy stanovením osobitných požiadaviek a povinností, a to aj pokiaľ ide o transparentnosť, technickú dokumentáciu a vedenie záznamov o systémoch AI. Povinnosti uložené rôznym prevádzkovateľom zapojeným do hodnotového reťazca AI podľa tohto nariadenia by sa zároveň mali uplatňovať bez toho, aby bolo dotknuté vnútroštátne právo, ktoré je v súlade s právom Únie a ktorým sa obmedzuje používanie určitých systémov AI v prípadoch, keď takéto právo nepatrí do rozsahu pôsobnosti tohto nariadenia alebo sleduje iné legitímne ciele verejného záujmu, než sú ciele tohto nariadenia. Toto nariadenie by napríklad nemalo mať vplyv na vnútroštátne pracovné právo a právne predpisy o ochrane maloletých, teda osôb mladších ako 18 rokov, s prihliadnutím na všeobecnú poznámku č. 25 (2021) Dohovoru OSN o právach dieťaťa v súvislosti s digitálnym prostredím, pokiaľ sa osobitne netýkajú systémov AI a sú zamerané na iné legitímne ciele verejného záujmu.

(10) Základné právo na ochranu osobných údajov je zaručené najmä nariadeniami Európskeho parlamentu a Rady (EÚ) 2016/679[11] a (EÚ) 2018/1725[12] a smernicou Európskeho parlamentu a Rady (EÚ) 2016/680[13]. Súkromný život a dôvernosť komunikácií dodatočne chráni smernica Európskeho parlamentu a Rady 2002/58/ES[14], okrem iného prostredníctvom stanovenia podmienok akéhokoľvek uchovávania osobných a iných ako osobných údajov, ktoré boli uložené v koncovom zariadení a ku ktorým sa pristupuje prostredníctvom tohto zariadenia. Uvedené legislatívne akty Únie vytvárajú základ udržateľného a zodpovedného spracúvania údajov vrátane prípadov, keď súbory údajov obsahujú kombináciu osobných a iných ako osobných údajov. Cieľom tohto nariadenia nie je ovplyvniť uplatňovanie existujúcich právnych predpisov Únie upravujúcich spracúvanie osobných údajov vrátane úloh a právomocí nezávislých dozorných orgánov zodpovedných za monitorovanie súladu s týmito nástrojmi.

---

11 Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1).

12 Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES (Ú. v. EÚ L 295, 21.11.2018, s. 39).

13 Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV (smernica o presadzovaní práva) (Ú. v. EÚ L 119, 4.5.2016, s. 89).

14 Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) (Ú. v. ES L 201, 31.7.2002, s. 37).

Nie sú ním dotknuté ani povinnosti poskytovateľov systémov AI a subjektov nasadzujúcich systémy AI v ich úlohe prevádzkovateľov alebo sprostredkovateľov vyplývajúce z práva Únie alebo vnútroštátneho práva o ochrane osobných údajov, pokiaľ dizajn, vývoj alebo používanie systémov AI zahŕňa spracúvanie osobných údajov. Takisto je vhodné objasniť, že dotknuté osoby naďalej požívajú všetky práva a záruky, ktoré im takéto právo Únie priznáva, vrátane práv súvisiacich s výlučne automatizovaným individuálnym rozhodovaním vrátane profilovania. Harmonizované pravidlá uvádzania na trh, uvádzania do prevádzky a používania systémov AI stanovené v tomto nariadení by mali uľahčiť účinné vykonávanie a umožniť uplatňovanie práv dotknutých osôb a iných prostriedkov nápravy zaručených právom Únie o ochrane osobných údajov a iných základných práv.

(11) Týmto nariadením by nemali byť dotknuté ustanovenia o zodpovednosti poskytovateľov sprostredkovateľských služieb stanovené v nariadení Európskeho parlamentu a Rady (EÚ) 2022/2065[15].

[15] Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES (akt o digitálnych službách) (Ú. v. EÚ L 277, 27.10.2022, s. 1).

(12) Pojem „systém AI“ v tomto nariadení by sa mal jasne vymedziť a mal by sa úzko zosúladiť s prácou medzinárodných organizácií, ktoré sa zaoberajú AI, s cieľom zabezpečiť právnu istotu, uľahčiť medzinárodné zbližovanie a širokú akceptáciu, a zároveň poskytnúť flexibilitu na prispôsobenie sa rýchlemu technologickému vývoju v tejto oblasti. Okrem toho by vymedzenie malo byť založené na kľúčových charakteristikách systémov AI, ktorými sa odlišuje od jednoduchších tradičných softvérových systémov alebo programovacích prístupov, a nemalo by sa vzťahovať na systémy, ktoré sú založené na pravidlách vymedzených výlučne fyzickými osobami na automatické vykonávanie operácií. Kľúčovou charakteristikou systémov AI je ich spôsobilosť odvodzovať. Táto spôsobilosť odvodzovať sa týka procesu získavania výstupov, ako sú predpovede, obsah, odporúčania alebo rozhodnutia, ktoré môžu ovplyvniť fyzické alebo virtuálne prostredie, a spôsobilosti systémov AI odvodzovať zo vstupov alebo údajov modely alebo algoritmy, alebo oboje. Techniky, ktoré umožňujú odvodzovať pri budovaní systému AI, zahŕňajú prístupy strojového učenia, ktoré sa z údajov učia, ako dosiahnuť určité ciele, a prístupy založené na logike a vedomostiach, ktoré odvodzujú riešenie úloh zo zakódovaných poznatkov alebo symbolického znázornenia. Schopnosť systému AI odvodzovať presahuje základné spracúvanie údajov tým, že umožňuje učenie sa, odôvodňovanie alebo modelovanie. Pojem „strojový“ sa vzťahuje na skutočnosť, že systémy AI fungujú na strojoch.

Odkaz na explicitné alebo implicitné ciele zdôrazňuje, že systémy AI môžu fungovať podľa explicitných definovaných cieľov alebo podľa implicitných cieľov. Ciele systému AI sa môžu líšiť od zamýšľaného účelu systému AI v konkrétnom kontexte. Na účely tohto nariadenia by sa pod prostrediami mali rozumieť kontexty, v ktorých systémy AI fungujú, zatiaľ čo výstupy generované systémom AI odrážajú rôzne funkcie vykonávané systémami AI a zahŕňajú predpovede, obsah, odporúčania alebo rozhodnutia. Systémy AI sú dizajnované tak, aby fungovali s rôznymi úrovňami autonómnosti, čo znamená, že pri svojej činnosti majú určitý stupeň nezávislosti od ľudskej účasti a určitý stupeň spôsobilosti fungovať bez ľudského zásahu. Adaptabilita, ktorú by systém AI mohol preukázať po nasadení, sa týka samovzdelávacích spôsobilostí, vďaka ktorým sa môže systém zmeniť počas používania. Systémy AI sa môžu používať samostatne alebo ako komponent výrobku bez ohľadu na to, či je tento systém do výrobku fyzicky integrovaný (zabudovaný) alebo či slúži funkčnosti tohto výrobku bez toho, aby doň bol integrovaný (nezabudovaný).

(13) Pojem „nasadzujúci subjekt“ uvedený v tomto nariadení by sa mal vykladať ako akákoľvek fyzická alebo právnická osoba vrátane orgánu verejnej moci, verejnej agentúry alebo iného verejného subjektu, ktorá systém AI používa v rámci svojej právomoci, s výnimkou systému AI používaného počas osobnej neprofesionálnej činnosti. V závislosti od typu systému AI môže mať používanie systému vplyv na iné osoby, než je nasadzujúci subjekt.

(14) Pojem „biometrické údaje“ použitý v tomto nariadení by sa mal vykladať so zreteľom na pojem biometrické údaje v zmysle vymedzenia v článku 4 bode 14 nariadenia (EÚ) 2016/679, článku 3 bode 18 nariadenia (EÚ) 2018/1725 a článku 3 bode 13 smernice (EÚ) 2016/680. Biometrické údaje môžu umožniť autentifikáciu, identifikáciu alebo kategorizáciu fyzických osôb a rozpoznávanie emócií fyzických osôb.

(15) Pojem „biometrická identifikácia“ uvedený v tomto nariadení by sa mal vymedziť ako automatické rozpoznávanie fyzických, fyziologických a behaviorálnych ľudských znakov, ako sú tvár, pohyb očí, tvar tela, hlas, reč, chôdza, držanie tela, srdcová frekvencia, tlak krvi, vôňa, dynamika písania na klávesnici, na účely stanovenia totožnosti jednotlivca porovnaním biometrických údajov daného jednotlivca s biometrickými údajmi jednotlivcov uloženými v referenčnej databáze, bez ohľadu na to, či jednotlivec udelil súhlas alebo nie. To nezahŕňa systémy AI určené na biometrické overenie zahŕňajúce autentifikáciu, ktorého jediným účelom je potvrdiť, že konkrétna fyzická osoba je tou osobou, o ktorej tvrdí, že ňou je, a potvrdiť totožnosť fyzickej osoby výlučne na účely prístupu k službe, odomknutia zariadenia alebo získania bezpečnostného prístupu do priestorov.

(16) Pojem „biometrická kategorizácia“ uvedený v tomto nariadení by sa mal vymedziť ako zaradenie fyzických osôb do osobitných kategórií na základe ich biometrických údajov. Takéto špecifické kategórie sa môžu týkať aspektov ako pohlavie, vek, farba vlasov, farba očí, tetovania, behaviorálne alebo osobnostné črty, jazyk, náboženstvo, príslušnosť k národnostnej menšine, sexuálna alebo politická orientácia. Nezahŕňa to systémy biometrickej kategorizácie, ktoré sú čisto vedľajšou funkciou neoddeliteľne spojenou s inou komerčnou službou, čo znamená, že táto funkcia sa z objektívnych technických dôvodov nemôže používať bez hlavnej služby, a integrácia uvedenej funkcie alebo funkcionality nie je prostriedkom obchádzania uplatniteľnosti pravidiel tohto nariadenia. Napríklad filtre, ktoré kategorizujú tvárové alebo telesné znaky používané na online trhoch, by mohli predstavovať takúto vedľajšiu funkciu, keďže sa môžu použiť len v súvislosti s hlavnou službou, ktorá spočíva v predaji výrobku tým, že sa spotrebiteľovi umožní nahliadnuť do zobrazenia výrobku na sebe a pomôcť mu pri rozhodovaní o kúpe. Filtre používané pri online službách sociálnych sietí, ktoré kategorizujú tvárové alebo telesné znaky s cieľom umožniť používateľom pridávať alebo upravovať obrázky alebo videá, by sa takisto mohli považovať za vedľajšiu funkciu, keďže takýto filter nemožno použiť bez hlavnej služby sociálnej siete spočívajúcej v zdieľaní obsahu online.

(17) Pojem „systém diaľkovej biometrickej identifikácie“ uvedený v tomto nariadení by sa mal vymedziť funkčne ako systém AI určený na identifikáciu fyzických osôb bez ich aktívneho zapojenia, zvyčajne na diaľku, porovnávaním biometrických údajov osoby s biometrickými údajmi obsiahnutými v referenčnej databáze, a to bez ohľadu na konkrétne použité technológie, procesy alebo typy biometrických údajov. Takéto systémy diaľkovej biometrickej identifikácie sa zvyčajne používajú na vnímanie viacerých osôb alebo ich správania súčasne, a to s cieľom výrazne uľahčiť identifikáciu fyzických osôb bez ich aktívneho zapojenia. To nezahŕňa systémy AI určené na biometrické overenie zahŕňajúce autentifikáciu, ktorého jediným účelom je potvrdiť, že konkrétna fyzická osoba je tou osobou, o ktorej tvrdí, že ňou je, a potvrdiť totožnosť fyzickej osoby výlučne na účely prístupu k službe, odomknutia zariadenia alebo získania bezpečnostného prístupu do priestorov. Toto vylúčenie je odôvodnené skutočnosťou, že takéto systémy majú pravdepodobne malý vplyv na základné práva fyzických osôb v porovnaní so systémami diaľkovej biometrickej identifikácie, ktoré sa môžu použiť na spracúvanie biometrických údajov veľkého počtu osôb bez ich aktívneho zapojenia. V prípade systémov „v reálnom čase“ prebieha zachytávanie biometrických údajov, ich porovnávanie a identifikácia okamžite, takmer okamžite alebo v každom prípade bez výrazného časového odstupu. V tejto súvislosti by nemal existovať priestor na obchádzanie pravidiel tohto nariadenia o používaní predmetných systémov AI „v reálnom čase“ tým, že sa zavedú malé časové odstupy. Systémy „v reálnom čase“ zahŕňajú používanie materiálu „naživo“ alebo „s malým časovým posunom“, ako sú napríklad videozáznamy, generovaného kamerou alebo iným zariadením s podobnými funkciami. Naopak, v prípade systémov „následnej“ identifikácie už boli biometrické údaje zachytené a porovnanie a identifikácia sa uskutočňujú až s výrazným časovým odstupom. Ide o materiály, ako sú fotografie alebo videozáznamy generované kamerami priemyselnej televízie alebo súkromnými zariadeniami, ktoré boli vytvorené pred použitím tohto systému vo vzťahu k dotknutým fyzickým osobám.

(18) Pojem „systém na rozpoznávanie emócií“ uvedený v tomto nariadení by sa mal vymedziť ako systém AI na účely identifikácie alebo odvodenia emócií alebo úmyslov fyzických osôb na základe ich biometrických údajov. Tento pojem sa vzťahuje na emócie alebo úmysly, ako sú šťastie, smútok, hnev, prekvapenie, znechutenie, rozpaky, vzrušenie, hanba, pohŕdanie, spokojnosť a zábava. Nezahŕňa fyzické stavy, ako je bolesť alebo únava vrátane napríklad systémov používaných na zisťovanie stavu únavy profesionálnych pilotov alebo vodičov na účely prevencie nehôd. Nezahŕňa ani samotné zisťovanie ľahko viditeľných výrazov, gest alebo pohybov, pokiaľ sa nepoužívajú na identifikáciu alebo odvodenie emócií. Tieto výrazy môžu byť základnými výrazmi tváre, ako je zamračenie alebo úsmev, alebo gestami, ako je pohyb rúk, ramien alebo hlavy, alebo charakteristickými znakmi hlasu osoby, ako je zdvihnutý hlas alebo šepot.

(19) Na účely tohto nariadenia by sa pojem „verejne prístupný priestor“ mal vykladať tak, že sa vzťahuje na akýkoľvek fyzický priestor, ktorý je prístupný neurčenému počtu fyzických osôb a bez ohľadu na to, či je daný priestor v súkromnom alebo verejnom vlastníctve, bez ohľadu na činnosť, na ktorú sa priestor môže používať, napríklad na obchodovanie, ako napríklad predajne, reštaurácie, kaviarne, pre služby, ako napríklad banky, profesionálne činnosti, ubytovanie a pohostinské služby, na šport, ako napríklad plavecké bazény, posilňovne, štadióny, pre dopravu, ako napríklad autobusové zastávky, stanice metra a železničné stanice, letiská, dopravné prostriedky, na zábavu, ako napríklad kiná, divadlá, múzeá, koncertné a konferenčné siene, alebo na voľný čas alebo iné činnosti, ako napríklad verejné cesty a námestia, parky, lesy, ihriská. Priestor by sa mal klasifikovať ako verejne prístupný vtedy, ak bez ohľadu na potenciálne kapacitné alebo bezpečnostné obmedzenia podlieha prístup určitým vopred určeným podmienkam, ktoré môže splniť neurčený počet osôb, ako je kúpa vstupenky alebo cestovného lístka, predchádzajúca registrácia alebo určitá veková hranica. Naopak, priestor by sa nemal považovať za verejne prístupný, ak je prístup naň obmedzený na konkrétne a vymedzené fyzické osoby buď prostredníctvom práva Únie alebo vnútroštátneho práva priamo súvisiaceho s verejnou bezpečnosťou alebo ochranou, alebo prostredníctvom jasného prejavu vôle osoby, ktorá má nad daným priestorom príslušné právomoci. Samotná faktická možnosť prístupu, ako napríklad nezamknuté dvere alebo otvorená brána v oplotení, neznamená, že priestor je verejne prístupný, ak existujú náznaky alebo okolnosti, ktoré naznačujú opak, napríklad označenia zakazujúce alebo obmedzujúce prístup. Priestory spoločností a tovární, ako aj kancelárie a pracoviská, ku ktorým majú prístup len príslušní zamestnanci a poskytovatelia služieb, sú priestory, ktoré nie sú verejne prístupné. Verejne prístupné priestory by nemali zahŕňať väznice ani hraničnú kontrolu. Niektoré ďalšie priestory môžu zahŕňať verejne prístupné aj neverejne prístupné priestory, ako napríklad vstupná hala súkromnej obytnej budovy potrebná na vstup do ordinácie lekára alebo letisko. Nezahŕňajú online priestory, pretože nejde o fyzické priestory. To, či je daný priestor prístupný verejnosti, by sa však malo určovať od prípadu k prípadu so zreteľom na osobitosti konkrétnej situácie.

(20) S cieľom získať čo najväčšie výhody systémov AI a zároveň chrániť základné práva, zdravie a bezpečnosť a umožniť demokratickú kontrolu by gramotnosť v oblasti AI mala vybaviť poskytovateľov, nasadzujúce subjekty a dotknuté osoby znalosťami potrebnými na prijímanie informovaných rozhodnutí týkajúcich sa systémov AI. Tieto znalosti sa môžu líšiť, pokiaľ ide o príslušný kontext, a môžu zahŕňať pochopenie správneho uplatňovania technických prvkov počas fázy vývoja systému AI, opatrenia, ktoré sa majú uplatňovať počas jeho používania, vhodné spôsoby výkladu výstupu systému AI a v prípade dotknutých osôb znalosti potrebné na pochopenie toho, ako na ne budú mať rozhodnutia prijaté s pomocou AI vplyv. V kontexte uplatňovania tohto nariadenia by gramotnosť v oblasti AI mala všetkým relevantným aktérom v hodnotovom reťazci AI poskytnúť spoľahlivé poznatky potrebné na zabezpečenie primeraného súladu a jeho správneho presadzovania. Okrem toho by rozsiahle vykonávanie opatrení týkajúcich sa gramotnosti v oblasti AI a zavedenie vhodných následných opatrení mohlo prispieť k zlepšeniu pracovných podmienok a v konečnom dôsledku k zachovaniu konsolidácie a inovačnej cesty dôveryhodnej AI v Únii. Európska rada pre umelú inteligenciu (ďalej len „rada pre AI“) by mala podporovať Komisiu pri presadzovaní gramotnosti v oblasti AI, informovanosti verejnosti a chápaní prínosov, rizík, záruk, práv a povinností v súvislosti s používaním systémov AI. V spolupráci s relevantnými zainteresovanými stranami by Komisia a členské štáty mali uľahčiť vypracovanie dobrovoľných kódexov správania na podporu gramotnosti v oblasti AI medzi osobami, ktoré sa zaoberajú vývojom, prevádzkou a používaním AI.

(21) S cieľom zabezpečiť rovnaké podmienky a účinnú ochranu práv a slobôd fyzických osôb v celej Únii by sa pravidlá stanovené v tomto nariadení mali uplatňovať na poskytovateľov systémov AI nediskriminačným spôsobom bez ohľadu na to, či sú usadení v Únii alebo v tretej krajine, a na subjekty nasadzujúce systémy AI usadené v Únii.

(22) Určité systémy AI by vzhľadom na svoju digitálnu povahu mali patriť do rozsahu pôsobnosti tohto nariadenia, aj keď sa v Únii neuvádzajú na trh ani do prevádzky, ani sa v nej nepoužívajú. Ide napríklad o prevádzkovateľa usadeného v Únii, ktorý zmluvne zadáva určité služby prevádzkovateľovi usadenému v tretej krajine v súvislosti s činnosťou vykonávanou systémom AI, ktorý by mohol byť označený ako vysokorizikový. Za týchto okolností by systém AI, ktorý používa prevádzkovateľ v tretej krajine, mohol spracúvať údaje zákonne zozbierané v Únii a prenášané z Únie a poskytovať zadávajúcemu prevádzkovateľovi v Únii výstup uvedeného systému AI vyplývajúci z tohto spracúvania bez toho, aby sa uvedený systém AI uvádzal na trh, do prevádzky alebo sa používal v Únii. S cieľom zabrániť obchádzaniu tohto nariadenia a zabezpečiť účinnú ochranu fyzických osôb nachádzajúcich sa v Únii by sa toto nariadenie malo vzťahovať aj na poskytovateľov systémov AI a subjekty nasadzujúce systémy AI, ktoré sú usadené v tretej krajine, a to v rozsahu, v akom je výstup generovaný týmito systémami určený na používanie v Únii.

S cieľom zohľadniť existujúce dojednania a osobitné potreby budúcej spolupráce so zahraničnými partnermi, s ktorými sa vymieňajú informácie a dôkazy, by sa však toto nariadenie nemalo vzťahovať na orgány verejnej moci tretej krajiny a medzinárodné organizácie, ak konajú v rámci spolupráce alebo medzinárodných dohôd uzavretých na únijnej alebo vnútroštátnej úrovni v oblasti presadzovania práva a justičnej spolupráce s Úniou alebo členskými štátmi, pod podmienkou, že príslušná tretia krajina alebo medzinárodná organizácia poskytuje primerané záruky týkajúce sa ochrany základných práv a slobôd jednotlivcov. V relevantných prípadoch sa to môže vzťahovať na činnosti subjektov, ktoré tretie krajiny poverili vykonávaním osobitných úloh na podporu takejto spolupráce v oblasti presadzovania práva a justičnej spolupráce. Takéto rámce spolupráce alebo dohody boli zriadené dvojstranne medzi členskými štátmi a tretími krajinami alebo medzi Európskou úniou, Europolom a inými agentúrami Únie a tretími krajinami a medzinárodnými organizáciami. Orgány zodpovedné za dohľad nad orgánmi presadzovania práva a justičnými orgánmi podľa tohto nariadenia by mali posúdiť, či tieto rámce spolupráce alebo medzinárodné dohody obsahujú primerané záruky, pokiaľ ide o ochranu základných práv a slobôd jednotlivcov. Prijímajúce vnútroštátne orgány a prijímajúce inštitúcie, orgány, úrady a agentúry Únie využívajúce takéto výstupy v Únii zostávajú zodpovedné za zabezpečenie súladu ich využívania s právom Únie. Pri revízii uvedených medzinárodných dohôd alebo uzatváraní nových dohôd v budúcnosti by zmluvné strany mali vynaložiť maximálne úsilie na zosúladenie týchto dohôd s požiadavkami tohto nariadenia.

(23) Toto nariadenie by sa malo vzťahovať aj na inštitúcie, orgány, úrady a agentúry Únie, ak konajú ako poskytovateľ systému AI alebo subjekt nasadzujúci systém AI.

(24) V rozsahu, v akom sa systémy AI uvádzajú na trh, uvádzajú do prevádzky alebo s úpravami alebo bez nich používajú na vojenské alebo obranné účely alebo na účely národnej bezpečnosti, by takéto systémy mali byť vylúčené z rozsahu pôsobnosti tohto nariadenia bez ohľadu na to, ktorý typ subjektu vykonáva uvedené činnosti, napríklad či ide o verejný alebo súkromný subjekt. Pokiaľ ide o vojenské a obranné účely, takéto vylúčenie je odôvodnené článkom 4 ods. 2 Zmluvy o EÚ, ako aj osobitosťami obrannej politiky členských štátov a spoločnej obrannej politiky Únie, na ktoré sa vzťahuje hlava V kapitola 2 Zmluvy o EÚ a ktoré podliehajú medzinárodnému právu verejnému, ktoré je preto vhodnejším právnym rámcom na reguláciu systémov AI v kontexte používania smrtiacej sily a iných systémov AI v kontexte vojenských a obranných činností. Pokiaľ ide o účely národnej bezpečnosti, vylúčenie je odôvodnené skutočnosťou, že národná bezpečnosť zostáva výlučnou zodpovednosťou členských štátov v súlade s článkom 4 ods. 2 Zmluvy o EÚ, ako aj osobitnou povahou a operačnými potrebami činností v oblasti národnej bezpečnosti a osobitnými vnútroštátnymi pravidlami uplatniteľnými na tieto činnosti. Ak sa však systém AI, ktorý je vyvinutý, uvedený na trh, uvedený do prevádzky alebo používaný na vojenské alebo obranné účely alebo na účely národnej bezpečnosti, používa dočasne alebo trvalo na iné účely, napríklad na civilné alebo humanitárne účely, účely presadzovania práva alebo verejnej bezpečnosti, takýto systém by patril do rozsahu pôsobnosti tohto nariadenia. V takom prípade by subjekt, ktorý používa systém AI na iné ako vojenské alebo obranné účely alebo na účely národnej bezpečnosti, mal zabezpečiť súlad systému AI s týmto nariadením, pokiaľ systém už s ním nie je v súlade. Systémy AI uvedené na trh alebo do prevádzky na účely vylúčené z pôsobnosti, konkrétne vojenské alebo obranné účely alebo účely národnej bezpečnosti, a jeden alebo viacero účelov nevylúčených z pôsobnosti, napríklad civilné účely alebo presadzovanie práva atď., patria do rozsahu pôsobnosti tohto nariadenia a poskytovatelia týchto systémov by mali zabezpečiť ich súlad s týmto nariadením. V takýchto prípadoch by skutočnosť, že systém AI môže patriť do rozsahu pôsobnosti tohto nariadenia, nemala mať vplyv na možnosť subjektov vykonávajúcich činnosti v oblasti národnej bezpečnosti, obrany a vojenské činnosti, a to bez ohľadu na typ subjektu vykonávajúceho uvedené činnosti, používať systémy AI na účely národnej bezpečnosti, na vojenské a obranné účely, ktoré sú vylúčené z rozsahu pôsobnosti tohto nariadenia. Systém AI uvedený na trh na civilné účely alebo na účely presadzovania práva, ktorý sa s úpravami alebo bez nich používa na vojenské alebo obranné účely alebo na účely národnej bezpečnosti, by nemal patriť do rozsahu pôsobnosti tohto nariadenia bez ohľadu na typ subjektu vykonávajúceho tieto činnosti.

(25) Toto nariadenie by malo podporovať inováciu, malo by rešpektovať slobodu vedy a nemalo by oslabovať výskumnú a vývojovú činnosť. Preto je potrebné vylúčiť z jeho pôsobnosti systémy a modely AI osobitne vyvinuté a uvedené do prevádzky výlučne na účely vedeckého výskumu a vývoja. Navyše je potrebné zabezpečiť, aby toto nariadenie iným spôsobom neovplyvňovalo vedeckú, výskumnú a vývojovú činnosť týkajúcu sa systémov alebo modelov AI pred ich uvedením na trh alebo do prevádzky. Pokiaľ ide o výskumnú, testovaciu a vývojovú činnosť zameranú na výrobky v oblasti systémov alebo modelov AI, ustanovenia tohto nariadenia by sa taktiež nemali uplatňovať pred uvedením týchto systémov a modelov do prevádzky alebo pred ich uvedením na trh. Týmto vylúčením nie je dotknutá povinnosť dodržiavať toto nariadenie, keď sa systém AI patriaci do rozsahu pôsobnosti tohto nariadenia uvádza na trh alebo do prevádzky ako výsledok takejto výskumnej a vývojovej činnosti, ani uplatňovanie ustanovení o regulačných experimentálnych prostrediach pre AI a testovaní v reálnych podmienkach. Navyše, bez toho, aby bolo dotknuté vylúčenie systémov AI osobitne vyvinutých a uvedených do prevádzky výlučne na účely vedeckého výskumu a vývoja, akýkoľvek iný systém AI, ktorý sa môže používať na vykonávanie akejkoľvek výskumnej a vývojovej činnosti, by mal naďalej podliehať ustanoveniam tohto nariadenia. Každá výskumná a vývojová činnosť by sa v každom prípade mala vykonávať v súlade s uznávanými etickými a profesijnými normami pre vedecký výskum, ako aj v súlade s uplatniteľným právom Únie.

(26) Na účely zavedenia primeraného a účinného súboru záväzných pravidiel pre systémy AI by sa mal dodržiavať jasne vymedzený prístup založený na riziku. Týmto prístupom by sa mal typ a obsah takýchto pravidiel prispôsobiť intenzite a rozsahu rizík, ktoré môžu systémy AI vytvárať. Preto je potrebné zakázať určité neakceptovateľné praktiky využívajúce AI, stanoviť požiadavky na vysokorizikové systémy AI a povinnosti príslušných prevádzkovateľov, ako aj stanoviť povinnosti transparentnosti pre určité systémy AI.

(27) Hoci je prístup založený na riziku základom pre primeraný a účinný súbor záväzných pravidiel, je dôležité pripomenúť etické usmernenia pre dôveryhodnú AI z roku 2019, ktoré vypracovala nezávislá expertná skupina na vysokej úrovni pre umelú inteligenciu vymenovaná Komisiou. V týchto usmerneniach expertná skupina na vysokej úrovni pre umelú inteligenciu stanovila sedem nezáväzných etických zásad pre AI, ktorých účelom je pomôcť zabezpečiť, aby bola AI dôveryhodná a etická. Uvedenými siedmimi zásadami sú ľudský faktor a dohľad; technická spoľahlivosť a bezpečnosť; súkromie a správa údajov; transparentnosť; rozmanitosť, nediskriminácia a spravodlivosť; spoločenský a environmentálny blahobyt a zodpovednosť. Bez toho, aby boli dotknuté právne záväzné požiadavky tohto nariadenia a akéhokoľvek iného uplatniteľného práva Únie, tieto usmernenia prispievajú k dizajnu súdržnej, dôveryhodnej a na človeka sústredenej AI v súlade s chartou a hodnotami, na ktorých je Únia založená. Podľa usmernení expertnej skupiny na vysokej úrovni pre umelú inteligenciu „ľudský faktor a dohľad“ znamená, že systémy AI sa vyvíjajú a používajú ako nástroj, ktorý slúži ľuďom, rešpektuje ľudskú dôstojnosť a osobnú samostatnosť a funguje spôsobom umožňujúcim primeranú kontrolu a dohľad človekom.

„Technická spoľahlivosť a bezpečnosť“ znamená, že systémy AI sa vyvíjajú a používajú tak, aby sa umožnila spoľahlivosť v prípade problémov a odolnosť voči pokusom o zmenu použitia alebo výkonu systému AI na účely nezákonného používania tretími stranami a aby sa minimalizovala nechcená ujma. „Súkromie a správa údajov“ znamená, že systémy AI sa vyvíjajú a používajú v súlade s pravidlami ochrany súkromia a údajov pri súčasnom spracúvaní údajov podľa vysokých noriem kvality a integrity. „Transparentnosť“ znamená, že systémy AI sa vyvíjajú a používajú tak, aby umožňovali náležitú vysledovateľnosť a vysvetliteľnosť, pričom upozorňujú ľudí na to, že komunikujú a interagujú so systémom AI, a zároveň náležite informujú subjekty nasadzujúce systém AI o spôsobilostiach a obmedzeniach daného systému a dotknuté osoby o ich právach. „Rozmanitosť, nediskriminácia a spravodlivosť“ znamená, že systémy AI sa vyvíjajú a používajú tak, aby zapájali rôznych aktérov, podporovali rovnosť prístupu, rodovú rovnosť a kultúrnu rozmanitosť a zároveň predchádzali diskriminačným vplyvom a nespravodlivej zaujatosti, ktoré právo Únie a vnútroštátne právo zakazuje. „Spoločenský a environmentálny blahobyt“ znamená, že systémy AI sa vyvíjajú a používajú udržateľným spôsobom priaznivým pre životného prostredie, ako aj v prospech všetkých ľudí, pričom sa monitoruje a posudzuje dlhodobý vplyv na jednotlivca, spoločnosť a demokraciu. Uplatňovanie týchto zásad by sa malo podľa možnosti premietnuť do dizajnu a používania modelov AI. V každom prípade by mali slúžiť ako základ pre vypracovanie kódexov správania podľa tohto nariadenia. Všetky zainteresované strany vrátane priemyselných odvetví, akademickej obce, občianskej spoločnosti a normalizačných organizácií sa vyzývajú, aby tieto etické zásady podľa potreby zohľadnili pri vypracúvaní dobrovoľných najlepších postupov a noriem.

(28) Hoci využívanie AI prináša mnoho výhod, možno ju zneužiť a môže sa stať zdrojom nových a výkonných nástrojov umožňujúcich manipulatívne a zneužívajúce praktiky a praktiky ovládania spoločnosti. Takéto praktiky sú mimoriadne škodlivé a zneužívajúce a mali by sa zakázať, pretože sú v rozpore s hodnotami Únie týkajúcimi sa rešpektovania ľudskej dôstojnosti, slobody, rovnosti, demokracie a právneho štátu a základných práv ukotvených v charte vrátane práva na nediskrimináciu, ochranu údajov a súkromia a práv dieťaťa.

(29) Manipulatívne techniky, ktoré umožňuje AI, sa môžu použiť na presviedčanie osôb, aby sa správali neželaným spôsobom, alebo na ich zavádzanie nabádaním na rozhodnutia spôsobom, ktorý narúša a oslabuje ich samostatnosť, rozhodovacie schopnosti a slobodnú voľbu. Uvádzanie na trh, uvádzanie do prevádzky alebo používanie určitých systémov AI, ktorých cieľom alebo účinkom je podstatné narušenie ľudského správania, pri ktorom je pravdepodobné, že dôjde k značnej ujme, najmä dostatočne závažným nepriaznivým vplyvom na fyzické zdravie, psychické zdravie alebo finančné záujmy, je obzvlášť nebezpečné a malo by sa preto zakázať. Takéto systémy AI využívajú podprahové komponenty, ako sú zvukové a obrazové podnety alebo videopodnety, ktoré osoby nemôžu vnímať, keďže tieto podnety sú mimo ľudského vnímania, alebo iné manipulatívne alebo klamlivé techniky, ktoré narúšajú alebo oslabujú samostatnosť, rozhodovacie schopnosti alebo slobodnú voľbu osôb takým spôsobom, že si ľudia tieto techniky neuvedomujú, alebo ak si ich uvedomujú, napriek tomu môžu byť zavádzaní alebo nie sú schopní ich ovládať alebo im odolávať. To by sa mohlo uľahčiť napríklad rozhraniami medzi strojom a mozgom alebo virtuálnou realitou, pretože umožňujú vyšší stupeň kontroly toho, akým stimulom sú osoby vystavené, pokiaľ môžu výrazne škodlivým a podstatným spôsobom narušiť ich správanie. Systémy AI môžu okrem toho aj iným spôsobom zneužívať zraniteľnosti osôb alebo osobitných skupín osôb z dôvodu ich veku, zdravotného postihnutia v zmysle smernice Európskeho parlamentu a Rady (EÚ) 2019/882[16] alebo osobitnej sociálnej alebo ekonomickej situácie, v dôsledku čoho môžu byť tieto osoby zraniteľnejšie voči zneužívaniu, ako napríklad osoby žijúce v extrémnej chudobe, etnické alebo náboženské menšiny.

---

[16] Smernica Európskeho parlamentu a Rady (EÚ) 2019/882 zo 17. apríla 2019 o požiadavkách na prístupnosť výrobkov a služieb (Ú. v. EÚ L 151, 7.6.2019, s. 70).

Takéto systémy AI sa môžu uvádzať na trh, uvádzať do prevádzky alebo používať s cieľom alebo účinkom podstatného narušenia správania osoby spôsobom, ktorý spôsobuje alebo pri ktorom je odôvodnené predpokladať, že spôsobí značnú ujmu tejto alebo inej osobe alebo skupinám osôb vrátane škôd, ktoré sa môžu časom kumulovať, a preto by sa mali zakázať. Môže sa stať, že úmysel narušiť správanie nie je možné predpokladať, ak narušenie vyplýva z faktorov mimo systému AI, ktoré nie sú pod kontrolou poskytovateľa alebo nasadzujúceho subjektu, konkrétne faktorov, ktoré poskytovateľ systému AI alebo subjekt nasadzujúci systém AI nemôže odôvodnene predvídať, a teda zmierňovať. V každom prípade nie je potrebné, aby poskytovateľ alebo subjekt nasadzujúci systém AI mal úmysel spôsobiť značnú ujmu, pokiaľ takáto ujma vyplýva z manipulatívnych alebo zneužívajúcich praktík využívajúcich AI. Zákazmi takýchto praktík využívajúcich AI sa dopĺňajú ustanovenia smernice Európskeho parlamentu a Rady 2005/29/ES[17], najmä to, že nekalé obchodné praktiky vedúce k hospodárskej alebo finančnej ujme pre spotrebiteľov sú zakázané za každých okolností bez ohľadu na to, či sú zavedené prostredníctvom systémov AI alebo inak. Zákazmi manipulatívnych a zneužívajúcich praktík v tomto nariadení by nemali byť dotknuté zákonné postupy v súvislosti s liečbou, ako je psychologická liečba duševnej choroby alebo fyzická rehabilitácia, ak sa tieto praktiky vykonávajú v súlade s platnými lekárskymi normami a právnymi predpismi, napríklad výslovný súhlas fyzických osôb alebo ich právnych zástupcov. Okrem toho by sa bežné a legitímne obchodné praktiky, napríklad v oblasti reklamy, ktoré sú v súlade s uplatniteľným právom, nemali samy osebe považovať za škodlivé manipulatívne praktiky využívajúce AI.

---

17 Smernica Európskeho parlamentu a Rady 2005/29/ES z 11. mája 2005 o nekalých obchodných praktikách podnikateľov voči spotrebiteľom na vnútornom trhu, a ktorou sa mení a dopĺňa smernica Rady 84/450/EHS, smernice Európskeho parlamentu a Rady 97/7/ES, 98/27/ES a 2002/65/ES a nariadenie Európskeho parlamentu a Rady (ES) č. 2006/2004 („smernica o nekalých obchodných praktikách“) (Ú. v. EÚ L 149, 11.6.2005, s. 22).

(30) Mali by sa zakázať systémy biometrickej kategorizácie založené na biometrických údajoch fyzických osôb, ako je tvár alebo odtlačky prstov, s cieľom alebo odvodiť politické názory osôb, členstvo v odboroch, náboženské alebo filozofické presvedčenie, rasu, sexuálny život alebo sexuálnu orientáciu. Tento zákaz by sa nemal vzťahovať na zákonné označovanie, filtrovanie alebo kategorizáciu súborov biometrických údajov získaných v súlade s právom Únie alebo vnútroštátnym právom v oblasti biometrických údajov, ako je triedenie obrázkov podľa farby vlasov alebo farby očí, ktoré možno použiť napríklad v oblasti presadzovania práva.

(31) Systémy AI na sociálne bodovanie fyzických osôb používané orgánmi verejnej moci alebo súkromnými aktérmi môžu viesť k diskriminačným výsledkom a vylúčeniu určitých skupín. Môžu porušovať právo na dôstojnosť a nediskrimináciu a hodnoty rovnosti a spravodlivosti. Takéto systémy AI hodnotia alebo klasifikujú fyzické osoby alebo skupiny fyzických osôb na základe viacerých dátových bodov týkajúcich sa ich spoločenského správania vo viacerých kontextoch alebo známych, odvodených či predpokladaných osobných alebo osobnostných charakteristík za určité časové obdobia. Sociálne skóre získané na základe takýchto systémov AI môže viesť k škodlivému alebo nepriaznivému zaobchádzaniu s fyzickými osobami alebo celými skupinami takýchto osôb v sociálnych kontextoch nesúvisiacich s kontextom, v ktorom boli údaje pôvodne vygenerované alebo zhromaždené, prípadne k poškodzujúcemu zaobchádzaniu, ktoré je neprimerané alebo neodôvodnené vzhľadom na závažnosť ich spoločenského správania. Systémy AI, ktoré zahŕňajú takéto neprijateľné bodovacie praktiky a vedú k takýmto škodlivým alebo nepriaznivým výsledkom, by sa preto mali zakázať. Tento zákaz by nemal mať vplyv na zákonné postupy hodnotenia fyzických osôb vykonávané na špecifické účely v súlade s právom Únie a vnútroštátnym právom.

(32) Používanie systémov AI na diaľkovú biometrickú identifikáciu fyzických osôb „v reálnom čase“ vo verejne prístupných priestoroch na účely presadzovania práva sa považuje za obzvlášť rušivý zásah do práv a slobôd dotknutých osôb, keďže môže ovplyvniť súkromie veľkej časti obyvateľstva, vyvoláva pocit neustáleho sledovania a nepriamo odrádza od využívania slobody zhromažďovania a iných základných práv. Technické nepresnosti systémov AI určených na diaľkovú biometrickú identifikáciu fyzických osôb môžu viesť ku skresleným výsledkom a mať diskriminačné účinky. Takéto možné skreslené výsledky a diskriminačné účinky sú obzvlášť relevantné z hľadiska veku, etnickej príslušnosti, rasy, pohlavia alebo zdravotného postihnutia. Okrem toho, bezprostrednosť vplyvu a obmedzené možnosti ďalších kontrol alebo opráv v súvislosti s používaním takýchto systémov fungujúcich „v reálnom čase“ so sebou prinášajú zvýšené riziká z hľadiska práv a slobôd dotknutých osôb v súvislosti s činnosťami presadzovania práva alebo v ich dôsledku.

(33) Používanie týchto systémov na účely presadzovania práva by sa preto malo zakázať s výnimkou taxatívne vymenovaných a úzko vymedzených situácií, keď je toto použitie nevyhnutne potrebné na dosiahnutie významného verejného záujmu, ktorého význam prevažuje nad rizikami. Tieto situácie zahŕňajú pátranie po určitých obetiach trestných činov vrátane nezvestných osôb; určité ohrozenie života alebo fyzickej bezpečnosti fyzických osôb alebo hrozby teroristického útoku; a lokalizáciu alebo identifikáciu páchateľov trestných činov uvedených v prílohe k tomuto nariadeniu alebo osôb podozrivých zo spáchania týchto trestných činov, ak za tieto trestné činy možno v dotknutom členskom štáte uložiť trest odňatia slobody alebo ochranné opatrenie spojené s obmedzením osobnej slobody s hornou hranicou trestnej sadzby najmenej štyri roky a podľa ich vymedzenia v práve tohto členského štátu. Takáto hranica trestu odňatia slobody alebo ochranného opatrenia spojeného s obmedzením osobnej slobody v súlade s vnútroštátnym právom prispieva k zabezpečeniu toho, že daný trestný čin bude dostatočne závažný na to, aby sa ním dalo potenciálne odôvodniť použitie systémov diaľkovej biometrickej identifikácie „v reálnom čase“. Okrem toho zoznam trestných činov uvedený v prílohe k tomuto nariadeniu vychádza z 32 trestných činov uvedených v rámcovom rozhodnutí Rady 2002/584/SVV[18], pričom sa zohľadňuje skutočnosť, že niektoré z uvedených trestných činov sú v praxi pravdepodobne relevantnejšie ako iné v tom zmysle, že nevyhnutnosť a primeranosť použitia diaľkovej biometrickej identifikácie „v reálnom čase“ by mohli byť pravdepodobne veľmi rôznorodé jednak z hľadiska praktického vykonávania lokalizácie alebo identifikácie páchateľa jednotlivých uvedených trestných činov alebo osôb podozrivých z ich spáchania a jednak vzhľadom na pravdepodobné rozdiely v závažnosti, pravdepodobnosti a rozsahu spôsobenej ujmy alebo možných negatívnych dôsledkov.

---

[18] Rámcové rozhodnutie Rady 2002/584/SVV z 13. júna 2002 o európskom zatykači a postupoch odovzdávania osôb medzi členskými štátmi (Ú. v. ES L 190, 18.7.2002, s. 1).

Bezprostredné ohrozenie života alebo fyzickej bezpečnosti fyzických osôb by mohlo vyplývať aj zo závažného narušenia kritickej infraštruktúry v zmysle vymedzenia uvedeného v článku 2 bode 4 smernice Európskeho parlamentu a Rady (EÚ) 2022/2557[19], ak by narušenie alebo zničenie takejto kritickej infraštruktúry viedlo k bezprostrednému ohrozeniu života alebo fyzickej bezpečnosti osoby, a to aj v dôsledku vážnej ujmy na poskytovaní základných dodávok pre obyvateľstvo alebo výkone základných funkcií štátu. Okrem toho by sa týmto nariadením mala zachovať možnosť orgánov presadzovania práva, kontroly hraníc, imigračných alebo azylových orgánov vykonávať kontroly totožnosti v prítomnosti dotknutej osoby v súlade s podmienkami stanovenými v práve Únie a vo vnútroštátnom práve pre takéto kontroly. Orgány presadzovania práva, kontroly hraníc, imigračné alebo azylové orgány by konkrétne mali mať možnosť využívať informačné systémy v súlade s právom Únie alebo vnútroštátnym právom na identifikáciu osôb, ktoré sa počas kontroly totožnosti buď odmietnu identifikovať, alebo nie sú schopné uviesť alebo preukázať svoju totožnosť, a to bez toho, aby sa podľa tohto nariadenia vyžadovalo získanie povolenia vopred. Môže ísť napríklad o osobu zapojenú do trestného činu, ktorá nie je ochotná alebo z dôvodu úrazu alebo zdravotného stavu nie je schopná uviesť svoju totožnosť orgánom presadzovania práva.

[19] Smernica Európskeho parlamentu a Rady (EÚ) 2022/2557 zo 14. decembra 2022 o odolnosti kritických subjektov a o zrušení smernice Rady 2008/114/ES (Ú. v. EÚ L 333, 27.12.2022, s. 164).

(34) S cieľom zabezpečiť, aby sa tieto systémy používali zodpovedným a primeraným spôsobom, je tiež dôležité stanoviť, že v každej z týchto taxatívne vymenovaných a úzko vymedzených situácií by sa mali zohľadniť určité prvky, najmä pokiaľ ide o povahu situácie, ktorá viedla k predloženiu žiadosti, o dôsledky využívania týchto systémov na práva a slobody všetkých dotknutých osôb a o záruky a podmienky zabezpečené pri tomto používaní. Okrem toho by sa používanie systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva malo nasadzovať len na potvrdenie totožnosti špecificky zacieleného jednotlivca a malo by sa obmedziť na to, čo je nevyhnutne potrebné, pokiaľ ide o časové obdobie, ako aj geografický a osobný rozsah, najmä so zreteľom na dôkazy alebo indície týkajúce sa hrozieb, obetí alebo páchateľa. Používanie systému diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch by sa malo povoliť len vtedy, ak príslušný orgán presadzovania práva ukončil posúdenie vplyvu na základné práva a, pokiaľ sa v tomto nariadení nestanovuje inak, zaregistroval systém v databáze, ako sa stanovuje v tomto nariadení. Referenčná databáza osôb by mala byť vhodná pre každý prípad použitia v každej z uvedených situácií.

(35) Každé použitie systému diaľkovej biometrickej identifikácie „v reálnom čase“ vo verejne prístupných priestoroch na účely presadzovania práva by malo podliehať výslovnému a osobitnému povoleniu justičného orgánu alebo nezávislého správneho orgánu členského štátu, ktorého rozhodnutie je záväzné. Takéto povolenie by sa v zásade malo získať pred použitím systému AI s cieľom identifikovať osobu alebo osoby. Výnimky z tohto pravidla by mali byť povolené v riadne odôvodnených naliehavých situáciách, teda v situáciách, v ktorých je natoľko potrebné použiť predmetné systémy, že je naozaj objektívne nemožné získať povolenie pred začatím použitia systému AI. V takýchto naliehavých situáciách by sa používanie systému AI malo obmedziť na absolútne nevyhnutné minimum a malo by podliehať primeraným zárukám a podmienkam stanoveným vo vnútroštátnom práve a špecifikovaným v kontexte každého jednotlivého naliehavého prípadu použitia samotným orgánom presadzovania práva. Okrem toho by orgán presadzovania práva mal v takýchto situáciách požiadať o takéto povolenie a zároveň uviesť dôvody, prečo oň nemohol požiadať skôr, a to bez zbytočného odkladu a najneskôr do 24 hodín. Ak sa takéto povolenie zamietne, používanie systémov biometrickej identifikácie v reálnom čase spojených s daným povolením by sa malo s okamžitou účinnosťou ukončiť a všetky údaje súvisiace s takýmto použitím by sa mali zlikvidovať a vymazať. Takéto údaje zahŕňajú vstupné údaje priamo získané systémom AI v priebehu používania takéhoto systému, ako aj výsledky a výstupy používania spojeného s daným povolením. Nemalo by zahŕňať vstupy, ktoré sú zákonne získané v súlade s iným právom Únie alebo vnútroštátnym právom. V každom prípade, žiadne rozhodnutie, ktoré má nepriaznivé právne účinky na osobu, by sa nemalo prijať výlučne na základe výstupu systému diaľkovej biometrickej identifikácie.

(36) S cieľom vykonávať svoje úlohy v súlade s požiadavkami stanovenými v tomto nariadení, ako aj vo vnútroštátnych predpisoch by mal byť o každom použití systému biometrickej identifikácie v reálnom čase informovaný príslušný orgán dohľadu nad trhom a vnútroštátny orgán pre ochranu údajov. Orgány dohľadu nad trhom a vnútroštátne orgány pre ochranu údajov, ktoré boli informované, by mali Komisii predkladať výročnú správu o používaní systémov biometrickej identifikácie v reálnom čase.

(37) Navyše je vhodné v rámci podrobne opísanom týmto nariadením stanoviť, že takéto použitie na území členského štátu v súlade s týmto nariadením by malo byť možné len vtedy a do takej miery, do akej sa dotknutý členský štát rozhodol výslovne stanoviť možnosť povoliť toto použitie vo svojich podrobných pravidlách vnútroštátneho práva. V dôsledku toho sa členské štáty môžu podľa tohto nariadenia naďalej na základe vlastného uváženia rozhodnúť, že takúto možnosť vôbec nestanovia alebo ju stanovia len v súvislosti s niektorými z cieľov, ktorými možno odôvodniť povolené použitie určené v tomto nariadení. Takéto vnútroštátne pravidlá by sa mali oznámiť Komisii do 30 dní od ich prijatia.

(38) Používanie systémov AI na diaľkovú biometrickú identifikáciu fyzických osôb v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva nevyhnutne zahŕňa spracúvanie biometrických údajov. Pravidlá tohto nariadenia, ktorými sa s výhradou určitých výnimiek takéto používanie zakazuje a ktoré sú založené na článku 16 ZFEÚ, by sa mali uplatňovať ako *lex specialis*, pokiaľ ide o pravidlá spracúvania biometrických údajov uvedené v článku 10 smernice (EÚ) 2016/680, čím by sa takéto používanie a spracúvanie príslušných biometrických údajov upravovalo vyčerpávajúcim spôsobom. Takéto používanie a spracúvanie by preto malo byť možné, len pokiaľ je zlučiteľné s rámcom stanoveným v tomto nariadení, a mimo tohto rámca by nemal existovať priestor na to, aby príslušné orgány, ak konajú na účely presadzovania práva, používali takéto systémy a spracúvali takéto údaje v súvislosti s týmto použitím z dôvodov uvedených v článku 10 smernice (EÚ) 2016/680. V tejto súvislosti nie je cieľom tohto nariadenia poskytnúť právny základ pre spracúvanie osobných údajov podľa článku 8 smernice (EÚ) 2016/680. Na používanie systémov na diaľkovú biometrickú identifikáciu v reálnom čase vo verejne prístupných priestoroch na iné účely ako na presadzovanie práva, a to aj príslušnými orgánmi, by sa však nemal vzťahovať osobitný rámec týkajúci sa takéhoto použitia na účely presadzovania práva stanovený v tomto nariadení. Takéto použitie na iné účely ako na presadzovanie práva by preto nemalo podliehať požiadavke povolenia podľa tohto nariadenia a uplatniteľných podrobných pravidiel vnútroštátneho práva, na základe ktorých sa toto povolenie môže vykonávať.

(39) Každé spracúvanie biometrických údajov a iných osobných údajov súvisiace s používaním systémov AI na biometrickú identifikáciu, okrem spracúvania v súvislosti s používaním systémov na diaľkovú biometrickú identifikáciu fyzických osôb „v reálnom čase“ vo verejne prístupných priestoroch na účely presadzovania práva, ako sa stanovuje v tomto nariadení, by malo naďalej spĺňať všetky požiadavky vyplývajúce z článku 10 smernice (EÚ) 2016/680. Pokiaľ ide o iné účely ako presadzovanie práva, v článku 9 ods. 1 nariadenia (EÚ) 2016/679 a v článku 10 ods. 1 nariadenia (EÚ) 2018/1725 zakazuje spracúvanie biometrických údajov s výhradou obmedzených výnimiek stanovených v uvedených článkoch. Používanie diaľkovej biometrickej identifikácie na iné účely ako na účely presadzovania práva už podliehalo rozhodnutiam vnútroštátnych orgánov pre ochranu údajov o zákaze v kontexte uplatňovania článku 9 ods. 1 nariadenia (EÚ) 2016/679.

(40) V súlade s článkom 6a Protokolu č. 21 o postavení Spojeného kráľovstva a Írska s ohľadom na priestor slobody, bezpečnosti a spravodlivosti, ktorý je pripojený k Zmluve o EÚ a ZFEÚ, nie je Írsko viazané pravidlami stanovenými v článku 5 ods. 1 prvom pododseku písm. g) v rozsahu, v akom sa uplatňuje na použitie systémov biometrickej kategorizácie pri činnostiach v oblasti policajnej spolupráce a justičnej spolupráce v trestných veciach, v článku 5 ods. 1 prvom pododseku písm. d) v rozsahu, v akom sa uplatňuje na používanie systémov AI, na ktoré sa vzťahuje uvedené ustanovenie, v článku 5 ods. 1 prvom pododseku písm. h), článku 5 ods. 2 až 6 a v článku 26 ods. 10 tohto nariadenia, prijatými na základe článku 16 ZFEÚ, ktoré sa týkajú spracúvania osobných údajov členskými štátmi pri vykonávaní činností, ktoré patria do rozsahu pôsobnosti tretej časti hlavy V kapitoly 4 alebo kapitoly 5 ZFEÚ, ak Írsko nie je viazané pravidlami, ktorými sa spravujú formy justičnej spolupráce v trestných veciach alebo policajnej spolupráce, v rámci ktorých sa musia dodržiavať ustanovenia prijaté na základe článku 16 ZFEÚ.

(41) V súlade s článkami 2 a 2a Protokolu č. 22 o postavení Dánska, ktorý je pripojený k Zmluve o EÚ a ZFEÚ, nie je Dánsko viazané pravidlami stanovenými v článku 5 ods. 1 prvom pododseku písm. g) v rozsahu, v akom sa uplatňuje na použitie systémov biometrickej kategorizácie pri činnostiach v oblasti policajnej spolupráce a justičnej spolupráce v trestných veciach, v článku 5 ods. 1 prvom pododseku písm. d) v rozsahu, v akom sa uplatňuje na používanie systémov AI, na ktoré sa vzťahuje uvedené ustanovenie, v článku 5 ods. 1 prvom pododseku písm. h), článku 5 ods. 2 až 6 a v článku 26 ods. 10 tohto nariadenia, prijatými na základe článku 16 ZFEÚ, ktoré sa týkajú spracúvania osobných údajov členskými štátmi pri vykonávaní činností, ktoré patria do rozsahu pôsobnosti tretej časti hlavy V kapitoly 4 alebo kapitoly 5 ZFEÚ, ani nepodlieha ich uplatňovaniu.

(42) V súlade s prezumpciou neviny by sa fyzické osoby v Únii mali vždy posudzovať podľa ich skutočného správania. Fyzické osoby by sa nikdy nemali posudzovať podľa správania predpokladaného AI výlučne na základe ich profilovania, osobnostných čŕt alebo charakteristík, ako je štátna príslušnosť, miesto narodenia, miesto bydliska, počet detí, výška dlhu alebo typ ich vozidla, bez odôvodneného podozrenia, že daná osoba je zapojená do trestnej činnosti na základe objektívnych overiteľných skutočností a bez ich ľudského posúdenia. Preto by sa malo zakázať vykonávanie posudzovania rizika fyzických osôb s cieľom posúdiť pravdepodobnosť spáchania trestného činu takýmito osobami alebo s cieľom predpovedať skutočný alebo potenciálny trestný čin výlučne na základe profilovania fyzických osôb alebo posúdenia ich osobnostných čŕt a charakteristík. Takýto zákaz v žiadnom prípade ale neodkazuje na analýzu rizika ani sa netýka analýzy rizika, ktorá nie je založená na profilovaní jednotlivcov ani na osobnostných črtách a charakteristikách jednotlivcov, ako sú systémy AI využívajúce analýzu rizika na posúdenie pravdepodobnosti finančného podvodu zo strany podnikov na základe podozrivých transakcií, alebo nástroje analýzy rizika na predpovedanie pravdepodobnosti lokalizácie omamných látok alebo nezákonného tovaru colnými orgánmi, napríklad na základe známych pašeráckych trás.

(43) Uvádzanie na trh, uvádzanie do prevádzky na tento konkrétny účel alebo používanie systémov AI, ktoré vytvárajú alebo rozširujú databázy na rozpoznávanie tváre prostredníctvom necielenej extrakcie podôb tváre z internetu alebo zo záznamov CCTV, by sa mali zakázať, pretože takáto prax zvyšuje pocit hromadného sledovania a môže viesť k hrubému porušovaniu základných práv vrátane práva na súkromie.

(44) Existujú vážne obavy v súvislosti s vedeckým základom systémov AI, ktorých cieľom je identifikovať alebo odvodzovať emócie, najmä preto, že prejav emócií sa v jednotlivých kultúrach a situáciách a dokonca aj v prípade jedného jednotlivca značne líši. Medzi hlavné nedostatky takýchto systémov patrí obmedzená spoľahlivosť, nedostatočná špecifickosť a obmedzená možnosť zovšeobecnenia. Systémy AI, ktoré identifikujú alebo odvodzujú emócie alebo zámery fyzických osôb na základe ich biometrických údajov, preto môžu viesť k diskriminačným výsledkom a môžu zasahovať do práv a slobôd dotknutých osôb. Vzhľadom na nerovnováhu moci v kontexte práce alebo vzdelávania v kombinácii s rušivým charakterom týchto systémov by takéto systémy mohli viesť k škodlivému alebo nepriaznivému zaobchádzaniu s niektorými fyzickými osobami alebo celými skupinami fyzických osôb. Preto by sa malo zakázať uvádzanie na trh, uvádzanie do prevádzky alebo používanie systémov AI na zisťovanie emocionálneho stavu jednotlivcov v situáciách súvisiacich s pracoviskom a vzdelávaním. Tento zákaz by sa nemal vzťahovať na systémy AI uvádzané na trh výlučne zo zdravotných alebo bezpečnostných dôvodov, ako sú systémy určené na terapeutické použitie.

(45) Postupy, ktoré sú zakázané právom Únie, okrem iného právom v oblasti ochrany údajov, nediskriminácie, ochrany spotrebiteľa a právom hospodárskej súťaže, by nemali byť týmto nariadením dotknuté.

(46) Vysokorizikové systémy AI by sa mali uviesť na trh Únie alebo do prevádzky alebo by sa mali využívať len vtedy, ak spĺňajú určité povinné požiadavky. Týmito požiadavkami by sa malo zabezpečiť, aby vysokorizikové systémy AI, ktoré sú dostupné v Únii alebo ktorých výstupy sú v Únii inak využívané, nepredstavovali neprijateľné riziká pre dôležité verejné záujmy Únie uznané a chránené právom Únie. Na základe nového legislatívneho rámca, ako sa uvádza v oznámení Komisie s názvom „Modrá príručka na vykonávanie právnych predpisov EÚ týkajúcich sa výrobkov 2022“[20], všeobecným pravidlom je, že viac ako jeden právny akt z harmonizačných právnych predpisov Únie, ako sú nariadenia Európskeho parlamentu a Rady (EÚ) 2017/745[21] a (EÚ) 2017/746[22] alebo smernica Európskeho parlamentu a Rady 2006/42/ES[23], sa môže uplatňovať na jeden výrobok, keďže sprístupnenie alebo uvedenie do prevádzky sa môže uskutočniť len vtedy, keď je výrobok v súlade so všetkými uplatniteľnými harmonizačnými právnymi predpismi Únie. S cieľom zabezpečiť konzistentnosť a zabrániť zbytočnému administratívnemu zaťaženiu alebo nákladom by poskytovatelia výrobku, ktorý obsahuje jeden alebo viacero vysokorizikových systémov AI, na ktoré sa vzťahujú požiadavky tohto nariadenia a požiadavky harmonizačných právnych predpisov Únie uvedených v prílohe k tomuto nariadeniu, mali mať flexibilitu, pokiaľ ide o operačné rozhodnutia týkajúce sa zabezpečenia súladu výrobku obsahujúceho jeden alebo viacero systémov AI so všetkými uplatniteľnými požiadavkami harmonizačných právnych predpisov Únie optimálnym spôsobom. Systémy AI označené ako vysokorizikové by sa mali obmedziť na tie, ktoré majú významný škodlivý vplyv na zdravie, bezpečnosť a základné práva osôb v Únii, a takéto obmedzenie by malo minimalizovať akékoľvek prípadné obmedzenie medzinárodného obchodu.

---

20 Ú. v. EÚ C 247, 29.6.2022, s. 1.

21 Nariadenie Európskeho parlamentu a Rady (EÚ) 2017/745 z 5. apríla 2017 o zdravotníckych pomôckach, zmene smernice 2001/83/ES, nariadenia (ES) č. 178/2002 a nariadenia (ES) č. 1223/2009 a o zrušení smerníc Rady 90/385/EHS a 93/42/EHS (Ú. v. EÚ L 117, 5.5.2017, s. 1).

22 Nariadenie Európskeho parlamentu a Rady (EÚ) 2017/746 z 5. apríla 2017 o diagnostických zdravotníckych pomôckach *in vitro* a o zrušení smernice 98/79/ES a rozhodnutia Komisie 2010/227/EÚ (Ú. v. EÚ L 117, 5.5.2017, s. 176).

23 Smernica Európskeho parlamentu a Rady 2006/42/ES zo 17. mája 2006 o strojových zariadeniach a o zmene a doplnení smernice 95/16/ES (Ú. v. EÚ L 157, 9.6.2006, s. 24).

(47) Systémy AI by mohli mať nepriaznivý vplyv na zdravie a bezpečnosť osôb, najmä ak takéto systémy fungujú ako bezpečnostné komponenty výrobkov. V súlade s cieľmi harmonizačných právnych predpisov Únie uľahčiť voľný pohyb výrobkov na vnútornom trhu a zabezpečiť, aby sa na trh dostali len bezpečné a inak vyhovujúce výrobky, je dôležité, aby sa riadne predchádzalo bezpečnostným rizikám, ktoré môže výrobok ako celok vytvárať svojimi digitálnymi komponentmi vrátane systémov AI, a aby sa tieto riziká náležite zmierňovali. Napríklad čoraz autonómnejšie roboty, či už v kontexte výroby alebo osobnej asistencie a starostlivosti, by mali byť schopné bezpečne fungovať a vykonávať svoje funkcie v zložitých prostrediach. Podobne v sektore zdravotníctva, kde existuje obzvlášť vysoké riziko v oblasti života a zdravia, by mali byť čoraz sofistikovanejšie diagnostické systémy a systémy podporujúce ľudské rozhodnutia spoľahlivé a presné.

(48) Pri klasifikácii systému AI ako vysokorizikového je obzvlášť dôležitý rozsah nepriaznivého vplyvu systému AI na základné práva chránené chartou. Medzi tieto práva patrí právo na ľudskú dôstojnosť, rešpektovanie súkromného a rodinného života, ochrana osobných údajov, sloboda prejavu a právo na informácie, sloboda zhromažďovania a združovania, právo na nediskrimináciu, právo na vzdelávanie, ochrana spotrebiteľa, pracovné práva, práva osôb so zdravotným postihnutím, rodová rovnosť, práva duševného vlastníctva, právo na účinný prostriedok nápravy a na spravodlivý proces, právo na obhajobu a prezumpcia neviny a právo na dobrú správu vecí verejných. Okrem týchto práv je dôležité zdôrazniť, že deti majú osobitné práva zakotvené v článku 24 charty a v Dohovore Organizácie Spojených národov o právach dieťaťa, ďalej rozpracované vo všeobecnej poznámke č. 25 Dohovoru OSN o právach dieťaťa v súvislosti s digitálnym prostredím, ktoré si v oboch prípadoch vyžadujú zváženie zraniteľnosti detí a poskytnutie takejto ochrany a starostlivosti nevyhnutných pre ich blaho. Pri posudzovaní závažnosti ujmy, ktorú môže systém AI spôsobiť, a to aj v súvislosti so zdravím a bezpečnosťou osôb, by sa malo zohľadniť aj základné právo na vysokú úroveň ochrany životného prostredia zakotvené v charte a vykonávané v politikách Únie.

(49) Pokiaľ ide o vysokorizikové systémy AI, ktoré sú bezpečnostnými komponentmi výrobkov alebo systémov, alebo ktoré sú samy výrobkami alebo systémami patriacimi do rozsahu pôsobnosti nariadenia Európskeho parlamentu a Rady (ES) č. 300/2008[24], nariadenia Európskeho parlamentu a Rady (EÚ) č. 167/2013[25], nariadenia Európskeho parlamentu a Rady (EÚ) č. 168/2013[26], smernice Európskeho parlamentu a Rady 2014/90/EÚ[27], smernice Európskeho parlamentu a Rady (EÚ) 2016/797[28],

---

24 Nariadenie Európskeho parlamentu a Rady (ES) č. 300/2008 z 11. marca 2008 o spoločných pravidlách v oblasti bezpečnostnej ochrany civilného letectva a o zrušení nariadenia (ES) č. 2320/2002 (Ú. v. EÚ L 97, 9.4.2008, s. 72).

25 Nariadenie Európskeho parlamentu a Rady (EÚ) č. 167/2013 z 5. februára 2013 o schvaľovaní poľnohospodárskych a lesných vozidiel a o dohľade nad trhom s týmito vozidlami (Ú. v. EÚ L 60, 2.3.2013, s. 1).

26 Nariadenie Európskeho parlamentu a Rady (EÚ) č. 168/2013 z 15. januára 2013 o schvaľovaní a dohľade nad trhom dvoj- alebo trojkolesových vozidiel a štvorkoliek (Ú. v. EÚ L 60, 2.3.2013, s. 52).

27 Smernica Európskeho parlamentu a Rady 2014/90/EÚ z 23. júla 2014 o vybavení námorných lodí a o zrušení smernice Rady 96/98/ES (Ú. v. EÚ L 257, 28.8.2014, s. 146).

28 Smernica Európskeho parlamentu a Rady (EÚ) 2016/797 z 11. mája 2016 o interoperabilite železničného systému v Európskej únii (Ú. v. EÚ L 138, 26.5.2016, s. 44).

nariadenia Európskeho parlamentu a Rady (EÚ) 2018/858[29], nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1139[30] a nariadenia Európskeho parlamentu a Rady (EÚ) 2019/2144[31], je vhodné uvedené akty zmeniť s cieľom zaistiť, aby Komisia pri prijímaní akýchkoľvek relevantných delegovaných alebo vykonávacích aktov na základe uvedených aktov zohľadňovala povinné požiadavky na vysokorizikové systémy AI stanovené v tomto nariadení na základe technických a regulačných osobitostí jednotlivých odvetví bez toho, aby zasahovala do existujúcich mechanizmov správy, posudzovania zhody a presadzovania a do orgánov zriadených v rámci uvedených aktov.

---

29 Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/858 z 30. mája 2018 o schvaľovaní motorových vozidiel a ich prípojných vozidiel, ako aj systémov, komponentov a samostatných technických jednotiek určených pre takéto vozidlá a o dohľade nad trhom s nimi, ktorým sa menia nariadenia (ES) č. 715/2007 a (ES) č. 595/2009 a zrušuje smernica 2007/46/ES (Ú. v. EÚ L 151, 14.6.2018, s. 1).

30 Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1139 zo 4. júla 2018 o spoločných pravidlách v oblasti civilného letectva, ktorým sa zriaďuje Agentúra Európskej únie pre bezpečnosť letectva a ktorým sa menia nariadenia Európskeho parlamentu a Rady (ES) č. 2111/2005, (ES) č. 1008/2008, (EÚ) č. 996/2010, (EÚ) č. 376/2014 a smernice Európskeho parlamentu a Rady 2014/30/EÚ a 2014/53/EÚ a zrušujú nariadenia Európskeho parlamentu a Rady (ES) č. 552/2004 a (ES) č. 216/2008 a nariadenie Rady (EHS) č. 3922/91 (Ú. v. EÚ L 212, 22.8.2018, s. 1).

31 Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/2144 z 27. novembra 2019 o požiadavkách na typové schvaľovanie motorových vozidiel a ich prípojných vozidiel a systémov, komponentov a samostatných technických jednotiek určených pre tieto vozidlá, pokiaľ ide o ich všeobecnú bezpečnosť a ochranu cestujúcich vo vozidle a zraniteľných účastníkov cestnej premávky, ktorým sa mení nariadenie Európskeho parlamentu a Rady (EÚ) 2018/858 a ktorým sa zrušujú nariadenia Európskeho parlamentu a Rady (ES) č. 78/2009, (ES) č. 79/2009 a (ES) č. 661/2009 a nariadenia Komisie (ES) č. 631/2009, (EÚ) č. 406/2010, (EÚ) č. 672/2010, (EÚ) č. 1003/2010, (EÚ) č. 1005/2010, (EÚ) č. 1008/2010, (EÚ) č. 1009/2010, (EÚ) č. 19/2011, (EÚ) č. 109/2011, (EÚ) č. 458/2011, (EÚ) č. 65/2012, (EÚ) č. 130/2012, (EÚ) č. 347/2012, (EÚ) č. 351/2012, (EÚ) č. 1230/2012 a (EÚ) 2015/166 (Ú. v. EÚ L 325, 16.12.2019, s. 1).

(50) Pokiaľ ide o systémy AI, ktoré sú bezpečnostnými komponentmi výrobkov alebo ktoré sú samy výrobkami, ktoré patria do rozsahu pôsobnosti určitých harmonizačných právnych predpisov Únie uvedených v prílohe k tomuto nariadeniu, je vhodné klasifikovať ich podľa tohto nariadenia ako vysokorizikové, pokiaľ v prípade dotknutého výrobku vykonáva postup posudzovania zhody orgán posudzovania zhody tretej strany podľa príslušných harmonizačných právnych predpisov Únie. Medzi takéto výrobky patria najmä strojové zariadenia, hračky, výťahy, zariadenia a ochranné systémy určené na použitie v potenciálne výbušnej atmosfére, rádiové zariadenia, tlakové zariadenia, vybavenie rekreačných plavidiel, lanovkové zariadenia, spotrebiče spaľujúce plynné palivá, zdravotnícke pomôcky, diagnostické zdravotnícke pomôcky *in vitro*, automobilový a letecký priemysel.

(51) Klasifikácia systému AI ako vysokorizikového podľa tohto nariadenia by nemala nevyhnutne znamenať, že sa výrobok, ktorého bezpečnostným komponentom je systém AI, alebo samotný systém AI ako výrobok považuje za vysokorizikový podľa kritérií stanovených v príslušných harmonizačných právnych predpisoch Únie, ktoré sa vzťahujú na daný výrobok. Platí to najmä pre nariadenia (EÚ) 2017/745 a (EÚ) 2017/746, kde sa pre výrobky so stredným a vysokým rizikom vyžaduje posudzovanie zhody treťou stranou.

(52) Pokiaľ ide o samostatné systémy AI, konkrétne iné vysokorizikové systémy AI ako tie, ktoré sú bezpečnostnými komponentmi výrobkov alebo ktoré sú samy výrobkami, je vhodné klasifikovať ich ako vysokorizikové, ak vzhľadom na svoj zamýšľaný účel predstavujú vysoké riziko poškodenia zdravia a bezpečnosti alebo základných práv osôb, pričom sa berie do úvahy závažnosť možnej ujmy a pravdepodobnosť jej výskytu, a ak sa využívajú vo viacerých oblastiach uvedených v tomto nariadení, ktoré sú jasne vopred vymedzené. Identifikácia týchto systémov je založená na rovnakej metodike a kritériách, aké sa predpokladajú aj v prípade akýchkoľvek budúcich zmien zoznamu vysokorizikových systémov AI, ktoré by Komisia mala byť splnomocnená prijímať prostredníctvom delegovaných aktov s cieľom zohľadniť rýchle tempo technologického vývoja, ako aj potenciálne zmeny v používaní systémov AI.

(53) Takisto je dôležité upresniť, že môžu existovať osobitné prípady, v ktorých systémy AI uvedené vo vopred vymedzených oblastiach špecifikovaných v tomto nariadení nevedú k významnému riziku ujmy na právnych záujmoch chránených v týchto oblastiach, pretože podstatne neovplyvňujú rozhodovanie ani nespôsobujú týmto záujmom podstatnú ujmu. Na účely tohto nariadenia by sa mal systém AI, ktorý významne neovplyvňuje výsledok rozhodovania, chápať ako systém AI, ktorý nemá vplyv na podstatu, a teda na výsledok rozhodovania, či už ľudského alebo automatizovaného. Systém AI, ktorý významne neovplyvňuje výsledok rozhodovania, by mohol zahŕňať situácie, v ktorých je splnená jedna alebo viaceré z ďalej uvedených podmienok. Prvou takouto podmienkou by malo byť, že systém AI má plniť úzku procedurálnu úlohu, ako je systém AI, ktorý transformuje neštruktúrované údaje na štruktúrované údaje; systém AI, ktorý klasifikuje prichádzajúce dokumenty do kategórií; alebo systém AI, ktorý sa používa na odhaľovanie duplikátov medzi veľkým počtom aplikácií. Tieto úlohy sú takej úzkej a obmedzenej povahy, že predstavujú len obmedzené riziká, ktoré sa nezvýšia používaním systému AI v kontexte, ktorý sa v prílohe k tomuto nariadeniu uvádza ako vysokorizikové použitie. Druhou podmienkou by malo byť, že systém AI vykonáva úlohu s cieľom zlepšiť výsledok predtým ukončenej ľudskej činnosti, ktorá môže byť relevantná na účely vysokorizikových použití uvedených v prílohe k tomuto nariadeniu. Vzhľadom na tieto vlastnosti poskytuje systém AI len ďalšiu vrstvu k ľudskej činnosti s následne zníženým rizikom. Táto podmienka by sa vzťahovala napríklad na systémy AI, ktorých cieľom je zlepšiť jazyk používaný v predchádzajúcich dokumentoch, napríklad v súvislosti s profesionálnym tónom, akademickým štýlom jazyka alebo zosúladením textu s určitou brandovou komunikáciou. Treťou podmienkou by malo byť, že systém AI je určený na odhaľovanie vzorcov rozhodovania alebo odchýlok od predchádzajúcich vzorcov rozhodovania.

Riziko by sa znížilo, pretože používanie systému AI sa riadi predtým dokončeným ľudským posúdením, ktoré nemá nahradiť ani ovplyvniť bez náležitého ľudského preskúmania. Medzi takéto systémy AI patria napríklad tie, ktoré sa vzhľadom na určitý známkovací vzorec učiteľa môžu použiť na ex post kontrolu toho, či sa učiteľ neodchýlil od známkovacieho vzorca, aby sa upozornilo na možné nezrovnalosti alebo anomálie. Štvrtou podmienkou by malo byť, že systém AI má plniť úlohu, ktorá je len prípravou na posúdenie relevantné na účely systémov AI uvedených v prílohe k tomuto nariadeniu, čím sa možný vplyv výstupu systému z hľadiska rizika pre posúdenie, ktoré sa má vykonať, výrazne zníži. Táto podmienka sa týka najmä inteligentných riešení na spracovanie súborov, ktoré zahŕňajú rôzne funkcie ako indexovanie, vyhľadávanie, spracovanie textu a reči alebo prepojenie údajov s inými zdrojmi údajov, alebo systémy AI používané na preklad pôvodných dokumentov. V každom prípade by sa systémy AI používané vo vysokorizikových prípadoch použitia uvedených v prílohe k tomuto nariadeniu mali považovať za systémy predstavujúce významné riziko ujmy na zdraví, bezpečnosti alebo základných právach, ak systém AI zahŕňa profilovanie v zmysle článku 4 bodu 4 nariadenia (EÚ) 2016/679 alebo článku 3 bodu 4 smernice (EÚ) 2016/680 alebo článku 3 bodu 5 nariadenia (EÚ) 2018/1725. S cieľom zabezpečiť vysledovateľnosť a transparentnosť by mal poskytovateľ, ktorý sa na základe vyššie uvedených podmienok domnieva, že systém AI nie je vysokorizikový, vypracovať dokumentáciu posúdenia pred uvedením tohto systému na trh alebo do prevádzky a na požiadanie by mal túto dokumentáciu poskytnúť vnútroštátnym príslušným orgánom. Takýto poskytovateľ by mal byť povinný zaregistrovať systém AI v databáze Únie zriadenej podľa tohto nariadenia. S cieľom poskytnúť ďalšie usmernenia pre praktické vykonávanie podmienok, za ktorých systémy AI uvedené v prílohe k tomuto nariadeniu výnimočne nepredstavujú vysoké riziko, by Komisia mala po konzultácii s radou pre AI poskytnúť usmernenia, v ktorých sa uvedie, že praktické vykonávanie doplnené komplexným zoznamom praktických príkladov prípadov použitia systémov AI, ktoré sú vysokorizikové, a prípadov použitia, ktoré nie sú vysokorizikové.

(54) Keďže biometrické údaje predstavujú osobitnú kategóriu osobných údajov, je vhodné klasifikovať ako vysokorizikové niekoľko prípadov kritického použitia biometrických systémov, pokiaľ ich použitie povoľuje príslušné právo Únie a vnútroštátne právo. Technické nepresnosti systémov AI určených na diaľkovú biometrickú identifikáciu fyzických osôb môžu viesť ku skresleným výsledkom a mať diskriminačné účinky. Riziko takýchto skreslených výsledkov a diskriminačných účinkov je obzvlášť relevantné z hľadiska veku, etnickej príslušnosti, rasy, pohlavia alebo zdravotného postihnutia. Systémy diaľkovej biometrickej identifikácie by sa preto mali klasifikovať ako vysokorizikové vzhľadom na riziká, ktoré predstavujú. Takáto klasifikácia nezahŕňa systémy AI určené na biometrické overenie zahŕňajúce autentifikáciu, ktorých jediným účelom je potvrdiť, že konkrétna fyzická osoba je tou osobou, o ktorej tvrdí, že ňou je, a potvrdiť totožnosť fyzickej osoby výlučne na účely prístupu k službe, odomknutia zariadenia alebo získania bezpečnostného prístupu do priestorov. Okrem toho by sa systémy AI určené na biometrickú kategorizáciu podľa citlivých atribútov alebo charakteristík chránených podľa článku 9 ods. 1 nariadenia (EÚ) 2016/679 na základe biometrických údajov, pokiaľ nie sú zakázané podľa tohto nariadenia, a systémy na rozpoznávanie emócií, ktoré nie sú zakázané podľa tohto nariadenia, mali klasifikovať ako vysokorizikové. Biometrické systémy určené výlučne na účely umožnenia kybernetickej bezpečnosti a opatrení na ochranu osobných údajov, by sa nemali považovať za vysokorizikové systémy AI.

(55) Pokiaľ ide o riadenie a prevádzku kritickej infraštruktúry, je vhodné klasifikovať ako vysokorizikové také systémy AI, ktoré sú určené na používanie ako bezpečnostné komponenty pri riadení a prevádzke kritickej digitálnej infraštruktúry, ako sa uvádza v bode 8 prílohy k smernici (EÚ) 2022/2557, cestnej premávky a pri dodávkach vody, plynu, tepla a elektrickej energie, keďže ich zlyhanie alebo porucha môžu ohroziť život a zdravie osôb vo veľkom rozsahu a viesť k značným narušeniam bežného vykonávania spoločenských a hospodárskych činností. Bezpečnostné komponenty kritickej infraštruktúry vrátane kritickej digitálnej infraštruktúry sú systémy používané na priamu ochranu fyzickej integrity kritickej infraštruktúry alebo zdravia a bezpečnosti osôb a majetku, ktoré však nie sú potrebné na fungovanie systému. Zlyhanie alebo porucha takýchto komponentov môže priamo viesť k rizikám pre fyzickú integritu kritickej infraštruktúry, a tým k rizikám pre zdravie a bezpečnosť osôb a majetku. Komponenty, ktoré sa majú používať výlučne na účely kybernetickej bezpečnosti, by sa nemali považovať za bezpečnostné komponenty. Príklady bezpečnostných komponentov takejto kritickej infraštruktúry môžu zahŕňať systémy monitorovania tlaku vody alebo systémy riadenia požiarneho poplachu v centrách cloud computingu.

(56) Nasadzovanie systémov AI v oblasti vzdelávania je dôležité na podporu vysokokvalitného digitálneho vzdelávania a odbornej prípravy a na to, aby sa všetkým vzdelávajúcim sa osobám a učiteľom umožnilo získať a zdieľať potrebné digitálne zručnosti a kompetencie vrátane mediálnej gramotnosti a kritického myslenia, aby mohli zohrávať aktívnu úlohu v hospodárstve, spoločnosti a demokratických procesoch. Systémy AI používané v oblasti vzdelávania alebo odbornej prípravy, obzvlášť na určovanie prístupu alebo prijatia, na prideľovanie osôb do inštitúcií alebo programov vzdelávania a odbornej prípravy na všetkých stupňoch, na hodnotenie učebných výsledkov osôb, na posúdenie primeranej úrovne vzdelania pre jednotlivca a podstatné ovplyvňovanie úrovne vzdelávania a odbornej prípravy, ktoré jednotlivci dostanú alebo ku ktorým budú mať prístup, alebo na jeho monitorovanie a odhaľovanie zakázaného správania študentov počas testov by sa mali klasifikovať ako vysokorizikové systémy AI, pretože môžu určovať vzdelávací a profesijný priebeh života osoby, a tým môžu ovplyvňovať jej schopnosť zabezpečiť si živobytie. Ak sú takéto systémy dizajnované a používané nesprávne, môžu byť obzvlášť rušivé a môžu porušovať právo na vzdelanie a odbornú prípravu, ako aj právo nebyť diskriminovaný, a tým zachovávať zaužívané vzorce diskriminácie, napríklad žien, určitých vekových skupín, osôb so zdravotným postihnutím alebo osôb určitého rasového alebo etnického pôvodu alebo s určitou sexuálnou orientáciou.

(57) Ako vysokorizikové by sa mali klasifikovať aj systémy AI používané v oblasti zamestnania, pri riadení pracovníkov a prístupe k samostatnej zárobkovej činnosti, najmä pri nábore a výbere osôb, pri prijímaní rozhodnutí ovplyvňujúcich vzťah súvisiaci s pracovnými podmienkami, pri kariérnom postupe v zamestnaní a ukončení zmluvného pracovnoprávneho vzťahu, pri prideľovaní úloh na základe individuálneho správania, osobných čŕt alebo charakteristík a pri monitorovaní alebo hodnotení osôb v zmluvných pracovnoprávnych vzťahoch, pretože tieto systémy môžu významne ovplyvniť budúce kariérne vyhliadky a živobytie týchto osôb a práva pracovníkov. Príslušné zmluvné pracovnoprávne vzťahy by mali zmysluplne zahŕňať zamestnancov a osoby poskytujúce služby prostredníctvom platforiem, ako sa uvádza v pracovnom programe Komisie na rok 2021. Takéto systémy môžu počas celého procesu prijímania do zamestnania a počas hodnotenia, povyšovania alebo udržiavania osôb v zmluvných pracovnoprávnych vzťahoch zachovávať zaužívané vzorce diskriminácie, napríklad žien, určitých vekových skupín, osôb so zdravotným postihnutím alebo osôb určitého rasového alebo etnického pôvodu alebo sexuálnej orientácie. Systémy AI používané na monitorovanie výkonu a správania týchto osôb môžu mať vplyv aj na ich základné práva na ochranu údajov a súkromia.

(58) Ďalšou oblasťou, v ktorej si využívanie systémov AI zaslúži osobitnú pozornosť, je prístup k určitým základným súkromným a verejným službám a dávkam, ktoré sú potrebné na to, aby sa ľudia mohli plne zapojiť do spoločnosti alebo si mohli zlepšiť životnú úroveň, a ich využívanie. Najmä fyzické osoby, ktoré žiadajú orgány verejnej moci o základné dávky a služby verejnej pomoci alebo ktoré ich od týchto orgánov dostávajú, konkrétne služby zdravotnej starostlivosti, dávky sociálneho zabezpečenia, sociálne služby poskytujúce ochranu v prípadoch, ako je materstvo, choroba, pracovné úrazy, závislosť alebo staroba a strata zamestnania a sociálna pomoc a pomoc pri bývaní, sú zvyčajne závislé od týchto dávok a služieb a sú vo vzťahu k zodpovedným orgánom v zraniteľnom postavení. Ak sa systémy AI používajú na určenie toho, či by orgány mali takéto dávky a služby poskytnúť, zamietnuť, znížiť, zrušiť alebo žiadať o ich vrátenie, vrátane toho, či majú poberatelia oprávnený nárok na takéto dávky alebo služby, takéto systémy môžu mať významný vplyv na živobytie osôb a môžu porušovať ich základné práva, ako je právo na sociálnu ochranu, nediskrimináciu, ľudskú dôstojnosť alebo účinný prostriedok nápravy, a mali by sa preto klasifikovať ako vysokorizikové. Toto nariadenie by však nemalo brániť vývoju a využívaniu inovačných prístupov vo verejnej správe, pre ktorú by mohlo byť širšie využívanie vyhovujúcich a bezpečných systémov AI prospešné, za predpokladu, že tieto systémy nepredstavujú vysoké riziko pre právnické a fyzické osoby.

Ako vysokorizikové by sa okrem toho mali klasifikovať aj systémy AI používané na bodové hodnotenie kreditného rizika alebo hodnotenie úverovej bonity fyzických osôb, pretože určujú prístup týchto osôb k finančným zdrojom alebo základným službám, ako sú bývanie, elektrická energia a telekomunikačné služby. Systémy AI používané na takéto účely môžu viesť k diskriminácii osôb alebo skupín a môžu zachovávať zaužívané vzorce diskriminácie, napríklad na základe rasového alebo etnického pôvodu, rodu, zdravotných postihnutí, veku alebo sexuálnej orientácie, alebo môžu vytvárať nové formy diskriminačných vplyvov. Systémy AI stanovené v práve Únie na účely odhaľovania podvodov pri ponúkaní finančných služieb a na prudenciálne účely výpočtu kapitálových požiadaviek úverových inštitúcií a poisťovní by sa však podľa tohto nariadenia nemali považovať za vysokorizikové. Okrem toho systémy AI, ktoré sa majú používať na posudzovanie rizika a stanovovanie cien v súvislosti s fyzickými osobami na účely zdravotného a životného poistenia, môžu mať tiež významný vplyv na živobytie osôb, a ak nie sú riadne dizajnované, vyvinuté a používané, môžu porušovať ich základné práva a viesť k vážnym dôsledkom pre život a zdravie ľudí vrátane finančného vylúčenia a diskriminácie. Napokon, ako vysokorizikové by sa mali klasifikovať aj systémy AI používané na hodnotenie a klasifikáciu tiesňových volaní fyzických osôb alebo na vysielanie alebo prioritizáciu vysielania záchranných služieb prvej reakcie, vrátane polície, hasičov a zdravotnej pomoci, ako aj systémy triedenia pacientov v rámci pohotovostnej zdravotnej starostlivosti, pretože prijímajú rozhodnutia v situáciách, ktoré sú veľmi kritické z hľadiska života a zdravia osôb a ich majetku.

(59) Konanie orgánov presadzovania práva zahŕňajúce určité použitia systémov AI sa vzhľadom na ich úlohu a zodpovednosť vyznačuje značným stupňom nerovnováhy moci a môže viesť k sledovaniu, zadržaniu alebo pozbaveniu slobody fyzickej osoby, ako aj k iným nepriaznivým vplyvom na základné práva zaručené chartou. Najmä ak systém AI nie je trénovaný na vysokokvalitných údajoch, nespĺňa primerané požiadavky, pokiaľ ide o jeho výkon, presnosť alebo spoľahlivosť, alebo nie je pred uvedením na trh alebo do prevádzky riadne dizajnovaný a otestovaný, môže ľudí selektovať diskriminačným alebo inak nesprávnym či nespravodlivým spôsobom. Okrem toho by mohlo byť obmedzené uplatňovanie dôležitých procesných základných práv, ako je právo na účinný prostriedok nápravy a na spravodlivý proces, ako aj právo na obhajobu a prezumpcia neviny, najmä ak takéto systémy AI nie sú dostatočne transparentné, vysvetliteľné a zdokumentované. Preto je vhodné klasifikovať ako vysokorizikové viaceré systémy AI, pokiaľ je ich používanie povolené na základe relevantného práva Únie alebo vnútroštátneho práva, určené na používanie v kontexte presadzovania práva, kde je presnosť, spoľahlivosť a transparentnosť obzvlášť dôležitá, aby sa zabránilo nepriaznivým vplyvom, zachovala dôvera verejnosti a zabezpečila zodpovednosť a účinná náprava.

Vzhľadom na povahu predmetných činností a s nimi súvisiace riziká by tieto vysokorizikové systémy AI mali zahŕňať najmä systémy AI určené na používanie orgánmi presadzovania práva alebo v ich mene alebo inštitúciami, orgánmi, úradmi alebo agentúrami Únie na podporu orgánov presadzovania práva na posúdenie rizika, že sa fyzická osoba stane obeťou trestných činov, ako sú polygrafy a podobné nástroje, na hodnotenie spoľahlivosti dôkazov v priebehu vyšetrovania alebo stíhania trestných činov, a pokiaľ sa to týmto nariadením nezakazuje, aj na posúdenie rizika, že fyzická osoba spácha alebo opakovane spácha trestný čin, a to nielen na základe profilovania fyzických osôb, alebo na základe posúdenia osobnostných čŕt a charakteristík alebo trestnej činnosti fyzických osôb alebo skupín v minulosti, na profilovanie v priebehu odhaľovania, vyšetrovania alebo stíhania trestných činov. Systémy AI, ktoré sú osobitne určené na používanie v správnych konaniach daňovými a colnými orgánmi, ako aj finančnými spravodajskými jednotkami vykonávajúcimi administratívne úlohy spočívajúce v analýze informácií podľa právnych predpisov Únie v oblasti boja proti praniu špinavých peňazí, by sa nemali klasifikovať ako vysokorizikové systémy AI používané orgánmi presadzovania práva na účely predchádzania trestným činom, ich odhaľovania, vyšetrovania a stíhania. Používanie nástrojov AI orgánmi presadzovania práva a inými relevantnými orgánmi by sa nemalo stať faktorom nerovnosti alebo vylúčenia. Vplyv používania nástrojov AI na právo podozrivých osôb na obhajobu by sa nemal ignorovať, predovšetkým pokiaľ ide o ťažkosti pri získavaní zmysluplných informácií o fungovaní takýchto systémov a z toho vyplývajúce ťažkosti pri napadnutí ich výsledkov na súde, najmä zo strany vyšetrovaných fyzických osôb.

(60) Systémy AI používané v oblastiach migrácie, azylu a riadenia kontroly hraníc majú vplyv na osoby, ktoré sú často v mimoriadne zraniteľnom postavení a ktoré sú závislé od výsledku konania príslušných orgánov verejnej moci. Presnosť, nediskriminačný charakter a transparentnosť systémov AI používaných v tomto kontexte sú preto mimoriadne dôležité na zaručenie dodržiavania základných práv dotknutých osôb, najmä ich práva na voľný pohyb, nediskrimináciu, ochranu súkromia a osobných údajov, medzinárodnú ochranu a dobrú správu vecí verejných. Je preto vhodné klasifikovať ako vysokorizikové tie systémy AI, pokiaľ je ich používanie povolené na základe relevantného práva Únie alebo vnútroštátneho práva, ktoré majú používať príslušné orgány verejnej moci alebo sa majú používať v ich mene, alebo ktoré majú používať inštitúcie, orgány, úrady alebo agentúry Únie poverené úlohami v oblasti migrácie, azylu a riadenia kontroly hraníc, ako napríklad polygrafy a podobné nástroje, na posudzovanie určitých rizík, ktoré predstavujú fyzické osoby vstupujúce na územie členského štátu alebo žiadajúce o vízum alebo azyl, na pomoc príslušným orgánom verejnej moci pri skúmaní žiadostí o azyl, víza a povolenia na pobyt, vrátane súvisiaceho posúdenia spoľahlivosti dôkazov, a súvisiacich sťažností, pokiaľ ide o cieľ zistiť oprávnenosť fyzických osôb žiadajúcich o určitý status, na účely odhaľovania, rozpoznávania alebo identifikácie fyzických osôb v kontexte migrácie, azylu a riadenia kontroly hraníc s výnimkou overovania cestovných dokladov.

Systémy AI v oblasti migrácie, azylu a riadenia kontroly hraníc, na ktoré sa vzťahuje toto nariadenie, by mali spĺňať príslušné procedurálne požiadavky stanovené v nariadení Európskeho parlamentu a Rady (ES) č. 810/2009[32], smernici Európskeho parlamentu a Rady 2013/32/EÚ[33] a iných príslušných právnych predpisoch Únie. Používanie systémov AI v oblasti migrácie, azylu a riadenia kontroly hraníc by členské štáty alebo inštitúcie, orgány, úrady alebo agentúry Únie za žiadnych okolností nemali využívať ako prostriedok na obchádzanie svojich medzinárodných záväzkov podľa Dohovoru OSN o právnom postavení utečencov podpísaného v Ženeve 28. júla 1951 a zmeneného protokolom z 31. januára 1967. Tieto systémy by sa nemali používať ani na to, aby sa akýmkoľvek spôsobom porušovala zásada zákazu vyhostenia alebo vrátenia, alebo aby sa odopierali bezpečné a účinné zákonné spôsoby vstupu na územie Únie vrátane práva na medzinárodnú ochranu.

---

[32] Nariadenie európskeho parlamentu a Rady (ES) č. 810/2009 z 13. júla 2009, ktorým sa ustanovuje vízový kódex Spoločenstva (vízový kódex) (Ú. v. EÚ L 243, 15.9.2009, s. 1).

[33] Smernica Európskeho parlamentu a Rady 2013/32/EÚ z 26. júna 2013 o spoločných konaniach o poskytovaní a odnímaní medzinárodnej ochrany (Ú. v. EÚ L 180, 29.6.2013, s. 60).

(61) Niektoré systémy AI určené na výkon spravodlivosti a demokratických procesov by sa mali klasifikovať ako vysokorizikové vzhľadom na ich potenciálne významný vplyv na demokraciu, právny štát, osobné slobody, ako aj právo na účinný prostriedok nápravy a na spravodlivý proces. Ako vysokorizikové je vhodné kvalifikovať systémy AI určené na použitie zo strany justičného orgánu alebo v jeho mene na pomoc justičným orgánom pri skúmaní a výklade skutkových okolností a práva a pri uplatňovaní práva na konkrétny súbor skutkových okolností, najmä z dôvodu riešenia rizík možného skreslenia, chýb a nepriehľadnosti. Systémy AI, ktoré majú používať subjekty alternatívneho riešenia sporov na tieto účely, by sa takisto mali považovať za vysokorizikové, ak výsledky konania o alternatívnom riešení sporov majú pre strany právne účinky. Používanie nástrojov AI môže podporiť rozhodovaciu právomoc sudcov alebo nezávislosť súdnictva, ale nemalo by ju nahrádzať: konečné rozhodovanie musí zostať ľudskou činnosťou. Kvalifikácia systémov AI ako vysokorizikových by sa však nemala vzťahovať na systémy AI určené na čisto pomocné administratívne činnosti, ktoré nemajú vplyv na samotný výkon spravodlivosti v jednotlivých prípadoch, ako napríklad anonymizácia alebo pseudonymizácia súdnych rozhodnutí, dokumentov alebo údajov, komunikácia medzi zamestnancami alebo administratívne úlohy.

(62) Bez toho, aby boli dotknuté pravidlá stanovené v nariadení Európskeho parlamentu a Rady (EÚ) 2024/...[34+], a s cieľom riešiť riziká neprimeraného vonkajšieho zasahovania do práva voliť zakotveného v článku 39 charty a riziká neprimeraných účinkov na demokraciu a právny štát by sa systémy AI, ktoré sa majú používať na ovplyvňovanie výsledku volieb alebo referenda alebo volebného správania fyzických osôb pri výkone ich hlasovania vo voľbách alebo referendách, mali klasifikovať ako vysokorizikové systémy AI s výnimkou systémov AI, ktorých výstupom nie sú fyzické osoby priamo vystavené, ako sú nástroje používané na organizovanie, optimalizáciu a štruktúrovanie politických kampaní z administratívneho a logistického hľadiska.

(63) Skutočnosť, že systém AI sa podľa tohto nariadenia klasifikuje ako vysokorizikový systém AI, by sa nemala vykladať ako naznačujúca, že používanie tohto systému je zákonné podľa iných aktov práva Únie alebo vnútroštátneho práva zlučiteľného s právom Únie, ako napríklad práva v oblasti ochrany osobných údajov, používania polygrafov a podobných nástrojov alebo iných systémov na zisťovanie emocionálneho stavu fyzických osôb. Akékoľvek takéto použitie by sa malo naďalej vykonávať výlučne v súlade s uplatniteľnými požiadavkami vyplývajúcimi z charty a z uplatniteľných aktov sekundárneho práva Únie a vnútroštátneho práva. Toto nariadenie by sa nemalo vykladať tak, že poskytuje právny základ pre spracúvanie osobných údajov v relevantných prípadoch vrátane osobitných kategórií osobných údajov, pokiaľ sa v tomto nariadení výslovne neustanovuje inak.

---

[34] Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/... z ... o transparentnosti a cielení politickej reklamy (Ú. v. EÚ L, ..., ELI: ...).

[+] Ú. v.: vložte do textu číslo nariadenia nachádzajúceho sa v dokumente PE 90/23 (2021/0381 (COD)) a doplňte príslušnú poznámku pod čiarou.

(64) S cieľom zmierniť riziká, ktoré vyplývajú z vysokorizikových systémov AI uvedených na trh alebo do prevádzky, a zabezpečiť vysokú úroveň dôveryhodnosti, by sa na vysokorizikové systémy AI mali uplatňovať určité povinné požiadavky, pričom by sa mal zohľadniť zamýšľaný účel a kontext používania systému AI a podľa systému riadenia rizík, ktorý má zaviesť poskytovateľ. Opatrenia prijaté poskytovateľmi na dosiahnutie súladu s povinnými požiadavkami tohto nariadenia by mali zohľadňovať všeobecne uznávaný aktuálny stav vývoja AI a mali by byť primerané a účinné na splnenie cieľov tohto nariadenia. Na základe nového legislatívneho rámca, ako sa objasňuje v oznámení Komisie s názvom „Modrá príručka na vykonávanie právnych predpisov EÚ týkajúcich sa výrobkov 2022“, všeobecným pravidlom je, že viac ako jeden právny akt z harmonizačných právnych predpisov Únie sa môže uplatňovať na jeden výrobok, keďže sprístupnenie alebo uvedenie do prevádzky sa môže uskutočniť len vtedy, keď je výrobok v súlade so všetkými uplatniteľnými harmonizačnými právnymi predpismi Únie. Nebezpečenstvá systémov AI, na ktoré sa vzťahujú požiadavky tohto nariadenia, sa týkajú iných aspektov ako existujúce harmonizačné právne predpisy Únie, a preto by požiadavky tohto nariadenia dopĺňali existujúci súbor harmonizačných právnych predpisov Únie. Napríklad strojové zariadenia alebo zdravotnícke pomôcky obsahujúce systém AI by mohli predstavovať riziká, ktoré sa neriešia v základných zdravotných a bezpečnostných požiadavkách stanovených v príslušných harmonizovaných právnych predpisoch Únie, keďže toto odvetvové právo sa nezaoberá rizikami špecifickými pre systémy AI.

Je preto potrebné súbežné a komplementárne uplatňovanie rôznych legislatívnych aktov. S cieľom zabezpečiť konzistentnosť a zabrániť zbytočnému administratívnemu zaťaženiu a nákladom by poskytovatelia výrobku, ktorý obsahuje jeden alebo viacero vysokorizikových systémov AI, na ktoré sa vzťahujú požiadavky tohto nariadenia a požiadavky harmonizačných právnych predpisov Únie založených na novom legislatívnom rámci a uvedených v prílohe k tomuto nariadeniu, mali mať flexibilitu, pokiaľ ide o operačné rozhodnutia o tom, ako zabezpečiť súlad výrobku obsahujúceho jeden alebo viacero systémov AI so všetkými uplatniteľnými požiadavkami daných harmonizovaných právnych predpisov Únie optimálnym spôsobom. Uvedená flexibilita by mohla znamenať napríklad rozhodnutie poskytovateľa začleniť časť potrebných postupov testovania a podávania správ, informácií a dokumentácie požadovaných podľa tohto nariadenia do existujúcej dokumentácie a postupov požadovaných podľa existujúcich harmonizačných právnych predpisov Únie založených na novom legislatívnom rámci a uvedených v prílohe k tomuto nariadeniu. To by v žiadnom prípade nemalo oslabiť povinnosť poskytovateľa dodržiavať všetky uplatniteľné požiadavky.

(65) Systém riadenia rizík by mal pozostávať z nepretržitého iteratívneho procesu plánovaného a prebiehajúceho počas celého životného cyklu vysokorizikového systému AI. Tento proces by mal byť zameraný na identifikáciu a zmiernenie relevantných rizík systémov AI v oblasti zdravia, bezpečnosti a základných práv. Systém riadenia rizík by sa mal pravidelne preskúmavať a aktualizovať, aby sa zabezpečila jeho trvalá účinnosť, ako aj odôvodnenie a dokumentácia všetkých významných rozhodnutí a opatrení prijatých podľa tohto nariadenia. Týmto procesom by sa malo zabezpečiť, aby poskytovateľ identifikoval riziká alebo nepriaznivé vplyvy a vykonal zmierňujúce opatrenia zamerané na známe a odôvodnene predvídateľné riziká systémov AI pre zdravie, bezpečnosť a základné práva vzhľadom na ich zamýšľaný účel a rozumne predvídateľné nesprávne použitie vrátane možných rizík vyplývajúcich z interakcie medzi systémom AI a prostredím, v ktorom funguje. Systém riadenia rizík by mal prijať najvhodnejšie opatrenia na riadenie rizík vzhľadom na aktuálny stav vývoja AI. Pri určovaní najvhodnejších opatrení na riadenie rizík by mal poskytovateľ zdokumentovať a vysvetliť prijaté rozhodnutia a v prípade potreby by mal zapojiť odborníkov a externé zainteresované strany. Pri identifikácii odôvodnene predvídateľného nesprávneho použitia vysokorizikových systémov AI by sa poskytovateľ mal zaoberať použitím systémov AI, na ktoré sa síce priamo nevzťahuje zamýšľaný účel a ktoré sú stanovené v návode na použitie, možno však odôvodnene očakávať, že budú výsledkom ľahko predvídateľného ľudského správania v kontexte osobitných vlastností a používania konkrétneho systému AI. Všetky známe alebo predvídateľné okolnosti súvisiace s používaním vysokorizikového systému AI v súlade s jeho zamýšľaným účelom alebo za podmienok odôvodnene predvídateľného nesprávneho použitia, ktoré môžu viesť k rizikám pre zdravie a bezpečnosť alebo pre základné práva, by sa mali zahrnúť do návodu na použitie, ktorý poskytuje poskytovateľ. Cieľom je zabezpečiť, aby ich nasadzujúci subjekt poznal a zohľadnil pri používaní vysokorizikového systému AI. Identifikácia a vykonávanie opatrení na zmiernenie rizika predvídateľného nesprávneho použitia podľa tohto nariadenia by si nemali vyžadovať osobitnú dodatočnú odbornú prípravu zo strany poskytovateľa pre vysokorizikový systém AI na riešenie predvídateľného nesprávneho použitia. Poskytovatelia sa však nabádajú, aby zvážili takéto dodatočné opatrenia odbornej prípravy s cieľom zmierniť odôvodnene predvídateľné nesprávne použitie, ak je to potrebné a vhodné.

(66) Požiadavky by sa mali vzťahovať na vysokorizikové systémy AI, pokiaľ ide o riadenie rizík, kvalitu a relevantnosť použitých súborov údajov, technickú dokumentáciu a uchovávanie záznamov, transparentnosť a poskytovanie informácií nasadzujúcim subjektom, ľudský dohľad a spoľahlivosť, presnosť a kybernetickú bezpečnosť. Tieto požiadavky sú potrebné na účinné zmiernenie rizík pre zdravie, bezpečnosť a základné práva. Keďže nie sú primerane dostupné žiadne iné opatrenia menej obmedzujúce obchod, nie sú uvedené požiadavky neodôvodnenými obmedzeniami obchodu.

(67) Pre poskytovanie štruktúry a zabezpečovanie výkonu mnohých systémov AI zohrávajú kľúčovú úlohu vysokokvalitné údaje a prístup k nim, najmä ak sa využívajú techniky zahŕňajúce trénovanie modelov s cieľom zabezpečiť, aby vysokorizikový systém AI fungoval podľa zamýšľaného účelu a bezpečne a aby sa nestal zdrojom diskriminácie zakázanej právom Únie. Súbory vysokokvalitných trénovacích, validačných a testovacích údajov si vyžadujú vykonávanie primeraných postupov správy a riadenia údajov. Súbory údajov na trénovanie, validáciu a testovanie vrátane štítkov by mali byť relevantné, dostatočne reprezentatívne a v čo najväčšej možnej miere bez chýb a úplné vzhľadom na zamýšľaný účel systému. S cieľom uľahčiť dodržiavanie právnych predpisov Únie v oblasti ochrany údajov, ako je nariadenie (EÚ) 2016/679, by postupy správy a riadenia údajov mali v prípade osobných údajov zahŕňať transparentnosť v súvislosti s pôvodným účelom zberu údajov. Súbory údajov by mali mať aj primerané štatistické vlastnosti, a to aj pokiaľ ide o osoby alebo skupiny osôb, v súvislosti s ktorými sa má vysokorizikový systém AI používať, s osobitným dôrazom na zmiernenie možného skreslenia v súboroch údajov, ktoré by mohlo ovplyvniť zdravie a bezpečnosť osôb, mať negatívny vplyv na základné práva alebo viesť k diskriminácii zakázanej podľa práva Únie, najmä ak výstupy údajov ovplyvňujú vstupy pre budúce operácie (uzavretý kruh spätnej väzby). Skreslenie môže byť napríklad inherentné v základných súboroch údajov, najmä ak sa používajú historické údaje alebo údaje vygenerované pri implementácii systémov v reálnych podmienkach.

Výsledky poskytované systémami AI by mohli byť ovplyvnené takýmto inherentným skreslením, ktoré má tendenciu postupne sa zvyšovať, a tým aj zachovávať a prehlbovať existujúcu diskrimináciu, najmä v prípade osôb patriacich k určitým zraniteľným skupinám vrátane rasových a etnických skupín. Požiadavka, aby boli súbory údajov v čo najväčšej miere úplné a bez chýb, by nemala mať v súvislosti s vývojom a testovaním systémov AI vplyv na používanie techník na zachovanie súkromia. Súbory údajov by mali v rozsahu, v akom si to vyžaduje zamýšľaný účel, zohľadňovať najmä znaky, charakteristiky alebo prvky, ktoré sú špecifické pre konkrétne geografické, kontextuálne, behaviorálne alebo funkčné podmienky, za ktorých sa má systém AI používať. Požiadavky týkajúce sa správy údajov možno splniť využitím tretích strán, ktoré ponúkajú certifikované služby dodržiavania predpisov vrátane overovania správy údajov, integrity súborov údajov a postupov trénovania, validácie a testovania údajov, pokiaľ je zabezpečený súlad s požiadavkami na údaje stanovenými v tomto nariadení.

(68) Pokiaľ ide o vývoj a posudzovanie vysokorizikových systémov AI, niektorí aktéri, ako sú poskytovatelia, notifikované osoby a iné príslušné subjekty, ako napríklad centrá digitálnych inovácií, testovacie a experimentálne zariadenia a výskumní pracovníci, by mali mať prístup k súborom vysokokvalitných údajov a využívať ich v rámci oblastí svojich činností, ktoré súvisia s týmto nariadením. Pri poskytovaní dôveryhodného, zodpovedného a nediskriminačného prístupu k vysokokvalitným údajom na účely trénovania, validácie a testovania systémov AI budú mať zásadný význam spoločné európske dátové priestory zriadené Komisiou a uľahčenie výmeny údajov medzi podnikmi a s verejnou správou vo verejnom záujme. Napríklad v oblasti zdravia uľahčí európsky priestor pre údaje týkajúce sa zdravia nediskriminačný prístup k údajom týkajúcim sa zdravia a trénovanie algoritmov AI na týchto súboroch údajov, a to bezpečným, včasným, transparentným a dôveryhodným spôsobom chrániacim súkromie, pričom sa zabezpečí primerané inštitucionálne riadenie. Relevantné príslušné orgány vrátane sektorových orgánov, ktoré poskytujú alebo podporujú prístup k údajom, môžu takisto podporovať poskytovanie vysokokvalitných údajov na trénovanie, validáciu a testovanie systémov AI.

(69) Právo na súkromie a ochranu osobných údajov musí byť zaručené počas celého životného cyklu systému AI. V tejto súvislosti sú pri spracúvaní údajov uplatniteľné zásady špecificky navrhnutej a štandardnej minimalizácie údajov a ochrany údajov stanovené v právnych predpisoch Únie o ochrane údajov. Opatrenia prijaté poskytovateľmi na zabezpečenie súladu s týmito zásadami môžu zahŕňať nielen anonymizáciu a šifrovanie, ale aj používanie technológie, ktorá umožňuje uplatňovanie algoritmov na údaje a umožňuje trénovanie systémov AI bez prenosu medzi stranami alebo kopírovania samotných nespracovaných alebo štruktúrovaných údajov bez toho, aby boli dotknuté požiadavky na správu údajov stanovené v tomto nariadení.

(70) S cieľom chrániť právo iných osôb pred diskrimináciou, ktorá by mohla byť dôsledkom skreslenia v systémoch AI, by poskytovatelia mali výnimočne v rozsahu, v akom je to nevyhnutne potrebné na účely zabezpečenia zisťovania zaujatosti a nápravy v súvislosti s vysokorizikovými systémami AI, s výhradou primeraných záruk základných práv a slobôd fyzických osôb a po uplatnení všetkých uplatniteľných podmienok stanovených v tomto nariadení popri podmienkach stanovených v nariadeniach (EÚ) 2016/679 a (EÚ) 2018/1725 a smernici (EÚ) 2016/680, mať možnosť spracúvať aj osobitné kategórie osobných údajov ako záležitosť podstatného verejného záujmu v zmysle článku 9 ods. 2 písm. g) nariadenia (EÚ) 2016/679 a článku 10 ods. 2 písm. g) nariadenia (EÚ) 2018/1725.

(71) Na umožnenie vysledovateľnosti týchto systémov, overenie súladu s požiadavkami podľa tohto nariadenia, ako aj monitorovanie ich prevádzky a ich monitorovanie po uvedení na trh je nevyhnutné mať zrozumiteľné informácie o tom, ako boli vysokorizikové systémy AI vyvinuté a ako fungujú počas celej svojej životnosti. To si vyžaduje vedenie záznamov a dostupnosť technickej dokumentácie obsahujúcej informácie, ktoré sú potrebné na posúdenie súladu systému AI s príslušnými požiadavkami a uľahčenie ich monitorovania po uvedení na trh. Takéto informácie by mali zahŕňať všeobecné charakteristiky, spôsobilosti a obmedzenia systému, algoritmy, údaje, postupy trénovania, testovania a validácie, ktoré boli použité, ako aj dokumentáciu o príslušnom systéme riadenia rizík vypracovanú jasne a komplexne. Technická dokumentácia by sa mala náležite aktualizovať počas celého životného cyklu systému AI. Vysokorizikové systémy AI by mali okrem toho technicky umožňovať automatické zaznamenávanie udalostí prostredníctvom logov počas celej životnosti systému.

(72) S cieľom riešiť obavy súvisiace s neprehľadnosťou a zložitosťou určitých systémov AI a pomôcť nasadzujúcim subjektom plniť si povinnosti podľa tohto nariadenia by sa v prípade vysokorizikových systémov AI mala pred ich uvedením na trh alebo do prevádzky vyžadovať transparentnosť. Vysokorizikové systémy AI by mali byť dizajnované tak, aby umožnili nasadzujúcim subjektom pochopiť, ako systém AI funguje, vyhodnotiť jeho funkčnosť a pochopiť jeho silné stránky a obmedzenia. K vysokorizikovým systémom AI by mali byť priložené vhodné informácie vo forme návodu na použitie. Takéto informácie by mali zahŕňať charakteristiky, spôsobilosti a obmedzenia výkonu systému AI. Tie by zahŕňali informácie o možných známych a predvídateľných okolnostiach súvisiacich s používaním vysokorizikového systému AI vrátane činností nasadzujúcich subjektov, ktoré môžu ovplyvniť správanie a výkon systému, pri ktorých môže systém AI viesť k rizikám pre zdravie, bezpečnosť a základné práva, o zmenách, ktoré poskytovateľ vopred určil a posúdil z hľadiska zhody, a o príslušných opatreniach ľudského dohľadu vrátane opatrení na uľahčenie výkladu výstupov systému AI nasadzujúcimi subjektmi. Transparentnosť vrátane sprievodného návodu na použitie by mala pomáhať nasadzujúcim subjektom pri používaní systému a podporovať ich informované rozhodovanie. Nasadzujúce subjekty by okrem iného mali mať lepšiu pozíciu na to, aby si mohli správne vybrať systém, ktorý majú v úmysle používať vzhľadom na povinnosti, ktoré sa na nich vzťahujú, mali by sa vzdelávať o zamýšľaných a vylúčených použitiach a používať systém AI správne a náležite. S cieľom zlepšiť čitateľnosť a prístupnosť informácií uvedených v návode na použitie by sa v prípade potreby mali uviesť názorné príklady, napríklad pokiaľ ide o obmedzenia a zamýšľané a vylúčené použitia systému AI. Poskytovatelia by mali zabezpečiť, aby všetka dokumentácia vrátane návodu na použitie obsahovala zmysluplné, komplexné, prístupné a zrozumiteľné informácie, pričom sa zohľadnia potreby a predvídateľné znalosti cieľových nasadzujúcich subjektov. Návod na použitie by mal byť k dispozícii v jazyku, ktorý je podľa dotknutého členského štátu ľahko zrozumiteľný pre cieľový nasadzujúci subjekt.

(73) Vysokorizikové systémy AI by mali byť dizajnované a vyvinuté tak, aby fyzické osoby mohli dohliadať na ich fungovanie, zabezpečiť, aby sa používali podľa zámeru a aby sa ich vplyvy riešili počas životného cyklu systému. Na tento účel by mal poskytovateľ systému určiť pred jeho uvedením na trh alebo do prevádzky vhodné opatrenia na zabezpečenie ľudského dohľadu. Takýmito opatreniami by sa malo prípadne zaručiť najmä to, že do systému budú zabudované prevádzkové obmedzenia, ktoré samotný systém nedokáže potlačiť, a že systém bude reagovať na ľudského operátora a fyzické osoby, ktorým bol zverený ľudský dohľad, budú mať potrebnú spôsobilosť, odbornú prípravu a právomoc vykonávať túto úlohu. Takisto je podľa potreby nevyhnutné zabezpečiť, aby vysokorizikové systémy AI zahŕňali mechanizmy na usmernenie a informovanie fyzickej osoby, ktorej bol pridelený ľudský dohľad, aby mohla prijímať informované rozhodnutia, či, kedy a ako zasiahnuť s cieľom vyhnúť sa negatívnym dôsledkom alebo rizikám, alebo zastaviť systém, ak nefunguje tak, ako sa plánovalo. Vzhľadom na významné dôsledky pre osoby v prípade nesprávneho stanovenia zhody určitými systémami biometrickej identifikácie je vhodné stanoviť požiadavku posilneného ľudského dohľadu nad týmito systémami, aby nasadzujúci subjekt nemohol prijať žiadne opatrenie ani rozhodnutie na základe identifikácie vyplývajúcej zo systému, pokiaľ to samostatne neoverili a nepotvrdili aspoň dve fyzické osoby. Tieto osoby by mohli byť z jedného alebo viacerých subjektov a mohli by zahŕňať osobu, ktorá prevádzkuje alebo používa systém. Táto požiadavka by nemala spôsobovať zbytočnú záťaž alebo oneskorenia a mohlo by stačiť, aby sa samostatné overenia uvedenými týmito jednotlivými osobami automaticky zaznamenávali do logov generovaných systémom. Vzhľadom na osobitosti oblastí presadzovania práva, migrácie, kontroly hraníc a azylu by sa táto požiadavka nemala uplatňovať, keď sa podľa práva Únie alebo vnútroštátneho práva uplatňovanie uvedenej požiadavky považuje za neprimerané.

(74) Vysokorizikové systémy AI by mali fungovať konzistentne počas celého svojho životného cyklu a mali by spĺňať primeranú úroveň presnosti, spoľahlivosti a kybernetickej bezpečnosti vzhľadom na ich zamýšľaný účel a v súlade so všeobecne uznávaným aktuálnym stavom vývoja. Komisia a relevantné organizácie a zainteresované strany sa nabádajú, aby náležite zvážili zmierňovanie rizík a negatívne vplyvy systému AI. Očakávaná úroveň parametrov výkonu by sa mala uviesť v sprievodnom návode na použitie. Poskytovatelia sa vyzývajú, aby uvedené informácie oznamovali nasadzujúcim subjektom jasným a ľahko zrozumiteľným spôsobom bez nezrozumiteľností alebo zavádzajúcich vyhlásení. Cieľom práva Únie v oblasti legálnej metrológie vrátane smerníc Európskeho parlamentu a Rady 2014/31/EÚ[35] a 2014/32/EÚ[36] je zabezpečiť presnosť meraní a pomôcť pri zabezpečovaní transparentnosti a spravodlivosti obchodných transakcií. V uvedenej súvislosti by Komisia v spolupráci s príslušnými zainteresovanými stranami a organizáciou, ako sú orgány v oblasti metrológie a referenčného porovnávania, mala podľa potreby podporovať vypracovanie referenčných hodnôt a metodík merania pre systémy AI. Komisia by pritom mala vziať na vedomie činnosť medzinárodných partnerov pracujúcich v oblasti metrológie a príslušných ukazovateľov merania súvisiacich s AI a spolupracovať s nimi.

---

35 Smernica Európskeho parlamentu a Rady 2014/31/EÚ z 26. februára 2014 o harmonizácii právnych predpisov členských štátov týkajúcich sa sprístupňovania váh s neautomatickou činnosťou na trhu (Ú. v. EÚ L 96, 29.3.2014, s. 107).

36 Smernica Európskeho parlamentu a Rady 2014/32/EÚ z 26. februára 2014 o harmonizácii právnych predpisov členských štátov týkajúcich sa sprístupnenia meradiel na trhu (Ú. v. EÚ L 96, 29.3.2014, s. 149).

(75) Technická spoľahlivosť je kľúčovou požiadavkou pre vysokorizikové systémy AI. Mali by byť odolné voči škodlivému alebo inak nežiaducemu správaniu, ktoré môže vyplynúť z obmedzení systémov alebo prostredia, v ktorom systémy fungujú (napríklad chyby, poruchy, nezrovnalosti, neočakávané situácie). Preto by sa mali prijať technické a organizačné opatrenia na zabezpečenie spoľahlivosti vysokorizikových systémov AI, napríklad dizajnovaním a vývojom vhodných technických riešení na prevenciu alebo minimalizáciu škodlivého alebo inak nežiaduceho správania. Toto technické riešenie môže zahŕňať napríklad mechanizmy umožňujúce systému bezpečne prerušiť svoju prevádzku (plány pre prípad zlyhania) za určitých anomálií alebo ak sa prevádzka uskutočňuje mimo určitých vopred stanovených hraníc. Neschopnosť chrániť pred týmito rizikami by mohla mať vplyv na bezpečnosť alebo negatívne ovplyvniť základné práva, napríklad v dôsledku chybných rozhodnutí alebo nesprávnych alebo skreslených výstupov vygenerovaných systémom AI.

(76) Kybernetická bezpečnosť zohráva kľúčovú úlohu pri zabezpečovaní odolnosti systémov AI voči pokusom o zmenu ich použitia, správania, výkonnosti alebo o ohrozenie ich bezpečnostných vlastností tretími stranami, ktoré so škodlivým úmyslom zneužívajú zraniteľné miesta systému. Kybernetické útoky na systémy AI môžu využívať aktíva špecifické pre AI, ako sú súbory trénovacích údajov (napríklad otrávenie údajov) alebo trénované modely (napríklad nepriateľské útoky alebo zasahovanie do členstva), alebo zneužívať zraniteľné miesta digitálnych aktív systému AI alebo základnej infraštruktúry informačných a komunikačných technológií. Na zabezpečenie úrovne kybernetickej bezpečnosti primeranej rizikám by preto poskytovatelia vysokorizikových systémov AI mali prijať vhodné opatrenia ako napríklad bezpečnostné kontroly a náležite pritom zohľadniť základnú infraštruktúru informačných a komunikačných technológií.

(77) Bez toho, aby boli dotknuté požiadavky týkajúce sa spoľahlivosti a presnosti stanovené v tomto nariadení, môžu vysokorizikové systémy AI, ktoré patria do rozsahu pôsobnosti nariadenia Európskeho parlamentu a Rady o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami, v súlade s uvedeným nariadením preukázať súlad s kybernetickobezpečnostnými požiadavkami tohto nariadenia splnením základných požiadaviek kybernetickej bezpečnosti stanovených v uvedenom nariadení. Ak vysokorizikové systémy AI spĺňajú základné požiadavky nariadenia Európskeho parlamentu a Rady o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami, mali by sa považovať za systémy spĺňajúce požiadavky kybernetickej bezpečnosti stanovené v tomto nariadení, pokiaľ sa splnenie týchto požiadaviek preukáže v EÚ vyhlásení o zhode alebo jeho častiach vydanom podľa uvedeného nariadenia. Na tento účel by sa v posúdení kybernetickobezpečnostných rizík spojených s produktom s digitálnymi prvkami klasifikovanými ako vysokorizikový systém AI podľa tohto nariadenia, ktoré sa vykonáva podľa nariadenia Európskeho parlamentu a Rady o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami, mali zohľadniť riziká pre kybernetickú odolnosť systému AI, pokiaľ ide o pokusy neoprávnených tretích strán zmeniť jeho používanie, správanie alebo výkon vrátane zraniteľností špecifických pre AI, ako sú otrávenie údajov alebo nepriateľské útoky, ako aj prípadné riziká pre základné práva, ako sa vyžaduje v tomto nariadení.

(78) Postup posudzovania zhody stanovený v tomto nariadení by sa mal uplatňovať v súvislosti so základnými požiadavkami kybernetickej bezpečnosti produktu s digitálnymi prvkami, na ktorý sa vzťahuje nariadenie Európskeho parlamentu a Rady o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a ktorý je podľa tohto nariadenia klasifikovaný ako vysokorizikový systém AI. Toto pravidlo by však nemalo viesť k zníženiu potrebnej úrovne záruky pre kritické produkty s digitálnymi prvkami, na ktoré sa vzťahuje nariadenie Európskeho parlamentu a Rady o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami. Odchylne od tohto pravidla by preto vysokorizikové systémy AI, ktoré patria do rozsahu pôsobnosti nariadenia a zároveň sú kvalifikované ako významné a kritické produkty s digitálnymi prvkami podľa nariadenia Európskeho parlamentu a Rady o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a na ktoré sa uplatňuje postup posudzovania zhody na základe vnútornej kontroly stanovený v prílohe k tomuto nariadeniu, mali podliehať ustanoveniam nariadenia Európskeho parlamentu a Rady o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami týkajúcim sa posudzovania zhody, pokiaľ ide o základné požiadavky uvedeného nariadenia na kybernetickú bezpečnosť. V tomto prípade by sa na všetky ostatné aspekty, na ktoré sa vzťahuje toto nariadenie, mali uplatňovať príslušné ustanovenia o posudzovaní zhody na základe vnútornej kontroly stanovené v prílohe k tomuto nariadeniu. Na základe poznatkov a odborných znalostí agentúry ENISA v oblasti politiky kybernetickej bezpečnosti a úloh pridelených agentúre ENISA podľa nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881[37] by Komisia mala spolupracovať s agentúrou ENISA v otázkach týkajúcich sa kybernetickej bezpečnosti systémov AI.

---

[37] Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (Ú. v. EÚ L 151, 7.6.2019, s. 15).

(79) Je vhodné, aby konkrétna fyzická alebo právnická osoba vymedzená ako poskytovateľ prevzala zodpovednosť za uvedenie vysokorizikového systému AI na trh alebo do prevádzky bez ohľadu na to, či je táto fyzická alebo právnická osoba osobou, ktorá systém dizajnovala alebo vyvinula.

(80) Únia a členské štáty sú ako signatári Dohovoru OSN o právach osôb so zdravotným postihnutím právne zaviazané chrániť osoby so zdravotným postihnutím pred diskrimináciou a podporovať ich rovnosť, zabezpečiť, aby osoby so zdravotným postihnutím mali rovnaký prístup k informačným a komunikačným technológiám a systémom ako ostatní, a zabezpečiť rešpektovanie súkromia osôb so zdravotným postihnutím. Vzhľadom na rastúci význam a využívanie systémov AI by sa uplatňovaním zásad univerzálneho dizajnu na všetky nové technológie a služby mal zabezpečiť úplný a rovnaký prístup pre každého, koho sa technológie AI potenciálne týkajú alebo kto ich používa, vrátane osôb so zdravotným postihnutím, a to spôsobom, ktorý plne zohľadňuje ich prirodzenú dôstojnosť a rozmanitosť. Preto je nevyhnutné, aby poskytovatelia zabezpečili úplný súlad s požiadavkami na prístupnosť vrátane smernice Európskeho parlamentu a Rady (EÚ) 2016/2102[38] a smernice (EÚ) 2019/882. Poskytovatelia by mali zabezpečiť súlad s týmito požiadavkami už v štádiu návrhu. Potrebné opatrenia by sa preto mali čo najviac začleniť do dizajnu vysokorizikového systému AI.

---

[38] Smernica Európskeho parlamentu a Rady (EÚ) 2016/2102 z 26. októbra 2016 o prístupnosti webových sídel a mobilných aplikácií subjektov verejného sektora (Ú. v. EÚ L 327, 2.12.2016, s. 1).

(81) Poskytovateľ by mal zaviesť spoľahlivý systém riadenia kvality, zabezpečiť dokončenie požadovaného postupu posudzovania zhody, vypracovať príslušnú dokumentáciu a vytvoriť spoľahlivý systém monitorovania po uvedení na trh. Poskytovatelia vysokorizikových systémov AI, na ktorých sa vzťahujú povinnosti týkajúce sa systémov riadenia kvality podľa príslušných odvetvových právnych predpisov Únie, by mali mať možnosť zahrnúť prvky systému riadenia kvality stanoveného v tomto nariadení ako súčasť existujúceho systému riadenia kvality stanoveného v uvedených iných odvetvových právnych predpisov Únie. Pri budúcich normalizačných činnostiach alebo usmerneniach prijatých Komisiou by sa mala zohľadniť aj komplementárnosť medzi týmto nariadením a existujúcim odvetvovým právom Únie. Orgány verejnej moci, ktoré uvádzajú do prevádzky vysokorizikové systémy AI pre vlastnú potrebu, môžu prijať a vykonávať pravidlá systému riadenia kvality ako súčasť systému riadenia kvality prijatého na vnútroštátnej prípadne regionálnej úrovni, pričom zohľadnia osobitosti odvetvia a právomoci a organizáciu dotknutého orgánu verejnej moci.

(82) S cieľom umožniť presadzovanie tohto nariadenia a vytvoriť rovnaké podmienky pre prevádzkovateľov je pri zohľadnení rôznych foriem sprístupňovania digitálnych produktov dôležité zabezpečiť, aby osoba usadená v Únii mohla za každých okolností poskytnúť orgánom všetky potrebné informácie o súlade systému AI. Preto poskytovatelia usadení v tretích krajinách by mali vymenovať písomným mandátom pred sprístupnením svojich systémov AI v Únii splnomocneného zástupcu usadeného v Únii. V prípade poskytovateľov, ktorí nie sú usadení v Únii, zohráva tento splnomocnený zástupca kľúčovú úlohu pri zabezpečovaní súladu vysokorizikových systémov AI uvedených na trh alebo do prevádzky v Únii týmito poskytovateľmi a slúži ako ich kontaktná osoba usadená v Únii.

(83) Vzhľadom na povahu a zložitosť hodnotového reťazca systémov AI a v súlade s novým legislatívnym rámcom je nevyhnutné zabezpečiť právnu istotu a uľahčiť súlad s týmto nariadením. Preto je potrebné objasniť úlohu a osobitné povinnosti príslušných prevádzkovateľov v uvedenom hodnotovom reťazci, ako sú dovozcovia a distribútori, ktorí môžu prispievať k vývoju systémov AI. V určitých situáciách by takíto prevádzkovatelia mohli konať vo viac ako jednej role súčasne, a preto by mali kumulatívne plniť všetky príslušné povinnosti spojené s týmito rolami. Prevádzkovateľ by napríklad mohol konať súčasne ako distribútor a dovozca.

(84) V záujme zabezpečenia právnej istoty je potrebné objasniť, že za určitých osobitných podmienok by sa každý distribútor, dovozca, nasadzujúci subjekt alebo iná tretia strana mali považovať za poskytovateľa vysokorizikového systému AI, a preto by mali prevziať všetky príslušné povinnosti. Bolo by to tak v prípade, ak by táto strana uviedla svoje meno alebo ochrannú známku na vysokorizikovom systéme AI, ktorý už bol uvedený na trh alebo do prevádzky, bez toho, aby boli dotknuté zmluvné dojednania, v ktorých sa stanovuje, že povinnosti sú pridelené inak. Bolo by to tak aj v prípade, ak táto strana vykoná podstatnú zmenu vysokorizikového systému AI, ktorý už bol uvedený na trh alebo už do prevádzky, a to tak, že zostane vysokorizikovým systémom AI v súlade s týmto nariadením, alebo ak zmení zamýšľaný účel systému AI vrátane systému AI na všeobecné účely, ktorý nebol klasifikovaný ako vysokorizikový a už bol uvedený na trh alebo do prevádzky, a to tak, že systém AI sa stane vysokorizikovým systémom AI v súlade s týmto nariadením. Uvedené ustanovenia by sa mali uplatňovať bez toho, aby boli dotknuté konkrétnejšie ustanovenia zavedené v určitých harmonizačných právnych predpisoch Únie založených na novom legislatívnom rámci, spolu s ktorými by sa malo uplatňovať toto nariadenie. Napríklad článok 16 ods. 2 nariadenia (EÚ) 2017/745, v ktorom sa stanovuje, že určité zmeny by sa nemali považovať za úpravy pomôcky, ktoré by mohli ovplyvniť jej súlad s uplatniteľnými požiadavkami, by sa mal naďalej uplatňovať na vysokorizikové systémy AI, ktoré sú zdravotníckymi pomôckami v zmysle uvedeného nariadenia.

(85) Systémy AI na všeobecné účely sa môžu používať ako vysokorizikové systémy AI samy osebe alebo môžu byť komponentmi iných vysokorizikových systémov AI. Vzhľadom na osobitnú povahu systémov AI na všeobecné účely a s cieľom zabezpečiť spravodlivé rozdelenie zodpovednosti v rámci hodnotového reťazca AI by poskytovatelia takýchto systémov mali bez ohľadu na to, či ich iní poskytovatelia používajú ako vysokorizikové systémy AI ako také alebo ako komponenty vysokorizikových systémov AI, a ak sa nestanovuje inak v tomto nariadení, mali úzko spolupracovať s poskytovateľmi príslušných vysokorizikových systémov AI s cieľom umožniť ich súlad s príslušnými povinnosťami podľa tohto nariadenia a spolupracovať aj s príslušnými orgánmi zriadenými podľa tohto nariadenia.

(86) Ak by sa za podmienok stanovených v tomto nariadení poskytovateľ, ktorý pôvodne uviedol systém AI na trh alebo do prevádzky, už nemal považovať za poskytovateľa na účely tohto nariadenia a ak tento poskytovateľ výslovne nevylúčil zmenu systému AI na vysokorizikový systém AI, tento bývalý poskytovateľ by mal napriek tomu úzko spolupracovať a sprístupniť potrebné informácie a poskytnúť odôvodnene očakávaný technický prístup a inú pomoc, ktoré sú potrebné na splnenie povinností stanovených v tomto nariadení, najmä pokiaľ ide o súlad s posudzovaním zhody vysokorizikových systémov AI.

(87) Ak sa navyše vysokorizikový systém AI, ktorý je bezpečnostným komponentom výrobku, ktorý patrí do rozsahu pôsobnosti harmonizačných právnych predpisov Únie založených na novom legislatívnom rámci, neuvádza na trh ani do prevádzky nezávisle od daného výrobku, výrobca výrobku vymedzený v uvedených právnych predpisoch by mal dodržiavať povinnosti poskytovateľa stanovené v tomto nariadení a mal by najmä zabezpečiť, aby systém AI zabudovaný do konečného výrobku spĺňal požiadavky tohto nariadenia.

(88) V rámci hodnotového reťazca AI viaceré strany často dodávajú systémy, nástroje a služby AI, ale aj komponenty alebo procesy, ktoré poskytovateľ začlení do systému AI s rôznymi cieľmi vrátane trénovania modelov, pretrénovania modelov, testovania a hodnotenia modelov, integrácie do softvéru alebo iných aspektov vývoja modelu. Uvedené strany zohrávajú dôležitú úlohu v hodnotovom reťazci vo vzťahu k poskytovateľovi vysokorizikového systému AI, do ktorého sú ich systémy, nástroje, služby, komponenty alebo procesy AI integrované, a mali by tomuto poskytovateľovi poskytnúť na základe písomnej dohody potrebné informácie, spôsobilosti, technický prístup a inú pomoc na základe všeobecne uznávaného aktuálneho stavu vývoja, aby si tento poskytovateľ mohol v plnej miere plniť povinnosti stanovené v tomto nariadení, a to bez toho, aby boli ohrozené ich vlastné práva duševného vlastníctva alebo obchodné tajomstvá.

(89) Tretie strany, ktoré sprístupňujú verejnosti nástroje, služby, procesy, alebo komponenty AI iné ako modely AI na všeobecné účely, by nemali byť povinné dodržiavať požiadavky zamerané na povinnosti v celom hodnotovom reťazci AI, najmä voči poskytovateľovi, ktorý ich použil alebo integroval, ak sa tieto nástroje, služby, procesy alebo komponenty AI sprístupňujú na základe bezplatnej licencie s otvoreným zdrojovým kódom. Vývojári nástrojov, služieb, procesov, alebo komponentov AI iných ako modely AI na všeobecné účely, dostupných zdarma a s otvoreným zdrojovým kódom, by sa mali nabádať, aby implementovali všeobecne prijaté postupy pre dokumentáciu, ako sú vzorové karty a údajové hárky, ako spôsob urýchlenia výmeny informácií v rámci hodnotového reťazca AI, čím sa umožní podpora dôveryhodných systémov AI v Únii.

(90) Komisia by mohla vypracovať a odporučiť nezáväzné vzorové zmluvné podmienky medzi poskytovateľmi vysokorizikových systémov AI a tretími stranami, ktoré dodávajú nástroje, služby, komponenty alebo procesy, ktoré sa používajú vo vysokorizikových systémoch AI alebo integrujú do takýchto systémov, s cieľom uľahčiť spoluprácu v celom hodnotovom reťazci. Pri vypracúvaní nezáväzných vzorových zmluvných podmienok by Komisia mala zohľadniť možné zmluvné požiadavky uplatniteľné v konkrétnych odvetviach alebo obchodných prípadoch.

(91) Vzhľadom na povahu systémov AI a riziká pre bezpečnosť a základné práva, ktoré môžu súvisieť s ich používaním, a to aj pokiaľ ide o potrebu zabezpečiť riadne monitorovanie výkonu systému AI v reálnom prostredí, je vhodné stanoviť osobitné povinnosti nasadzujúce subjekty. Nasadzujúce subjekty by hlavne mali prijať technické a organizačné opatrenia s cieľom zabezpečiť, že používajú vysokorizikové systémy AI v súlade s návodom na použitie a mali by sa stanoviť určité ďalšie povinnosti, pokiaľ ide o monitorovanie fungovania systémov AI a prípadne aj vedenie záznamov. Nasadzujúce subjekty by okrem toho mali zabezpečiť, aby osoby poverené implementáciou návodu na použitie a vykonávaním ľudského dohľadu, ako sa stanovuje v tomto nariadení, mali potrebnú spôsobilosť, najmä primeranú úroveň gramotnosti v oblasti AI, odbornú prípravu a právomoc riadne plniť tieto úlohy. Týmito povinnosťami by nemali byť dotknuté iné povinnosti nasadzujúcich subjektov v súvislosti s vysokorizikovými systémami AI podľa práva Únie alebo vnútroštátneho práva.

(92) Týmto nariadením nie sú dotknuté povinnosti zamestnávateľov informovať pracovníkov alebo ich zástupcov a konzultovať s nimi podľa práva a praxe Únie alebo vnútroštátneho práva a praxe vrátane smernice Európskeho parlamentu a Rady 2002/14/ES[39], pokiaľ ide o rozhodnutia o uvedení do prevádzky alebo používaní systémov AI. Naďalej je potrebné zabezpečiť informovanie pracovníkov a ich zástupcov o plánovanom nasadení vysokorizikových systémov AI na pracovisku, keď nie sú splnené podmienky pre uvedené informovanie alebo informačné a konzultačné povinnosti stanovené v iných právnych nástrojoch. Takéto právo na informácie je navyše doplnkové a nevyhnutné z hľadiska cieľa ochrany základných práv, ktorý je základom tohto nariadenia. Preto by sa v tomto nariadení mala stanoviť požiadavka na informácie na tento účel bez toho, aby boli dotknuté akékoľvek existujúce práva pracovníkov.

[39] Smernica Európskeho parlamentu a Rady 2002/14/ES z 11. marca 2002, ktorá ustanovuje všeobecný rámec pre informovanie a porady so zamestnancami v Európskom spoločenstve (Ú. v. ES L 80, 23.3.2002, s. 29).

(93) Aj keď riziká súvisiace so systémami AI môžu vyplývať zo spôsobu, akým sú tieto systémy dizajnované, riziká môžu vyplývať aj z toho, ako sa tieto systémy AI používajú. Subjekty nasadzujúce vysokorizikový systém AI preto zohrávajú rozhodujúcu úlohu pri zabezpečovaní ochrany základných práv a dopĺňajú povinnosti poskytovateľa pri vývoji systému AI. Nasadzujúce subjekty majú najlepšie predpoklady na to, aby pochopili, ako sa bude vysokorizikový systém AI konkrétne používať, preto môžu identifikovať potenciálne významné riziká, ktoré sa vo fáze vývoja nepredpokladali, a to vďaka presnejším znalostiam kontextu používania, osôb alebo skupín osôb, ktorých sa to môže týkať, vrátane zraniteľných skupín. Subjekty nasadzujúce vysokorizikové systémy AI uvedené v prílohe k tomuto nariadeniu zároveň zohrávajú kritickú úlohu pri informovaní fyzických osôb a pri prijímaní rozhodnutí alebo prípadne pri pomoci s prijímaním rozhodnutí týkajúcich sa fyzických osôb by mali informovať fyzické osoby o tom, že sa na ne vzťahuje použitie vysokorizikového systému AI. Tieto informácie zahŕňajú zamýšľaný účel a typ rozhodnutí, ktoré prijímajú. Nasadzujúci subjekt by mal takisto informovať fyzické osoby o ich práve na vysvetlenie stanovenom v tomto nariadení. Pokiaľ ide o vysokorizikové systémy AI používané na účely presadzovania práva, uvedená povinnosť by sa mala implementovať v súlade s článkom 13 smernice (EÚ) 2016/680.

(94) Každé spracúvanie biometrických údajov pri používaní systémov AI na biometrickú identifikáciu na účely presadzovania práva musí byť v súlade s článkom 10 smernice (EÚ) 2016/680, ktorý umožňuje takéto spracúvanie len vtedy, keď je to nevyhnutne potrebné, s výhradou primeraných záruk ochrany práv a slobôd dotknutej osoby a ak je to povolené právom Únie alebo členského štátu. Pri takomto používaní, ak je povolené, sa musia dodržiavať aj zásady stanovené v článku 4 ods. 1 smernice (EÚ) 2016/680 vrátane zákonnosti, spravodlivosti a transparentnosti, obmedzenia účelu, presnosti a obmedzenia uchovávania.

(95) Bez toho, aby bolo dotknuté uplatniteľné právo Únie, najmä nariadenie (EÚ) 2016/679 a smernica (EÚ) 2016/680, vzhľadom na rušivý charakter systémov následnej diaľkovej biometrickej identifikácie, by používanie systémov následnej diaľkovej biometrickej identifikácie malo podliehať zárukám. Systémy následnej diaľkovej biometrickej identifikácie by sa mali vždy používať spôsobom, ktorý je primeraný, legitímny a nevyhnutne potrebný, a teda cielený, pokiaľ ide o osoby, ktoré sa majú identifikovať, miesto a časový rozsah a mali by vychádzať z uzavretého súboru údajov zo zákonne získaných videozáznamov. V každom prípade by sa systémy následnej diaľkovej biometrickej identifikácie nemali používať v rámci presadzovania práva s cieľom viesť k nerozlišujúcemu sledovaniu. Podmienky pre následnú diaľkovú biometrickú identifikáciu by v žiadnom prípade nemali poskytovať základ na obchádzanie podmienok zákazu a prísnych výnimiek pre diaľkovú biometrickú identifikáciu v reálnom čase.

(96) S cieľom účinne zabezpečiť ochranu základných práv by subjekty nasadzujúce vysokorizikové systémy AI, ktoré sú subjektmi, ktoré sa spravujú verejným právom, alebo súkromnými subjektmi poskytujúcimi verejné služby a subjekty nasadzujúce určité vysokorizikové systémy AI uvedené v zozname v prílohe k tomuto nariadeniu, ako sú bankové alebo poisťovacie subjekty, mali pred ich uvedením do používania vykonať posúdenie vplyvu na základné práva. Služby dôležité pre jednotlivcov, ktoré sú verejného charakteru, môžu poskytovať aj súkromné subjekty. Súkromné subjekty poskytujúce takéto verejné služby sú spojené s úlohami vo verejnom záujme, ako napríklad v oblastiach vzdelávania, zdravotnej starostlivosti, sociálnych služieb, bývania, výkonu spravodlivosti. Cieľom posúdenia vplyvu na základné práva je, aby nasadzujúci subjekt identifikoval konkrétne riziká pre práva jednotlivcov alebo skupín jednotlivcov, ktorí by mohli byť dotknutí, a určiť opatrenia, ktoré sa majú prijať v prípade naplnenia uvedených rizík. Posúdenie vplyvu by sa malo vykonať pred nasadením vysokorizikového systému AI a malo by sa aktualizovať, keď nasadzujúci subjekt usúdi, že sa niektorý z relevantných faktorov zmenil. V posúdení vplyvu by sa mali určiť príslušné procesy nasadzujúceho subjektu, v ktorých sa bude vysokorizikový systém AI používať v súlade s jeho zamýšľaným účelom, a malo by obsahovať opis obdobia a frekvencie, v ktorých sa má systém používať, ako aj konkrétnych kategórií fyzických osôb a skupín, ktoré by mohli byť ovplyvnené v konkrétnom kontexte používania.

Posúdenie by malo zahŕňať aj identifikáciu osobitných rizík ujmy, ktoré by mohli mať vplyv na základné práva uvedených osôb alebo skupín. Pri vykonávaní tohto posúdenia by nasadzujúci subjekt mal zohľadniť informácie relevantné pre riadne posúdenie vplyvu, okrem iného vrátane informácií, ktoré poskytovateľ vysokorizikového systému AI poskytol v návode na použitie. Vzhľadom na zistené riziká by nasadzujúce subjekty mali určiť opatrenia, ktoré sa majú prijať v prípade naplnenia uvedených rizík, vrátane napríklad mechanizmov správy a riadenia v tomto konkrétnom kontexte používania, ako sú mechanizmy ľudského dohľadu podľa návodu na použitie alebo postupy vybavovania sťažností a nápravy, keďže by mohli byť nápomocné pri zmierňovaní rizík pre základné práva v konkrétnych prípadoch použitia. Po vykonaní uvedeného posúdenia vplyvu by nasadzujúci subjekt mal informovať príslušný orgán dohľadu nad trhom.

Na zhromažďovanie relevantných informácií potrebných na vykonanie posúdenia vplyvu by subjekty nasadzujúce vysokorizikový systém AI, najmä ak sa systémy AI používajú vo verejnom sektore, mohli do vykonávania takýchto posúdení vplyvu a koncipovania opatrení, ktoré sa majú prijať v prípade naplnenia rizík, zapojiť príslušné zainteresované strany vrátane zástupcov skupín osôb, ktoré by mohli byť ovplyvnené systémom AI, nezávislých expertov a organizácie občianskej spoločnosti. Európsky úrad pre umelú inteligenciu (ďalej len „úrad pre AI“) by mal vypracovať vzor dotazníka s cieľom uľahčiť dodržiavanie predpisov a znížiť administratívne zaťaženie nasadzujúcich subjektov.

(97) Pojem modely AI na všeobecné účely by sa mal jasne vymedziť a oddeliť od pojmu systémy AI, aby sa umožnila právna istota. Toto vymedzenie by malo byť založené na kľúčových funkčných charakteristikách modelu AI na všeobecné účely, najmä na všeobecnej povahe a spôsobilosti kompetentne vykonávať širokú škálu rôznych úloh. Tieto modely sa zvyčajne trénujú na veľkých množstvách údajov prostredníctvom rôznych metód, ako je učenie sa pod vlastným dohľadom, učenie sa bez dohľadu alebo posilňovacie učenie. Modely AI na všeobecné účely sa môžu uvádzať na trh rôznymi spôsobmi, a to aj prostredníctvom knižníc, aplikačných programovacích rozhraní, priamym sťahovaním alebo fyzickým kopírovaním. Tieto modely sa môžu ďalej upravovať alebo dolaďovať na nové modely. Hoci sú modely AI základnými komponentmi systémov AI, samy osebe nepredstavujú systémy AI. Modely AI si vyžadujú pridanie ďalších komponentov, ako je napríklad používateľské rozhranie, aby sa z nich stali systémy AI. Modely AI sú zvyčajne integrované do systémov AI a tvoria ich súčasť. V tomto nariadení sa stanovujú osobitné pravidlá pre modely AI na všeobecné účely a modely AI na všeobecné účely, ktoré predstavujú systémové riziká, ktoré by sa mali uplatňovať aj vtedy, keď sú tieto modely integrované do systému AI alebo tvoria jeho súčasť. Malo by byť zrejmé, že povinnosti poskytovateľov modelov AI na všeobecné účely by sa mali uplatňovať po uvedení modelov AI na všeobecné účely na trh.

Ak poskytovateľ modelu AI na všeobecné účely integruje vlastný model do svojho vlastného systému AI, ktorý je sprístupnený na trhu alebo do prevádzky, tento model by sa mal považovať za uvedený na trh, a preto by sa povinnosti stanovené v tomto nariadení pre modely mali naďalej uplatňovať popri povinnostiach týkajúcich sa systémov AI. Povinnosti stanovené pre modely by sa v žiadnom prípade nemali uplatňovať, ak sa vlastný model používa na čisto vnútorné procesy, ktoré nie sú nevyhnutné na poskytovanie výrobku alebo služby tretím stranám, a práva fyzických osôb nie sú dotknuté. Vzhľadom na ich potenciálne výrazne negatívne účinky by sa na modely AI na všeobecné účely so systémovým rizikom mali vždy vzťahovať príslušné povinnosti podľa tohto nariadenia. Vymedzenie pojmu by sa nemalo vzťahovať na modely AI používané pred ich uvedením na trh výlučne na účely činností v oblasti výskumu, vývoja a vytvárania prototypov. Týmto nie je dotknutá povinnosť dodržiavať toto nariadenie, keď sa po uskutočnení týchto činností uvádza model na trh.

(98) Zatiaľ čo všeobecná povaha modelu by sa mohla okrem iného určiť aj na základe viacerých parametrov, modely s aspoň miliardou parametrov a trénované s veľkým množstvom údajov s využitím vlastného dohľadu vo veľkom rozsahu by sa mali považovať za modely, ktoré vykazujú významnú všeobecnú povahu a kompetentne vykonávajú širokú škálu osobitných úloh.

(99) Veľké generatívne modely AI sú typickým príkladom modelu AI na všeobecné účely vzhľadom na to, že umožňujú flexibilnú tvorbu obsahu napríklad vo forme textu, zvuku, obrázkov alebo videa, pričom dokážu ľahko zvládnuť širokú škálu osobitných úloh.

(100) Ak je model AI na všeobecné účely integrovaný do systému AI alebo je jeho súčasťou, tento systém by sa mal považovať za systém AI na všeobecné účely, ak je tento systém v dôsledku tejto integrácie spôsobilý slúžiť na rôzne účely. Systém AI na všeobecné účely sa môže používať priamo alebo môže byť integrovaný do iných systémov AI.

(101) Poskytovatelia modelov AI na všeobecné účely majú osobitnú úlohu a zodpovednosť v hodnotovom reťazci AI, keďže modely, ktoré poskytujú, môžu tvoriť základ pre celý rad nadväzujúcich systémov, ktoré často poskytujú nadväzujúci poskytovatelia, čo si vyžaduje dobré pochopenie modelov a ich spôsobilostí, a to s cieľom umožniť integráciu takýchto modelov do ich výrobkov, ako aj plniť svoje povinnosti podľa tohto alebo iných nariadení. Preto by sa mali stanoviť primerané opatrenia v oblasti transparentnosti vrátane vypracovania a aktualizácie dokumentácie a poskytovania informácií o modeli AI na všeobecné účely na jeho používanie nadväzujúcimi poskytovateľmi. Poskytovateľ modelu AI na všeobecné účely by mal vypracovať a aktualizovať technickú dokumentáciu na účely jej sprístupnenia na požiadanie úradu pre AI a vnútroštátnym príslušným orgánom. V osobitných prílohách k tomuto nariadeniu by sa mal stanoviť minimálny súbor prvkov, ktoré sa majú zahrnúť do takejto dokumentácie. Vzhľadom na nepretržitý technologický vývoj by Komisia mala byť oprávnená meniť uvedené prílohy prostredníctvom delegovaných aktov.

(102) Softvér a údaje vrátane modelov, ktoré sa vydávajú na základe bezplatnej licencie s otvoreným zdrojovým kódom, ktorá umožňuje ich otvorené zdieľanie a v rámci ktorej majú používatelia voľný prístup k nim alebo ich upraveným verziám, môžu ich voľne používať, upravovať a redistribuovať, majú potenciál prispieť k výskumu a inovácii na trhu a poskytnúť hospodárstvu Únie významné príležitosti na rast. Modely AI na všeobecné účely, ktoré sa vydávajú na základe bezplatných licencií s otvoreným zdrojovým kódom, by sa mali považovať za zabezpečujúce vysokú úroveň transparentnosti a otvorenosti, ak sú ich parametre vrátane váh, informácií o architektúre modelu a informácií o používaní modelu verejne dostupné. Licencia by sa mala považovať za bezplatnú a s otvoreným zdrojovým kódom aj vtedy, keď umožňuje používateľom prevádzkovať, kopírovať, distribuovať, študovať, meniť a zlepšovať softvér a údaje vrátane modelov pod podmienkou, že sa pôvodnému poskytovateľovi modelu pripíše kredit a že sa dodržia rovnaké alebo porovnateľné podmienky distribúcie.

(103) Bezplatné komponenty AI s otvoreným zdrojovým kódom zahŕňajú softvér a údaje vrátane modelov a modelov AI na všeobecné účely, nástrojov, služieb alebo procesov systému AI. Bezplatné komponenty AI s otvoreným zdrojovým kódom možno poskytovať prostredníctvom rôznych kanálov vrátane ich vývoja v otvorených archívoch. Na účely tohto nariadenia by sa na komponenty AI, ktoré sa poskytujú za odplatu alebo inak speňažujú, a to aj prostredníctvom poskytovania technickej podpory alebo iných služieb, vrátane softvérovej platformy, ktoré súvisia s komponentom AI, alebo použitia osobných údajov z iných dôvodov než výlučne na zlepšenie bezpečnosti, kompatibility alebo interoperability softvéru, s výnimkou transakcií medzi mikropodnikmi, nemali vzťahovať výnimky poskytované bezplatným komponentom AI s otvoreným zdrojovým kódom. Sprístupnenie komponentov AI prostredníctvom otvorených archívov by samo osebe nemalo predstavovať speňaženie.

(104) Poskytovatelia modelov AI na všeobecné účely, ktoré sa vydávajú na základe bezplatnej licencie s otvoreným zdrojovým kódom a ktorých parametre vrátane váh, informácií o architektúre modelu a informácií o používaní modelu sú verejne dostupné, by mali podliehať výnimkám, pokiaľ ide o požiadavky na transparentnosť týkajúce sa modelov AI na všeobecné účely, pokiaľ ich nemožno považovať za modely predstavujúce systémové riziko, pričom v takom prípade by sa okolnosť, že model je transparentný a sprevádzaný licenciou s otvoreným zdrojovým kódom, nemala považovať za dostatočný dôvod na vylúčenie dodržiavania povinností podľa tohto nariadenia. V každom prípade vzhľadom na to, že pri vydávaní modelov AI na všeobecné účely na základe bezplatnej licencie s otvoreným zdrojovým kódom sa nemusia nevyhnutne odhaliť podstatné informácie o súbore údajov použitom na trénovanie alebo doladenie modelu a o tom, ako sa tým zabezpečilo dodržiavanie autorského práva, výnimka stanovená pre modely AI na všeobecné účely z dodržiavania požiadaviek týkajúcich sa transparentnosti by sa nemala týkať povinnosti predložiť zhrnutie obsahu použitého na trénovanie modelu a povinnosti zaviesť politiku dodržiavania autorského práva Únie, najmä s cieľom identifikovať a rešpektovať výhrady práv vyjadrené podľa článku 4 ods. 3 smernice Európskeho parlamentu a Rady (EÚ) 2019/790[40].

[40] Smernica Európskeho parlamentu a Rady (EÚ) 2019/790 zo 17. apríla 2019 o autorskom práve a právach súvisiacich s autorským právom na digitálnom jednotnom trhu a o zmene smerníc 96/9/ES a 2001/29/ES (Ú. v. EÚ L 130, 17.5.2019, s. 92).

(105) Modely AI na všeobecné účely, najmä veľké generatívne modely AI schopné generovať text, obrázky a iný obsah, predstavujú jedinečné inovačné príležitosti, ale aj výzvy pre umelcov, autorov a iných tvorcov a pre spôsob, akým sa ich tvorivý obsah vytvára, distribuuje, používa a spotrebúva. Vývoj a trénovanie takýchto modelov si vyžaduje prístup k obrovskému množstvu textov, obrázkov, videí a iných údajov. Techniky hĺbkovej analýzy textov a údajov sa môžu v tejto súvislosti vo veľkej miere používať na vyhľadávanie a analýzu takéhoto obsahu, ktorý môže byť chránený autorským právom a s ním súvisiacimi právami. Akékoľvek použitie obsahu chráneného autorským právom si vyžaduje povolenie príslušného nositeľa práv, pokiaľ sa neuplatňujú príslušné výnimky a obmedzenia autorského práva. Smernicou (EÚ) 2019/790 sa zaviedli výnimky a obmedzenia, ktoré za určitých podmienok umožňujú rozmnožovanie a extrakciu diel alebo iných predmetov ochrany na účely hĺbkovej analýzy textov a údajov. Podľa týchto pravidiel sa nositelia práv môžu rozhodnúť vyhradiť svoje práva na svoje diela alebo iné predmety ochrany s cieľom zabrániť hĺbkovej analýze textov a údajov, pokiaľ sa to neuskutočňuje na účely vedeckého výskumu. Ak boli práva na neposkytnutie prístupu výslovne vyhradené vhodným spôsobom, poskytovatelia modelov AI na všeobecné účely musia získať povolenie nositeľov práv, ak chcú vykonať hĺbkovú analýzu textov a údajov v súvislosti s takýmito dielami.

(106) Poskytovatelia, ktorí uvádzajú modely AI na všeobecné účely na trh Únie, by mali zabezpečiť súlad s príslušnými povinnosťami stanovenými v tomto nariadení. Na tento účel by poskytovatelia modelov AI na všeobecné účely mali zaviesť politiku dodržiavania práva Únie v oblasti autorského práva a s ním súvisiacich práv, najmä s cieľom identifikovať a dodržiavať výhradu práv vyjadrenú nositeľmi práv podľa článku 4 ods. 3 smernice (EÚ) 2019/790. Každý poskytovateľ, ktorý uvádza model AI na všeobecné účely na trh Únie, by mal splniť túto povinnosť bez ohľadu na jurisdikciu, v ktorej sa uskutočňujú akty týkajúce sa autorských práv, ktoré sú základom trénovania uvedených modelov AI na všeobecné účely. Je to potrebné na zabezpečenie rovnakých podmienok medzi poskytovateľmi modelov AI na všeobecné účely, v rámci ktorých by žiadny poskytovateľ nemal mať možnosť získať konkurenčnú výhodu na trhu Únie uplatňovaním nižších noriem v oblasti autorských práv, ako sú normy stanovené v Únii.

(107) S cieľom zvýšiť transparentnosť údajov, ktoré sa používajú pri predbežnom trénovaní a trénovaní modelov AI na všeobecné účely vrátane textu a údajov chránených autorským právom, je vhodné, aby poskytovatelia takýchto modelov vypracovali a zverejnili dostatočne podrobné zhrnutie obsahu použitého na trénovanie modelu AI na všeobecné účely. Pri náležitom zohľadnení potreby chrániť obchodné tajomstvo a dôverné obchodné informácie by toto zhrnutie malo byť vo všeobecnosti komplexné, pokiaľ ide o jeho rozsah pôsobnosti, a nie technicky podrobné, aby sa stranám s oprávnenými záujmami vrátane nositeľov autorských práv uľahčilo uplatňovanie a presadzovanie ich práv podľa práva Únie, napríklad uvedením hlavných zbierok alebo súborov údajov, ktoré boli súčasťou trénovania modelu, ako sú veľké súkromné alebo verejné databázy alebo archívy údajov, a poskytnutím opisného vysvetlenia k iným použitým zdrojom údajov. Je vhodné, aby úrad pre AI poskytol vzor zhrnutia, ktorý by mal byť jednoduchý, efektívny a mal by poskytovateľovi umožniť poskytnúť požadované zhrnutie v opisnej forme.

(108) Pokiaľ ide o povinnosti uložené poskytovateľom modelov AI na všeobecné účely zaviesť politiku dodržiavania autorského práva Únie a zverejniť zhrnutie obsahu použitého na trénovanie, úrad pre AI by mal monitorovať, či poskytovateľ splnil tieto povinnosti bez toho, aby overil trénovacie údaje alebo pristúpil k ich posúdeniu podľa jednotlivých diel, pokiaľ ide o dodržiavanie autorských práv. Toto nariadenie nemá vplyv na presadzovanie pravidiel v oblasti autorského práva, ako sa stanovuje v práve Únie.

(109) Dodržiavanie povinností, ktoré sa vzťahujú na poskytovateľov modelov AI na všeobecné účely by malo byť primerané a proporcionálne vzhľadom na typ poskytovateľa modelu, s výnimkou potreby dodržiavania predpisov v prípade osôb, ktoré vyvíjajú alebo používajú modely na neprofesionálne alebo vedecké výskumné účely, ktoré by sa však mali nabádať, aby tieto požiadavky dodržiavali dobrovoľne. Bez toho, aby bolo dotknuté autorské právo Únie, by sa pri dodržiavaní uvedených povinností mala náležite zohľadniť veľkosť poskytovateľa a mali by sa umožniť zjednodušené spôsoby dodržiavania predpisov pre MSP vrátane startupov, ktoré by nemali predstavovať nadmerné náklady a odrádzať od používania takýchto modelov. V prípade úpravy alebo doladenia modelu by sa povinnosti poskytovateľov modelov AI na všeobecné účely mali obmedziť na túto úpravu alebo doladenie, napríklad doplnením už existujúcej technickej dokumentácie informáciami o úpravách vrátane nových zdrojov tréningových údajov ako prostriedku na splnenie povinností týkajúcich sa hodnotového reťazca stanovených v tomto nariadení.

(110) Modely AI na všeobecné účely by mohli predstavovať systémové riziká, ktoré zahŕňajú okrem iného akékoľvek skutočné alebo odôvodnene predvídateľné negatívne účinky v súvislosti so závažnými nehodami, narušeniami kritických odvetví a závažnými dôsledkami pre verejné zdravie a bezpečnosť; akékoľvek skutočné alebo odôvodnene predvídateľné negatívne účinky na demokratické procesy, verejnú a hospodársku bezpečnosť; šírenie nezákonného, falošného alebo diskriminačného obsahu. Systémové riziká by sa mali chápať tak, že sa zvyšujú spôsobilosťami modelu a dosahom modelu, môžu vzniknúť počas celého životného cyklu modelu a sú ovplyvnené podmienkami nesprávneho použitia, spoľahlivosťou modelu, spravodlivosťou modelu a bezpečnosťou modelu, úrovňou autonómnosti modelu, jeho prístupom k nástrojom, novými alebo kombinovanými modalitami, stratégiami vydávania a distribúcie, potenciálom odstrániť ochranné prvky a inými faktormi. V medzinárodných prístupoch sa doteraz identifikovala najmä potreba venovať pozornosť rizikám vyplývajúcim z potenciálneho úmyselného nesprávneho použitia alebo neúmyselných problémov kontroly týkajúcich sa zosúladenia s ľudským zámerom; chemickým, biologickým, rádiologickým a jadrovým rizikám, ako sú spôsoby, akými možno znížiť prekážky vstupu vrátane vývoja zbraní, získavania dizajnu alebo používania zbraní; umožneniu ofenzívnych kybernetických spôsobilostí, ako sú spôsoby odhaľovania, využívania alebo operačného využívania zraniteľnosti; účinkom interakcie a používania nástrojov, napríklad vrátane schopnosti kontrolovať fyzické systémy a zasahovať do kritickej infraštruktúry; rizikám vyplývajúcim z modelov vyhotovovania vlastných kópií alebo „samoreplikácie“ alebo trénovania iných modelov; spôsobom, akými môžu modely viesť k škodlivému skresleniu a diskriminácii s rizikami pre jednotlivcov, komunity alebo spoločnosti; uľahčovaniu dezinformácií alebo poškodzovania súkromia hrozbami pre demokratické hodnoty a ľudské práva; riziku, že konkrétna udalosť by mohla viesť k reťazovej reakcii so značnými negatívnymi účinkami, ktoré by mohli ovplyvniť celé mesto, celú oblasť činnosti alebo celú komunitu.

(111) Je vhodné zaviesť metodiku pre klasifikáciu modelov AI na všeobecné účely ako modelu AI na všeobecné účely so systémovým rizikom. Keďže systémové riziká vyplývajú z mimoriadne vysokých spôsobilostí, mal by sa model AI na všeobecné účely považovať za model predstavujúci systémové riziká, ak má spôsobilosti s veľkým vplyvom, hodnotené na základe vhodných technických nástrojov a metodík, alebo významný vplyv na vnútorný trh z dôvodu jeho dosahu. Spôsobilosti s veľkým vplyvom v modeloch AI na všeobecné účely sú spôsobilosti, ktoré zodpovedajú spôsobilostiam zaznamenaným v najvyspelejších modeloch AI na všeobecné účely alebo ich prekračujú. Celú škálu spôsobilostí modelu možno lepšie pochopiť po jeho uvedení na trh alebo pri interakcii nasadzujúcich subjektov s modelom. Podľa aktuálneho stavu vývoja v čase nadobudnutia účinnosti tohto nariadenia je kumulatívny počet výpočtov použitých na trénovanie modelu AI na všeobecné účely meraný v operáciách s pohyblivou rádovou čiarkou jednou z relevantných aproximácií spôsobilostí modelu. Kumulatívny počet výpočtov použitých na trénovanie zahŕňa výpočty použité v rámci činností a metód, ktoré sú určené na posilnenie spôsobilostí modelu pred nasadením, ako je predbežné trénovanie, syntetické generovanie údajov a doladenie. Preto by sa mala stanoviť počiatočná prahová hodnota pre operácie s pohyblivou rádovou čiarkou, ktorá, ak je modelom AI na všeobecné účely splnená, vedie k predpokladu, že model je modelom AI na všeobecné účely so systémovými rizikami. Táto prahová hodnota by sa mala časom upraviť tak, aby odrážala technologické a priemyselné zmeny, ako sú algoritmické zlepšenia alebo zvýšená efektívnosť hardvéru, a mala by sa doplniť o referenčné hodnoty a ukazovatele spôsobilosti modelu.

Úrad pre AI by mal spolupracovať s vedeckou obcou, priemyslom, občianskou spoločnosťou a ďalšími odborníkmi s cieľom poskytnúť na to podklady. Prahové hodnoty, ako aj nástroje a referenčné hodnoty na posudzovanie spôsobilostí s veľkým vplyvom by mali byť silnými predikátormi všeobecnej povahy, spôsobilostí a súvisiaceho systémového rizika modelov AI na všeobecné účely a mohli by zohľadňovať spôsob uvádzania modelu na trh alebo počet používateľov, na ktorých môže mať vplyv. Na doplnenie tohto systému by Komisia mala mať možnosť prijímať individuálne rozhodnutia označujúce model AI na všeobecné účely ako model AI na všeobecné účely so systémovým rizikom, ak zistí, že takýto model má spôsobilosti alebo vplyv rovnocenné tým, ktoré sú zachytené stanovenou prahovou hodnotou. Uvedené rozhodnutie by sa malo prijať na základe celkového posúdenia kritérií na určenie modelu AI na všeobecné účely so systémovým rizikom stanovených v prílohe k tomuto nariadeniu, ako je kvalita alebo veľkosť súboru tréningových údajov, počet korporátnych a koncových používateľov, modality jeho vstupov a výstupov, úroveň jeho autonómnosti a škálovateľnosti alebo nástroje, ku ktorým má prístup. Po odôvodnenej žiadosti poskytovateľa, ktorého model bol označený za model AI na všeobecné účely so systémovým rizikom, by Komisia mala žiadosť zohľadniť a môže rozhodnúť o prehodnotení, či model AI na všeobecné účely možno stále považovať za model predstavujúci systémové riziká.

(112) Je tiež potrebné objasniť postup klasifikácie modelu AI na všeobecné účely so systémovým rizikom. Model AI na všeobecné účely, ktorý spĺňa príslušnú prahovú hodnotu pre spôsobilosti s veľkým vplyvom, by sa mal považovať za model AI na všeobecné účely so systémovým rizikom. Poskytovateľ by mal informovať úrad pre AI najneskôr dva týždne po splnení požiadaviek alebo po tom, ako sa zistí, že model AI na všeobecné účely bude spĺňať požiadavky, ktoré vedú k tomuto predpokladu. To je obzvlášť relevantné v súvislosti s prahovou hodnotou pre operácie s pohyblivou rádovou čiarkou, pretože trénovanie modelov AI na všeobecné účely si vyžaduje značné plánovanie, ktoré zahŕňa predbežné prideľovanie výpočtových zdrojov, a preto sú poskytovatelia modelov AI na všeobecné účely schopní vedieť, či by ich model dosiahol prahovú hodnotu pred ukončením trénovania. V súvislosti s uvedeným informovaním by poskytovateľ mal byť schopný preukázať, že model AI na všeobecné účely vzhľadom na svoje osobitné vlastnosti výnimočne nepredstavuje systémové riziká, a preto by sa nemal klasifikovať ako model AI na všeobecné účely so systémovými rizikami. Uvedené informácie sú pre úrad pre AI cenné pri predvídaní uvedenia modelov AI na všeobecné účely so systémovými rizikami na trh a poskytovatelia môžu začať s úradom pre AI včas spolupracovať. Uvedené informácie sú obzvlášť dôležité, pokiaľ ide o modely AI na všeobecné účely, ktoré sa majú vydať ako modely s otvoreným zdrojovým kódom, keďže po vydaní modelu s otvoreným zdrojovým kódom môže byť ťažšie vykonať potrebné opatrenia na zabezpečenie súladu s povinnosťami podľa tohto nariadenia.

(113) Ak sa Komisia dozvie o skutočnosti, že model AI na všeobecné účely spĺňa požiadavky na to, aby sa klasifikoval ako model AI na všeobecné účely so systémovým rizikom, ktorá predtým buď nebola známa, alebo o ktorej príslušný poskytovateľ Komisiu neinformoval, Komisia by mala byť oprávnená takto ho označiť. Systém kvalifikovaných upozornení by mal zabezpečiť, aby vedecký panel informoval úrad pre AI popri jeho monitorovacích činnostiach o modeloch AI na všeobecné účely, ktoré by sa prípadne mali klasifikovať ako modely AI na všeobecné účely so systémovým rizikom.

(114) Poskytovatelia modelov AI na všeobecné účely predstavujúcich systémové riziká by mali okrem povinností stanovených pre poskytovateľov modelov AI na všeobecné účely podliehať povinnostiam zameraným na identifikáciu a zmiernenie týchto rizík a zabezpečenie primeranej úrovne ochrany kybernetickej bezpečnosti bez ohľadu na to, či sa poskytujú ako samostatný model alebo sú zabudované do systému AI alebo produktu. Na dosiahnutie uvedených cieľov by sa v tomto nariadení malo od poskytovateľov vyžadovať, aby vykonávali potrebné hodnotenia modelov, najmä pred ich prvým uvedením na trh, vrátane vykonávania a zdokumentovania testovania modelov na nepriateľské útoky, prípadne aj prostredníctvom interného alebo nezávislého externého testovania. Okrem toho by poskytovatelia modelov AI na všeobecné účely so systémovými rizikami mali neustále posudzovať a zmierňovať systémové riziká, a to napríklad aj zavádzaním politík riadenia rizík, ako sú procesy zodpovednosti a správy a riadenia, vykonávaním monitorovania po uvedení na trh, prijímaním vhodných opatrení v rámci celého životného cyklu modelu a spoluprácou s príslušnými aktérmi v celom hodnotovom reťazci AI.

(115) Poskytovatelia modelov AI na všeobecné účely so systémovými rizikami by mali posúdiť a zmierniť možné systémové riziká. Ak napriek úsiliu identifikovať riziká súvisiace s modelom AI na všeobecné účely, ktoré môžu predstavovať systémové riziká, a predchádzať im, vývoj alebo používanie modelu spôsobí závažný incident, poskytovateľ modelu AI na všeobecné účely by mal bez zbytočného odkladu sledovať incident a oznámiť všetky relevantné informácie a možné nápravné opatrenia Komisii a vnútroštátnym príslušným orgánom. Okrem toho by poskytovatelia mali zabezpečiť primeranú úroveň ochrany kybernetickej bezpečnosti modelu a jeho fyzickej infraštruktúry, ak je to vhodné, počas celého životného cyklu modelu. Pri ochrane kybernetickej bezpečnosti v súvislosti so systémovými rizikami spojenými so zlomyseľným používaním alebo útokmi by sa mal náležite zvážiť náhodný únik modelu, jeho nepovolené vydanie, obchádzanie bezpečnostných opatrení a ochrana pred kybernetickými útokmi, neoprávneným prístupom alebo krádežou modelu. Uvedená ochrana by sa mohla uľahčiť zabezpečením váh, algoritmov, serverov a súborov údajov modelu, napríklad prostredníctvom prevádzkových bezpečnostných opatrení v oblasti informačnej bezpečnosti, osobitných politík kybernetickej bezpečnosti, primeraných technických a zavedených riešení a kontrol kybernetického a fyzického prístupu, ktoré sú primerané príslušným okolnostiam a súvisiacim rizikám.

(116) Úrad pre AI by mal podporovať a uľahčovať vypracovanie, preskúmanie a úpravu kódexov postupov s prihliadnutím na medzinárodné prístupy. Na účasť by mohli byť prizvaní všetci poskytovatelia modelov AI na všeobecné účely. S cieľom zabezpečiť, aby kódexy postupov odrážali aktuálny stav vývoja a náležite zohľadňovali rôznorodý súbor perspektív, by mal úrad pre AI spolupracovať s vnútroštátnymi príslušnými orgánmi a v prípade potreby by sa pri vypracúvaní takýchto kódexov mohol poradiť s organizáciami občianskej spoločnosti a inými príslušnými zainteresovanými stranami a odborníkmi vrátane vedeckého panelu. Kódexy postupov by sa mali vzťahovať na povinnosti poskytovateľov modelov AI na všeobecné účely a modelov AI na všeobecné účely predstavujúcich systémové riziká. Okrem toho, pokiaľ ide o systémové riziká, kódexy postupov by mali pomôcť zaviesť taxonómiu typov a povahy systémových rizík na úrovni Únie vrátane ich zdrojov. Kódexy postupov by sa mali zamerať aj na osobitné posúdenie rizika a zmierňujúce opatrenia.

(117) Kódexy postupov by mali predstavovať ústredný nástroj na riadne dodržiavanie povinností stanovených v tomto nariadení pre poskytovateľov modelov AI na všeobecné účely. Poskytovatelia by mali mať možnosť odvolávať sa na kódexy postupov na preukázanie dodržiavania povinností. Komisia môže prostredníctvom vykonávacích aktov rozhodnúť o schválení kódexu postupov a udeliť mu všeobecnú platnosť v rámci Únie, alebo prípadne stanoviť spoločné pravidlá vykonávania príslušných povinností, ak pred nadobudnutím účinnosti tohto nariadenia nie je možné kódex postupov finalizovať alebo ho úrad pre AI nepovažuje za primeraný. Keď sa harmonizovaná norma uverejní a posúdi úradom pre AI ako vhodná na pokrytie príslušných povinností, súlad s európskou harmonizovanou normou by mal poskytovateľom poskytnúť predpoklad zhody. Poskytovatelia modelov AI na všeobecné účely by okrem toho mali byť schopní preukázať súlad pomocou alternatívnych primeraných prostriedkov, ak kódexy postupov alebo harmonizované normy nie sú k dispozícii alebo sa rozhodnú na ne neodvolávať.

(118) Týmto nariadením sa regulujú systémy AI a modely AI uložením určitých požiadaviek a povinností relevantným aktérom trhu, ktorí ich uvádzajú na trh, uvádzajú do prevádzky alebo používajú v Únii, čím sa dopĺňajú povinnosti poskytovateľov sprostredkovateľských služieb, ktorí takéto systémy alebo modely začlenili do svojich služieb regulovaných nariadením (EÚ) 2022/2065. Pokiaľ sú takéto systémy alebo modely zabudované do určených veľmi veľkých online platforiem alebo veľmi veľkých internetových vyhľadávačov, podliehajú rámcu riadenia rizík stanovenému v nariadení (EÚ) 2022/2065. Príslušné povinnosti stanovené v tomto nariadení by sa preto mali považovať za splnené, pokiaľ sa v takýchto modeloch nevyskytnú a neidentifikujú významné systémové riziká, na ktoré sa nevzťahuje nariadenie (EÚ) 2022/2065. V tomto rámci sú poskytovatelia veľmi veľkých online platforiem a veľmi veľkých online vyhľadávačov povinní posúdiť potenciálne systémové riziká vyplývajúce z dizajnu, fungovania a používania ich služieb vrátane toho, ako môže koncepcia algoritmických systémov používaných v danej službe prispievať k takýmto rizikám, ako aj systémové riziká vyplývajúce z potenciálneho nesprávneho použitia. Títo poskytovatelia sú tiež povinní prijať primerané zmierňujúce opatrenia v súlade so základnými právami.

(119) Vzhľadom na rýchle tempo inovácie a technologický vývoj digitálnych služieb v rozsahu pôsobnosti rôznych nástrojov práva Únie, najmä so zreteľom na používanie a vnímanie ich príjemcov, sa systémy AI, na ktoré sa vzťahuje toto nariadenie, môžu poskytovať ako sprostredkovateľské služby alebo ich časti v zmysle nariadenia (EÚ) 2022/2065, čo by sa malo vykladať technologicky neutrálnym spôsobom. Systémy AI sa napríklad môžu používať na poskytovanie internetových vyhľadávačov, najmä v rozsahu, v akom systém AI, ako je online chatbot, vyhľadáva v zásade na všetkých webových sídlach, potom začleňuje výsledky do svojich existujúcich poznatkov a využíva aktualizované poznatky na vytvorenie jediného výstupu, v ktorom sa kombinujú rôzne zdroje informácií.

(120) Okrem toho povinnosti uložené poskytovateľom určitých systémov AI a subjektom nasadzujúcim určité systémy AI v tomto nariadení s cieľom umožniť odhaľovanie a zverejňovanie toho, že výstupy týchto systémov sú umelo generované alebo manipulované, sú osobitne relevantné na uľahčenie účinného vykonávania nariadenia (EÚ) 2022/2065. Týka sa to najmä povinností poskytovateľov veľmi veľkých online platforiem alebo veľmi veľkých internetových vyhľadávačov identifikovať a zmierňovať systémové riziká, ktoré môžu vyplynúť zo šírenia obsahu, ktorý bol umelo vytvorený alebo manipulovaný, najmä riziko skutočných alebo predvídateľných negatívnych účinkov na demokratické procesy, občiansku diskusiu a volebné procesy, a to aj prostredníctvom dezinformácií.

(121) Normalizácia by mala zohrávať kľúčovú úlohu pri poskytovaní technických riešení poskytovateľom na zabezpečenie súladu s týmto nariadením v súlade s aktuálnym stavom vývoja s cieľom podporovať inováciu, ako aj konkurencieschopnosť a rast na vnútornom trhu. Dodržiavanie harmonizovaných noriem v zmysle vymedzenia v článku 2 bode 1 písm. c) nariadenia Európskeho parlamentu a Rady (EÚ) č. 1025/2012[41], ktoré by za bežných okolností mali odzrkadľovať aktuálny stav vývoja, by malo byť pre poskytovateľov prostriedkom na preukázanie zhody s požiadavkami tohto nariadenia. Malo by sa preto podporovať vyvážené zastúpenie záujmov za účasti všetkých relevantných zainteresovaných strán pri vypracúvaní noriem, najmä MSP, spotrebiteľských organizácií a zainteresovaných strán v oblasti životného prostredia a sociálnej oblasti v súlade s článkami 5 a 6 nariadenia (EÚ) č. 1025/2012. S cieľom uľahčiť dodržiavanie predpisov by Komisia mala žiadosti o normalizáciu vydávať bez zbytočného odkladu. Pri príprave žiadosti o normalizáciu by Komisia mala konzultovať s poradným fórom a radou pre AI s cieľom zhromaždiť príslušné odborné poznatky. Ak však neexistujú relevantné odkazy na harmonizované normy, Komisia by mala mať možnosť stanoviť prostredníctvom vykonávacích aktov a po konzultácii s poradným fórom spoločné špecifikácie pre určité požiadavky podľa tohto nariadenia.

---

41 Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1025/2012 z 25. októbra 2012 o európskej normalizácii, ktorým sa menia a dopĺňajú smernice Rady 89/686/EHS a 93/15/EHS a smernice Európskeho parlamentu a Rady 94/9/ES, 94/25/ES, 95/16/ES, 97/23/ES, 98/34/ES, 2004/22/ES, 2007/23/ES, 2009/23/ES a 2009/105/ES a ktorým sa zrušuje rozhodnutie Rady 87/95/EHS a rozhodnutie Európskeho parlamentu a Rady č. 1673/2006/ES (Ú. v. EÚ L 316, 14.11.2012, s. 12).

Spoločná špecifikácia by mala byť výnimočným záložným riešením na uľahčenie povinnosti poskytovateľa dodržiavať požiadavky tohto nariadenia, ak žiadosť o normalizáciu neakceptovala žiadna z európskych normalizačných organizácií alebo ak príslušné harmonizované normy nedostatočne riešia obavy týkajúce sa základných práv, alebo ak harmonizované normy nie sú v súlade so žiadosťou, alebo ak dôjde k oneskoreniam pri prijímaní vhodnej harmonizovanej normy. Ak je takéto oneskorenie pri prijímaní harmonizovanej normy spôsobené technickou zložitosťou uvedenej normy, Komisia by to mala zohľadniť pred tým, ako zváži ustanovenie spoločných špecifikácií. Komisia sa vyzýva, aby pri vypracúvaní spoločných špecifikácií spolupracovala s medzinárodnými partnermi a medzinárodnými normalizačnými orgánmi.

(122) Bez toho, aby bolo dotknuté používanie harmonizovaných noriem a spoločných špecifikácií, je vhodné predpokladať, že poskytovatelia vysokorizikového systému AI, ktorý bol trénovaný a testovaný na údajoch odrážajúcich konkrétne geografické, behaviorálne, kontextuálne alebo funkčné prostredie, v ktorom sa má systém AI používať, by mali byť v súlade s príslušným opatrením stanoveným v rámci požiadavky na správu údajov stanovenej v tomto nariadení. Bez toho, aby boli dotknuté požiadavky týkajúce sa spoľahlivosti a presnosti stanovené v tomto nariadení, v súlade s článkom 54 ods. 3 nariadenia (EÚ) 2019/881 by sa vysokorizikové systémy AI, ktoré boli certifikované alebo pre ktoré bolo vydané vyhlásenie o zhode v rámci schémy kybernetickej bezpečnosti podľa uvedeného nariadenia, na ktorý boli uverejnené odkazy v *Úradnom vestníku Európskej únie*, mali považovať za systémy, ktoré sú v súlade s požiadavkou na kybernetickú bezpečnosť podľa tohto nariadenia, pokiaľ certifikát kybernetickej bezpečnosti alebo vyhlásenie o zhode alebo ich časti pokrývajú požiadavku kybernetickej bezpečnosti stanovenú v tomto nariadení. Touto skutočnosťou zostáva nedotknutá nezáväzná povaha uvedenej schémy kybernetickej bezpečnosti.

(123) Na zabezpečenie vysokej úrovne dôveryhodnosti vysokorizikových systémov AI by tieto systémy mali pred svojím uvedením na trh alebo do prevádzky podliehať posudzovaniu zhody.

(124) S cieľom minimalizovať zaťaženie prevádzkovateľov a predchádzať prípadnej duplicite je vhodné, aby sa v prípade vysokorizikových systémov AI súvisiacich s výrobkami, na ktoré sa vzťahujú existujúce harmonizačné právne predpisy Únie založené na novom legislatívnom rámci, posudzoval súlad týchto systémov AI s požiadavkami tohto nariadenia v rámci posudzovania zhody, ktoré je už stanovené v uvedených právnych predpisov. Uplatniteľnosť požiadaviek tohto nariadenia by preto nemala mať vplyv na konkrétnu logiku, metodiku ani všeobecnú štruktúru posudzovania zhody podľa príslušných harmonizačných právnych predpisov Únie.

(125) Vzhľadom na zložitosť vysokorizikových systémov AI a riziká, ktoré s nimi súvisia, je dôležité vyvinúť primeraný postup posudzovania zhody pre vysokorizikové systémy AI, do ktorého sú zapojené notifikované osoby, tzv. posudzovanie zhody treťou stranou. Vzhľadom na súčasné skúsenosti profesionálnych certifikačných subjektov, ktoré vykonávajú certifikáciu pred uvedením na trh v oblasti bezpečnosti výrobkov, a na odlišnú povahu súvisiacich rizík je však vhodné aspoň v počiatočnej fáze uplatňovania tohto nariadenia obmedziť rozsah uplatňovania posudzovania zhody treťou stranou v prípade iných vysokorizikových systémov AI, než tých, ktoré sa týkajú výrobkov. Posudzovanie zhody takýchto systémov by preto mal spravidla vykonávať poskytovateľ na vlastnú zodpovednosť, s jedinou výnimkou, ktorou sú systémy AI určené na použitie v biometrii.

(126) S cieľom vykonávať podľa potreby posudzovania zhody treťou stranou by notifikované osoby mali byť notifikované podľa tohto nariadenia vnútroštátnymi príslušnými orgánmi za predpokladu, že spĺňajú súbor požiadaviek, najmä pokiaľ ide o nezávislosť, kompetentnosť, absenciu konfliktov záujmov a vhodné požiadavky na kybernetickú bezpečnosť. Notifikáciu týchto osôb by mali vnútroštátne príslušné orgány zasielať Komisii a ostatným členským štátom prostredníctvom elektronického nástroja notifikácie vyvinutého a riadeného Komisiou podľa článku R23 prílohy I k rozhodnutiu č. 768/2008/ES.

(127) V súlade so záväzkami Únie vyplývajúcimi z Dohody Svetovej obchodnej organizácie o technických prekážkach obchodu je primerané uľahčiť vzájomné uznávanie výsledkov posudzovania zhody, ku ktorým dospeli príslušné orgány posudzovania zhody nezávislé od územia, na ktorom sú usadené, za predpokladu, že tieto orgány posudzovania zhody zriadené podľa práva tretej krajiny spĺňajú uplatniteľné požiadavky tohto nariadenia a Únia v tomto rozsahu uzavrela dohodu. V tejto súvislosti by Komisia mala na tento účel aktívne preskúmať možné medzinárodné nástroje, a najmä usilovať sa o uzavretie dohôd o vzájomnom uznávaní s tretími krajinami.

(128) V súlade so všeobecne zaužívaným pojmom podstatnej zmeny pre výrobky regulované harmonizačnými právnymi predpismi Únie je vhodné, aby sa vždy, keď nastane zmena, ktorá môže ovplyvniť súlad vysokorizikového systému AI s týmto nariadením (napríklad zmena operačného systému alebo softvérovej architektúry), alebo ak sa zmení zamýšľaný účel systému, tento systém AI považoval za nový systém AI, ktorý by sa mal podrobiť novému posudzovaniu zhody. Zmeny algoritmu a výkonu systémov AI, ktoré sa po uvedení na trh alebo do prevádzky ďalej „učia“, čiže automaticky prispôsobujú spôsob vykonávania funkcií, by však nemali predstavovať podstatnú zmenu za predpokladu, že tieto zmeny vopred stanovil poskytovateľ a posúdili sa v čase posudzovania zhody.

(129) Vysokorizikové systémy AI by mali mať označenie CE, ktoré by preukazovalo ich súlad s týmto nariadením, aby im bol umožnený voľný pohyb v rámci vnútorného trhu. V prípade vysokorizikových systémov AI zabudovaných do výrobku by sa malo umiestniť fyzické označenie CE, ktoré môže byť doplnené digitálnym označením CE. V prípade vysokorizikových systémov AI poskytovaných len digitálne by sa malo použiť digitálne označenie CE. Členské štáty by nemali vytvárať neodôvodnené prekážky uvedeniu na trh ani do prevádzky v prípade vysokorizikových systémov AI, ktoré spĺňajú požiadavky stanovené v tomto nariadení a majú označenie CE.

(130) Rýchla dostupnosť inovačných technológií môže mať za určitých podmienok zásadný význam pre zdravie a bezpečnosť osôb, ochranu životného prostredia a zmenu klímy a pre spoločnosť ako celok. Je preto vhodné, aby orgány dohľadu nad trhom mohli z výnimočných dôvodov verejnej bezpečnosti alebo ochrany života a zdravia fyzických osôb, ochrany životného prostredia a ochrany kľúčových priemyselných a infraštruktúrnych aktív povoliť uvedenie na trh alebo do prevádzky systémov AI, ktoré neboli podrobené posudzovaniu zhody. V riadne odôvodnených situáciách stanovených v tomto nariadení môžu orgány presadzovania práva alebo orgány civilnej ochrany uviesť do prevádzky konkrétny vysokorizikový systém AI bez povolenia orgánu dohľadu nad trhom za predpokladu, že o takéto povolenie sa požiada počas používania alebo po ňom bez zbytočného odkladu.

(131) S cieľom uľahčiť prácu Komisie a členských štátov v oblasti AI, ako aj zvýšiť transparentnosť voči verejnosti by sa od poskytovateľov vysokorizikových systémov AI, ktoré nesúvisia s výrobkami patriacimi do rozsahu pôsobnosti príslušných existujúcich harmonizačných právnych predpisov Únie, ako aj od poskytovateľov, ktorí sa domnievajú, že vysokorizikový systém AI uvedený vo vysokorizikových prípadoch použitia v prílohe k tomuto nariadeniu nie je na základe výnimky vysokorizikový, malo vyžadovať, aby seba a informácie o svojom systéme AI zaregistrovali v databáze Únie, ktorú má zriadiť a spravovať Komisia. Pred použitím systému AI uvedeného vo vysokorizikových prípadoch použitia v prílohe k tomuto nariadeniu by sa subjekty nasadzujúce vysokorizikové systémy AI, ktoré sú orgánmi verejnej moci, verejnými agentúrami alebo verejnými subjektmi, mali zaregistrovať v takejto databáze a zvoliť si systém, ktorý plánujú používať.

Ostatné nasadzujúce subjekty by mali mať právo tak urobiť dobrovoľne. Táto časť databázy Únie by mala byť bezplatne verejne prístupná a informácie by mali byť ľahko vyhľadateľné, zrozumiteľné a strojovo čitateľné. Databáza Únie by tiež mala byť používateľsky ústretová, napríklad poskytovaním funkcií vyhľadávania, a to aj prostredníctvom kľúčových slov, čo širokej verejnosti umožní nájsť relevantné informácie, ktoré majú byť predložené pri registrácii vysokorizikových systémov AI, a informácie o prípadoch použitia vysokorizikových systémov AI, ktoré sa uvádzajú v prílohe k tomuto nariadeniu a ktorým vysokorizikové systémy AI zodpovedajú. V databáze Únie by sa mala zaregistrovať aj každá podstatná zmena vysokorizikových systémov AI. V prípade vysokorizikových systémov AI v oblasti presadzovania práva, migrácie, azylu a riadenia kontroly hraníc by sa registračné povinnosti mali splniť v bezpečnej neverejnej časti databázy Únie. Prístup k bezpečnej neverejnej časti by sa mal prísne obmedziť na Komisiu, ako aj orgány dohľadu nad trhom, pokiaľ ide o ich vnútroštátnu časť uvedenej databázy. Vysokorizikové systémy AI v oblasti kritickej infraštruktúry by sa mali registrovať len na vnútroštátnej úrovni. Prevádzkovateľom databázy Únie by mala byť Komisia v súlade s nariadením (EÚ) 2018/1725. Aby sa zaistila plná funkčnosť databázy Únie pri jej zavedení, postup pri vytváraní databázy by mal zahŕňať vývoj funkčných špecifikácií Komisiou a nezávislú audítorskú správu. Komisia by mala pri plnení svojich úloh prevádzkovateľa údajov v databáze Únie zohľadniť riziká kybernetickej bezpečnosti. V záujme maximalizácie dostupnosti a využívania databázy Únie verejnosťou by databáza Únie vrátane informácií, ktoré sa prostredníctvom nej sprístupňujú, mala spĺňať požiadavky podľa smernice (EÚ) 2019/882.

(132) Určité systémy AI určené na interakciu s fyzickými osobami alebo generovanie obsahu môžu predstavovať osobitné riziko podvodu predstieraním identity alebo klamania bez ohľadu na to, či sú klasifikované ako vysokorizikové alebo nie. Používanie týchto systémov by preto malo za určitých okolností podliehať osobitným povinnostiam transparentnosti bez toho, aby boli dotknuté požiadavky a povinnosti týkajúce sa vysokorizikových systémov AI a s výhradou cielených výnimiek, aby sa zohľadnila osobitná potreba presadzovania práva. Fyzické osoby mali byť predovšetkým informované o tom, že interagujú so systémom AI, pokiaľ to nie je zrejmé z pohľadu fyzickej osoby, ktorá je primerane informovaná, pozorná a obozretná s prihliadnutím na okolnosti a kontext používania. Pri vykonávaní tejto povinnosti by sa mali zohľadniť charakteristiky fyzických osôb, ktoré z dôvodu ich veku alebo zdravotného postihnutia patria do zraniteľných skupín, a to v rozsahu, v akom je systém AI určený aj na interakciu s týmito skupinami. Okrem toho by fyzické osoby mali byť informované, keď sú vystavené systémom AI, ktoré spracúvaním ich biometrických údajov dokážu identifikovať alebo odvodiť emócie alebo zámery týchto osôb alebo ich zaradiť do osobitných kategórií. Takéto osobitné kategórie sa môžu týkať aspektov, ako je pohlavie, vek, farba vlasov, farba očí, tetovania, osobné črty, etnický pôvod, osobné preferencie a záujmy. Takéto informácie a oznámenia by sa mali poskytovať vo formátoch prístupných pre osoby so zdravotným postihnutím.

(133) Rôzne systémy AI môžu vytvárať veľké množstvá syntetického obsahu, ktorý je pre ľudí čoraz ťažšie odlíšiť od obsahu vytvoreného človekom a autentického obsahu. Široká dostupnosť a zvyšujúce sa spôsobilosti týchto systémov majú významný vplyv na integritu a dôveru v informačný ekosystém, čo zvyšuje nové riziká mylných informácií a manipulácie vo veľkom rozsahu, podvodov, predstierania identity a klamania spotrebiteľov. Vzhľadom na tieto vplyvy, rýchle tempo technologického vývoja a potrebu nových metód a techník na vysledovanie pôvodu informácií je vhodné vyžadovať od poskytovateľov týchto systémov, aby začlenili technické riešenia, ktoré umožnia označovanie v strojovo čitateľnom formáte a zisťovanie toho, že výstup bol vytvorený alebo manipulovaný systémom AI a nie človekom. Takéto techniky a metódy by mali byť dostatočne spoľahlivé, interoperabilné, účinné a robustné, pokiaľ je to technicky možné, pričom by sa mali zohľadniť dostupné techniky alebo kombinácia takýchto techník, ako sú vodoznak, identifikácia metaúdajov, kryptografické metódy na preukázanie pôvodu a pravosti obsahu, metódy logovania, odtlačky prstov alebo iné vhodné techniky. Pri implementovaní tejto povinnosti by poskytovatelia mali zohľadňovať aj osobitosti a obmedzenia rôznych typov obsahu a relevantný technologický a trhový vývoj v tejto oblasti odrážajúci sa vo všeobecne uznávanom aktuálnom stave vývoja. Takéto techniky a metódy možno implementovať na úrovni systému AI alebo na úrovni modelu AI vrátane modelov AI na všeobecné účely vytvárajúcich obsah, čím sa uľahčí plnenie tejto povinnosti nadväzujúcim poskytovateľom systému AI. V záujme zachovania primeranosti je vhodné predpokladať, že táto povinnosť označovania by sa nemala vzťahovať na systémy AI, ktoré vykonávajú predovšetkým pomocnú funkciu pre štandardné redakčné úpravy, alebo systémy AI, ktoré podstatne nemenia vstupné údaje, ktoré poskytuje subjekt nasadzujúci systém AI, alebo ich sémantiku.

(134) V nadväznosti na technické riešenia, ktoré používajú poskytovatelia systému AI, nasadzujúce subjekty, ktoré používajú systém AI na generovanie alebo manipulovanie obrazového obsahu, audioobsahu alebo videoobsahu, ktorý sa zjavne podobá existujúcim osobám, objektom, miestam, subjektom alebo udalostiam a ktorý by sa osobe falošne javil ako autentický alebo pravdivý (ďalej len „deep fake“), by takisto mali jasne a zreteľne zverejniť, že obsah bol umelo vytvorený alebo manipulovaný, a to zodpovedajúcim označením výstupu AI a zverejnením jeho umelého pôvodu. Dodržiavanie tejto povinnosti transparentnosti by sa nemalo vykladať tak, že naznačuje, že používanie systému AI alebo jeho výstupu bráni právu na slobodu prejavu a právu na slobodu umenia a vedeckého bádania, ktoré sú zaručené v charte, najmä ak je obsah súčasťou zjavne tvorivého, satirického, umeleckého, fiktívneho alebo analogického diela alebo programu s výhradou primeraných záruk pre práva a slobody tretích strán. V týchto prípadoch sa povinnosť transparentnosti v prípade deep fake stanovená v tomto nariadení obmedzuje na zverejnenie existencie takéhoto vytvoreného alebo manipulovaného obsahu primeraným spôsobom, ktorý nebráni zobrazovaniu alebo užívaniu diela vrátane jeho bežného využívania a používania pri zachovaní užitočnosti a kvality diela. Okrem toho je takisto vhodné stanoviť podobnú povinnosť zverejňovania v súvislosti s textom vytvoreným alebo manipulovaným AI v rozsahu, v akom sa uverejňuje na účely informovania verejnosti o záležitostiach verejného záujmu, pokiaľ obsah vytvorený AI neprešiel procesom ľudskej kontroly alebo redakčnej kontroly a pokiaľ fyzická alebo právnická osoba nenesie redakčnú zodpovednosť za uverejnenie obsahu.

(135) Bez toho, aby bola dotknutá povinná povaha a úplná uplatniteľnosť povinností transparentnosti, môže Komisia takisto podporovať a uľahčovať vypracovanie kódexov postupov na úrovni Únie s cieľom uľahčiť účinnú implementáciu povinností týkajúcich sa odhaľovania a označovania umelo vytvoreného alebo manipulovaného obsahu vrátane podpory praktických opatrení na prípadné sprístupnenie mechanizmov odhaľovania a uľahčenie spolupráce s inými aktérmi v hodnotovom reťazci, šírenie obsahu alebo kontrolu jeho pravosti a pôvodu s cieľom umožniť verejnosti účinne rozlišovať obsah vytvorený AI.

(136) Povinnosti uložené poskytovateľom a nasadzujúcim subjektom určitých systémov AI v tomto nariadení s cieľom umožniť odhaľovanie a zverejňovanie toho, že výstupy týchto systémov sú umelo generované alebo manipulované, sú osobitne relevantné na uľahčenie účinného vykonávania nariadenia (EÚ) 2022/2065. Týka sa to najmä povinností poskytovateľov veľmi veľkých online platforiem alebo veľmi veľkých internetových vyhľadávačov identifikovať a zmierňovať systémové riziká, ktoré môžu vyplynúť zo šírenia obsahu, ktorý bol umelo vytvorený alebo manipulovaný, najmä riziko skutočných alebo predvídateľných negatívnych účinkov na demokratické procesy, občiansku diskusiu a volebné procesy, a to aj prostredníctvom dezinformácií. Požiadavkou na označovanie obsahu vytvoreného systémami AI podľa tohto nariadenia nie je dotknutá povinnosť poskytovateľov hostingových služieb podľa článku 16 ods. 6 nariadenia (EÚ) 2022/2065 spracúvať oznámenia o nezákonnom obsahu prijaté podľa článku 16 ods. 1 uvedeného nariadenia a nemala by ovplyvňovať posúdenie a rozhodnutie o nezákonnosti konkrétneho obsahu. Toto posúdenie by sa malo vykonať výlučne s odkazom na pravidlá upravujúce zákonnosť obsahu.

(137) Dodržiavanie povinností transparentnosti v prípade systémov AI, na ktoré sa vzťahuje toto nariadenie, by sa nemalo vykladať ako naznačujúce to, že používanie systému AI alebo jeho výstupov je podľa tohto nariadenia alebo iných právnych predpisov Únie a členských štátov zákonné, a nemali by ním byť dotknuté iné povinnosti transparentnosti uložené subjektom nasadzujúcim systémy AI stanovené v práve Únie alebo vo vnútroštátnom práve.

(138) AI je rýchlo sa rozvíjajúca skupina technológií, ktorá si vyžaduje regulačný dohľad a bezpečný a kontrolovaný priestor na experimentovanie, pričom sa musí zabezpečiť zodpovedná inovácia a integrovanie primeraných záruk a opatrení na zmiernenie rizika. Na zabezpečenie právneho rámca, ktorý podporuje inováciu, je vhodný do budúcnosti a odolný voči narušeniu, by členské štáty mali zabezpečiť, aby ich vnútroštátne príslušné orgány zriadili na vnútroštátnej úrovni aspoň jedno regulačné experimentálne prostredie pre AI s cieľom uľahčiť vývoj a testovanie inovačných systémov AI pod prísnym regulačným dohľadom skôr, než sa tieto systémy uvedú na trh alebo inak uvedú do prevádzky. Členské štáty by mohli splniť túto povinnosť aj účasťou v už existujúcich regulačných experimentálnych prostrediach alebo spoločným zriadením experimentálneho prostredia s jedným alebo viacerými príslušnými orgánmi členských štátov, pokiaľ táto účasť poskytuje zúčastneným členským štátom rovnocennú úroveň vnútroštátneho pokrytia. Regulačné experimentálne prostredia pre AI by sa mohli zriadiť vo fyzickej, digitálnej alebo hybridnej forme a môžu zahŕňať fyzické, ako aj digitálne produkty. Zriaďujúce orgány by mali takisto zabezpečiť, aby regulačné experimentálne prostredia pre AI mali na svoje fungovanie primerané zdroje vrátane finančných a ľudských zdrojov.

(139) Cieľmi regulačných experimentálnych prostredí pre AI by mala byť podpora inovácie v oblasti AI vytvorením kontrolovaného experimentálneho a testovacieho prostredia vo fáze vývoja a pred uvedením na trh, aby sa zabezpečil súlad inovačných systémov AI s týmto nariadením a iným relevantný právom Únie a vnútroštátnym právom. Okrem toho by sa regulačné experimentálne prostredia pre AI mali zamerať na zvýšenie právnej istoty inovátorov a dohľadu príslušných orgánov a pochopenie príležitostí, vznikajúcich rizík a vplyvov používania AI, na uľahčenie regulačného vzdelávania orgánov a podnikov, a to aj vzhľadom na budúce úpravy právneho rámca, na podporu spolupráce a výmeny najlepších postupov s orgánmi zapojenými do regulačných experimentálnych prostredí pre AI, a na urýchlenie prístupu na trhy, a to aj odstránením prekážok pre MSP vrátane startupov. Regulačné experimentálne prostredia pre AI by mali byť široko dostupné v celej Únii a osobitná pozornosť by sa mala venovať ich dostupnosti pre MSP vrátane startupov. Účasť v regulačnom experimentálnom prostredí pre AI by sa mala zamerať na otázky, ktoré vyvolávajú právnu neistotu pre poskytovateľov a potenciálnych poskytovateľov pri inovácii a experimentovaní s AI v Únii, a prispievať k regulačnému vzdelávaniu založenému na dôkazoch. Dohľad nad systémami AI v regulačnom experimentálnom prostredí pre AI by sa preto mal vzťahovať na ich vývoj, trénovanie, testovanie a validáciu pred ich uvedením na trh alebo do prevádzky, ako aj na pojem podstatná zmena a výskyt takýchto zmien, ktoré si môžu vyžadovať nový postup posudzovania zhody. Ak sa počas vývoja a testovania takýchto systémov AI zistia akékoľvek významné riziká, malo by sa pristúpiť k primeranému zmierneniu rizík, a ak to nie je možné, k pozastaveniu procesu vývoja a testovania.

Vnútroštátne príslušné orgány, ktoré zriaďujú regulačné experimentálne prostredia pre AI, by mali v prípade potreby spolupracovať s inými relevantnými orgánmi vrátane tých, ktoré dohliadajú na ochranu základných práv, a mohli by umožniť zapojenie ďalších aktérov v rámci ekosystému AI, ako sú vnútroštátne alebo európske normalizačné organizácie, notifikované osoby, skúšobné a experimentálne zariadenia, výskumné a experimentálne laboratóriá, európske centrá digitálnych inovácií a príslušné zainteresované strany a organizácie občianskej spoločnosti. S cieľom zabezpečiť jednotné vykonávanie v celej Únii a úspory z rozsahu je vhodné stanoviť spoločné pravidlá pre zavádzanie regulačných experimentálnych prostredí pre AI a rámec pre spoluprácu medzi príslušnými orgánmi zapojenými do dohľadu nad experimentálnymi prostrediami. Regulačné experimentálne prostredia pre AI zriadené podľa tohto nariadenia by nemali mať vplyv na iné právne predpisy umožňujúce zriadenie iných experimentálnych prostredí zameraných na zabezpečenie súladu s iným právnym predpisom, než je toto nariadenie. V prípade potreby by relevantné príslušné orgány zodpovedné za tieto iné regulačné experimentálne prostredia mali zvážiť výhody používania týchto experimentálnych prostredí aj na účely zabezpečenia súladu systémov AI s týmto nariadením. Na základe dohody medzi vnútroštátnymi príslušnými orgánmi a účastníkmi regulačného experimentálneho prostredia pre AI sa testovanie v reálnych podmienkach môže vykonávať a môže sa naň dohliadať aj v rámci regulačného experimentálneho prostredia pre AI.

(140) Toto nariadenie by malo poskytnúť právny základ pre poskytovateľov a potenciálnych poskytovateľov v regulačných experimentálnych prostrediach pre AI na používanie osobných údajov, ktoré boli získané na iné účely, pri vývoji určitých systémov AI vo verejnom záujme v rámci regulačného experimentálneho prostredia pre AI v súlade s článkom 6 ods. 4 a článkom 9 ods. 2 písm. g) nariadenia (EÚ) 2016/679 a článkami 5, 6 a 10 nariadenia (EÚ) 2018/1725, a bez toho, aby bol dotknutý článok 4 ods. 2 a článok 10 smernice (EÚ) 2016/680. Všetky ostatné povinnosti prevádzkovateľov a práva dotknutých osôb podľa nariadenia (EÚ) 2016/679, nariadenia (EÚ) 2018/1725 a smernice (EÚ) 2016/680 zostávajú uplatniteľné. Toto nariadenie by predovšetkým nemalo poskytovať právny základ v zmysle článku 22 ods. 2 písm. b) nariadenia (EÚ) 2016/679 a článku 24 ods. 2 písm. b) nariadenia (EÚ) 2018/1725. Poskytovatelia a potenciálni poskytovatelia v regulačnom experimentálnom prostredí pre AI by mali zabezpečiť primerané záruky a spolupracovať s príslušnými orgánmi, a to aj tým, že budú postupovať podľa ich usmernení a konať promptne a v dobrej viere s cieľom primerane zmierniť akékoľvek zistené vysoké riziká pre bezpečnosť, zdravie a základné práva, ktoré môžu vzniknúť počas vývoja, testovania a experimentácie v uvedenom experimentálnom prostredí.

(141) S cieľom urýchliť proces vývoja a uvádzania na trh vysokorizikových systémov AI uvedených v prílohe k tomuto nariadeniu je dôležité, aby poskytovatelia alebo potenciálni poskytovatelia takýchto systémov mohli využívať aj osobitný režim testovania týchto systémov v reálnych podmienkach bez toho, aby sa zapojili do regulačného experimentálneho prostredia pre AI. V takýchto prípadoch by sa však pri zohľadnení možných dôsledkov takéhoto testovania na fyzické osoby malo zabezpečiť, aby sa nariadením zaviedli primerané a dostatočné záruky a podmienky pre poskytovateľov alebo potenciálnych poskytovateľov. Takéto záruky by okrem iného mali zahŕňať požadovanie informovaného súhlasu fyzických osôb s účasťou na testovaní v reálnych podmienkach s výnimkou presadzovania práva v prípadoch, keď by vyžiadanie informovaného súhlasu bránilo testovaniu systému AI. Súhlas účastníkov s účasťou na takomto testovaní podľa tohto nariadenia je odlišný od súhlasu dotknutých osôb so spracúvaním ich osobných údajov podľa príslušného práva o ochrane údajov a nie je ním dotknutý.

Takisto je dôležité minimalizovať riziká a umožniť dohľad zo strany príslušných orgánov, a preto požadovať, aby potenciálni poskytovatelia predložili príslušnému orgánu dohľadu nad trhom plán testovania v reálnych podmienkach, registrovali testovanie v špecializovaných oddieloch v databáze Únie s určitými obmedzenými výnimkami, stanovili obmedzenia obdobia, počas ktorého možno testovanie vykonávať, a vyžadovali dodatočné záruky pre osoby patriace do určitých zraniteľných skupín, ako aj písomnú dohodu, v ktorej sa vymedzia úlohy a povinnosti potenciálnych poskytovateľov a nasadzujúcich subjektov a účinný dohľad zo strany príslušných pracovníkov zapojených do testovania v reálnych podmienkach. Okrem toho je vhodné stanoviť dodatočné záruky na zabezpečenie toho, aby sa predpovede, odporúčania alebo rozhodnutia systému AI mohli účinne zvrátiť a ignorovať a aby boli osobné údaje chránené a vymazané, keď účastníci stiahli svoj súhlas s účasťou na testovaní bez toho, aby boli dotknuté ich práva ako dotknutých osôb podľa právnych predpisov Únie v oblasti ochrany údajov. Pokiaľ ide o prenos údajov, je tiež vhodné stanoviť, že údaje zozbierané a spracúvané na účely testovania v reálnych podmienkach by sa mali prenášať do tretích krajín len za predpokladu, že sa implementujú primerané a uplatniteľné záruky podľa práva Únie, najmä v súlade so základňami pre prenos osobných údajov podľa práva Únie o ochrane údajov, zatiaľ čo v prípade iných ako osobných údajov sa zavedú primerané záruky v súlade s právom Únie, ako sú nariadenia Európskeho parlamentu a Rady (EÚ) 2022/868[42] a (EÚ) 2023/2854[43].

---

[42] Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/868 z 30. mája 2022 o európskej správe údajov a o zmene nariadenia (EÚ) 2018/1724 (akt o správe údajov) (Ú. v. EÚ L 152, 3.6.2022, s. 1).

[43] Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/2854 z 13. decembra 2023 o harmonizovaných pravidlách týkajúcich sa spravodlivého prístupu k údajom a ich používania, ktorým sa mení nariadenie (EÚ) 2017/2394 a smernica (EÚ) 2020/1828 (akt o údajoch) (Ú. v. EÚ L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).

(142) S cieľom zabezpečiť, aby AI viedla k sociálne a environmentálne prospešným výsledkom, sa členské štáty nabádajú, aby podporovali a propagovali výskum a vývoj riešení AI na podporu sociálne a environmentálne prospešných činností, ako sú riešenia založené na AI, s cieľom zvýšiť prístupnosť pre osoby so zdravotným postihnutím, riešiť sociálno-ekonomické nerovnosti alebo plniť environmentálne ciele, a to vyčlenením dostatočných zdrojov vrátane verejných finančných prostriedkov a finančných prostriedkov Únie, a vo vhodných prípadoch a za predpokladu, že sú splnené kritériá oprávnenosti a výberu, so zohľadnením najmä projektov, ktoré sledujú takéto ciele. Takéto projekty by mali byť založené na zásade interdisciplinárnej spolupráce medzi vývojármi AI, odborníkmi na nerovnosť a nediskrimináciu, prístupnosť, spotrebiteľské, environmentálne a digitálne práva, ako aj akademickými pracovníkmi.

(143) V záujme podpory a ochrany inovácií je dôležité, aby sa osobitne prihliadalo na záujmy MSP vrátane startupov, ktoré sú poskytovateľmi systémov AI alebo subjektmi nasadzujúcimi systémy AI. Na tento účel by členské štáty mali vyvíjať iniciatívy zamerané na týchto prevádzkovateľov vrátane zvyšovania informovanosti a informačnej komunikácie. Členské štáty by mali poskytnúť MSP vrátane startupov, ktoré majú sídlo alebo pobočku v Únii, prednostný prístup do regulačných experimentálnych prostredí pre AI za predpokladu, že spĺňajú podmienky oprávnenosti a podmienky účasti a nebránia iným poskytovateľom a potenciálnym poskytovateľom v prístupe do experimentálnych prostredí za predpokladu, že sú splnené rovnaké podmienky a kritériá. Členské štáty by mali použiť existujúce kanály a v prípade potreby vytvoriť nové vyhradené kanály na komunikáciu s MSP vrátane startupov, subjektmi nasadzujúcimi systémy AI, ďalšími inovátormi a podľa potreby s miestnymi orgánmi verejnej moci s cieľom podporovať MSP v celom štádiu ich rozvoja poskytovaním usmernení a odpovedaním na otázky týkajúce sa vykonávania tohto nariadenia. Vo vhodných prípadoch by tieto kanály mali navzájom spolupracovať s cieľom vytvoriť synergie a zabezpečiť homogénnosť v ich usmerneniach pre MSP vrátane startupov a subjektov nasadzujúcich systémy AI. Členské štáty by taktiež mali uľahčovať účasť MSP a iných relevantných zainteresovaných strán na procese tvorby noriem. Pri stanovovaní poplatkov za posudzovanie zhody notifikovanými osobami by sa okrem toho mali zohľadňovať osobitné záujmy a potreby poskytovateľov, ktorí sú MSP vrátane startupov. Komisia by mala pravidelne posudzovať náklady MSP vrátane startupov na certifikáciu a dodržiavanie predpisov, a to aj transparentnými konzultáciami, a mala by spolupracovať s členskými štátmi na znižovaní týchto nákladov.

Napríklad, značné náklady pre poskytovateľov a iných prevádzkovateľov, najmä menších prevádzkovateľov, môžu predstavovať náklady na preklady súvisiace s povinnou dokumentáciou a komunikáciou s orgánmi. Členské štáty by mali podľa možnosti zabezpečiť, aby jedným z jazykov, ktoré určili a akceptovali na účely dokumentácie vedenej príslušnými poskytovateľmi a komunikácie s prevádzkovateľmi, bol jazyk, ktorému vo všeobecnosti rozumie čo najväčší počet cezhraničných nasadzujúcich subjektov. S cieľom riešiť osobitné potreby MSP vrátane startupov by Komisia mala na žiadosť rady pre AI poskytnúť štandardizované vzory pre oblasti, na ktoré sa vzťahuje toto nariadenie. Okrem toho by Komisia mala dopĺňať úsilie členských štátov tým, že všetkým poskytovateľom a nasadzujúcim subjektom poskytne jednotnú informačnú platformu s ľahko použiteľnými informáciami o tomto nariadení, organizovaním vhodných komunikačných kampaní na zvýšenie informovanosti o povinnostiach vyplývajúcich z tohto nariadenia a hodnotením a podporou zbližovania najlepších postupov v postupoch verejného obstarávania v súvislosti so systémami AI. Stredné podniky, ktoré sa donedávna považovali za malé podniky v zmysle prílohy k odporúčaniu Komisie 2003/361/ES[44], by mali mať prístup k týmto podporným opatreniam, keďže týmto novým stredným podnikom môžu niekedy chýbať právne zdroje a odborná príprava potrebné na zabezpečenie riadneho pochopenia a dodržiavania tohto nariadenia.

[44] Odporúčanie Komisie zo 6. mája 2003 o vymedzení mikropodnikov, malých a stredných podnikov (Ú. v. EÚ L 124, 20.5.2003, s. 36).

(144) S cieľom podporovať a chrániť inovácie by k dosiahnutiu cieľov tohto nariadenia mala prispievať platforma AI na požiadanie a všetky relevantné programy a projekty financovania Únie, ako je program Digitálna Európa alebo Horizont Európa, ktoré Komisia a členské štáty vykonávajú na vnútroštátnej úrovni alebo na úrovni Únie.

(145) S cieľom minimalizovať riziká spojené s vykonávaním vyplývajúce z nedostatku poznatkov a odborných znalostí na trhu, ako aj uľahčiť poskytovateľom, najmä MSP vrátane startupov, a notifikovaným osobám plnenie ich povinností podľa tohto nariadenia by k vykonávaniu tohto nariadenia mali predovšetkým prispievať platforma AI na požiadanie, európske centrá digitálnych inovácií a testovacie a experimentálne zariadenia zriadené Komisiou a členskými štátmi na úrovni Únie alebo na vnútroštátnej úrovni. Platforma AI na požiadanie, európske centrá digitálnych inovácií a testovacie a experimentálne zariadenia sú v rámci svojho poslania a oblastí svojej pôsobnosti schopné poskytovať poskytovateľom a notifikovaným osobám najmä technickú a vedeckú podporu.

(146) Okrem toho, vzhľadom na to, že niektorí prevádzkovatelia sú veľmi malí, a s cieľom zabezpečiť proporcionalitu v súvislosti s nákladmi na inovácie je vhodné umožniť mikropodnikom splniť jednu z najnákladnejších povinností, konkrétne zavedenie systému riadenia kvality, zjednodušeným spôsobom, čím by sa znížilo administratívne zaťaženie a náklady týchto podnikov bez toho, aby to malo vplyv na úroveň ochrany a potrebu súladu s požiadavkami na vysokorizikové systémy AI. Komisia by mala vypracovať usmernenia na spresnenie prvkov systému riadenia kvality, ktoré majú mikropodniky splniť týmto zjednodušeným spôsobom.

(147) Je vhodné, aby Komisia v čo najväčšej možnej miere uľahčila prístup k testovacím a experimentálnym zariadeniam orgánom, skupinám alebo laboratóriám zriadeným alebo akreditovaným podľa akýchkoľvek príslušných harmonizačných právnych predpisov Únie, ktoré plnia úlohy v súvislosti s posudzovaním zhody výrobkov alebo zariadení, na ktoré sa uvedené harmonizačné právne predpisy Únie vzťahujú. Týka sa to najmä panelov odborníkov, odborných laboratórií a referenčných laboratórií v oblasti zdravotníckych pomôcok podľa nariadení (EÚ) 2017/745 a (EÚ) 2017/746.

(148) Týmto nariadením by sa mal stanoviť rámec správy a riadenia, ktorý umožní koordináciu a podporu uplatňovania tohto nariadenia na vnútroštátnej úrovni, ako aj budovanie spôsobilostí na úrovni Únie a integráciu zainteresovaných strán v oblasti AI. Účinné vykonávanie a presadzovanie tohto nariadenia si vyžaduje rámec správy a riadenia, ktorý umožňuje koordináciu a budovanie centrálnej expertízy na úrovni Únie. Rozhodnutím Komisie[45] bol zriadený úrad pre AI, ktorého poslaním je rozvíjať odborné znalosti a spôsobilosti Únie v oblasti AI a prispievať k vykonávaniu právnych predpisov Únie v oblasti AI. Členské štáty by mali uľahčovať úlohy úradu pre AI s cieľom podporiť rozvoj odborných znalostí a spôsobilostí Únie na úrovni Únie a posilniť fungovanie digitálneho jednotného trhu. Okrem toho by sa mala zriadiť rada pre AI zložená zo zástupcov členských štátov, vedecký panel na integráciu vedeckej komunity a poradné fórum, prostredníctvom ktorého by zainteresované strany prispievali k vykonávaniu tohto nariadenia na úrovni Únie a na vnútroštátnej úrovni. Rozvoj odborných znalostí a spôsobilostí Únie by mal zahŕňať aj využívanie existujúcich zdrojov a odborných znalostí, najmä prostredníctvom synergií so štruktúrami vytvorenými v kontexte presadzovania iných právnych predpisov na úrovni Únie a synergií so súvisiacimi iniciatívami na úrovni Únie, ako je spoločný podnik EuroHPC a testovacie a experimentálne zariadenia AI v rámci programu Digitálna Európa.

[45] Rozhodnutie Komisie z 24. januára 2024, ktorým sa zriaďuje Európsky úrad pre umelú inteligenciu, C(2024) 390.

(149) Na uľahčenie bezproblémového, účinného a harmonizovaného vykonávania tohto nariadenia by sa mala zriadiť rada pre AI. Rada pre AI by mala zohľadňovať rôzne záujmy ekosystému AI a mala by byť zložená zo zástupcov členských štátov. Rada pre AI by mala byť zodpovedná za viacero poradných úloh vrátane vydávania stanovísk, odporúčaní a poradenstva alebo prispievania k usmerneniam v záležitostiach týkajúcich sa vykonávania tohto nariadenia vrátane otázok presadzovania, technických špecifikácií alebo existujúcich noriem týkajúcich sa požiadaviek stanovených v tomto nariadení, a poskytovania poradenstva Komisii a členským štátom a ich vnútroštátnym príslušným orgánom v špecifických otázkach súvisiacich s AI. S cieľom poskytnúť členským štátom určitú flexibilitu pri určovaní ich zástupcov v rade pre AI môžu byť takýmito zástupcami akékoľvek osoby z verejných subjektov, ktoré by mali mať príslušné kompetencie a právomoci na uľahčenie koordinácie na vnútroštátnej úrovni a prispievanie k plneniu úloh rady pre AI. Rada pre AI by mala zriadiť dve stále podskupiny s cieľom poskytnúť platformu na spoluprácu a výmenu informácií medzi orgánmi dohľadu nad trhom a notifikujúcimi orgánmi v otázkach týkajúcich sa dohľadu nad trhom, ako aj v otázkach týkajúcich sa notifikovaných osôb. Stála podskupina pre dohľad nad trhom by mala konať ako skupina pre administratívnu spoluprácu (ADCO) pre toto nariadenie v zmysle článku 30 nariadenia (EÚ) 2019/1020. V súlade s článkom 33 uvedeného nariadenia by Komisia mala podporovať činnosti stálej podskupiny pre dohľad nad trhom vykonávaním hodnotení alebo štúdií trhu, najmä s cieľom identifikovať aspekty tohto nariadenia, ktoré si vyžadujú osobitnú a naliehavú koordináciu medzi orgánmi dohľadu nad trhom. Na účely preskúmania konkrétnych otázok môže rada pre AI podľa potreby zriaďovať ďalšie stále alebo dočasné podskupiny. Rada pre AI by mala podľa potreby spolupracovať aj s príslušnými orgánmi, expertnými skupinami a sieťami Únie, ktoré pôsobia v kontexte príslušného práva Únie, a to najmä s tými, na ktorých činnosť sa vzťahuje príslušné právo Únie o údajoch, digitálnych produktoch a službách.

(150) S cieľom zabezpečiť zapojenie zainteresovaných strán do vykonávania a uplatňovania tohto nariadenia by sa malo zriadiť poradné fórum, ktoré bude rade pre AI a Komisii poskytovať poradenstvo a technické odborné znalosti. S cieľom zabezpečiť rôznorodé a vyvážené zastúpenie zainteresovaných strán medzi komerčnými a nekomerčnými záujmami a v rámci kategórie obchodných záujmov, pokiaľ ide o MSP a iné podniky, by poradné fórum malo okrem iného zahŕňať priemysel, startupy, MSP, akademickú obec, občiansku spoločnosť vrátane sociálnych partnerov, ako aj Agentúru pre základné práva, agentúru ENISA, Európsky výbor pre normalizáciu (CEN), Európsky výbor pre normalizáciu v elektrotechnike (CENELEC) a Európsky inštitút pre telekomunikačné normy (ETSI).

(151) Na podporu vykonávania a presadzovania tohto nariadenia, najmä monitorovacích činností úradu pre AI, pokiaľ ide o modely AI na všeobecné účely, by sa mal zriadiť vedecký panel nezávislých expertov. Nezávislí experti, ktorí tvoria vedecký panel, by sa mali vyberať na základe aktuálnych vedeckých alebo technických odborných znalostí v oblasti AI, mali by svoje úlohy vykonávať nestranne, objektívne a mali by zabezpečovať dôvernosť informácií a údajov získaných pri vykonávaní svojich úloh a činností. S cieľom umožniť posilnenie vnútroštátnych kapacít potrebných na účinné presadzovanie tohto nariadenia by členské štáty mali mať možnosť požiadať o podporu zo strany skupiny odborníkov tvoriacich vedecký panel pre ich činnosti v oblasti presadzovania práva.

(152) S cieľom podporiť primerané presadzovanie, pokiaľ ide o systémy AI, a posilniť kapacity členských štátov by sa mali zriadiť podporné štruktúry Únie na testovanie AI, ktoré by sa mali sprístupniť členským štátom.

(153) Pri uplatňovaní a presadzovaní tohto nariadenia zohrávajú kľúčovú úlohu členské štáty. V tejto súvislosti by mal každý členský štát určiť na účely dohľadu nad uplatňovaním a vykonávaním tohto nariadenia aspoň jeden notifikujúci orgán a aspoň jeden orgán dohľadu nad trhom ako vnútroštátne príslušné orgány. Členské štáty môžu rozhodnúť o vymenovaní akéhokoľvek druhu verejného subjektu na plnenie úloh vnútroštátnych príslušných orgánov v zmysle tohto nariadenia v súlade so svojimi osobitnými vnútroštátnymi organizačnými charakteristikami a potrebami. Aby sa zvýšila efektívnosť organizácie zo strany členských štátov a zriadilo jednotné kontaktné miesto vo vzťahu k verejnosti a iným protistranám na úrovni členských štátov a Únie, každý členský štát by mal určiť jeden orgán dohľadu nad trhom, aby konal ako jediné kontaktné miesto.

(154) Vnútroštátne príslušné orgány by mali vykonávať svoje právomoci nezávisle, nestranne a bez zaujatosti s cieľom chrániť zásady objektivity svojich činností a úloh a zabezpečiť uplatňovanie a vykonávanie tohto nariadenia. Členovia týchto orgánov by sa mali zdržať akéhokoľvek konania nezlučiteľného s ich povinnosťami a mali by podliehať pravidlám dôvernosti podľa tohto nariadenia.

(155) Všetci poskytovatelia vysokorizikových systémov AI by mali mať zavedený systém monitorovania po uvedení na trh, aby zabezpečili, že budú schopní zohľadniť skúsenosti s používaním vysokorizikových systémov AI na zlepšenie svojich systémov a procesu dizajnovania a vývoja, alebo aby mohli včas prijať akékoľvek možné nápravné opatrenia. V prípade potreby by monitorovanie po uvedení na trh malo zahŕňať analýzu interakcie s inými systémami AI vrátane iných zariadení a softvéru. Monitorovanie po uvedení na trh by sa nemalo vzťahovať na citlivé operačné údaje nasadzujúcich subjektov, ktoré sú orgánmi presadzovania práva. Tento systém je takisto kľúčový na zabezpečenie toho, aby sa možné riziká vyplývajúce zo systémov AI, ktoré sa po uvedení na trh alebo do prevádzky ďalej učia, mohli efektívnejšie a včas riešiť. V tejto súvislosti by sa od poskytovateľov malo vyžadovať, aby mali zavedený systém na ohlasovanie všetkých závažných incidentov vyplývajúcich z používania ich systémov AI relevantným orgánom, t. j. incidentov alebo porúch, ktoré vedú k smrti alebo vážnemu poškodeniu zdravia, závažnému a nezvratnému narušeniu riadenia a prevádzky kritickej infraštruktúry, porušeniam povinností podľa práva Únie určených na ochranu základných práv alebo k vážnej škode na majetku alebo životnom prostredí.

(156) S cieľom zabezpečiť primerané a účinné presadzovanie požiadaviek a povinností stanovených v tomto nariadení, ktoré predstavuje harmonizačný právny predpis Únie, by sa mal v celom rozsahu uplatňovať systém dohľadu nad trhom a súladu výrobkov stanovený nariadením (EÚ) 2019/1020. Orgány dohľadu nad trhom určené podľa tohto nariadenia by mali mať všetky právomoci v oblasti presadzovania stanovené v tomto nariadení a v nariadení (EÚ) 2019/1020 a mali by svoje právomoci a povinnosti vykonávať nezávisle, nestranne a bez zaujatosti. Hoci väčšina systémov AI nepodlieha osobitným požiadavkám ani povinnostiam podľa tohto nariadenia, orgány dohľadu nad trhom môžu prijať opatrenia vo vzťahu ku všetkým systémom AI, ak predstavujú riziko podľa tohto nariadenia. Vzhľadom na osobitnú povahu inštitúcií, agentúr a orgánov Únie, ktoré patria do rozsahu pôsobnosti tohto nariadenia, je vhodné pre ne určiť ako príslušný orgán dohľadu nad trhom európskeho dozorného úradníka pre ochranu údajov. Tým by nemalo byť dotknuté určenie vnútroštátnych príslušných orgánov členskými štátmi. Činnosti dohľadu nad trhom by nemali mať vplyv na schopnosť subjektov pod dohľadom vykonávať svoje úlohy nezávisle, ak sa takáto nezávislosť vyžaduje podľa práva Únie.

(157) Týmto nariadením nie sú dotknuté kompetencie, úlohy, právomoci ani nezávislosť príslušných vnútroštátnych orgánov verejnej moci alebo subjektov, ktoré dohliadajú na uplatňovanie práva Únie na ochranu základných práv, vrátane subjektov pre rovnaké zaobchádzanie a orgánov pre ochranu osobných údajov. Takéto vnútroštátne orgány verejnej moci alebo subjekty by mali mať aj prístup k všetkej dokumentácii vytvorenej podľa tohto nariadenia, pokiaľ je to potrebné pre ich mandát. Na zabezpečenie primeraného a včasného presadzovania v prípade systémov AI, ktoré predstavujú riziko pre zdravie, bezpečnosť a základné práva, by sa mal stanoviť osobitný ochranný postup. Postup pre takéto systémy AI predstavujúce riziko by sa mal uplatňovať na vysokorizikové systémy AI predstavujúce riziko, zakázané systémy, ktoré boli uvedené na trh, do prevádzky alebo používané v rozpore s ustanoveniam tohto nariadenia o zakázaných praktikách, a na systémy AI, ktoré boli sprístupnené v rozpore s požiadavkami na transparentnosť stanovenými v tomto nariadení a predstavujú riziko.

(158) Právne predpisy Únie týkajúce sa finančných služieb zahŕňajú pravidlá a požiadavky vnútornej správy a riadenia a riadenia rizík, ktoré sa vzťahujú na regulované finančné inštitúcie počas poskytovania týchto služieb vrátane prípadov, keď využívajú systémy AI. S cieľom zabezpečiť jednotné uplatňovanie a presadzovanie povinností podľa tohto nariadenia a príslušných pravidiel a požiadaviek právnych aktov Únie v oblasti finančných služieb by mali byť príslušné orgány pre dohľad nad uvedenými právnymi aktmi a za ich presadzovanie, najmä príslušné orgány v zmysle vymedzenia v nariadení Európskeho parlamentu a Rady (EÚ) č. 575/2013[46], smerniciach Európskeho parlamentu a Rady 2008/48/ES[47], 2009/138/ES[48], (EÚ) 2013/36/EÚ[49], 2014/17/EÚ[50] a (EÚ) 2016/97[51] určené v rámci svojich príslušných právomocí za príslušné orgány na účely dohľadu nad vykonávaním tohto nariadenia vrátane činností dohľadu nad trhom, pokiaľ ide o systémy AI, poskytované alebo používané regulovanými finančnými inštitúciami podliehajúcimi dohľadu, pokiaľ členské štáty nerozhodnú o určení iného orgánu na plnenie týchto úloh dohľadu nad trhom.

---

46 Nariadenie Európskeho parlamentu a Rady (EÚ) č. 575/2013 z 26. júna 2013 o prudenciálnych požiadavkách na úverové inštitúcie a investičné spoločnosti a o zmene nariadenia (EÚ) č. 648/2012 (Ú. v. EÚ L 176, 27.6.2013, s. 1).

47 Smernica Európskeho parlamentu a Rady 2008/48/ES z 23. apríla 2008 o zmluvách o spotrebiteľskom úvere a o zrušení smernice Rady 87/102/EHS (Ú. v. EÚ L 133, 22.5.2008, s. 66).

48 Smernica Európskeho parlamentu a Rady 2009/138/ES z 25. novembra 2009 o začatí a vykonávaní poistenia a zaistenia (Solventnosť II) (Ú. v. EÚ L 335, 17.12.2009, s. 1).

49 Smernica Európskeho parlamentu a Rady 2013/36/EÚ z 26. júna 2013 o prístupe k činnosti úverových inštitúcií a prudenciálnom dohľade nad úverovými inštitúciami a investičnými spoločnosťami, o zmene smernice 2002/87/ES a o zrušení smerníc 2006/48/ES a 2006/49/ES (Ú. v. EÚ L 176, 27.6.2013, s. 338).

50 Smernica Európskeho parlamentu a Rady 2014/17/EÚ zo 4. februára 2014 o zmluvách o úvere pre spotrebiteľov týkajúcich sa nehnuteľností určených na bývanie a o zmene smerníc 2008/48/ES a 2013/36/EÚ a nariadenia (EÚ) č. 1093/2010 (Ú. v. EÚ L 60, 28.2.2014, s. 34).

51 Smernica Európskeho parlamentu a Rady (EÚ) 2016/97 z 20. januára 2016 o distribúcii poistenia (Ú. v. EÚ L 26, 2.2.2016, s. 19).

Tieto príslušné orgány by mali mať všetky právomoci podľa tohto nariadenia a nariadenia (EÚ) 2019/1020 na presadzovanie požiadaviek a povinností vyplývajúcich z tohto nariadenia vrátane právomocí vykonávať ex post činnosti dohľadu nad trhom, ktoré možno podľa potreby začleniť do ich existujúcich mechanizmov a postupov dohľadu podľa príslušných právnych predpisov Únie v oblasti finančných služieb. Je vhodné stanoviť, že keď vnútroštátne orgány zodpovedné za dohľad nad úverovými inštitúciami regulovanými podľa smernice 2013/36/EÚ, ktoré sa zúčastňujú na jednotnom mechanizme dohľadu zriadenom nariadením Rady (EÚ) č. 1024/2013[52], konajú ako orgány dohľadu nad trhom podľa tohto nariadenia, mali by Európskej centrálnej banke bezodkladne oznamovať všetky informácie identifikované v priebehu svojich činností dohľadu nad trhom, ktoré môžu byť potenciálne zaujímavé pre úlohy Európskej centrálnej banky v oblasti prudenciálneho dohľadu, ako sa uvádza v uvedenom nariadení. Na účely ďalšieho zvýšenia jednotnosti medzi týmto nariadením a pravidlami platnými pre úverové inštitúcie regulované podľa smernice 2013/36/EÚ, je tiež vhodné integrovať niektoré procesné povinnosti poskytovateľov, pokiaľ ide o riadenie rizika, monitorovanie po uvedení na trh a dokumentáciu, do existujúcich povinností a postupov podľa smernice 2013/36/EÚ. Na zabránenie prekrývaniu by sa mali zvážiť aj obmedzené výnimky v súvislosti so systémom riadenia kvality poskytovateľov a s povinnosťou monitorovania uloženou subjektom nasadzujúcim vysokorizikové systémy AI, pokiaľ sa vzťahujú na úverové inštitúcie regulované smernicou 2013/36/EÚ. Rovnaký režim by sa mal uplatňovať na poisťovne a zaisťovne a holdingové poisťovne podľa smernice 2009/138/ES a sprostredkovateľov poistenia podľa smernice (EÚ) 2016/97 a ďalšie typy finančných inštitúcií, na ktoré sa vzťahujú požiadavky týkajúce sa vnútornej správy a riadenia, dojednaní alebo postupov podľa relevantného práva Únie v oblasti finančných služieb, s cieľom zaistiť jednotnosť a rovnaké zaobchádzanie vo finančnom sektore.

---

[52] Nariadenie Rady (EÚ) č. 1024/2013 z 15. októbra 2013, ktorým sa Európska centrálna banka poveruje osobitnými úlohami, pokiaľ ide o politiky týkajúce sa prudenciálneho dohľadu nad úverovými inštitúciami (Ú. v. EÚ L 287, 29.10.2013, s. 63).

(159) Každý orgán dohľadu nad trhom pre vysokorizikové systémy AI v oblasti biometrie uvedené v prílohe k tomuto nariadeniu, pokiaľ sa tieto systémy používajú na účely presadzovania práva, migrácie, azylu a riadenia kontroly hraníc, alebo na účely výkonu spravodlivosti a demokratických procesov, by mal mať účinné vyšetrovacie a nápravné právomoci vrátane aspoň právomoci získať prístup ku všetkým spracúvaným osobným údajom a ku všetkým informáciám potrebným na plnenie svojich úloh. Orgány dohľadu nad trhom by mali mať možnosť vykonávať svoje právomoci tak, že budú konať úplne nezávisle. Akýmikoľvek obmedzeniami ich prístupu k citlivým operačným údajom podľa tohto nariadenia by nemali byť dotknuté právomoci, ktoré im boli udelené smernicou (EÚ) 2016/680. Žiadne vylúčenie poskytovania údajov vnútroštátnym orgánom pre ochranu údajov podľa tohto nariadenia by nemalo mať vplyv na súčasné ani budúce právomoci týchto orgánov nad rámec rozsahu pôsobnosti tohto nariadenia.

(160) Orgány dohľadu nad trhom a Komisia by mali mať možnosť navrhovať spoločné činnosti vrátane spoločných vyšetrovaní, ktoré majú vykonávať orgány dohľadu nad trhom alebo orgány dohľadu nad trhom spoločne s Komisiou a ktorých cieľom je podpora dodržiavania predpisov, identifikácia nesúladu, zvyšovanie informovanosti a poskytovanie usmernení v súvislosti s týmto nariadením, pokiaľ ide o konkrétne kategórie vysokorizikových systémov AI, o ktorých sa zistilo, že predstavujú vážne riziko v dvoch alebo viacerých členských štátoch. Spoločné činnosti na podporu dodržiavania predpisov by sa mali vykonávať v súlade s článkom 9 nariadenia (EÚ) 2019/1020. Úrad pre AI by mal poskytovať koordinačnú podporu pre spoločné vyšetrovania.

(161) Je potrebné objasniť povinnosti a právomoci na úrovni Únie a na vnútroštátnej úrovni, pokiaľ ide o systémy AI, ktoré sú postavené na modeloch AI na všeobecné účely. Aby sa predišlo prekrývaniu právomocí, ak je systém AI založený na modeli AI na všeobecné účely a tento model a systém poskytuje ten istý poskytovateľ, dohľad by sa mal vykonávať na úrovni Únie prostredníctvom úradu pre AI, ktorý by mal mať na tento účel právomoci orgánu dohľadu nad trhom v zmysle nariadenia (EÚ) 2019/1020. Vo všetkých ostatných prípadoch sú za dohľad nad systémami AI naďalej zodpovedné vnútroštátne orgány dohľadu nad trhom. V prípade systémov AI na všeobecné účely, ktoré môžu nasadzujúce subjekty priamo používať aspoň na jeden účel, ktorý je klasifikovaný ako vysokorizikový, by však orgány dohľadu nad trhom mali spolupracovať s úradom pre AI s cieľom vykonávať hodnotenia dodržiavania predpisov a zodpovedajúcim spôsobom informovať radu pre AI a ostatné orgány dohľadu nad trhom. Okrem toho by orgány dohľadu nad trhom mali mať možnosť požiadať úrad pre AI o pomoc, ak orgán dohľadu nad trhom nie je schopný uzavrieť vyšetrovanie vysokorizikového systému AI z dôvodu, že nemá prístup k určitým informáciám týkajúcim sa modelu AI na všeobecné účely, na ktorom je vysokorizikový systém AI vybudovaný. V takýchto prípadoch by sa mal *mutatis mutandis* uplatňovať postup týkajúci sa vzájomnej pomoci v cezhraničných prípadoch uvedený v kapitole VI nariadenia (EÚ) 2019/1020.

(162) S cieľom čo najlepšie využiť centralizované odborné znalosti a synergie Únie na úrovni Únie by právomoci dohľadu a presadzovania povinností mali vo vzťahu k poskytovateľom modelov AI na všeobecné účely patriť do právomoci Komisie. Úrad pre AI by mal byť schopný vykonávať všetky potrebné opatrenia na monitorovanie účinného vykonávania tohto nariadenia, pokiaľ ide o modely AI na všeobecné účely. Mal by byť schopný vyšetrovať možné porušenia pravidiel týkajúcich sa poskytovateľov modelov AI na všeobecné účely z vlastnej iniciatívy, a to na základe výsledkov svojich monitorovacích činností alebo na žiadosť orgánov dohľadu nad trhom v súlade s podmienkami stanovenými v tomto nariadení. Na podporu účinného monitorovania by mal úrad pre AI umožniť nadväzujúcim poskytovateľom podávať sťažnosti na možné porušenia pravidiel týkajúcich sa poskytovateľov modelov a systémov AI na všeobecné účely.

(163) S cieľom doplniť systémy riadenia a správy modelov AI na všeobecné účely by mal vedecký panel podporovať monitorovacie činnosti úradu pre AI, pričom v určitých prípadoch môže úradu pre AI poskytovať kvalifikované upozornenia, ktoré povedú k následným opatreniam, ako sú vyšetrovania. Malo by tomu tak byť v prípade, keď má vedecký panel dôvodné podozrenie, že model AI na všeobecné účely predstavuje konkrétne a identifikovateľné riziko na úrovni Únie. Okrem toho by tomu tak malo byť v prípade, keď má vedecký panel dôvodné podozrenie, že model AI na všeobecné účely spĺňa kritériá, ktoré by viedli ku klasifikácii tohto modelu ako modelu AI na všeobecné účely so systémovým rizikom. S cieľom poskytnúť vedeckému panelu informácie potrebné na plnenie týchto úloh by mal existovať mechanizmus, prostredníctvom ktorého by vedecký panel mohol požiadať Komisiu, aby od poskytovateľa vyžadovala dokumentáciu alebo informácie.

(164) Úrad pre AI by mal mať možnosť prijímať potrebné opatrenia na monitorovanie účinného vykonávania a dodržiavania povinností poskytovateľov modelov AI na všeobecné účely stanovených v tomto nariadení. Úrad pre AI by mal mať možnosť vyšetrovať možné porušenia v súlade s právomocami stanovenými v tomto nariadení, a to aj vyžiadaním dokumentácie a informácií, vykonávaním hodnotení, ako aj požadovaním opatrení od poskytovateľov modelov AI na všeobecné účely. S cieľom využiť nezávislé odborné znalosti by mal mať úrad pre AI pri vykonávaní hodnotení možnosť zapojiť nezávislých expertov do vykonávania hodnotení v jeho mene. Dodržiavanie povinností by malo byť vynútiteľné okrem iného prostredníctvom žiadostí o prijatie vhodných opatrení vrátane opatrení na zmiernenie rizika v prípade identifikovaných systémových rizík, ako aj prostredníctvom obmedzenia sprístupňovania na trhu, stiahnutia modelu z trhu alebo stiahnutia modelu od používateľa. Ako záruka v prípade, že je to potrebné nad rámec procesných práv stanovených v tomto nariadení, by poskytovatelia modelov AI na všeobecné účely mali mať procesné práva stanovené v článku 18 nariadenia (EÚ) 2019/1020, ktoré by sa mali *mutatis mutandis* uplatňovať bez toho, aby boli dotknuté konkrétnejšie procesné práva stanovené v tomto nariadení.

(165) Vývoj systémov AI, ktoré nie sú vysokorizikové, v súlade s požiadavkami tohto nariadenia môže viesť k rozsiahlejšiemu zavádzaniu etickej a dôveryhodnej AI v Únii. Poskytovatelia systémov AI, ktoré nie sú vysokorizikové, by sa mali nabádať, aby vytvárali kódexy správania vrátane súvisiacich mechanizmov správy a riadenia s cieľom podporiť dobrovoľné uplatňovanie niektorých alebo všetkých povinných požiadaviek uplatniteľných na vysokorizikové systémy AI, prispôsobených zamýšľanému účelu systémov a nižšiemu súvisiacemu riziku a s prihliadnutím na dostupné technické riešenia a najlepšie odvetvové postupy, ako sú modely a dátové karty. Poskytovatelia všetkých vysokorizikových alebo nerizikových systémov a modelov AI a prípadne subjekty nasadzujúce takéto systémy a modely by sa tiež mali nabádať, aby dobrovoľne uplatňovali dodatočné požiadavky týkajúce sa napríklad prvkov únijných etických usmernení pre dôveryhodnú AI, environmentálnej udržateľnosti, opatrení týkajúcich sa gramotnosti v oblasti AI, inkluzívneho a rôznorodého dizajnu a vývoja systémov AI vrátane pozornosti venovanej zraniteľným osobám a prístupnosti pre osoby so zdravotným postihnutím, účasti zainteresovaných strán, podľa potreby za účasti relevantných zainteresovaných strán, ako sú podniky a organizácie občianskej spoločnosti, akademická obec a výskumné organizácie, odborové zväzy a organizácie na ochranu spotrebiteľa, pri navrhovaní a vývoji systémov AI, ako aj rozmanitosti vývojárskych tímov vrátane rodovej rovnováhy. Aby sa zabezpečila účinnosť dobrovoľných kódexov správania, mali by byť založené na jasných cieľoch a kľúčových ukazovateľoch výkonu na meranie dosahovania týchto cieľov. Mali by sa podľa potreby rozvíjať inkluzívnym spôsobom aj so zapojením relevantných zainteresovaných strán, ako sú podniky a organizácie občianskej spoločnosti, akademická obec a výskumné organizácie, odborové zväzy a organizácie na ochranu spotrebiteľa. Komisia môže vypracovať iniciatívy, a to aj odvetvovej povahy, na uľahčenie znižovania technických prekážok, ktoré bránia cezhraničnej výmene údajov na účely rozvoja AI, a to aj v oblasti infraštruktúry prístupu k údajom a sémantickej a technickej interoperability rôznych typov údajov.

(166) Je dôležité, aby systémy AI týkajúce sa výrobkov, ktoré v súlade s týmto nariadením nie sú vysokorizikové, a preto sa v súvislosti s nimi nevyžaduje, aby spĺňali požiadavky stanovené pre vysokorizikové systémy AI, však boli pri uvádzaní na trh alebo do prevádzky bezpečné. S cieľom prispieť k dosiahnutiu tohto cieľa by sa ako záchranná sieť uplatňovalo nariadenie Európskeho parlamentu a Rady (EÚ) 2023/988[53].

(167) V záujme zabezpečenia dôvernej a konštruktívnej spolupráce príslušných orgánov na úrovni Únie a vnútroštátnej úrovni by všetky strany zapojené do uplatňovania tohto nariadenia mali rešpektovať dôvernosť informácií a údajov získaných pri výkone svojich úloh v súlade s právom Únie a vnútroštátnym právom. Svoje úlohy a činnosti by mali vykonávať takým spôsobom, aby chránili najmä práva duševného vlastníctva, dôverné obchodné informácie a obchodné tajomstvo, účinné vykonávanie tohto nariadenia, verejné záujmy a záujmy národnej bezpečnosti, integritu trestného a správneho konania a integritu utajovaných skutočností.

---

[53] Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/988 z 10. mája 2023 o všeobecnej bezpečnosti výrobkov, ktorým sa mení nariadenie Európskeho parlamentu a Rady (EÚ) č. 1025/2012 a smernica Európskeho parlamentu a Rady (EÚ) 2020/1828 a zrušuje smernica Európskeho parlamentu a Rady 2001/95/ES a smernica Rady 87/357/EHS (Ú. v. EÚ L 135, 23.5.2023, s. 1).

(168) Dodržiavanie tohto nariadenia by malo byť vymáhateľné prostredníctvom ukladania sankcií a iných opatrení na presadzovanie práva. Členské štáty by mali prijať všetky opatrenia potrebné na zabezpečenie vykonávania ustanovení tohto nariadenia vrátane stanovenia účinných, primeraných a odrádzajúcich sankcií za ich porušenie a na dodržiavanie zásady *ne bis in idem*. S cieľom posilniť a harmonizovať správne sankcie za porušenie tohto nariadenia by sa mali ustanoviť horné hranice na stanovenie správnych pokút za určité konkrétne porušenia. Pri posudzovaní výšky pokút by členské štáty mali v každom jednotlivom prípade zohľadniť všetky relevantné okolnosti konkrétnej situácie s náležitým zreteľom najmä na povahu, závažnosť a trvanie porušenia a jeho dôsledky, ako aj na veľkosť poskytovateľa, najmä ak je poskytovateľom MSP alebo startup. Európsky dozorný úradník pre ochranu údajov by mal mať právomoc ukladať správne pokuty inštitúciám, agentúram a orgánom Únie, ktoré patria do rozsahu pôsobnosti tohto nariadenia.

(169) Dodržiavanie povinností poskytovateľov modelov AI na všeobecné účely uložených podľa tohto nariadenia by malo byť vymáhateľné okrem iného prostredníctvom pokút. Na tento účel by sa mali stanoviť aj primerané úrovne pokút za porušenie týchto povinností vrátane nedodržania opatrení požadovaných Komisiou v súlade s týmto nariadením, s výhradou primeraných premlčacích lehôt v súlade so zásadou proporcionality. Všetky rozhodnutia prijaté Komisiou podľa tohto nariadenia môže preskúmať Súdny dvor Európskej únie v súlade so ZFEÚ vrátane neobmedzenej právomoci Súdneho dvora, pokiaľ ide o sankcie podľa článku 261 ZFEÚ.

(170) V práve Únie a vo vnútroštátnom práve sa už stanovujú účinné prostriedky nápravy pre fyzické a právnické osoby, ktorých práva a slobody sú nepriaznivo ovplyvnené používaním systémov AI. Bez toho, aby boli dotknuté tieto prostriedky nápravy, každá fyzická alebo právnická osoba, ktorá má dôvody domnievať sa, že došlo k porušeniu tohto nariadenia, by mala byť oprávnená podať sťažnosť príslušnému orgánu dohľadu nad trhom.

(171) Dotknuté osoby by mali mať právo dostať o vysvetlenie, keď sa rozhodnutie nasadzujúceho subjektu zakladá hlavne na výstupe z určitých vysokorizikových systémov AI, ktoré patria do rozsahu pôsobnosti tohto nariadenia, a keď má toto rozhodnutie právne účinky alebo podobne významne ovplyvňuje uvedené osoby spôsobom, ktorý podľa nich nepriaznivo ovplyvňuje ich zdravie, bezpečnosť alebo základné práva. Uvedené vysvetlenie by malo byť jasné a zmysluplné a malo by dotknutým osobám poskytnúť základ na uplatňovanie ich práv. Právo na vysvetlenie by sa nemalo vzťahovať na používanie systémov AI, pre ktoré z práva Únie alebo vnútroštátneho práva vyplývajú výnimky alebo obmedzenia, a malo by sa uplatňovať len v rozsahu, v akom toto právo ešte nie je stanovené v právnych predpisoch Únie.

(172) Osoby nahlasujúce porušenia tohto nariadenia by mali byť chránené podľa práva Únie. Na nahlasovanie porušení tohto nariadenia a na ochranu osôb nahlasujúcich tieto porušenia by sa preto mala vzťahovať smernica Európskeho parlamentu a Rady (EÚ) 2019/1937[54].

[54] Smernica Európskeho parlamentu a Rady (EÚ) 2019/1937 z 23. októbra 2019 o ochrane osôb, ktoré nahlasujú porušenia práva Únie (Ú. v. EÚ L 305, 26.11.2019, s. 17).

(173) S cieľom zabezpečiť, aby sa regulačný rámec mohol v prípade potreby upraviť, by sa mala na Komisiu delegovať právomoc prijímať akty v súlade s článkom 290 ZFEÚ na účely zmeny podmienok, za ktorých sa systém AI nemá považovať za vysokorizikový, zoznamu vysokorizikových systémov AI, ustanovení týkajúcich sa technickej dokumentácie, obsahu EÚ vyhlásenia o zhode, ustanovení týkajúcich sa postupov posudzovania zhody, ustanovení, ktorými sa stanovujú vysokorizikové systémy AI, na ktoré by sa mal vzťahovať postup posudzovania zhody založený na posúdení systému riadenia kvality a posúdení technickej dokumentácie, prahovej hodnoty, referenčných hodnôt a ukazovateľov, a to aj doplnením týchto referenčných hodnôt a ukazovateľov, v pravidlách pre klasifikáciu modelov AI na všeobecné účely so systémovým rizikom, kritérií označovania modelov AI na všeobecné účely so systémovým rizikom, technickej dokumentácie pre poskytovateľov modelov AI na všeobecné účely a transparentnosti informácií pre poskytovateľov modelov AI na všeobecné účely. Je osobitne dôležité, aby Komisia počas prípravných prác uskutočnila príslušné konzultácie, a to aj na úrovni expertov, a aby tieto konzultácie vykonávala v súlade so zásadami stanovenými v Medziinštitucionálnej dohode z 13. apríla 2016 o lepšej tvorbe práva[55]. Predovšetkým v záujme rovnakého zastúpenia pri príprave delegovaných aktov sa všetky dokumenty doručujú Európskemu parlamentu a Rade v rovnakom čase ako expertom z členských štátov, a experti Európskeho parlamentu a Rady majú systematicky prístup na zasadnutia skupín expertov Komisie, ktoré sa zaoberajú prípravou delegovaných aktov.

[55] Ú. v. EÚ L 123, 12.5.2016, s. 1.

(174) Vzhľadom na rýchly technologický vývoj a technické odborné znalosti potrebné na účinné uplatňovanie tohto nariadenia by Komisia mala toto nariadenie vyhodnotiť a preskúmať do ... [päť rokov odo dňa nadobudnutia účinnosti tohto nariadenia] a potom každé štyri roky a podať správu Európskemu parlamentu a Rade. Okrem toho, berúc do úvahy dôsledky pre rozsah pôsobnosti tohto nariadenia, by Komisia mala raz ročne posúdiť potrebu zmeniť zoznam vysokorizikových systémov AI a zoznam zakázaných praktík. Komisia by taktiež mala do ... [štyri roky odo dňa nadobudnutia účinnosti tohto nariadenia] a potom každé štyri roky vyhodnotiť potrebu zmeniť zoznam položiek vysokorizikových oblastí v prílohe k tomuto nariadeniu, systémy AI v rozsahu povinností týkajúcich sa transparentnosti, účinnosť systému dohľadu a správy a riadenia a pokrok vo vývoji normalizačných produktov týkajúcich sa energeticky efektívneho vývoja modelov AI na všeobecné účely vrátane potreby ďalších opatrení alebo krokov, a podať o tom správu Európskemu parlamentu a Rade. Komisia by mala do ... [štyri roky odo dňa nadobudnutia účinnosti tohto nariadenia] a potom každé tri roky vyhodnotiť vplyv a efektívnosť dobrovoľných kódexov správania na podporu uplatňovania požiadaviek stanovených pre vysokorizikové systémy AI v prípade systémov AI, ktoré nie sú vysokorizikové, a prípadne ďalších dodatočných požiadaviek na takéto systémy AI.

(175) S cieľom zabezpečiť jednotné podmienky vykonávania tohto nariadenia by sa mali na Komisiu preniesť vykonávacie právomoci. Uvedené právomoci by sa mali vykonávať v súlade s nariadením Európskeho parlamentu a Rady (EÚ) č. 182/2011[56].

(176) Keďže cieľ tohto nariadenia, a to zlepšiť fungovanie vnútorného trhu a podporovať zavádzanie dôveryhodnej AI sústredenej na človeka a súčasne zabezpečiť vysokú úroveň ochrany zdravia, bezpečnosti, základných práv zakotvených v charte vrátane demokracie, právneho štátu a ochranu životného prostredia pred škodlivými účinkami systémov AI v Únii, a zároveň podporovať inovácie, nie je možné uspokojivo dosiahnuť na úrovni členských štátov a z dôvodu rozsahu alebo dôsledkov činnosti ho možno lepšie dosiahnuť na úrovni Únie, môže Únia prijať opatrenia v súlade so zásadou subsidiarity podľa článku 5 Zmluvy o EÚ. V súlade so zásadou proporcionality podľa uvedeného článku toto nariadenie neprekračuje rámec nevyhnutný na dosiahnutie tohto cieľa.

---

[56] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 182/2011 zo 16. februára 2011, ktorým sa ustanovujú pravidlá a všeobecné zásady mechanizmu, na základe ktorého členské štáty kontrolujú vykonávanie vykonávacích právomocí Komisie (Ú. v. EÚ L 55, 28.2.2011, s. 13).

(177) S cieľom zabezpečiť právnu istotu a primerané adaptačné obdobie pre prevádzkovateľov a zabrániť narušeniu trhu, a to aj zabezpečením kontinuity používania systémov AI, je vhodné, aby sa toto nariadenie uplatňovalo na vysokorizikové systémy AI, ktoré boli uvedené na trh alebo do prevádzky pred všeobecným dňom začatia jeho uplatňovania, len ak od uvedeného dňa dizajn alebo zamýšľaný účel týchto systémov prešli významnými zmenami. Je vhodné spresniť, že v tejto súvislosti by sa pojem významnej zmeny mal vykladať tak, že je vo svojej podstate rovnocenný s pojmom podstatnej zmeny, ktorý sa používa len v súvislosti s vysokorizikovými systémami AI podľa tohto nariadenia. Výnimočne a vzhľadom na verejnú zodpovednosť by prevádzkovatelia systémov AI, ktoré sú komponentmi rozsiahlych informačných systémov zriadených právnymi aktmi uvedenými v prílohe k tomuto nariadeniu, a prevádzkovatelia vysokorizikových systémov AI, ktoré majú používať orgány verejnej moci, mali prijať potrebné kroky na dosiahnutie súladu s požiadavkami tohto nariadenia do konca roka 2030 a do ... [šesť rokov odo dňa nadobudnutia účinnosti tohto nariadenia].

(178) Poskytovatelia vysokorizikových systémov AI sa vyzývajú, aby dobrovoľne začali plniť príslušné povinnosti stanovené v tomto nariadení už počas prechodného obdobia.

(179) Toto nariadenie by sa malo uplatňovať … [dva roky odo dňa nadobudnutia účinnosti tohto nariadenia]. Vzhľadom na neprijateľné riziko spojené s používaním AI určitými spôsobmi by sa však zákazy, ako aj všeobecné ustanovenia tohto nariadenia, mali uplatňovať už od ... [šesť mesiacov odo dňa nadobudnutia účinnosti tohto nariadenia]. Zatiaľ čo plný účinok týchto zákazov vyplýva zo zavedenia správy a riadenia a presadzovania tohto nariadenia, je dôležité predpokladať uplatňovanie zákazov, aby sa zohľadnili neprijateľné riziká a aby sa dosiahol vplyv na iné postupy, napríklad v občianskom práve. Taktiež platí, že infraštruktúra súvisiaca so správou a riadením a so systémom posudzovania zhody by však mala byť funkčná pred ... [dva roky odo dňa nadobudnutia účinnosti tohto nariadenia], a preto by sa ustanovenia o notifikovaných osobách a štruktúre správy a riadenia mali uplatňovať od ... [12 mesiacov odo dňa nadobudnutia účinnosti tohto nariadenia]. Vzhľadom na rýchle tempo technologického pokroku a prijímanie modelov AI na všeobecné účely by sa povinnosti poskytovateľov modelov AI na všeobecné účely mali začať uplatňovať od ... [12 mesiacov odo dňa nadobudnutia účinnosti tohto nariadenia]. Kódexy postupov by mali byť pripravené do ... [deväť mesiacov odo dňa nadobudnutia účinnosti tohto nariadenia], aby sa poskytovateľom umožnilo včas preukázať plnenie predpisov. Úrad pre AI by mal zabezpečiť, aby pravidlá a postupy klasifikácie boli aktuálne vzhľadom na technologický vývoj. Okrem toho by členské štáty mali stanoviť pravidlá týkajúce sa sankcií vrátane správnych pokút, oznámiť ich Komisii a zabezpečiť ich riadne a účinné vykonávanie do dátumu začatia uplatňovania tohto nariadenia. Ustanovenia o sankciách by sa preto mali začať uplatňovať od ... [12 mesiacov odo dňa nadobudnutia účinnosti tohto nariadenia].

(180) V súlade s článkom 42 ods. 1 a 2 nariadenia (EÚ) 2018/1725 sa konzultovalo s európskym dozorným úradníkom pre ochranu údajov a s Európskym výborom na ochranu údajov, ktorí 18. júna 2021 vydali svoje spoločné stanovisko,

PRIJALI TOTO NARIADENIE:

Kapitola I
Všeobecné ustanovenia

Článok 1

Predmet úpravy

1. Účelom tohto nariadenia je zlepšiť fungovanie vnútorného trhu a podporiť zavádzanie dôveryhodnej umelej inteligencie (ďalej len „AI“) sústredenej na človeka, a pritom zabezpečiť vysokú úroveň ochrany zdravia, bezpečnosti, základných práv zakotvených v charte vrátane demokracie, právneho štátu a ochrany životného prostredia pred škodlivými účinkami systémov AI v Únii a podporovať inovácie.

2. V tomto nariadení sa stanovujú:

   a) harmonizované pravidlá uvádzania na trh, uvádzania do prevádzky a používania systémov AI v Únii;

   b) zákazy určitých praktík využívajúcich AI;

   c) osobitné požiadavky na vysokorizikové systémy AI a povinnosti prevádzkovateľov takýchto systémov;

   d) harmonizované pravidlá transparentnosti pre určité systémy AI;

   e) harmonizované pravidlá uvádzania modelov AI na všeobecné účely na trh;

f) pravidlá monitorovania trhu, dohľadu nad trhom, správy a riadenia a presadzovania;

g) opatrenia na podporu inovácií s osobitným dôrazom na MSP vrátane startupov.

Článok 2

Rozsah pôsobnosti

1. Toto nariadenie sa vzťahuje na:

a) poskytovateľov, ktorí v Únii uvádzajú na trh alebo do prevádzky systémy AI alebo uvádzajú na trh modely AI na všeobecné účely, bez ohľadu na to, či sú títo poskytovatelia usadení alebo sa nachádzajú v Únii alebo v tretej krajine;

b) subjekty nasadzujúce systémy AI, ktoré majú miesto usadenia alebo sa nachádzajú v Únii;

c) poskytovateľov systémov AI a subjekty nasadzujúce systémy AI, ktoré majú miesto usadenia alebo sa nachádzajú v tretej krajine, ak sa výstup vytvorený systémom AI používa v Únii;

d) dovozcov a distribútorov systémov AI;

e) výrobcov výrobkov, ktorí uvádzajú na trh alebo do prevádzky systém AI spolu so svojím výrobkom a pod vlastným menom alebo ochrannou známkou;

f) splnomocnených zástupcov poskytovateľov, ktorí nie sú usadení v Únii;

g) dotknuté osoby, ktoré sa nachádzajú v Únii.

2. Na systémy AI klasifikované v súlade s článkom 6 ods. 1 ako vysokorizikové systémy AI súvisiace s výrobkami, na ktoré sa vzťahujú harmonizačné právne predpisy Únie uvedené v prílohe I oddiele B, sa uplatňuje len článok 6 ods. 1, články 102 až 109 a článok 112. Článok 57 sa uplatňuje len v rozsahu, v akom boli požiadavky na vysokorizikové systémy AI podľa tohto nariadenia začlenené do uvedených harmonizačných právnych predpisov Únie.

3. Toto nariadenie sa neuplatňuje na oblasti mimo rozsahu pôsobnosti práva Únie a v žiadnom prípade nemá vplyv na právomoci členských štátov týkajúce sa národnej bezpečnosti, a to bez ohľadu na typ subjektu, ktorý členské štáty poverili vykonávaním úloh v súvislosti s týmito právomocami.

Toto nariadenie sa neuplatňuje na systémy AI, ak a pokiaľ sa uvádzajú na trh, uvádzajú do prevádzky alebo sa používajú, či už upravené alebo nie, výlučne na vojenské alebo obranné účely alebo na účely národnej bezpečnosti, a to bez ohľadu na typ subjektu vykonávajúceho tieto činnosti.

Toto nariadenie sa neuplatňuje na systémy AI, ktoré sa neuvádzajú na trh ani do prevádzky v Únii, ak sa výstup používa v Únii výlučne na vojenské alebo obranné účely alebo na účely národnej bezpečnosti, a to bez ohľadu na typ subjektu vykonávajúceho tieto činnosti.

4. Toto nariadenie sa neuplatňuje na orgány verejnej moci v tretej krajine ani na medzinárodné organizácie, ktoré podľa odseku 1 patria do rozsahu pôsobnosti tohto nariadenia, ak tieto orgány alebo organizácie používajú systémy AI v rámci medzinárodných dohôd o spolupráci alebo dohôd o presadzovaní práva a justičnej spolupráci s Úniou alebo s jedným alebo viacerými členskými štátmi, pod podmienkou, že táto tretia krajina alebo medzinárodná organizácia poskytuje primerané záruky, pokiaľ ide o ochranu základných práv a slobôd jednotlivcov.

5. Týmto nariadením nie je dotknuté uplatňovanie ustanovení o zodpovednosti poskytovateľov sprostredkovateľských služieb uvedených v kapitole II nariadenia (EÚ) 2022/2065.

6. Toto nariadenie sa neuplatňuje na systémy alebo modely AI vrátane ich výstupov, ktoré sú osobitne vyvinuté a uvedené do prevádzky výlučne na účely vedeckého výskumu a vývoja.

7. Na osobné údaje spracúvané v súvislosti s právami a povinnosťami stanovenými v tomto nariadení sa vzťahuje právo Únie o ochrane osobných údajov, súkromia a dôvernosti komunikácie. Toto nariadenie nemá vplyv na nariadenie (EÚ) 2016/679 či (EÚ) 2018/1725, ani na smernicu 2002/58/ES alebo (EÚ) 2016/680 bez toho, aby bol dotknutý článok 10 ods. 5 a článok 59 tohto nariadenia.

8. Toto nariadenie sa neuplatňuje na žiadnu výskumnú, testovaciu ani vývojovú činnosť týkajúcu sa systémov AI alebo modelov AI pred ich uvedením na trh alebo do prevádzky. Takéto činnosti sa vykonávajú v súlade s uplatniteľným právom Únie. Toto vylúčenie sa nevzťahuje na testovanie v reálnych podmienkach.

9. Týmto nariadením nie sú dotknuté pravidlá stanovené v iných právnych aktoch Únie týkajúcich sa ochrany spotrebiteľa a bezpečnosti výrobkov.

10. Toto nariadenie sa neuplatňuje na povinnosti nasadzujúcich subjektov, ktoré sú fyzickými osobami používajúcimi systémy AI v rámci čisto osobnej neprofesionálnej činnosti.

11. Toto nariadenie nebráni Únii ani členským štátom v tom, aby zachovali v platnosti alebo prijali zákony, iné právne predpisy alebo správne opatrenia, ktoré sú pre pracovníkov priaznivejšie z hľadiska ochrany ich práv v súvislosti s používaním systémov AI zamestnávateľmi, alebo aby podporovali alebo umožňovali uplatňovanie kolektívnych zmlúv, ktoré sú pre pracovníkov priaznivejšie.

12. Toto nariadenie sa neuplatňuje na systémy AI vydané na základe bezplatných licencií s otvoreným zdrojovým kódom, pokiaľ nie sú uvedené na trh alebo do prevádzky ako vysokorizikové systémy AI alebo ako systém AI, na ktorý sa vzťahuje článok 5 alebo článok 50.

Článok 3

Vymedzenie pojmov

Na účely tohto nariadenia sa uplatňuje toto vymedzenie pojmov:

1. „systém AI“ je strojový systém, ktorý je dizajnovaný na prevádzku s rôznymi úrovňami autonómnosti, ktorý môže po nasadení prejavovať adaptabilitu a ktorý pre explicitné alebo implicitné ciele odvodzuje zo vstupov, ktoré dostáva, spôsob generovania výstupov, ako sú predpovede, obsah, odporúčania alebo rozhodnutia, ktoré môžu ovplyvniť fyzické alebo virtuálne prostredie;

2. „riziko“ je kombinácia pravdepodobnosti výskytu ujmy a závažnosti tejto ujmy;

3. „poskytovateľ“ je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý vyvíja systém AI alebo model AI na všeobecné účely alebo ktorý si dáva vyvinúť systém AI alebo model AI na všeobecné účely a uvádza ho na trh alebo uvádza systém AI do prevádzky pod svojím vlastným menom alebo ochrannou známkou, či už za odplatu alebo bezodplatne;

4. „nasadzujúci subjekt“ je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý používa systém AI v rámci svojej právomoci, s výnimkou prípadov, keď sa systém AI používa v rámci osobnej neprofesionálnej činnosti;

5. „splnomocnený zástupca“ je fyzická alebo právnická osoba nachádzajúca sa alebo usadená v Únii, ktorá od poskytovateľa systému AI alebo modelu AI na všeobecné účely dostala a akceptovala písomné splnomocnenie plniť v jeho mene povinnosti a vykonávať postupy stanovené týmto nariadením;

6. „dovozca“ je fyzická alebo právnická osoba nachádzajúca sa alebo usadená v Únii, ktorá uvádza na trh systém AI, ktorý je označený menom alebo ochrannou známkou fyzickej alebo právnickej osoby usadenej v tretej krajine;

7. „distribútor“ je fyzická alebo právnická osoba v dodávateľskom reťazci okrem poskytovateľa alebo dovozcu, ktorá na trhu Únie sprístupňuje systém AI;

8. „prevádzkovateľ“ je poskytovateľ, výrobca výrobku, nasadzujúci subjekt, splnomocnený zástupca, dovozca alebo distribútor;

9. „uvedenie na trh“ je prvé sprístupnenie systému AI alebo modelu AI na všeobecné účely na trhu Únie;

10. „sprístupnenie na trhu“ je dodanie systému AI alebo modelu AI na všeobecné účely s cieľom distribuovať ho alebo používať ho na trhu Únie v rámci komerčnej činnosti, či už za odplatu alebo bezodplatne;

11. „uvedenie do prevádzky“ je dodanie systému AI na prvé použitie priamo nasadzujúcemu subjektu alebo na vlastné použitie v Únii na jeho zamýšľaný účel;

12. „zamýšľaný účel“ je použitie, na ktoré systém AI určil poskytovateľ vrátane konkrétneho kontextu a podmienok používania, ako sa uvádza v informáciách od poskytovateľa v návode na použitie, v propagačných alebo predajných materiáloch a vyhláseniach, ako aj v technickej dokumentácii;

13. „odôvodnene predvídateľné nesprávne použitie“ je také použitie systému AI, ktoré nie je v súlade so zamýšľaným účelom, ale ktoré môže byť výsledkom odôvodnene predvídateľného ľudského správania alebo interakcie s inými systémami vrátane iných systémov AI;

14. „bezpečnostný komponent“ je komponent výrobku alebo systému AI, ktorý pre daný výrobok alebo systém AI plní bezpečnostnú funkciu alebo ktorého zlyhanie alebo porucha ohrozuje zdravie a bezpečnosť osôb alebo majetku;

15. „návod na použitie“ sú informácie, ktoré poskytuje poskytovateľ s cieľom informovať nasadzujúci subjekt najmä o zamýšľanom účele a správnom používaní systému AI;

16. „stiahnutie systému AI od používateľa“ je každé opatrenie, ktorého cieľom je dosiahnutie navrátenia systému AI, ktorý sa sprístupnil nasadzujúcim subjektom, poskytovateľovi alebo jeho stiahnutie z prevádzky, alebo znemožnenie jeho používania;

17. „stiahnutie systému AI z trhu“ je každé opatrenie, ktorého cieľom je zabrániť, aby sa systém AI, ktorý sa nachádza v dodávateľskom reťazci, sprístupnil na trhu;

18. „výkon systému AI“ je schopnosť systému AI dosiahnuť jeho zamýšľaný účel;

19. „notifikujúci orgán“ je vnútroštátny orgán zodpovedný za stanovenie a vykonávanie nevyhnutných postupov na posudzovanie, určovanie a notifikáciu orgánov posudzovania zhody a za ich monitorovanie;

20. „posudzovanie zhody“ je postup preukázania, či boli splnené požiadavky stanovené v kapitole III oddiele 2 týkajúce sa vysokorizikového systému AI;

21. „orgán posudzovania zhody“ je orgán, ktorý ako tretia strana vykonáva činnosti posudzovania zhody vrátane skúšania, certifikácie a kontroly;

22. „notifikovaná osoba“ je orgán posudzovania zhody notifikovaný v súlade s týmto nariadením a inými relevantnými harmonizačnými právnymi predpismi Únie;

23. „podstatná zmena“ je zmena systému AI po jeho uvedení na trh alebo do prevádzky, ktorú poskytovateľ v počiatočnom posudzovaní zhody nepredpokladal ani neplánoval a v dôsledku ktorej je ovplyvnený súlad systému AI s požiadavkami stanovenými v kapitole III oddiele 2 alebo ktorá vedie k zmene zamýšľaného účelu, z hľadiska ktorého bol systém AI posudzovaný;

24. „označenie CE“ je označenie, ktorým poskytovateľ vyjadruje, že systém AI je v zhode s požiadavkami stanovenými v kapitole III oddiele 2 a v iných uplatniteľných harmonizačných právnych predpisoch Únie, v ktorých sa stanovuje umiestňovanie tohto označenia;

25. „systém monitorovania po uvedení na trh“ sú všetky činnosti, ktoré vykonávajú poskytovatelia systémov AI na zhromažďovanie a skúmanie skúseností získaných z používania systémov AI, ktoré uvádzajú na trh alebo do prevádzky, a to na účely zisťovania akejkoľvek potreby okamžite uplatniť všetky potrebné nápravné či preventívne opatrenia;

26. „orgán dohľadu nad trhom“ je vnútroštátny orgán, ktorý vykonáva činnosti a prijíma opatrenia podľa nariadenia (EÚ) 2019/1020;

27. „harmonizovaná norma“ je harmonizovaná norma v zmysle vymedzenia v článku 2 bode 1 písm. c) nariadenia (EÚ) č. 1025/2012;

28. „spoločná špecifikácia“ je súbor technických špecifikácií v zmysle vymedzenia v článku 2 bode 4 nariadenia (EÚ) č. 1025/2012, ktorý predstavuje prostriedok na dosiahnutie súladu s určitými požiadavkami stanovenými v tomto nariadení;

29. „trénovacie údaje“ sú údaje, ktoré sa používajú na trénovanie systému AI adaptáciou jeho parametrov, ktoré sa dajú naučiť;

30. „validačné údaje“ sú údaje, ktoré sa používajú na vyhodnotenie natrénovaného systému AI a na doladenie jeho parametrov, ktoré sa nedajú naučiť, a jeho procesu učenia, okrem iného s cieľom zabrániť podtrénovaniu alebo pretrénovaniu;

31. „validačný súbor údajov“ je samostatný súbor údajov alebo časť súboru trénovacích údajov, a to buď ako pevné alebo variabilné rozdelenie;

32. „testovacie údaje“ sú údaje, ktoré sa používajú na nezávislé hodnotenie systému AI s cieľom potvrdiť očakávaný výkon tohto systému pred jeho uvedením na trh alebo do prevádzky;

33. „vstupné údaje“ sú údaje poskytnuté systému AI alebo priamo získané týmto systémom, na základe ktorých systém vytvára výstup;

34. „biometrické údaje“ sú osobné údaje, ktoré sú výsledkom osobitného technického spracúvania týkajúceho sa fyzických, fyziologických alebo behaviorálnych charakteristických znakov fyzickej osoby, ako sú podoby tváre alebo daktyloskopické údaje;

35. „biometrická identifikácia“ je automatizované rozpoznávanie fyzických, fyziologických, behaviorálnych alebo psychologických znakov človeka na účely stanovenia totožnosti fyzickej osoby porovnaním biometrických údajov daného jednotlivca s biometrickými údajmi jednotlivcov uloženými v databáze;

36. „biometrické overenie“ je automatizované overenie totožnosti fyzických osôb porovnaním ich biometrických údajov s biometrickými údajmi, ktoré boli poskytnuté skôr, spočívajúce v porovnaní jedného údaja s príslušným druhým údajom vrátane autentifikácie;

37. „osobitné kategórie osobných údajov“ sú kategórie osobných údajov uvedené v článku 9 ods. 1 nariadenia (EÚ) 2016/679, článku 10 smernice (EÚ) 2016/680 a článku 10 ods. 1 nariadenia (EÚ) 2018/1725;

38. „citlivé operačné údaje“ sú operačné údaje súvisiace s činnosťami predchádzania trestným činom, ich odhaľovania, vyšetrovania alebo stíhania, ktorých zverejnenie by mohlo ohroziť integritu trestného konania;

39. „systém na rozpoznávanie emócií“ je systém AI na účely identifikácie alebo odvodenia emócií alebo úmyslov fyzických osôb na základe ich biometrických údajov;

40. „systém biometrickej kategorizácie“ je systém AI na účely zaraďovania fyzických osôb do špecifických kategórií na základe ich biometrických údajov, pokiaľ to nie je pomocný úkon pre inú komerčnú službu a nevyhnutne potrebné z objektívnych technických dôvodov;

41. „systém diaľkovej biometrickej identifikácie“ je systém AI na účely identifikácie fyzických osôb bez ich aktívneho zapojenia, zvyčajne na diaľku prostredníctvom porovnania biometrických údajov osoby s biometrickými údajmi obsiahnutými v referenčnej databáze;

42. „systém diaľkovej biometrickej identifikácie v reálnom čase“ je systém diaľkovej biometrickej identifikácie, v ktorom zachytávanie biometrických údajov, ich porovnávanie a identifikácia prebiehajú bez výrazného oneskorenia, pričom zahŕňa nielen okamžitú identifikáciu, ale aj identifikáciu s limitovanými menšími oneskoreniami, aby sa zabránilo obchádzaniu pravidiel;

43. „systém následnej diaľkovej biometrickej identifikácie“ je systém diaľkovej biometrickej identifikácie, ktorý nie je systémom diaľkovej biometrickej identifikácie v reálnom čase;

44. „verejne prístupný priestor“ je akékoľvek fyzické miesto vo verejnom alebo v súkromnom vlastníctve prístupné neurčenému počtu fyzických osôb bez ohľadu na to, či možno uplatniť určité podmienky prístupu, a bez ohľadu na možné obmedzenia kapacity;

45. „orgán presadzovania práva“ je:

a) každý orgán verejnej moci príslušný v oblasti predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania, alebo v oblasti výkonu trestných sankcií vrátane ochrany pred ohrozením verejnej bezpečnosti a predchádzania takémuto ohrozeniu, alebo

b) každý iný orgán alebo subjekt, ktorý bol právom členského štátu poverený vykonávať verejnú moc a verejné právomoci na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií vrátane ochrany pred ohrozením verejnej bezpečnosti a predchádzania takémuto ohrozeniu;

46. „presadzovanie práva“ sú činnosti vykonávané orgánmi presadzovania práva alebo v ich mene na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania, alebo na účely výkonu trestných sankcií vrátane ochrany pred ohrozením verejnej bezpečnosti a predchádzania takémuto ohrozeniu;

47. „úrad pre AI“ je úloha Komisie prispievať k vykonávaniu, monitorovaniu a dohľadu nad systémami AI a modelmi AI na všeobecné účely a k správe a riadeniu AI stanovená v rozhodnutí Komisie z 24. januára 2024; odkazy v tomto nariadení na úrad pre AI sa považujú za odkazy na Komisiu;

48. „vnútroštátny príslušný orgán“ je notifikujúci orgán alebo orgán dohľadu nad trhom; pokiaľ ide o systémy AI uvedené do prevádzky alebo používané inštitúciami, orgánmi, úradmi a agentúrami Únie, odkazy na príslušné vnútroštátne orgány alebo orgány dohľadu nad trhom v tomto nariadení sa považujú za odkazy na európskeho dozorného úradníka pre ochranu údajov;

49. „závažný incident“ je incident alebo porucha systému AI, ktoré priamo alebo nepriamo vyústia do ktorejkoľvek z týchto situácií:

a) smrť osoby alebo vážna ujma na zdraví osoby;

b) vážne a nezvratné narušenie riadenia alebo prevádzky kritickej infraštruktúry;

c) porušenie povinností vyplývajúcich z práva Únie, ktorých cieľom je ochrana základných práv;

d) vážna ujma na majetku alebo životnom prostredí;

50. „osobné údaje“ sú osobné údaje v zmysle vymedzenia v článku 4 bode 1 nariadenia (EÚ) 2016/679;

51. „iné ako osobné údaje“ sú údaje iné než osobné údaje v zmysle vymedzenia v článku 4 bode 1 nariadenia (EÚ) 2016/679;

52. „profilovanie“ je profilovanie v zmysle vymedzenia v článku 4 bode 4 nariadenia (EÚ) 2016/679;

53. „plán testovania v reálnych podmienkach“ je dokument, v ktorom sa opisujú ciele, metodika, geografický, populačný a časový rozsah, monitorovanie, organizácia a vykonávanie testovania v reálnych podmienkach;

54. „plán experimentálneho prostredia“ je dokument dohodnutý medzi zúčastneným poskytovateľom a príslušným orgánom, v ktorom sa opisujú ciele, podmienky, časový rámec, metodika a požiadavky na činnosti vykonávané v rámci experimentálneho prostredia;

55. „regulačné experimentálne prostredie pre AI“ je kontrolovaný rámec zriadený príslušným orgánom, ktorý poskytovateľom alebo potenciálnym poskytovateľom systémov AI ponúka možnosť vyvíjať, trénovať, validovať a testovať, v relevantnom prípade aj v reálnych podmienkach, inovačný systém AI podľa plánu experimentálneho prostredia na obmedzený čas pod regulačným dohľadom;

56. „gramotnosť v oblasti AI“ sú zručnosti, vedomosti a pochopenie, ktoré poskytovateľom, nasadzujúcim subjektom a dotknutým osobám umožňujú s ohľadom na ich príslušné práva a povinnosti v kontexte tohto nariadenia informovane nasadzovať systémy AI, ako aj získať povedomie o príležitostiach a rizikách AI a o prípadnej ujme, ktorú môže spôsobiť;

57. „testovanie v reálnych podmienkach“ je dočasné testovanie systému AI na jeho zamýšľaný účel v reálnych podmienkach mimo laboratória alebo inak simulovaného prostredia s cieľom zhromaždiť spoľahlivé a robustné údaje a posúdiť a overiť zhodu systému AI s požiadavkami tohto nariadenia a nepovažuje sa za uvedenie systému AI na trh alebo do prevádzky v zmysle tohto nariadenia za predpokladu, že sú splnené všetky podmienky stanovené v článku 57 alebo 60;

58. „účastník“ na účely testovania v reálnych podmienkach je fyzická osoba, ktorá sa zúčastňuje na testovaní v reálnych podmienkach;

59. „informovaný súhlas“ je slobodne poskytnuté, konkrétne, jednoznačné a dobrovoľné vyjadrenie vôle účastníka zúčastniť sa na konkrétnom testovaní v reálnych podmienkach, a to po tom, ako bol informovaný o všetkých aspektoch testovania, ktoré sú relevantné pre jeho rozhodnutie zúčastniť sa;

60. „deep fake“ je obrazový obsah, audioobsah alebo videoobsah vytvorený alebo zmanipulovaný pomocou AI, ktorý sa podobá na existujúce osoby, objekty, miesta, subjekty alebo udalosti a osobe by sa falošne javil ako autentický alebo pravdivý;

61. „rozsiahle porušovanie právnych predpisov“ je každé konanie alebo opomenutie v rozpore s právom Únie na ochranu záujmov jednotlivcov, ktoré:

a) spôsobilo alebo pravdepodobne spôsobí ujmu na kolektívnych záujmoch jednotlivcov s pobytom najmenej v dvoch iných členských štátoch, než je členský štát, v ktorom:

i) takéto konanie alebo opomenutie malo pôvod alebo sa uskutočnilo;

ii) sa nachádza alebo je usadený dotknutý poskytovateľ alebo v relevantnom prípade jeho splnomocnený zástupca; alebo

iii) je usadený nasadzujúci subjekt v čase, keď sa tento nasadzujúci subjekt dopúšťa porušenia právnych predpisov;

b) spôsobilo, spôsobuje alebo pravdepodobne spôsobí ujmu na kolektívnych záujmoch jednotlivcov a má spoločné znaky vrátane rovnakého protiprávneho konania alebo porušovania rovnakého záujmu, a ktorého sa dopustil súčasne ten istý prevádzkovateľ v najmenej troch členských štátoch;

62. „kritická infraštruktúra“ je kritická infraštruktúra v zmysle vymedzenia v článku 2 bode 4 smernice (EÚ) 2022/2557;

63. „model AI na všeobecné účely“ je model AI, a to aj model AI trénovaný veľkým množstvom údajov s použitím samokontroly vo veľkom rozsahu, ktorý má významnú všeobecnú povahu a je schopný kompetentne vykonávať širokú škálu odlišných úloh bez ohľadu na spôsob, akým sa model uvádza na trh, a ktorý možno integrovať do rôznych nadväzujúcich systémov alebo aplikácií, s výnimkou modelov AI, ktoré sa využívajú na účely výskumných, vývojových a prototypových činností pred ich uvedením na trh;

64. „spôsobilosti s veľkým vplyvom“ sú spôsobilosti, ktoré zodpovedajú spôsobilostiam zaznamenaným v najvyspelejších modeloch AI na všeobecné účely alebo tieto spôsobilosti prevyšujú;

65. „systémové riziko“ je riziko špecifické pre spôsobilosti s veľkým vplyvom pri modeloch AI na všeobecné účely, ktoré má významný vplyv na vnútorný trh Únie z dôvodu dosahu týchto modelov alebo z dôvodu skutočných alebo odôvodnene predvídateľných negatívnych účinkov na verejné zdravie, bezpečnosť, verejnú bezpečnosť, základné práva alebo spoločnosť ako celok, ktoré možno šíriť vo veľkom rozsahu v celom hodnotovom reťazci;

66. „systém AI na všeobecné účely“ je systém AI, ktorý je založený na modeli AI na všeobecné účely a ktorý je spôsobilý slúžiť na rôzne účely, a to na priame použitie, ako aj na integráciu do iných systémov AI;

67. „operácia s pohyblivou rádovou čiarkou“ je akákoľvek matematická operácia alebo funkcia obsahujúca čísla s pohyblivou rádovou čiarkou, ktoré sú podmnožinou reálnych čísel zvyčajne reprezentovaných v počítačoch celým číslom s pevným počtom číslic, škálovaným celočíselným exponentom pevného základu;

68. „nadväzujúci poskytovateľ“ je poskytovateľ systému AI vrátane systému AI na všeobecné účely, ktorý integruje model AI, bez ohľadu na to, či tento model AI poskytuje sám a je vertikálne integrovaný alebo ho poskytuje iný subjekt na základe zmluvných vzťahov.

Článok 4

Gramotnosť v oblasti AI

Poskytovatelia systémov AI a subjekty nasadzujúce systémy AI prijímajú opatrenia na čo najlepšie zabezpečenie dostatočnej úrovne gramotnosti v oblasti AI svojich zamestnancov a ostatných osôb, ktoré sa v ich mene zaoberajú prevádzkou a používaním systémov AI, pričom zohľadňujú ich technické znalosti, skúsenosti, vzdelanie a odbornú prípravu, ako aj kontext, v ktorom sa majú systémy AI používať, a berú do úvahy osoby alebo skupiny osôb, pri ktorých sa majú systémy AI používať.

Kapitola II
Zakázané praktiky využívajúce AI

Článok 5

Zakázané praktiky využívajúce AI

1. Zakazujú sa tieto praktiky využívajúce AI:

a) uvádzanie na trh, uvádzanie do prevádzky alebo používanie systému AI, ktorý využíva podprahové techniky mimo vedomia osoby alebo účelovo manipulatívne alebo klamlivé techniky s cieľom alebo účinkom podstatne narušiť správanie osoby alebo skupiny osôb tým, že sa citeľne oslabí ich schopnosť prijať informované rozhodnutie, čo zapríčiní, že prijmú rozhodnutie, ktoré by inak neprijali, a to spôsobom, ktorý tejto osobe, inej osobe alebo skupine osôb spôsobuje alebo pri ktorom je odôvodnené predpokladať, že pravdepodobne spôsobí značnú ujmu;

b) uvádzanie na trh, uvádzanie do prevádzky alebo používanie systému AI, ktorý využíva ktorúkoľvek zo zraniteľností fyzickej osoby alebo osobitnej skupiny osôb z dôvodu ich veku, zdravotného postihnutia alebo osobitnej sociálnej alebo ekonomickej situácie s cieľom alebo účinkom podstatne narušiť správanie tejto osoby alebo osoby patriacej do tejto skupiny spôsobom, ktorý tejto alebo inej osobe spôsobuje alebo pri ktorom je odôvodnené predpokladať, že pravdepodobne spôsobí značnú ujmu;

c) uvádzanie na trh, uvádzanie do prevádzky alebo používanie systémov AI na hodnotenie alebo klasifikáciu fyzických osôb alebo skupín osôb počas určitého obdobia na základe ich spoločenského správania alebo známych, odvodených či predpokladaných osobných alebo osobnostných charakteristík, pričom takto získané sociálne skóre vedie k jednému alebo obidvom z týchto výsledkov:

   i) ku škodlivému alebo nepriaznivému zaobchádzaniu s určitými fyzickými osobami alebo skupinami osôb v sociálnych kontextoch, ktoré nesúvisia s kontextami, v ktorých boli údaje pôvodne generované alebo zhromaždené;

   ii) ku škodlivému alebo nepriaznivému zaobchádzaniu s určitými fyzickými osobami alebo skupinami osôb, ktoré je neodôvodnené alebo neprimerané ich spoločenskému správaniu alebo jeho závažnosti;

d) uvádzanie na trh, uvádzanie do prevádzky na tento konkrétny účel alebo používanie systému AI na posudzovanie rizík fyzických osôb s cieľom posúdiť alebo predvídať riziko toho, že fyzická osoba spácha trestný čin, a to výlučne na základe profilovania fyzickej osoby alebo posúdenia jej osobnostných vlastností a charakteristík; tento zákaz sa nevzťahuje na systémy AI používané na podporu ľudského posúdenia zapojenia osoby do trestnej činnosti, ktoré je už založené na objektívnych a overiteľných skutočnostiach priamo spojených s trestnou činnosťou;

e) uvádzanie na trh, uvádzanie do prevádzky na tento konkrétny účel alebo používanie systémov AI, ktoré vytvárajú alebo rozširujú databázy na rozpoznávanie tváre prostredníctvom necielenej extrakcie podôb tváre z internetu alebo zo záznamov CCTV;

f) uvádzanie na trh, uvádzanie do prevádzky na tento konkrétny účel alebo používanie systémov AI na odvodzovanie emócií fyzickej osoby v oblasti pracoviska a vzdelávacích inštitúcií s výnimkou prípadov, keď je používanie systému AI určené na uvedenie do prevádzky alebo na trh zo zdravotných alebo bezpečnostných dôvodov;

g) uvádzanie na trh, uvádzanie do prevádzky na tento konkrétny účel alebo používanie systémov biometrickej kategorizácie, ktoré jednotlivo kategorizujú fyzické osoby na základe ich biometrických údajov s cieľom odvodiť alebo vyvodiť ich rasu, politické názory, členstvo v odboroch, náboženské alebo filozofické presvedčenie, sexuálny život alebo sexuálnu orientáciu; tento zákaz sa nevzťahuje na žiadne označovanie ani filtrovanie zákonne získaných súborov biometrických údajov, ako sú obrázky, na základe biometrických údajov alebo kategorizácie biometrických údajov v oblasti presadzovania práva;

h) používanie systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva, pokiaľ takéto použitie nie je nevyhnutne potrebné na jeden z týchto cieľov:

   i) cielené pátranie po konkrétnych obetiach únosov, obchodovania s ľuďmi alebo sexuálneho vykorisťovania ľudí, ako aj pátranie po nezvestných osobách;

   ii) predchádzanie konkrétnemu, závažnému a bezprostrednému ohrozeniu života alebo fyzickej bezpečnosti fyzických osôb alebo skutočnej a existujúcej alebo skutočnej a predvídateľnej hrozbe teroristického útoku;

iii) lokalizácia alebo identifikácia osoby podozrivej zo spáchania trestného činu na účel vedenia vyšetrovania alebo stíhania trestného činu alebo výkonu trestnej sankcie za trestné činy uvedené v prílohe II, za ktoré možno v dotknutom členskom štáte uložiť trest odňatia slobody alebo ochranné opatrenie obmedzujúce slobodu s hornou hranicou trestnej sadzby najmenej štyri roky.

Prvým pododsekom písm. h) nie je dotknutý článok 9 nariadenia (EÚ) 2016/679 na účely spracúvania biometrických údajov na iné účely ako je presadzovania práva.

2. Systémy diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch sa na účely presadzovania práva na dosiahnutie ktoréhokoľvek z cieľov uvedených v odseku 1 prvom pododseku písm. h) nasadzujú na účely stanovené v uvedenom písmene, len aby sa potvrdila totožnosť špecificky zacieleného jednotlivca, pričom sa zohľadnia tieto skutočnosti:

a) povaha situácie, ktorá viedla k možnému použitiu, najmä závažnosť, pravdepodobnosť a rozsah ujmy, ktorá by bola spôsobená v prípade nepoužitia systému;

b) dôsledky použitia systému pre práva a slobody všetkých dotknutých osôb, najmä závažnosť, pravdepodobnosť a rozsah týchto dôsledkov.

Používanie systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva na dosiahnutie ktoréhokoľvek z cieľov uvedených v odseku 1 prvom pododseku písm. h) tohto článku musí okrem toho byť v súlade s nevyhnutnými a primeranými zárukami a podmienkami týkajúcimi sa tohto používania, a to podľa vnútroštátnych právnych predpisov oprávňujúcich ich použitie, najmä pokiaľ ide o časové, geografické a osobné obmedzenia. Používanie systému diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch sa povolí len vtedy, ak orgán presadzovania práva dokončil posúdenie vplyvu na základné práva, ako sa stanovuje v článku 27, a zaregistroval systém v databáze Únie podľa článku 49. V riadne odôvodnených naliehavých prípadoch sa však používanie takýchto systémov môže začať bez registrácie v databáze Únie za predpokladu, že sa takáto registrácia dokončí bez zbytočného odkladu.

3. Na účely odseku 1 prvého pododseku písm. h) a odseku 2 podlieha každé použitie systému diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva predchádzajúcemu povoleniu, ktoré udeľuje justičný orgán alebo nezávislý správny orgán, ktorého rozhodnutie je záväzné, členského štátu, v ktorom sa má použitie uskutočniť, vydanému na základe odôvodnenej žiadosti a v súlade s podrobnými pravidlami vnútroštátneho práva uvedenými v odseku 5. V riadne odôvodnenej naliehavej situácii sa však použitie takéhoto systému môže začať bez povolenia za predpokladu, že sa o takéto povolenie požiada bez zbytočného odkladu, najneskôr však do 24 hodín. Ak sa takéto povolenie zamietne, používanie sa s okamžitou účinnosťou zastaví a všetky údaje, ako aj výsledky a výstupy tohto používania sa okamžite vyradia a vymažú.

Príslušný justičný orgán alebo nezávislý správny orgán, ktorého rozhodnutie je záväzné, udelí povolenie len vtedy, ak sa na základe objektívnych dôkazov alebo jasných indícií, ktoré mu boli predložené, presvedčí, že použitie predmetného systému diaľkovej biometrickej identifikácie v reálnom čase je potrebné a primerané na dosiahnutie niektorého z cieľov uvedených v odseku 1 prvom pododseku písm. h), ako sa uvádza v žiadosti, a najmä je naďalej obmedzené na to, čo je striktne nevyhnutné, pokiaľ ide o časový a geografický rozsah a rozsah týkajúci sa osobných aspektov. Pri rozhodovaní o žiadosti tento orgán zohľadní skutočnosti uvedené v odseku 2. Žiadne rozhodnutie, ktoré má pre osobu nepriaznivé právne účinky, sa nesmie prijať výlučne na základe výstupu systému diaľkovej biometrickej identifikácie v reálnom čase.

4. Bez toho, aby bol dotknutý odsek 3, každé použitie systému diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva sa oznámi príslušnému orgánu dohľadu nad trhom a vnútroštátnemu orgánu pre ochranu údajov v súlade s vnútroštátnymi pravidlami uvedenými v odseku 5. Oznámenie obsahuje aspoň informácie uvedené v odseku 6 a neobsahuje citlivé operačné údaje.

5. Členský štát sa môže rozhodnúť, že na účely presadzovania práva v rámci obmedzení a za podmienok uvedených v odseku 1 prvom pododseku písm. h) a odsekoch 2 a 3 stanoví možnosť úplne alebo čiastočne povoliť používanie systému diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch. Dotknuté členské štáty vo svojom vnútroštátnom práve stanovia potrebné podrobné pravidlá na podávanie žiadostí o povolenia uvedené v odseku 3, ich vydávanie a výkon, ako aj pre dohľad nad nimi a podávanie správ o nich. V týchto pravidlách sa takisto uvedie, v súvislosti s ktorým z cieľov uvedených v odseku 1 prvom pododseku písm. h) a s ktorým z trestných činov uvedených v bode iii) uvedeného písmena h) môžu byť príslušné orgány oprávnené používať tieto systémy na účely presadzovania práva. Členské štáty oznámia tieto pravidlá Komisii najneskôr 30 dní po ich prijatí. Členské štáty môžu v súlade s právom Únie zaviesť prísnejšie právne predpisy o používaní systémov diaľkovej biometrickej identifikácie.

6. Vnútroštátne orgány dohľadu nad trhom a vnútroštátne orgány pre ochranu údajov členských štátov, ktorým bolo oznámené používanie systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva podľa odseku 4, predkladajú Komisii výročné správy o takomto používaní. Na tento účel Komisia poskytne členským štátom a vnútroštátnym orgánom dohľadu nad trhom a orgánom pre ochranu údajov vzor vrátane informácií o počte rozhodnutí prijatých príslušnými justičnými orgánmi alebo nezávislým správnym orgánom, ktorého rozhodnutie je záväzné v nadväznosti na žiadosti o povolenie v súlade s odsekom 3, a o ich výsledku.

7. Komisia uverejňuje výročné správy o používaní systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva, pričom vychádza zo súhrnných údajov z členských štátov na základe výročných správ uvedených v odseku 6. Tieto výročné správy nesmú obsahovať citlivé operačné údaje o súvisiacich činnostiach v oblasti presadzovania práva.

8. Týmto článkom nie sú dotknuté zákazy, ktoré sa uplatňujú, ak určitá praktika využívajúca AI porušuje iné právne predpisy Únie.

Kapitola III

Vysokorizikové systémy AI

ODDIEL 1

KLASIFIKÁCIA SYSTÉMOV AI AKO VYSOKORIZIKOVÝCH

Článok 6

Pravidlá klasifikácie vysokorizikových systémov AI

1. Bez ohľadu na to, či sa systém AI uvádza na trh alebo uvádza do prevádzky nezávisle od výrobkov uvedených v písmenách a) a b), považuje sa daný systém AI za vysokorizikový, ak sú splnené obe tieto podmienky:

   a) systém AI je určený na používanie ako bezpečnostný komponent výrobku, na ktorý sa vzťahujú harmonizačné právne predpisy Únie uvedené v prílohe I, alebo je systém AI sám osebe takýmto výrobkom;

b) výrobok, ktorého bezpečnostným komponentom podľa písmena a) je systém AI, alebo samotný systém AI ako výrobok sa musí podrobiť posúdeniu zhody treťou stranou s cieľom uviesť daný výrobok na trh alebo do prevádzky podľa harmonizačných právnych predpisov Únie uvedených v prílohe I.

2. Okrem vysokorizikových systémov AI uvedených v odseku 1 sa za vysokorizikové považujú systémy AI uvedené v prílohe III.

3. Odchylne od odseku 2 sa systém AI uvedený v prílohe III nepovažuje za vysokorizikový, ak nepredstavuje významné riziko ujmy na zdraví, bezpečnosti alebo základných právach fyzických osôb, vrátane toho, že podstatným spôsobom neovplyvňuje výsledok rozhodovania.

Prvý pododsek sa uplatňuje, ak je splnená ktorákoľvek z týchto podmienok:

a) systém AI je určený na vykonávanie úzko vymedzenej procedurálnej úlohy;

b) systém AI je určený na zlepšenie výsledku predtým dokončenej ľudskej činnosti;

c) systém AI je určený na zisťovanie vzorcov rozhodovania alebo odchýlok od vzorcov predchádzajúceho rozhodovania a nie je určený na to, aby bez riadneho ľudského preskúmania nahradil alebo ovplyvnil predtým dokončené ľudské posúdenie, alebo

d) systém AI je určený na vykonávanie prípravnej úlohy pri posudzovaní relevantnom na účely prípadov použitia uvedených v prílohe III.

Bez ohľadu na prvý pododsek sa systém AI uvedený v prílohe III vždy považuje za vysokorizikový, ak sa ním vykonáva profilovanie fyzických osôb.

4. Poskytovateľ, ktorý sa domnieva, že systém AI uvedený v prílohe III nie je vysokorizikový, zdokumentuje svoje posúdenie pred uvedením tohto systému na trh alebo do prevádzky. Takýto poskytovateľ podlieha registračnej povinnosti stanovenej v článku 49 ods. 2. Na žiadosť vnútroštátnych príslušných orgánov poskytovateľ poskytne dokumentáciu o posúdení.

5. Komisia po konzultácii s Európskou radou pre AI (ďalej len „rada pre AI“) a najneskôr do... [18 mesiacov odo dňa nadobudnutia účinnosti tohto nariadenia] poskytne usmernenia, v ktorých spresní praktické vykonávanie tohto článku v súlade s článkom 96 spolu s komplexným zoznamom praktických príkladov prípadov použitia systémov AI, ktoré sú vysokorizikové, a prípadov použitia systémov AI, ktoré nie sú vysokorizikové.

6. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 97 s cieľom zmeniť odsek 3 druhý pododsek tohto článku doplnením nových podmienok k podmienkam v ňom stanoveným alebo ich upravením, ak existujú konkrétne a spoľahlivé dôkazy o existencii systémov AI, ktoré patria do rozsahu pôsobnosti prílohy III, ale nepredstavujú významné riziko ujmy na zdraví, bezpečnosti alebo základných právach fyzických osôb.

7. Komisia prijme delegované akty v súlade s článkom 97 s cieľom zmeniť odsek 3 druhý pododsek tohto článku vypustením ktorejkoľvek z podmienok v ňom stanovených, ak existujú konkrétne a spoľahlivé dôkazy o tom, že je to potrebné na zachovanie úrovne ochrany zdravia, bezpečnosti a základných práv stanovenej týmto nariadením.

8. Žiadna zmena podmienok stanovených v odseku 3 druhom pododseku prijatá v súlade s odsekmi 6 a 7 tohto článku nesmie znížiť celkovú úroveň ochrany zdravia, bezpečnosti a základných práv stanovenú týmto nariadením a musí zabezpečiť súlad s delegovanými aktmi prijatými podľa článku 7 ods. 1 a zohľadniť vývoj na trhu a technologický vývoj.

Článok 7

Zmeny prílohy III

1. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 97 s cieľom zmeniť prílohu III doplnením alebo úpravou prípadov používania vysokorizikových systémov AI, ak sú splnené obe tieto podmienky:

   a) systémy AI sú určené na používanie v ktorejkoľvek z oblastí uvedených v prílohe III;

   b) systémy AI predstavujú riziko ujmy na zdraví a bezpečnosti alebo riziko nepriaznivého vplyvu na základné práva a toto riziko je rovnocenné alebo väčšie než riziko poškodenia alebo nepriaznivého vplyvu, ktoré predstavujú vysokorizikové systémy AI už uvedené v prílohe III.

2. Pri posudzovaní podmienky podľa odseku 1 písm. b) Komisia zohľadní tieto kritériá:

a) zamýšľaný účel systému AI;

b) rozsah, v akom sa systém AI používa alebo sa pravdepodobne bude používať;

c) povahu a množstvo údajov spracúvaných a používaných systémom AI, najmä to, či sa spracúvajú osobitné kategórie osobných údajov;

d) rozsah, v akom systém AI koná samostatne, a možnosť človeka zvrátiť rozhodnutia alebo odporúčania, ktoré môžu viesť k potenciálnej ujme;

e) rozsah, v akom používanie systému AI už spôsobilo ujmu na zdraví a bezpečnosti alebo nepriaznivý vplyv na základné práva, alebo vyvolalo vážne obavy v súvislosti s pravdepodobnosťou takejto ujmy alebo nepriaznivého vplyvu, čo preukazujú napríklad správy alebo zdokumentované tvrdenia, ktoré sa predložili vnútroštátnym príslušným orgánom, alebo prípadne iné správy;

f) potenciálny rozsah takejto ujmu alebo nepriaznivého vplyvu, najmä pokiaľ ide o jeho intenzitu a schopnosť ovplyvniť viacero osôb alebo neúmerne ovplyvniť konkrétnu skupinu osôb;

g) rozsah, v akom sú osoby, ktoré potenciálne utrpeli ujmu alebo trpia nepriaznivým vplyvom, závislé od výsledku vytvoreného systémom AI, najmä preto, že z praktických alebo právnych dôvodov nie je primerane možné sa na tomto výsledku nepodieľať;

h) rozsah, v akom existuje nerovnováha moci, alebo osoby, ktoré potenciálne utrpeli ujmu alebo trpia nepriaznivým vplyvom, sú vo vzťahu k subjektu nasadzujúcemu systém AI v zraniteľnom postavení, najmä z dôvodu postavenia, autority, znalostí, hospodárskych alebo sociálnych okolností alebo veku;

i) rozsah, v akom je výsledok vytvorený pomocou systému AI ľahko napraviteľný alebo zvrátiteľný s prihliadnutím na technické riešenia, ktoré sú k dispozícii na jeho nápravu alebo zvrátenie, pričom výsledky s nepriaznivým vplyvom na zdravie, bezpečnosť alebo základné práva sa nepovažujú za ľahko napraviteľné alebo zvrátiteľné;

j) rozsah a pravdepodobnosť prínosu nasadenia systému AI pre jednotlivcov, skupiny alebo spoločnosť ako celok vrátane možných zlepšení bezpečnosti výrobkov;

k) rozsah, v akom sa v existujúcom práve Únie stanovujú:

   i) účinné nápravné opatrenia v súvislosti s rizikami, ktoré systém AI predstavuje, s výnimkou nárokov na náhradu škody;

   ii) účinné opatrenia na predchádzanie týmto rizikám alebo ich podstatnú minimalizáciu.

3. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 97 s cieľom zmeniť zoznam v prílohe III vypustením vysokorizikových systémov AI, ak sú splnené obe tieto podmienky:

a) dotknutý vysokorizikový systém AI už nepredstavuje významné riziká pre základné práva, zdravie alebo bezpečnosť, pričom sa zohľadňujú kritériá uvedené v odseku 2;

b) vypustením sa neznižuje celková úroveň ochrany zdravia, bezpečnosti a základných práv podľa práva Únie.

ODDIEL 2

POŽIADAVKY NA VYSOKORIZIKOVÉ SYSTÉMY AI

Článok 8

Súlad s požiadavkami

1. Vysokorizikové systémy AI musia spĺňať požiadavky stanovené v tomto oddiele s prihliadnutím na ich zamýšľaný účel, ako aj na všeobecne uznávaný aktuálny stav vývoja AI a technológií súvisiacich s AI. Pri zabezpečovaní súladu s týmito požiadavkami sa zohľadňuje systém riadenia rizík uvedený v článku 9.

2. Ak výrobok obsahuje systém AI, na ktorý sa vzťahujú požiadavky tohto nariadenia, ako aj požiadavky harmonizačných právnych predpisov Únie uvedených v prílohe I oddiele A, poskytovatelia sú zodpovední za zabezpečenie úplného súladu svojho výrobku so všetkými uplatniteľnými požiadavkami podľa uplatniteľných harmonizačných právnych predpisov Únie. Pri zabezpečovaní súladu vysokorizikových systémov AI uvedených v odseku 1 s požiadavkami stanovenými v tomto oddiele a s cieľom zabezpečiť konzistentnosť, zabrániť duplicite a minimalizovať dodatočné zaťaženie majú poskytovatelia možnosť podľa potreby začleniť potrebné procesy testovania a nahlasovania, informácie a dokumentáciu, ktorú poskytujú v súvislosti so svojím výrobkom, do už existujúcej dokumentácie a postupov požadovaných podľa harmonizačných právnych predpisov Únie uvedených v prílohe I oddiele A.

Článok 9

Systém riadenia rizík

1. V súvislosti s vysokorizikovými systémami AI sa zriadi, zavedie, zdokumentuje a udržiava systém riadenia rizík.

2. Systém riadenia rizík sa vykladá ako nepretržitý iteratívny proces plánovaný a uskutočňovaný počas celého životného cyklu vysokorizikového systému AI, ktorý si vyžaduje pravidelné systematické preskúmanie a aktualizovanie. Zahŕňa tieto kroky:

   a) identifikáciu a analýzu známych a odôvodnene predvídateľných rizík, ktoré vysokorizikový systém AI môže predstavovať pre zdravie, bezpečnosť alebo základné práva, keď sa vysokorizikový systém AI používa v súlade s jeho zamýšľaným účelom;

b) odhad a hodnotenie rizík, ktoré môžu vzniknúť, keď sa vysokorizikový systém AI používa v súlade s jeho zamýšľaným účelom a za podmienok odôvodnene predvídateľného nesprávneho použitia;

c) hodnotenie ďalších možných rizík na základe analýzy údajov získaných zo systému monitorovania po uvedení na trh v zmysle článku 72;

d) prijatie vhodných a cielených opatrení na riadenie rizík určených na riešenie rizík identifikovaných podľa písmena a).

3. Tento článok sa vzťahuje len na tie riziká, ktoré možno primerane zmierniť alebo odstrániť vývojom alebo dizajnom vysokorizikového systému AI alebo poskytnutím primeraných technických informácií.

4. V opatreniach na riadenie rizík uvedených v odseku 2 písm. d) sa náležite zohľadnia účinky a možné interakcie vyplývajúce z kombinovaného uplatňovania požiadaviek stanovených v tomto oddiele s cieľom účinnejšie minimalizovať riziká a zároveň dosiahnuť primeranú rovnováhu pri vykonávaní opatrení na splnenie týchto požiadaviek.

5. Opatrenia na riadenie rizík uvedené v odseku 2 písm. d) musia byť také, aby sa relevantné zvyškové riziká spojené s jednotlivými nebezpečenstvami, ako aj celkové zvyškové riziko vysokorizikových systémov AI považovali za prijateľné.

Pri určovaní najvhodnejších opatrení na riadenie rizík sa zabezpečí:

a) odstránenie alebo zníženie rizík identifikovaných a vyhodnotených podľa odseku 2, pokiaľ je to technicky možné prostredníctvom primeraného dizajnu a vývoja vysokorizikového systému AI;

b) v relevantnom prípade zavedenie primeraných zmierňujúcich a kontrolných opatrení na riešenie rizík, ktoré nemožno odstrániť;

c) poskytovanie informácií požadovaných podľa článku 13 a v relevantnom prípade odborná príprava pre nasadzujúce subjekty.

V záujme odstraňovania alebo znižovania rizík súvisiacich s používaním vysokorizikového systému AI sa náležite zohľadnia technické znalosti, skúsenosti, vzdelanie, odborná príprava, ktoré sa očakávajú od nasadzujúceho subjektu, ako aj predpokladaný kontext, v ktorom sa má systém používať.

6. Vysokorizikové systémy AI sa testujú na účel identifikácie najvhodnejších a cielených opatrení na riadenie rizík. Testovaním sa zabezpečí, aby vysokorizikové systémy AI fungovali konzistentne s ich zamýšľaným účelom a spĺňali požiadavky stanovené v tomto oddiele.

7. Postupy testovania môžu zahŕňať testovanie v reálnych podmienkach v súlade s článkom 60.

8. Testovanie vysokorizikových systémov AI sa vykonáva podľa potreby kedykoľvek počas celého procesu vývoja a v každom prípade pred ich uvedením na trh alebo do prevádzky. Testovanie sa vykonáva na základe vopred vymedzených metrík a pravdepodobnostných prahových hodnôt, ktoré sú primerané zamýšľanému účelu vysokorizikového systému AI.

9. Pri implementácii systému riadenia rizík stanoveného v odsekoch 1 až 7 poskytovatelia zvážia, či vysokorizikový systém AI vzhľadom na svoj zamýšľaný účel pravdepodobne nepriaznivo neovplyvní osoby mladšie ako 18 rokov a prípadne iné zraniteľné skupiny.

10. V prípade poskytovateľov vysokorizikových systémov AI, na ktorých sa vzťahujú požiadavky týkajúce sa vnútorných procesov riadenia rizík podľa iných príslušných ustanovení práva Únie, môžu byť aspekty stanovené v odsekoch 1 až 9 súčasťou postupov riadenia rizík stanovených podľa uvedeného práva alebo kombinované s týmito postupmi.

Článok 10

Údaje a správa údajov

1. Vysokorizikové systémy AI, ktoré využívajú techniky zahŕňajúce trénovanie modelov AI s údajmi, sa musia vyvíjať na základe súborov trénovacích, validačných a testovacích údajov, ktoré spĺňajú kritériá kvality uvedené v odsekoch 2 až 5, a to vždy, keď sa takéto súbory údajov používajú.

2. Na súbory trénovacích, validačných a testovacích údajov sa vzťahujú postupy správy a riadenia údajov vhodné na zamýšľaný účel vysokorizikového systému AI. Tieto postupy sa týkajú najmä:

a) príslušných dizajnových rozhodnutí;

b) procesov zberu údajov a pôvodu údajov a v prípade osobných údajov pôvodného účelu zberu údajov;

c) príslušných spracovateľských operácií prípravy údajov, ako je anotácia, označovanie, čistenie, aktualizácia, obohacovanie a agregácia;

d) formulovania predpokladov, najmä pokiaľ ide o informácie, ktoré majú údaje merať a reprezentovať;

e) posúdenia dostupnosti, množstva a vhodnosti potrebných súborov údajov;

f) preskúmania z hľadiska možnej zaujatosti, ktorá môže mať vplyv na zdravie a bezpečnosť osôb, negatívny vplyv na základné práva alebo môže viesť k diskriminácii zakázanej právom Únie, najmä ak výstupy údajov ovplyvňujú vstupy pre budúce operácie;

g) vhodných opatrení na odhaľovanie, prevenciu a zmierňovanie možnej zaujatosti identifikovanej podľa písmena f);

h) identifikácie relevantných medzier alebo nedostatkov v údajoch, ktoré bránia súladu s týmto nariadením, a spôsobu, akým možno tieto medzery a nedostatky odstrániť.

3. Súbory trénovacích, validačných a testovacích údajov musia byť relevantné, dostatočne reprezentatívne a v čo najväčšej možnej miere bez chýb a úplné vzhľadom na zamýšľaný účel. Musia mať primerané štatistické vlastnosti, a to prípadne aj pokiaľ ide o osoby alebo skupiny osôb, vo vzťahu ku ktorým sa má vysokorizikový systém AI používať. Uvedené charakteristiky súborov údajov sa môžu splniť na úrovni jednotlivých súborov údajov alebo na úrovni ich kombinácie.

4. Súbory údajov musia, pokiaľ si to vyžaduje zamýšľaný účel, zohľadňovať charakteristiky alebo prvky, ktoré sú špecifické pre konkrétne geografické, kontextuálne, behaviorálne alebo funkčné podmienky, v ktorých sa má vysokorizikový systém AI používať.

5. Pokiaľ je to nevyhnutne potrebné na účel zabezpečenia odhaľovania a nápravy zaujatosti v súvislosti s vysokorizikovými systémami AI v súlade s odsekom 2 písm. f) a g) tohto článku, poskytovatelia takýchto systémov môžu výnimočne spracúvať osobitné kategórie osobných údajov pod podmienkou primeraných záruk pre základné práva a slobody fyzických osôb. Okrem ustanovení uvedených v nariadeniach (EÚ) 2016/679 a (EÚ) 2018/1725 a v smernici (EÚ) 2016/680 na to, aby došlo k takémuto spracúvaniu, musia byť splnené všetky tieto podmienky:

   a) odhalenie a nápravu zaujatosti nemožno účinne dosiahnuť spracúvaním iných údajov vrátane syntetických alebo anonymizovaných údajov;

b) osobitné kategórie osobných údajov podliehajú technickým obmedzeniam opakovaného použitia osobných údajov a najmodernejším bezpečnostným opatreniam a opatreniam na zachovanie súkromia vrátane pseudonymizácie;

c) osobitné kategórie osobných údajov podliehajú opatreniam na zabezpečenie toho, aby spracúvané osobné údaje boli zabezpečené, chránené, podliehali primeraným zárukám vrátane prísnych kontrol a dokumentácie prístupu, aby sa zabránilo zneužitiu a zabezpečilo, aby k týmto osobným údajom mali prístup len oprávnené osoby s primeranými povinnosťami zachovávania dôvernosti;

d) osobitné kategórie osobných údajov sa nesmú zasielať, prenášať ani inak sprístupňovať iným stranám;

e) osobitné kategórie osobných údajov sa vymažú po náprave zaujatosti alebo uplynutí obdobia uchovávania osobných údajov, podľa toho, čo nastane skôr;

f) záznamy o spracovateľských činnostiach podľa nariadení (EÚ) 2016/679 a (EÚ) 2018/1725 a smernice (EÚ) 2016/680 obsahujú dôvody, prečo bolo spracúvanie osobitných kategórií osobných údajov nevyhnutne potrebné na odhaľovanie a nápravu zaujatosti a prečo uvedený cieľ nebolo možné dosiahnuť spracúvaním iných údajov.

6. Pri vývoji vysokorizikových systémov AI, pri ktorých sa nevyužívajú techniky zahŕňajúce trénovanie modelov AI, sa odseky 2 až 5 vzťahujú len na testovacie súbory údajov.

Článok 11

Technická dokumentácia

1. Pred uvedením vysokorizikového systému AI na trh alebo do prevádzky sa vypracuje technická dokumentácia tohto systému, ktorá sa aktualizuje.

   Technická dokumentácia sa vypracuje tak, aby sa v nej preukazovalo, že vysokorizikový systém AI spĺňa požiadavky stanovené v tomto oddiele, a aby sa vnútroštátnym príslušným orgánom a notifikovaným osobám poskytli v jasnej a komplexnej podobe všetky informácie potrebné na posúdenie súladu systému AI s uvedenými požiadavkami. Musí obsahovať aspoň prvky stanovené v prílohe IV. MSP vrátane startupov môžu poskytovať prvky technickej dokumentácie uvedené v prílohe IV zjednodušeným spôsobom. Na tento účel vytvorí Komisia zjednodušený formulár technickej dokumentácie zameraný na potreby malých podnikov a mikropodnikov. Ak sa MSP vrátane startupov rozhodnú poskytovať informácie požadované v prílohe IV zjednodušeným spôsobom, použijú formulár uvedený v tomto odseku. Notifikované osoby akceptujú formulár na účely posudzovania zhody.

2. Ak sa na trh alebo do prevádzky uvádza vysokorizikový systém AI súvisiaci s výrobkom, na ktorý sa vzťahujú harmonizačné právne predpisy Únie uvedené v prílohe I oddiele A, vypracuje sa jeden súbor technickej dokumentácie obsahujúci všetky informácie stanovené v odseku 1, ako aj informácie požadované podľa uvedených právnych aktov.

3. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 97 s cieľom zmeniť v prípade potreby prílohu IV, aby sa zabezpečilo, že technická dokumentácia bude vzhľadom na technický pokrok poskytovať všetky informácie potrebné na posúdenie súladu systému s požiadavkami stanovenými v tomto oddiele.

Článok 12

Vedenie záznamov

1. Vysokorizikové systémy AI musia technicky umožňovať automatické zaznamenávanie udalostí (ďalej len „logy“) počas životnosti systému.

2. S cieľom zabezpečiť úroveň vysledovateľnosti fungovania vysokorizikového systému AI, ktorá je primeraná zamýšľanému účelu systému, spôsobilosti logovania umožňujú zaznamenávanie udalostí relevantných pre:

   a) identifikáciu situácií, ktoré môžu viesť k tomu, že systém AI začne predstavovať riziko v zmysle článku 79 ods. 1, alebo k podstatnej zmene;

   b) uľahčenie monitorovania po uvedení na trh, ako sa uvádza v článku 72, a

   c) monitorovanie prevádzky vysokorizikových systémov AI uvedené v článku 26 ods. 5.

3. V prípade vysokorizikových systémov AI uvedených v prílohe III bode 1 písm. a) sa v rámci spôsobilostí logovania musí zabezpečiť aspoň:

   a) záznam každého časového úseku používania systému (dátum a čas začiatku a dátum a čas ukončenia každého použitia);

b) referenčná databáza, podľa ktorej systém skontroloval vstupné údaje;

c) vstupné údaje, pri ktorých vyhľadávanie viedlo k zhode;

d) identifikácia fyzických osôb zapojených podľa článku 14 ods. 5 do overovania výsledkov.

Článok 13

Transparentnosť a poskytovanie informácií nasadzujúcim subjektom

1. Vysokorizikové systémy AI musia byť dizajnované a vyvinuté tak, aby sa zabezpečilo, že ich prevádzka je dostatočne transparentná na to, aby nasadzujúcim subjektom umožnila interpretovať výstupy systému a vhodne ich používať. Zabezpečí sa primeraný druh a stupeň transparentnosti, aby poskytovatelia a nasadzujúce subjekty mohli dodržiavať príslušné povinnosti stanovené v oddiele 3.

2. K vysokorizikovým systémom AI sa vo vhodnom digitálnom formáte alebo inak prikladá návod na použitie obsahujúci stručné, úplné, správne a jasné informácie, ktoré sú pre nasadzujúce subjekty relevantné, prístupné a zrozumiteľné.

3. Návod na použitie obsahuje aspoň tieto informácie:

a) totožnosť a kontaktné údaje poskytovateľa a v príslušných prípadoch jeho splnomocneného zástupcu;

b) charakteristiky, spôsobilosti a obmedzenia výkonu vysokorizikového systému AI vrátane:

i) jeho zamýšľaného účelu;

ii) úrovne presnosti vrátane jej metriky, spoľahlivosti a kybernetickej bezpečnosti podľa článku 15, na základe ktorej bol vysokorizikový systém AI testovaný a validovaný a ktorú možno očakávať, ako aj všetky známe a predvídateľné okolnosti, ktoré môžu mať vplyv na túto očakávanú úroveň presnosti, spoľahlivosti a kybernetickej bezpečnosti;

iii) všetkých známych alebo predvídateľných okolností súvisiacich s používaním vysokorizikového systému AI v súlade s jeho zamýšľaným účelom alebo za podmienok odôvodnene predvídateľného nesprávneho používania, ktoré môžu viesť k rizikám pre zdravie a bezpečnosť alebo pre základné práva, ako sa uvádza v článku 9 ods. 2;

iv) v relevantných prípadoch, technických spôsobilostí a charakteristík vysokorizikového systému AI poskytovať informácie, ktoré sú relevantné na vysvetlenie jeho výstupu;

v) v príslušných prípadoch, jeho výkonu, pokiaľ ide o konkrétne osoby alebo skupiny osôb, v prípade ktorých sa má systém používať;

vi) v príslušných prípadoch, špecifikácií vstupných údajov alebo akýchkoľvek iných relevantných informácií z hľadiska použitých súborov trénovacích, validačných a testovacích údajov, pričom sa zohľadní zamýšľaný účel vysokorizikového systému AI;

vii) v relevantných prípadoch, informácií umožňujúcich nasadzujúcim subjektom interpretovať výstup vysokorizikového systému AI a vhodne ho používať;

c) prípadné zmeny vysokorizikového systému AI a jeho výkonu, ktoré v čase počiatočného posúdenia zhody vopred určil poskytovateľ;

d) opatrenia na zabezpečenie ľudského dohľadu uvedené v článku 14 vrátane technických opatrení zavedených na uľahčenie výkladu výstupov vysokorizikových systémov AI nasadzujúcimi subjektmi;

e) potrebné výpočtové a hardvérové zdroje, očakávaná životnosť vysokorizikového systému AI a všetky potrebné opatrenia údržby a starostlivosti vrátane frekvencie ich vykonávania, ktorými sa má zabezpečiť riadne fungovanie tohto systému AI, a to aj pokiaľ ide o aktualizácie softvéru;

f) v relevantnom prípade, opis mechanizmov zahrnutých do vysokorizikového systému AI, ktoré umožňujú nasadzujúcim subjektom riadne zhromažďovať, uchovávať a interpretovať logy v súlade s článkom 12 ods. 1.

Článok 14

Ľudský dohľad

1. Vysokorizikové systémy AI musia byť dizajnované a vyvinuté tak, aby nad nimi počas obdobia ich používania mohli fyzické osoby vykonávať účinný dohľad, a to aj pomocou vhodných nástrojov rozhrania človek – stroj.

2. Ľudský dohľad sa zameriava na prevenciu alebo minimalizáciu rizík pre zdravie, bezpečnosť alebo základné práva, ktoré môžu vzniknúť pri používaní vysokorizikového systému AI v súlade so zamýšľaným účelom alebo za podmienok odôvodnene predvídateľného nesprávneho použitia, najmä ak takéto riziká pretrvávajú napriek uplatňovaniu iných požiadaviek stanovených v tomto oddiele.

3. Opatrenia dohľadu musia byť primerané rizikám, úrovni autonómnosti a kontextu používania vysokorizikového systému AI a zabezpečia sa jedným alebo oboma z týchto druhov opatrení:

   a) opatrenia, ktoré identifikuje poskytovateľ, a ak je to technicky uskutočniteľné, začlení ich do vysokorizikového systému AI pred jeho uvedením na trh alebo do prevádzky;

   b) opatrenia, ktoré identifikuje poskytovateľ pred uvedením vysokorizikového systému AI na trh alebo do prevádzky a ktoré môže zaviesť nasadzujúci subjekt.

4. Na účely vykonávania odsekov 1, 2 a 3 sa vysokorizikový systém AI poskytuje nasadzujúcemu subjektu takým spôsobom, aby fyzickým osobám, ktorým je zverený ľudský dohľad, umožňoval podľa potreby a primerane:

   a) riadne pochopiť príslušné kapacity a obmedzenia vysokorizikového systému AI a byť schopný riadne monitorovať jeho prevádzku, a to aj s cieľom odhaľovať a riešiť anomálie, poruchy a neočakávaný výkon;

b) byť si neustále vedomý možnej tendencie automatického spoliehania sa alebo nadmerného spoliehania sa na výstupy vytvorené vysokorizikovým systémom AI (ďalej len „náchylnosť k automatizácii“), a to najmä v prípade vysokorizikových systémov AI používaných na poskytovanie informácií alebo odporúčaní pre rozhodnutia, ktoré majú prijať fyzické osoby;

c) správne interpretovať výstupy vysokorizikového systému AI, s prihliadnutím napríklad na dostupné interpretačné nástroje a metódy;

d) v akejkoľvek konkrétnej situácii rozhodnúť, že sa vysokorizikový systém AI nepoužije alebo sa výstup vysokorizikového systému AI inak nezohľadní, potlačí alebo zvráti;

e) zasiahnuť do prevádzky vysokorizikového systému AI alebo prerušiť systém pomocou tlačidla „stop“ alebo podobným postupom, ktorý umožňuje zastaviť systém v bezpečnom stave.

5. V prípade vysokorizikových systémov AI uvedených v prílohe III bode 1 písm. a) musia byť opatrenia podľa odseku 3 tohto článku také, aby sa navyše zabezpečilo, že nasadzujúci subjekt na základe identifikácie vyplývajúcej zo systému nekoná ani neprijme žiadne rozhodnutie, pokiaľ takáto identifikácia nebola zvlášť overená a potvrdená aspoň dvoma fyzickými osobami, ktoré majú potrebnú spôsobilosť, odbornú prípravu a právomoc.

Požiadavka na samostatné overenie aspoň dvoma fyzickými osobami sa nevzťahuje na vysokorizikové systémy AI používané na účely presadzovania práva, migrácie, kontroly hraníc alebo azylu, keď sa podľa práva Únie alebo vnútroštátneho práva uplatňovanie tejto požiadavky považuje za neprimerané.

Článok 15

Presnosť, spoľahlivosť a kybernetická bezpečnosť

1. Vysokorizikové systémy AI musia byť dizajnované a vyvinuté tak, aby dosahovali primeranú úroveň presnosti, spoľahlivosti a kybernetickej bezpečnosti a aby v týchto ohľadoch fungovali konzistentne počas celého svojho životného cyklu.

2. S cieľom riešiť technické aspekty spôsobu merania primeraných úrovní presnosti a spoľahlivosti stanovených v odseku 1 a akékoľvek iné relevantné metriky výkonu Komisia v spolupráci s príslušnými zainteresovanými stranami a organizáciami, ako sú orgány v oblasti metrológie a referenčného porovnávania, podľa potreby podporuje vypracovanie referenčných hodnôt a metodík merania.

3. Úrovne presnosti a príslušné metriky na meranie presnosti vysokorizikových systémov AI sa uvádzajú v priloženom návode na použitie.

4. Vysokorizikové systémy AI musia byť čo najodolnejšie, pokiaľ ide o chyby, poruchy alebo nezrovnalosti, ktoré sa môžu vyskytnúť v rámci systému alebo prostredia, v ktorom sa systém prevádzkuje, a to najmä z dôvodu ich interakcie s fyzickými osobami alebo inými systémami. V tejto súvislosti sa prijmú technické a organizačné opatrenia.

   Spoľahlivosť vysokorizikových systémov AI možno dosiahnuť technickými riešeniami na vytvorenie redundancie, ktoré môžu zahŕňať plány zálohovania alebo núdzového režimu.

Vysokorizikové systémy AI, ktoré sa po uvedení na trh alebo do prevádzky ďalej učia, sa vyvíjajú tak, aby sa odstránilo alebo v čo najväčšej miere znížilo riziko, že prípadné skreslené výstupy budú mať vplyv na vstup pre budúce operácie (ďalej len „slučky spätnej väzby“), a aby sa zaistilo, že akékoľvek takéto slučky spätnej väzby sa budú náležite riešiť vhodnými zmierňujúcimi opatreniami.

5. Vysokorizikové systémy AI musia byť odolné voči pokusom neoprávnených tretích strán o zmenu ich používania, výstupov alebo výkonu využívaním zraniteľností systému.

Technické riešenia zamerané na zabezpečenie kybernetickej bezpečnosti vysokorizikových systémov AI musia byť primerané príslušným okolnostiam a rizikám.

Technické riešenia zamerané na zraniteľnosti špecifické pre AI v prípade potreby zahŕňajú opatrenia na prevenciu, detekciu, reakciu, riešenie a kontrolu v prípade útokov, ktoré sa pokúšajú manipulovať súbor trénovacích údajov (ďalej len „otrávenie údajov“) alebo vopred natrénované komponenty používané pri tréningu (ďalej len „otrávenie modelov“), vstupov koncipovaných tak, aby model AI urobil chybu (ďalej len „odporujúce si príklady“ alebo „oklamanie modelov“), útokov na dôvernosť alebo nedostatkov modelu.

ODDIEL 3

POVINNOSTI VZŤAHUJÚCE SA NA POSKYTOVATEĽOV A NASADZUJÚCE SUBJEKTY VYSOKORIZIKOVÝCH SYSTÉMOV AI A INÉ STRANY

Článok 16

Povinnosti poskytovateľov vysokorizikových systémov AI

Poskytovatelia vysokorizikových systémov AI:

a) zabezpečujú, aby ich vysokorizikové systémy AI boli v súlade s požiadavkami stanovenými v oddiele 2;

b) na vysokorizikovom systéme AI, alebo ak to nie je možné, na jeho obale alebo prípadne v sprievodnej dokumentácii uvedú svoje meno, registrované obchodné meno alebo registrovanú ochrannú známku, adresu, na ktorej ich možno kontaktovať;

c) majú zavedený systém riadenia kvality, ktorý je v súlade s článkom 17;

d) uchovávajú dokumentáciu podľa článku 18;

e) uchovávajú logy automaticky generované ich vysokorizikovými systémami AI podľa článku 19, ak ich majú pod kontrolou;

f) zabezpečia, aby sa vysokorizikový systém AI pred uvedením na trh alebo do prevádzky podrobil príslušnému postupu posudzovania zhody, ako sa uvádza v článku 43;

g) vypracujú EÚ vyhlásenie o zhode v súlade s článkom 47;

h) umiestnia označenie CE na vysokorizikový systém AI, alebo ak to nie je možné, na jeho obal alebo prípadne do sprievodnej dokumentácie s cieľom označiť zhodu s týmto nariadením podľa článku 48;

i) splnia registračné povinnosti uvedené v článku 49 ods. 1;

j) prijmú potrebné nápravné opatrenia a poskytnú informácie, ako sa požaduje v článku 20;

k) na základe odôvodnenej žiadosti vnútroštátneho príslušného orgánu preukážu zhodu vysokorizikového systému AI s požiadavkami stanovenými v oddiele 2;

l) zabezpečia, aby vysokorizikový systém AI spĺňal požiadavky na prístupnosť v súlade so smernicami (EÚ) 2016/2102 a (EÚ) 2019/882.

Článok 17

Systém riadenia kvality

1. Poskytovatelia vysokorizikových systémov AI zavedú systém riadenia kvality, ktorým sa zabezpečí súlad s týmto nariadením. Tento systém sa systematicky a usporiadane zdokumentuje vo forme písomných zásad, postupov a pokynov a zahŕňa aspoň tieto aspekty:

   a) stratégiu dodržiavania regulačných požiadaviek vrátane dodržiavania postupov posudzovania zhody a postupov riadenia zmien vysokorizikového systému AI;

b) techniky, postupy a systematické opatrenia, ktoré sa majú použiť pri dizajnovaní vysokorizikového systému AI, kontrole jeho dizajnu a overovaní jeho dizajnu;

c) techniky, postupy a systematické opatrenia, ktoré sa majú použiť pri vývoji vysokorizikového systému AI a pri kontrole a zabezpečení jeho kvality;

d) postupy preskúmania, testovania a validácie, ktoré sa majú vykonávať pred vývojom vysokorizikového systému AI, počas neho a po ňom, a frekvencia, s akou sa musia vykonávať;

e) technické špecifikácie vrátane noriem, ktoré sa majú uplatňovať, a v prípade, že sa príslušné harmonizované normy neuplatňujú v plnom rozsahu alebo sa nevzťahujú na všetky príslušné požiadavky stanovené v oddiele 2, prostriedky, ktoré sa majú použiť na zabezpečenie toho, aby vysokorizikový systém AI spĺňal tieto požiadavky;

f) systémy a postupy správy údajov vrátane získavania údajov, zberu údajov, ich analýzy, označovania, ukladania, filtrovania, hĺbkovej analýzy, agregácie, uchovávania a všetkých ďalších operácií týkajúcich sa údajov, ktoré sa vykonávajú pred uvedením vysokorizikových systémov AI na trh alebo do prevádzky a na účely ich uvedenia na trh alebo do prevádzky;

g) systém riadenia rizík uvedený v článku 9;

h) vytvorenie, zavedenie a vedenie systému monitorovania po uvedení na trh v súlade s článkom 72;

i) postupy týkajúce sa oznamovania závažných incidentov v súlade s článkom 73;

j) vybavovanie komunikácie s vnútroštátnymi príslušnými orgánmi, inými relevantnými orgánmi vrátane tých, ktoré poskytujú alebo podporujú prístup k údajom, s notifikovanými osobami, inými prevádzkovateľmi, zákazníkmi alebo inými zainteresovanými stranami;

k) systémy a postupy vedenia záznamov o všetkých príslušných dokumentoch a informáciách;

l) riadenie zdrojov vrátane opatrení týkajúcich sa bezpečnosti dodávok;

m) rámec zodpovednosti, v ktorom sa stanovia povinnosti manažmentu a ostatných zamestnancov, pokiaľ ide o všetky aspekty uvedené v tomto odseku.

2. Implementácia aspektov uvedených v odseku 1 musí byť primeraná veľkosti organizácie poskytovateľa. Poskytovatelia musia v každom prípade dodržiavať mieru prísnosti a úroveň ochrany, ktoré sa vyžadujú na zabezpečenie súladu ich vysokorizikových systémov AI s týmto nariadením.

3. Poskytovatelia vysokorizikových systémov AI, na ktorých sa vzťahujú povinnosti týkajúce sa systémov riadenia kvality alebo rovnocennej funkcie podľa príslušného odvetvového práva Únie, môžu zahŕňať aspekty uvedené v odseku 1 ako súčasť systémov riadenia kvality stanovených podľa uvedeného práva.

4. V prípade poskytovateľov, ktorí sú finančnými inštitúciami, na ktoré sa vzťahujú požiadavky týkajúce sa ich vnútornej správy a riadenia, dojednaní alebo postupov podľa práva Únie v oblasti finančných služieb, sa povinnosť zaviesť systém riadenia kvality s výnimkou odseku 1 písm. g), h) a i) tohto článku považuje za splnenú dodržiavaním pravidiel týkajúcich sa vnútornej správy a riadenia, dojednaní alebo postupov podľa príslušného práva Únie v oblasti finančných služieb. Na tento účel sa zohľadnia všetky harmonizované normy uvedené v článku 40.

Článok 18

Uchovávanie dokumentácie

1. Počas obdobia končiaceho sa 10 rokov po uvedení vysokorizikového systému AI na trh alebo do prevádzky uchováva poskytovateľ pre potreby vnútroštátnych príslušných orgánov:

a) technickú dokumentáciu uvedenú v článku 11;

b) dokumentáciu týkajúcu sa systému riadenia kvality uvedenú v článku 17,

c) dokumentáciu týkajúcu sa prípadných zmien schválených notifikovanými osobami;

d) prípadné rozhodnutia a iné dokumenty vydané notifikovanými osobami;

e) EÚ vyhlásenie o zhode uvedené v článku 47.

2. Každý členský štát určí podmienky, za ktorých ostáva dokumentácia uvedená v odseku 1 k dispozícii vnútroštátnym príslušným orgánom počas obdobia stanoveného v uvedenom odseku pre prípady, keď je poskytovateľ alebo jeho splnomocnený zástupca usadený na jeho území v konkurze alebo ukončí svoju činnosť pred koncom tohto obdobia.

3. Poskytovatelia, ktorí sú finančnými inštitúciami, na ktoré sa vzťahujú požiadavky týkajúce sa ich vnútornej správy a riadenia, dojednaní alebo postupov podľa práva Únie v oblasti finančných služieb, uchovávajú technickú dokumentáciu ako súčasť dokumentácie uchovávanej podľa príslušného práva Únie v oblasti finančných služieb.

Článok 19

Automaticky generované logy

1. Poskytovatelia vysokorizikových systémov AI uchovávajú logy uvedené v článku 12 ods. 1 automaticky generované ich vysokorizikovými systémami AI, pokiaľ sú tieto logy pod ich kontrolou. Bez toho, aby bolo dotknuté uplatniteľné právo Únie alebo vnútroštátne právo, sa logy uchovávajú počas obdobia primeraného zamýšľanému účelu vysokorizikového systému AI, a to najmenej šesť mesiacov, pokiaľ sa v uplatniteľnom práve Únie alebo vo vnútroštátnom práve, najmä v práve Únie o ochrane osobných údajov, nestanovuje inak.

2. Poskytovatelia, ktorí sú finančnými inštitúciami, na ktoré sa vzťahujú požiadavky týkajúce sa ich vnútornej správy a riadenia, dojednaní alebo postupov podľa práva Únie v oblasti finančných služieb, uchovávajú logy automaticky generované ich vysokorizikovými systémami AI ako súčasť dokumentácie uchovávanej podľa príslušného práva v oblasti finančných služieb.

Článok 20

Nápravné opatrenia a informačná povinnosť

1. Poskytovatelia vysokorizikových systémov AI, ktorí sa domnievajú alebo majú dôvod domnievať sa, že vysokorizikový systém AI, ktorý uviedli na trh alebo do prevádzky, nie je v zhode s týmto nariadením, bezodkladne prijmú potrebné nápravné opatrenia s cieľom dosiahnuť podľa potreby zhodu tohto systému, stiahnuť ho z trhu, deaktivovať ho alebo stiahnuť od používateľa. Informujú o tom distribútorov dotknutého vysokorizikového systému AI a v relevantných prípadoch nasadzujúce subjekty, splnomocneného zástupcu a dovozcov.

2. Ak vysokorizikový systém AI predstavuje riziko v zmysle článku 79 ods. 1 a poskytovateľ sa o tomto riziku dozvie, bezodkladne, prípadne v spolupráci s nahlasujúcim nasadzujúcim subjektom, vyšetrí príčiny a informuje orgány dohľadu nad trhom príslušné pre dotknutý vysokorizikový systém AI a v relevantnom prípade notifikovanú osobu, ktorá vydala pre uvedený vysokorizikový systém AI certifikát v súlade s článkom 44, a to najmä o povahe nesúladu a o všetkých relevantných nápravných opatreniach, ktoré boli prijaté.

Článok 21

Spolupráca s príslušnými orgánmi

1. Poskytovatelia vysokorizikových systémov AI na odôvodnenú žiadosť príslušného orgánu poskytnú tomuto orgánu všetky informácie a dokumentáciu potrebnú na preukázanie zhody vysokorizikového systému AI s požiadavkami stanovenými v oddiele 2, a to v jednom z úradných jazykov inštitúcií Únie určenom dotknutým členským štátom, ktorému orgán bez problémov rozumie.

2. Na základe odôvodnenej žiadosti príslušného orgánu poskytnú poskytovatelia žiadajúcemu príslušnému orgánu v prípade potreby aj prístup k automaticky generovaným logom vysokorizikového systému AI uvedeným v článku 12 ods. 1, pokiaľ sú tieto logy pod ich kontrolou.

3. So všetkými informáciami, ktoré príslušný orgán získal podľa tohto článku, sa zaobchádza v súlade s povinnosťami zachovávania dôvernosti podľa článku 78.

Článok 22

Splnomocnení zástupcovia poskytovateľov vysokorizikových systémov AI

1. Poskytovatelia usadení v tretích krajinách pred sprístupnením svojich vysokorizikových systémov AI na trhu Únie písomným splnomocnením vymenujú splnomocneného zástupcu usadeného v Únii.

2. Poskytovateľ umožní svojmu splnomocnenému zástupcovi vykonávať úlohy uvedené v splnomocnení, ktoré mu udelil poskytovateľ.

3. Splnomocnený zástupca vykonáva úlohy uvedené v splnomocnení, ktoré mu udelil poskytovateľ. Na požiadanie poskytne orgánom dohľadu nad trhom kópiu splnomocnenia v jednom z úradných jazykov inštitúcií Únie, ktorý určí príslušný orgán. Na účely tohto nariadenia sa splnomocnený zástupca splnomocnením poveruje, aby vykonával tieto úlohy:

   a) overiť, či sa vypracovalo EÚ vyhlásenie o zhode uvedené v článku 47 a technická dokumentácia uvedená v článku 11 a či poskytovateľ vykonal príslušný postup posudzovania zhody;

   b) uchovávať pre príslušné orgány a vnútroštátne orgány alebo subjekty uvedené v článku 74 ods. 10 počas obdobia 10 rokov po uvedení vysokorizikového systému AI na trh alebo do prevádzky, kontaktné údaje poskytovateľa, ktorý splnomocneného zástupcu vymenoval, kópiu EÚ vyhlásenia o zhode uvedeného v článku 47, technickú dokumentáciu a v relevantnom prípade certifikát vydaný notifikovanou osobou;

   c) poskytnúť príslušnému orgánu na základe odôvodnenej žiadosti všetky informácie a dokumentáciu vrátane dokumentácie uvedenej v písmene b) tohto pododseku potrebné na preukázanie súladu vysokorizikového systému AI s požiadavkami stanovenými v oddiele 2 vrátane prístupu k logom, ako sa uvádza v článku 12 ods. 1, automaticky generovaným vysokorizikovým systémom AI, pokiaľ sú tieto logy pod kontrolou poskytovateľa;

d) spolupracovať s príslušnými orgánmi na základe odôvodnenej žiadosti pri každom opatrení, ktoré takýto orgán prijme v súvislosti s vysokorizikovým systémom AI, najmä s cieľom znížiť a zmierniť riziká, ktoré vysokorizikový systém AI predstavuje;

e) v relevantných prípadoch plniť registračné povinnosti uvedené v článku 49 ods. 1, alebo ak registráciu vykonáva sám poskytovateľ, zabezpečiť správnosť informácií uvedených v prílohe VIII oddiele A bode 3.

Splnomocnením sa splnomocnený zástupca oprávňuje, aby sa okrem poskytovateľa alebo namiesto neho naň obracali príslušné orgány vo všetkých otázkach týkajúcich sa zabezpečenia súladu s týmto nariadením.

4. Splnomocnený zástupca splnomocnenie vypovie, ak sa domnieva alebo má dôvod domnievať sa, že poskytovateľ koná v rozpore so svojimi povinnosťami podľa tohto nariadenia. V takom prípade bezodkladne informuje príslušný orgán dohľadu nad trhom a v relevantnom prípade aj príslušnú notifikovanú osobu o výpovedi splnomocnenia a jej dôvodoch.

Článok 23

Povinnosti dovozcov

1. Pred uvedením vysokorizikového systému AI na trh jeho dovozcovia zabezpečia, aby bol tento systém v zhode s týmto nariadením, a to overením, že:

a) poskytovateľ vysokorizikového systému AI vykonal príslušný postup posudzovania zhody uvedený v článku 43;

b) poskytovateľ vypracoval technickú dokumentáciu v súlade s článkom 11 a prílohou IV;

c) systém bol označený požadovaným označením CE a bolo k nemu priložené EÚ vyhlásenie o zhode uvedené v článku 47 a návod na použitie;

d) poskytovateľ vymenoval splnomocneného zástupcu v súlade s článkom 22 ods. 1.

2. Ak má dovozca dostatočné dôvody domnievať sa, že vysokorizikový systém AI nie je v zhode s týmto nariadením, alebo je sfalšovaný, alebo že ho sprevádza sfalšovaná dokumentácia, neuvedie tento systém na trh, kým sa tento systém neuvedie do súladu. Ak vysokorizikový systém AI predstavuje riziko v zmysle článku 79 ods. 1, dovozca o tom informuje poskytovateľa tohto systému, splnomocneného zástupcu a orgány dohľadu nad trhom.

3. Dovozcovia uvedú svoje meno, registrované obchodné meno alebo registrovanú ochrannú známku a adresu, na ktorej ich možno kontaktovať, na vysokorizikovom systéme AI, na obale tohto systému, alebo v relevantnom prípade v jeho sprievodnej dokumentácii.

4. Dovozcovia zabezpečia, aby v čase, keď nesú za vysokorizikový systém AI zodpovednosť, podmienky jeho uskladnenia alebo prepravy v relevantných prípadoch neohrozovali jeho súlad s požiadavkami stanovenými v oddiele 2.

5. Dovozcovia uchovávajú kópiu prípadného certifikátu vydaného notifikovanou osobou, návodu na použitie a EÚ vyhlásenia o zhode uvedeného v článku 47 počas obdobia 10 rokov po uvedení vysokorizikového systému AI na trh alebo do prevádzky.

6. Dovozcovia poskytnú relevantným príslušným orgánom na základe odôvodnenej žiadosti všetky potrebné informácie a dokumentáciu vrátane tej, ktorá je uvedená v odseku 5, na preukázanie zhody vysokorizikového systému AI s požiadavkami stanovenými v oddiele 2 v jazyku, ktorému tieto orgány bez problémov rozumejú. Na tento účel takisto zabezpečia, aby sa týmto orgánom mohla sprístupniť technická dokumentácia.

7. Dovozcovia spolupracujú s relevantnými príslušnými orgánmi pri každom opatrení, ktoré tieto orgány prijmú v súvislosti s vysokorizikovým systémom AI, ktorý dovozcovia uviedli na trh, najmä s cieľom znížiť a zmierniť riziká, ktoré takýto systém predstavuje.

Článok 24

Povinnosti distribútorov

1. Pred sprístupnením vysokorizikového systému AI na trhu distribútori overia, či je tento systém označený požadovaným označením CE, či je k nemu pripojená kópia EÚ vyhlásenia o zhode uvedeného v článku 47 a návod na použitie a či si poskytovateľ tohto systému splnil svoje povinnosti stanovené v článku 16 písm. b) a c) a dovozca tohto systému svoje povinnosti stanovené v článku 23 ods. 3.

2. Ak sa distribútor na základe informácií, ktoré má k dispozícii, domnieva alebo má dôvod domnievať sa, že vysokorizikový systém AI nie je v zhode s požiadavkami stanovenými v oddiele 2, tento vysokorizikový systém AI nesprístupní na trhu, kým sa tento systém neuvedie do súladu s uvedenými požiadavkami. Ak vysokorizikový systém AI navyše predstavuje riziko v zmysle článku 79 ods. 1, distribútor o tom informuje poskytovateľa alebo v relevantnom prípade dovozcu systému.

3. Distribútori zabezpečia, aby v čase, keď nesú za vysokorizikový systém AI zodpovednosť, podmienky jeho uskladnenia alebo prepravy v relevantných prípadoch neohrozovali súlad systému s požiadavkami stanovenými v oddiele 2.

4. Distribútor, ktorý sa na základe informácií, ktoré má k dispozícii, domnieva alebo má dôvod domnievať sa, že vysokorizikový systém AI, ktorý sprístupnil na trhu, nie je v zhode s požiadavkami stanovenými v oddiele 2, prijme nápravné opatrenia potrebné na dosiahnutie zhody tohto systému s uvedenými požiadavkami, na jeho stiahnutie z trhu alebo stiahnutie od používateľa, alebo zabezpečí, aby uvedené nápravné opatrenia prijal poskytovateľ, dovozca alebo v relevantnom prípade akýkoľvek relevantný prevádzkovateľ. Ak vysokorizikový systém AI predstavuje riziko v zmysle článku 79 ods. 1, distribútor o tom bezodkladne informuje poskytovateľa alebo dovozcu systému a orgány príslušné pre dotknutý vysokorizikový systém AI, pričom uvedie podrobnosti najmä o nedodržaní požiadaviek a o všetkých prijatých nápravných opatreniach.

5. Na základe odôvodnenej žiadosti relevantného príslušného orgánu distribútori vysokorizikového systému AI poskytnú tomuto orgánu všetky informácie a dokumentáciu o svojej činnosti podľa odsekov 1 až 4 potrebné na preukázanie zhody tohto systému s požiadavkami stanovenými v oddiele 2.

6. Distribútori spolupracujú s relevantnými príslušnými orgánmi pri každom opatrení, ktoré tieto orgány prijmú v súvislosti s vysokorizikovým systémom AI, ktorý distribútori sprístupnili na trhu, najmä s cieľom znížiť alebo zmierniť riziká, ktoré tento systém predstavuje.

Článok 25

Povinnosti v celom hodnotovom reťazci AI

1. Každý distribútor, dovozca, nasadzujúci subjekt alebo iná tretia strana sa na účely tohto nariadenia považuje za poskytovateľa vysokorizikového systému AI a vzťahujú sa na neho povinnosti poskytovateľa podľa článku 16 za ktorejkoľvek z týchto okolností:

   a) umiestnia svoje meno alebo ochrannú známku na vysokorizikový systém AI, ktorý už bol uvedený na trh alebo do prevádzky, bez toho, aby boli dotknuté zmluvné dojednania, v ktorých sa stanovuje, že povinnosti sú rozdelené inak;

   b) vykonajú podstatnú zmenu vysokorizikového systému AI, ktorý už bol uvedený na trh alebo už bol uvedený do prevádzky takým spôsobom, že zostáva vysokorizikovým systémom AI podľa článku 6;

c) menia zamýšľaný účel systému AI vrátane systému AI na všeobecné účely, ktorý nebol klasifikovaný ako vysokorizikový a už bol uvedený na trh alebo do prevádzky takým spôsobom, že sa z dotknutého systému AI stane vysokorizikový systém AI v súlade s článkom 6.

2. Ak nastanú okolnosti uvedené v odseku 1, poskytovateľ, ktorý pôvodne uviedol systém AI na trh alebo do prevádzky, sa už na účely tohto nariadenia nepovažuje za poskytovateľa tohto konkrétneho systému AI. Tento pôvodný poskytovateľ úzko spolupracuje s novými poskytovateľmi a sprístupňuje potrebné informácie a poskytuje odôvodnene očakávaný technický prístup a inú pomoc, ktoré sú potrebné na plnenie povinností stanovených v tomto nariadení, najmä pokiaľ ide o súlad s posudzovaním zhody vysokorizikových systémov AI. Tento odsek sa neuplatňuje v prípadoch, keď pôvodný poskytovateľ jasne uviedol, že jeho systém AI sa nemá zmeniť na vysokorizikový systém AI, a preto sa naň nevzťahuje povinnosť odovzdať dokumentáciu.

3. V prípade vysokorizikových systémov AI, ktoré sú bezpečnostnými komponentmi výrobkov, na ktoré sa vzťahujú harmonizačné právne predpisy Únie uvedené v prílohe I oddiele A, sa výrobca týchto výrobkov považuje za poskytovateľa vysokorizikového systému AI a podlieha povinnostiam podľa článku 16 za ktorejkoľvek z týchto okolností:

a) vysokorizikový systém AI sa uvádza na trh spolu s výrobkom pod menom alebo ochrannou známkou výrobcu výrobku;

b) vysokorizikový systém AI sa po uvedení výrobku na trh uvedie do prevádzky pod menom alebo ochrannou známkou výrobcu výrobku.

4. Poskytovateľ vysokorizikového systému AI a tretia strana, ktorá dodáva systém AI, nástroje, služby, komponenty alebo procesy AI, ktoré sa používajú alebo sú integrované vo vysokorizikovom systéme AI, prostredníctvom písomnej dohody spresnia potrebné informácie, spôsobilosti, technický prístup a inú pomoc na základe všeobecne uznávaného aktuálneho stavu vývoja, aby poskytovateľ vysokorizikového systému AI mohol v plnej miere plniť povinnosti stanovené v tomto nariadení. Tento odsek sa nevzťahuje na tretie strany, ktoré sprístupňujú verejnosti nástroje, služby, procesy alebo komponenty, ktoré nie sú modelmi AI na všeobecné účely, na základe bezplatnej licencie s otvoreným zdrojovým kódom.

   Úrad pre AI môže vypracovať a odporučiť nezáväzné vzorové podmienky zmlúv medzi poskytovateľmi vysokorizikových systémov AI a tretími stranami, ktoré dodávajú nástroje, služby, komponenty alebo procesy, ktoré sa používajú alebo sú integrované vo vysokorizikových systémoch AI. Úrad pre AI by mal pri vypracúvaní týchto nezáväzných vzorových podmienok zohľadniť možné zmluvné požiadavky uplatniteľné v konkrétnych odvetviach alebo obchodných prípadoch. Nezáväzné vzorové podmienky sa uverejnia a bezplatne sprístupnia v ľahko použiteľnom elektronickom formáte.

5. Odsekmi 2 a 3 nie je dotknutá potreba dodržiavať a chrániť práva duševného vlastníctva, dôverné obchodné informácie a obchodné tajomstvo v súlade s právom Únie a vnútroštátnym právom.

Článok 26

Povinnosti subjektov nasadzujúcich vysokorizikové systémy AI

1. Subjekty nasadzujúce vysokorizikové systémy AI prijmú vhodné technické a organizačné opatrenia s cieľom zabezpečiť, aby používali takéto systémy v súlade s návodom na použitie, ktorý je k nim priložený, a to podľa odsekov 3 a 6.

2. Nasadzujúce subjekty pridelia ľudský dohľad fyzickým osobám, ktoré majú potrebnú spôsobilosť, odbornú prípravu a právomoci, ako aj nevyhnutnú podporu.

3. Povinnosťami uvedenými v odsekoch 1 a 2 nie sú dotknuté iné povinnosti nasadzujúceho subjektu vyplývajúce z práva Únie alebo vnútroštátneho práva ani slobodné rozhodovanie nasadzujúceho subjektu pri organizovaní svojich vlastných zdrojov a činností na účely vykonávania opatrení na zabezpečenie ľudského dohľadu, ako ich uviedol poskytovateľ.

4. Bez toho, aby boli dotknuté odseky 1 a 2, a pokiaľ má nasadzujúci subjekt kontrolu nad vstupnými údajmi, tento nasadzujúci subjekt zabezpečí, aby vstupné údaje boli relevantné a dostatočne reprezentatívne z hľadiska zamýšľaného účelu vysokorizikového systému AI.

5. Nasadzujúce subjekty monitorujú prevádzku vysokorizikového systému AI na základe návodu na použitie, a ak je to relevantné, informujú poskytovateľov v súlade s článkom 72. Ak majú nasadzujúce subjekty dôvod domnievať sa, že používanie vysokorizikového systému AI v súlade s návodom môže viesť k tomu, že uvedený systém AI predstavuje riziko v zmysle článku 79 ods. 1, bez zbytočného odkladu informujú poskytovateľa alebo distribútora a relevantný orgán dohľadu nad trhom a používanie tohto systému pozastavia. Ak nasadzujúce subjekty zistia závažný incident, bezodkladne o tom najprv informujú poskytovateľa a potom dovozcu alebo distribútora a príslušné orgány dohľadu nad trhom. V prípade, že nasadzujúci subjekt nedokáže poskytovateľa kontaktovať, uplatňuje sa *mutatis mutandis* článok 73. Táto povinnosť sa nevzťahuje na citlivé operačné údaje subjektov nasadzujúcich systémy AI, ktoré sú orgánmi presadzovania práva.

V prípade nasadzujúcich subjektov, ktoré sú finančnými inštitúciami, na ktoré sa vzťahujú požiadavky týkajúce sa ich vnútornej správy a riadenia, dojednaní alebo postupov podľa práva Únie v oblasti finančných služieb, sa monitorovacia povinnosť stanovená v prvom pododseku považuje za splnenú, ak sú dodržané pravidlá týkajúce sa vnútornej správy a riadenia, postupov a mechanizmov podľa príslušného práva v oblasti finančných služieb.

6. Subjekty nasadzujúce vysokorizikové systémy AI uchovávajú logy automaticky generované týmto vysokorizikovým systémom AI, pokiaľ sú takéto logy pod ich kontrolou, počas obdobia primeraného zamýšľanému účelu vysokorizikového systému AI, a to najmenej šesť mesiacov, ak sa v uplatniteľnom práve Únie alebo vo vnútroštátnom práve, najmä v práve Únie o ochrane osobných údajov nestanovuje inak.

Nasadzujúce subjekty, ktoré sú finančnými inštitúciami, a na ktoré sa vzťahujú požiadavky týkajúce sa ich vnútornej správy a riadenia, dojednaní alebo postupov podľa práva Únie v oblasti finančných služieb, uchovávajú logy ako súčasť dokumentácie uchovávanej v súlade s príslušným právom Únie v oblasti finančných služieb.

7. Pred uvedením vysokorizikového systému AI do prevádzky alebo používaním na pracovisku nasadzujúce subjekty, ktoré sú zamestnávateľmi, informujú zástupcov pracovníkov a dotknutých pracovníkov o tom, že budú vystavení používaniu vysokorizikového systému AI. Tieto informácie sa v uplatniteľných prípadoch poskytujú v súlade s pravidlami a postupmi stanovenými v práve Únie a vo vnútroštátnom práve a praxi v oblasti informovania pracovníkov a ich zástupcov.

8. Subjekty nasadzujúce vysokorizikové systémy AI, ktoré sú orgánmi verejnej moci alebo inštitúciami, orgánmi, úradmi alebo agentúrami Únie, plnia povinnosti týkajúce sa registrácie uvedené v článku 49. Ak nasadzujúce subjekty zistia, že vysokorizikový systém AI, ktorý plánujú používať, nebol zaregistrovaný v databáze Únie uvedenej v článku 71, nepoužívajú tento systém a informujú o tom poskytovateľa alebo distribútora.

9. Na splnenie svojej povinnosti vykonať posúdenie vplyvu na ochranu údajov podľa článku 35 nariadenia (EÚ) 2016/679 alebo článku 27 smernice (EÚ) 2016/680 subjekty nasadzujúce vysokorizikové systémy AI podľa okolností využijú informácie poskytnuté podľa článku 13 tohto nariadenia.

10. Bez toho, aby bola dotknutá smernica (EÚ) 2016/680, subjekt nasadzujúci vysokorizikový systém AI na účely následnej diaľkovej biometrickej identifikácie v rámci vyšetrovania v prípade cieleného pátrania po osobe podozrivej zo spáchania trestného činu alebo z tohto dôvodu odsúdenej požiada *ex ante* alebo bez zbytočného odkladu a najneskôr do 48 hodín o povolenie justičného orgánu alebo správneho orgánu, ktorého rozhodnutie je záväzné a podlieha súdnemu preskúmaniu, o použitie tohto systému, s výnimkou prípadov, keď sa systém používa na počiatočnú identifikáciu potenciálnej podozrivej osoby na základe objektívnych a overiteľných skutočností priamo súvisiacich s trestným činom. Každé použitie sa obmedzuje na to, čo je nevyhnutne potrebné na vyšetrovanie konkrétneho trestného činu.

    Ak sa povolenie požadované podľa prvého pododseku zamietne, používanie systému následnej diaľkovej biometrickej identifikácie súvisiace s týmto požadovaným povolením sa s okamžitou účinnosťou zastaví a osobné údaje súvisiace s používaním vysokorizikového systému AI, pre ktoré sa povolenie žiadalo, sa vymažú.

Takýto vysokorizikový systém AI na následnú diaľkovú biometrickú identifikáciu sa v žiadnom prípade nepoužíva na účely presadzovania práva necieleným spôsobom, bez akejkoľvek súvislosti s trestným činom, trestným konaním, skutočnou a existujúcou alebo skutočnou a predvídateľnou hrozbou trestného činu alebo pátraním po konkrétnej nezvestnej osobe. Zabezpečí sa, aby orgány presadzovania práva nemohli prijať žiadne rozhodnutie, ktoré má nepriaznivé právne účinky na danú osobu, a to výlučne na základe výstupu takýchto systémov následnej diaľkovej biometrickej identifikácie.

Týmto odsekom nie je dotknutý článok 9 nariadenia (EÚ) 2016/679 a článok 10 smernice (EÚ) 2016/680 týkajúce sa spracúvania biometrických údajov.

Bez ohľadu na účel alebo nasadzujúci subjekt sa každé použitie týchto vysokorizikových systémov AI zdokumentuje v príslušnom policajnom spise a na požiadanie sa sprístupní relevantnému orgánu dohľadu nad trhom a vnútroštátnemu orgánu pre ochranu údajov, s výnimkou zverejnenia citlivých operačných údajov týkajúcich sa presadzovania práva. Týmto pododsekom nie sú dotknuté právomoci, ktoré sa smernicou (EÚ) 2016/680 udeľujú orgánom dohľadu.

Nasadzujúce subjekty predkladajú relevantným orgánom dohľadu nad trhom a vnútroštátnym orgánom pre ochranu údajov výročné správy o ich používaní systémov následnej diaľkovej biometrickej identifikácie s výnimkou zverejňovania citlivých operačných údajov týkajúcich sa presadzovania práva. Správy možno agregovať tak, aby zahŕňali viac ako len jedno nasadenie.

Členské štáty môžu v súlade s právom Únie zaviesť prísnejšie právne predpisy pre používanie systémov následnej diaľkovej biometrickej identifikácie.

11. Bez toho, aby bol dotknutý článok 50 tohto nariadenia, subjekty nasadzujúce vysokorizikové systémy AI uvedené v prílohe III, ktoré prijímajú rozhodnutia alebo pomáhajú pri prijímaní rozhodnutí týkajúcich sa fyzických osôb, informujú tieto fyzické osoby o tom, že sa na ne vzťahuje používanie vysokorizikového systému AI.
Na vysokorizikové systémy AI používané na účely presadzovania práva sa uplatňuje článok 13 smernice (EÚ) 2016/680.

12. Nasadzujúce subjekty spolupracujú s relevantnými príslušnými orgánmi na každom opatrení, ktoré tieto orgány prijmú v súvislosti s vysokorizikovým systémom AI s cieľom vykonávať toto nariadenie.

Článok 27

Posúdenie vplyvu na základné práva v prípade vysokorizikových systémov AI

1. Pred nasadením vysokorizikového systému AI uvedeného v článku 6 ods. 2, s výnimkou vysokorizikových systémov AI určených na používanie v oblasti uvedenej v prílohe III bode 2, nasadzujúce subjekty, ktoré sú verejnoprávnymi orgánmi alebo súkromnými subjektmi poskytujúcimi verejné služby, a subjekty nasadzujúce vysokorizikové systémy AI uvedené v prílohe III bode 5 písm. b) a c) vykonajú posúdenie vplyvu na základné práva, ktorý môže mať použitie takéhoto systému. Na tento účel vykonajú nasadzujúce subjekty posúdenie, ktoré zahŕňa:

   a) opis procesov nasadzujúceho subjektu, v ktorých sa bude vysokorizikový systém AI používať v súlade s jeho zamýšľaným účelom;

   b) opis časového úseku a frekvencie, v ktorých sa má každý vysokorizikový systém AI používať;

c) kategórie fyzických osôb a skupín, ktoré pravdepodobne budú ovplyvnené jeho používaním v konkrétnom kontexte;

d) konkrétne riziká ujmy, ktoré pravdepodobne ovplyvnia kategórie fyzických osôb alebo skupín osôb identifikovaných podľa písmena c) tohto odseku s prihliadnutím na informácie od poskytovateľa podľa článku 13;

e) opis vykonávania opatrení v oblasti ľudského dohľadu podľa návodu na použitie;

f) opatrenia, ktoré sa majú prijať v prípade naplnenia týchto rizík, vrátane opatrení zameraných na vnútorné správu a riadenie a mechanizmy riešenia sťažností.

2. Povinnosť uvedená v odseku 1 sa vzťahuje na prvé použitie vysokorizikového systému AI. Nasadzujúci subjekt sa môže v podobných prípadoch odvolávať na predtým vykonané posúdenie vplyvu na základné práva alebo na existujúce posúdenie vplyvu, ktoré vykonal poskytovateľ. Ak sa počas používania vysokorizikového systému AI nasadzujúci subjekt domnieva, že sa ktorýkoľvek z prvkov uvedených v odseku 1 zmenil alebo už nie je aktuálny, podnikne kroky potrebné na aktualizáciu informácií.

3. Po vykonaní posúdenia vplyvu uvedeného v odseku 1 tohto článku nasadzujúci subjekt notifikuje orgán dohľadu nad trhom o výsledkoch, pričom ako súčasť notifikácie predloží vyplnený vzor uvedený v odseku 5 tohto článku. V prípade uvedenom v článku 46 ods. 1 môžu byť nasadzujúce subjekty oslobodené od notifikačnej povinnosti.

4. Ak je ktorákoľvek z povinností stanovených v tomto článku už splnená prostredníctvom posúdenia vplyvu na ochranu údajov vykonaného podľa článku 35 nariadenia (EÚ) 2016/679 alebo článku 27 smernice (EÚ) 2016/680, posúdenie vplyvu na základné práva uvedené v odseku 1 tohto článku doplní toto posúdenie vplyvu na ochranu údajov.

5. Úrad pre AI vypracuje vzor dotazníka, a to aj prostredníctvom automatizovaného nástroja, s cieľom uľahčiť nasadzujúcim subjektom plnenie ich povinností podľa tohto článku zjednodušeným spôsobom.

ODDIEL 4

NOTIFIKUJÚCE ORGÁNY A NOTIFIKOVANÉ OSOBY

Článok 28

Notifikujúce orgány

1. Každý členský štát určí alebo zriadi aspoň jeden notifikujúci orgán, ktorý je zodpovedný za stanovenie a vykonávanie potrebných postupov na hodnotenie, určovanie a notifikáciu orgánov posudzovania zhody a ich monitorovanie. Tieto postupy sa vypracujú v rámci spolupráce medzi notifikujúcimi orgánmi všetkých členských štátov.

2. Členské štáty môžu rozhodnúť, že posudzovanie a monitorovanie uvedené v odseku 1 má vykonať vnútroštátny akreditačný orgán v zmysle nariadenia (ES) č. 765/2008 a v súlade s ním.

3. Notifikujúce orgány sa zriaďujú, organizujú a prevádzkujú takým spôsobom, aby nevznikol konflikt záujmov s orgánmi posudzovania zhody a aby bola zaručená objektívnosť a nestrannosť ich činnosti.

4. Notifikujúce orgány majú takú organizačnú štruktúru, aby rozhodnutia týkajúce sa notifikácie orgánov posudzovania zhody prijímali iné odborne spôsobilé osoby ako osoby, ktoré vykonali posudzovanie týchto orgánov.

5. Notifikujúce orgány neponúkajú ani neposkytujú žiadne činnosti, ktoré vykonávajú orgány posudzovania zhody, ani žiadne poradenské služby na komerčnom alebo konkurenčnom základe.

6. Notifikujúce orgány zabezpečia v súlade s článkom 78 dôvernosť informácií, ktoré získajú.

7. Notifikujúce orgány musia mať na riadne vykonávanie svojich úloh k dispozícii primeraný počet odborne spôsobilých zamestnancov. Odborne spôsobilí zamestnanci musia mať v relevantných prípadoch na svoju funkciu potrebné odborné znalosti v oblastiach, ako sú informačné technológie, AI a právo vrátane dohľadu nad základnými právami.

Článok 29

Žiadosť orgánu posudzovania zhody o notifikáciu

1. Žiadosť o notifikáciu predkladajú orgány posudzovania zhody notifikujúcemu orgánu členského štátu, v ktorom sú usadené.

2. K žiadosti o notifikáciu sa prikladá opis činností posudzovania zhody, modulu alebo modulov posudzovania zhody a typov systémov AI, vo vzťahu ku ktorým orgán posudzovania zhody tvrdí, že je odborne spôsobilý, ako aj osvedčenie o akreditácii, ak existuje, vydané vnútroštátnym akreditačným orgánom, ktorým sa potvrdzuje, že orgán posudzovania zhody spĺňa požiadavky stanovené v článku 31.

   Priložia sa všetky platné dokumenty týkajúce sa existujúcich prípadov, v ktorých bola žiadajúca notifikovaná osoba určená podľa iných harmonizačných právnych predpisov Únie.

3. Ak dotknutý orgán posudzovania zhody nemôže poskytnúť osvedčenie o akreditácii, poskytne notifikujúcemu orgánu všetky písomné doklady, ktoré sú potrebné na overenie, uznanie a pravidelné monitorovanie plnenia požiadaviek stanovených v článku 31 z jeho strany.

4. V prípade notifikovaných osôb, ktoré boli určené podľa iných harmonizačných právnych predpisov Únie, sa ako podklady pre postup ich určenia podľa tohto nariadenia môžu podľa potreby použiť všetky dokumenty a osvedčenia súvisiace s týmito určeniami. Notifikovaná osoba aktualizuje dokumentáciu uvedenú v odsekoch 2 a 3 tohto článku vždy, keď dôjde k relevantným zmenám, aby orgán zodpovedný za notifikované osoby mohol monitorovať a overovať priebežné dodržiavanie všetkých požiadaviek stanovených v článku 31.

Článok 30

Notifikačný postup

1. Notifikujúce orgány môžu notifikovať iba orgány posudzovania zhody, ktoré splnili požiadavky stanovené v článku 31.

2. Notifikujúce orgány prostredníctvom elektronického notifikačného nástroja vyvinutého a spravovaného Komisiou oznamujú Komisii a ostatným členským štátom každý orgán posudzovania zhody uvedený v odseku 1.

3. Notifikácia uvedená v odseku 2 tohto článku obsahuje všetky podrobnosti o činnostiach posudzovania zhody, module alebo moduloch posudzovania zhody, typoch dotknutých systémov AI a príslušné potvrdenie odbornej spôsobilosti. Ak sa notifikácia nezakladá na osvedčení o akreditácii uvedenom v článku 29 ods. 2, notifikujúci orgán poskytne Komisii a ostatným členským štátom písomné doklady potvrdzujúce odbornú spôsobilosť orgánu posudzovania zhody a zavedené opatrenia s cieľom zabezpečiť, aby bol tento orgán pravidelne monitorovaný a naďalej spĺňal požiadavky stanovené v článku 31.

4. Dotknutý orgán posudzovania zhody môže vykonávať činnosti notifikovanej osoby len vtedy, ak Komisia ani ostatné členské štáty nevznesú námietky do dvoch týždňov od notifikácie notifikujúcim orgánom, ak táto notifikácia zahŕňa osvedčenie o akreditácii uvedené v článku 29 ods. 2, alebo do dvoch mesiacov od notifikácie notifikujúceho orgánu, ak táto notifikácia zahŕňa písomné doklady uvedené v článku 29 ods. 3.

5. V prípade vznesenia námietok Komisia bezodkladne začne konzultácie s dotknutými členskými štátmi a orgánom posudzovania zhody. Komisia so zreteľom na tieto konzultácie rozhodne, či je povolenie opodstatnené. Komisia svoje rozhodnutie oznámi dotknutému členskému štátu a príslušnému orgánu posudzovania zhody.

Článok 31

Požiadavky týkajúce sa notifikovaných osôb

1. Notifikovaná osoba je zriadená podľa vnútroštátneho práva členského štátu a má právnu subjektivitu.

2. Notifikované osoby musia spĺňať požiadavky týkajúce sa organizácie, riadenia kvality, zdrojov a postupov, ktoré sú potrebné na plnenie ich úloh, ako aj náležité požiadavky na kybernetickú bezpečnosť.

3. Organizačná štruktúra, rozdelenie zodpovedností, hierarchické vzťahy a fungovanie notifikovaných osôb musia zabezpečiť dôveru v ich konanie a vo výsledky činností posudzovania zhody, ktoré notifikované osoby vykonávajú.

4. Notifikované osoby musia byť nezávislé od poskytovateľa vysokorizikového systému AI, v súvislosti s ktorým vykonávajú činnosti posudzovania zhody. Notifikované osoby musia byť takisto nezávislé od akéhokoľvek iného prevádzkovateľa, ktorý má na posudzovaných vysokorizikových systémoch AI hospodársky záujem, ako aj od akýchkoľvek konkurentov poskytovateľa. Týmto sa nevylučuje používanie posudzovaných vysokorizikových systémov AI, ktoré sú potrebné na výkon činností orgánu posudzovania zhody, alebo používanie takýchto vysokorizikových systémov AI na osobné účely.

5. Orgán posudzovania zhody, jeho vrcholový manažment ani zamestnanci zodpovední za vykonávanie jeho úloh posudzovania zhody nesmú byť priamo zapojení do dizajnovania, vývoja, uvádzania na trh alebo používania vysokorizikových systémov AI, ani nesmú zastupovať strany zapojené do týchto činností. Nesmú sa podieľať na žiadnej činnosti, ktorá by mohla ovplyvniť nezávislosť ich úsudku alebo bezúhonnosť vo vzťahu k činnostiam posudzovania zhody, na ktorých vykonávanie sú notifikované. Platí to najmä pre poradenské služby.

6. Notifikované osoby musia mať takú organizačnú štruktúru a fungovať tak, aby sa zaručila nezávislosť, objektivita a nestrannosť ich činností. Notifikované osoby zdokumentujú a zavedú štruktúru a postupy, ktorými sa zaručí nestrannosť a ktorými sa presadzujú a uplatňujú zásady nestrannosti v celej ich organizačnej štruktúre, u všetkých zamestnancov a pri všetkých činnostiach posudzovania.

7. Notifikované osoby zavedú zdokumentované postupy, ktorými sa zabezpečí, aby ich zamestnanci, výbory, dcérske spoločnosti, subdodávatelia a akýkoľvek pridružený subjekt alebo zamestnanci externých subjektov zachovávali v súlade s článkom 78 dôvernosť informácií, ktoré získajú počas vykonávania činností posudzovania zhody, s výnimkou prípadov, keď sa zverejnenie týchto informácií vyžaduje podľa zákona. Zamestnanci notifikovaných osôb sú povinní zachovávať služobné tajomstvo vo vzťahu k všetkým informáciám, ktoré získali pri vykonávaní svojich úloh podľa tohto nariadenia; táto povinnosť sa neuplatňuje vo vzťahu k notifikujúcim orgánom členského štátu, v ktorom sa ich činnosti vykonávajú.

8. Na vykonávanie činností majú notifikované osoby postupy, pri ktorých sa náležite zohľadňuje veľkosť poskytovateľa, odvetvie, v ktorom podnik pôsobí, jeho štruktúra a stupeň zložitosti dotknutého systému AI

9. Notifikované osoby v súvislosti so svojimi činnosťami posudzovania zhody uzavrú primerané poistenie zodpovednosti, ak na seba v súlade s vnútroštátnym právom neprevzal zodpovednosť členský štát, v ktorom sú usadené, alebo ak za posudzovanie zhody nezodpovedá priamo tento samotný členský štát.

10. Všetky úlohy, ktoré im prináležia podľa tohto nariadenia, musia byť notifikované osoby spôsobilé vykonávať na najvyššej úrovni profesijnej bezúhonnosti a s náležitou odbornou spôsobilosťou v danej oblasti bez ohľadu na to, či tieto úlohy vykonávajú samotné notifikované osoby alebo sa vykonávajú v ich mene a na ich zodpovednosť.

11. Notifikované osoby musia byť na internej úrovni dostatočne spôsobilé, aby boli schopné hodnotiť úlohy, ktoré v ich mene vykonávajú externé subjekty. Notifikovaná osoba musí mať trvale k dispozícii dostatočný počet administratívnych, technických, právnických a vedeckých pracovníkov, ktorí majú skúsenosti a vedomosti týkajúce sa relevantných typov systémov AI, údajov a výpočtov údajov, ako aj požiadaviek stanovených v oddiele 2.

12. Notifikované osoby sa zúčastňujú na koordinačných činnostiach uvedených v článku 38. Takisto sa priamo zúčastňujú na činnosti európskych normalizačných organizácií alebo sú v nich zastúpené, alebo zabezpečia, aby boli nepretržite informované o aktuálnom stave príslušných noriem.

Článok 32

Predpoklad súladu s požiadavkami týkajúcimi sa notifikovaných osôb

Ak orgán posudzovania zhody preukáže splnenie kritérií stanovených v príslušných harmonizovaných normách alebo ich častiach, na ktoré boli uverejnené odkazy v *Úradnom vestníku Európskej únie*, predpokladá sa, že daný orgán spĺňa požiadavky stanovené v článku 31 v rozsahu, v akom sa na uvedené požiadavky uplatňujú harmonizované normy.

Článok 33

Dcérske spoločnosti notifikovaných osôb a subdodávatelia

1. Ak notifikovaná osoba zadáva osobitné úlohy spojené s posudzovaním zhody subdodávateľovi alebo ich prenesie na dcérsku spoločnosť, zabezpečí, aby tento subdodávateľ alebo táto dcérska spoločnosť spĺňali požiadavky stanovené v článku 31, a náležite o tom informuje notifikujúci orgán.

2. Notifikované osoby nesú plnú zodpovednosť za úlohy vykonávané akýmikoľvek subdodávateľmi alebo dcérskymi spoločnosťami.

3. Vykonávanie činností sa môže zadať subdodávateľovi alebo preniesť na dcérsku spoločnosť iba so súhlasom poskytovateľa. Notifikované osoby zverejnia zoznam svojich dcérskych spoločností.

4. Príslušná dokumentácia týkajúca sa posúdenia kvalifikácie subdodávateľa alebo dcérskej spoločnosti a práce, ktorú vykonali podľa tohto nariadenia, sa uchováva k dispozícii notifikujúcemu orgánu počas obdobia piatich rokov od dátumu ukončenia subdodávok.

Článok 34

Operačné povinnosti notifikovaných osôb

1. Notifikované osoby overujú zhodu vysokorizikových systémov AI v súlade s postupmi posudzovania zhody uvedenými v článku 43.

2. Notifikované osoby sa vyhýbajú zbytočnému zaťaženiu poskytovateľov pri vykonávaní ich činností a náležite zohľadňujú veľkosť poskytovateľa, odvetvie, v ktorom pôsobí, jeho štruktúru a stupeň zložitosti dotknutého vysokorizikového systému AI, najmä v záujme minimalizácie administratívneho zaťaženia a nákladov na dodržiavanie predpisov pre mikropodniky a malé podniky v zmysle odporúčania 2003/361/ES. Notifikovaná osoba však dodržiava mieru prísnosti a úroveň ochrany, ktoré sú potrebné na zabezpečenie súladu vysokorizikového systému AI s požiadavkami stanovenými v tomto nariadení.

3. Notifikované osoby sprístupnia a na požiadanie predložia všetky príslušné dokumenty vrátane dokumentácie poskytovateľa notifikujúcemu orgánu uvedenému v článku 28, aby mohol vykonávať svoje činnosti posudzovania, určovania, notifikácie a monitorovania a aby sa uľahčilo posudzovanie podľa tohto oddielu.

Článok 35

Identifikačné čísla a zoznamy notifikovaných osôb

1. Komisia pridelí každej notifikovanej osobe jedno identifikačné číslo, a to aj v prípade, že je osoba notifikovaná podľa viac ako jedného aktu Únie.

2. Komisia zverejní zoznam osôb notifikovaných podľa tohto nariadenia vrátane ich identifikačných čísiel a činností, v súvislosti s ktorými boli notifikované. Komisia tento zoznam aktualizuje.

Článok 36

Zmeny notifikácií

1. Notifikujúci orgán oznamuje Komisii a ostatným členským štátom všetky relevantné zmeny týkajúce sa notifikácie notifikovanej osoby prostredníctvom elektronického nástroja notifikácie uvedeného v článku 30 ods. 2.

2. Postupy stanovené v článkoch 29 a 30 sa uplatňujú na rozširovanie rozsahu notifikácie.

   V prípade iných zmien notifikácie, ako je rozšírenie jej rozsahu, sa uplatňujú postupy stanovené v odsekoch 3 až 9.

3. Ak sa notifikovaná osoba rozhodne ukončiť svoje činnosti posudzovania zhody, čo najskôr to oznámi notifikujúcemu orgánu a dotknutým poskytovateľom a v prípade plánovaného ukončenia svojich činností aspoň jeden rok pred ich ukončením. Certifikáty notifikovanej osoby môžu zostať v platnosti na obdobie deviatich mesiacov po ukončení činností notifikovanej osoby pod podmienkou, že ďalšia notifikovaná osoba písomne potvrdí, že prevezme zodpovednosť za vysokorizikové systémy AI, na ktoré sa tieto certifikáty vzťahujú. Notifikovaná osoba, ktorá prevzala zodpovednosť za vysokorizikové systémy AI, dokončí úplné posúdenie dotknutých vysokorizikových systémov AI do konca uvedenej deväťmesačnej lehoty pred vydaním nového certifikátu pre tieto systémy. Ak notifikovaná osoba ukončila svoju činnosť, notifikujúci orgán určenie zruší.

4. Ak má notifikujúci orgán dostatočný dôvod domnievať sa, že notifikovaná osoba už nespĺňa požiadavky stanovené v článku 31 alebo že si neplní svoje povinnosti, notifikujúci orgán túto záležitosť bezodkladne čo najdôkladnejšie prešetrí. V tejto súvislosti informuje dotknutú notifikovanú osobu o vznesených námietkach a poskytne jej možnosť na vyjadrenie stanoviska. Ak notifikujúci orgán dospeje k záveru, že notifikovaná osoba už nespĺňa požiadavky stanovené v článku 31 alebo že si neplní svoje povinnosti, podľa potreby obmedzí, pozastaví alebo zruší určenie v závislosti od závažnosti neplnenia týchto požiadaviek alebo povinností. Okamžite o tom informuje Komisiu a ostatné členské štáty.

5. Ak je určenie notifikovanej osoby pozastavené, obmedzené alebo úplne či čiastočne zrušené, notifikovaná osoba o tom do 10 dní informuje dotknutých poskytovateľov.

6. V prípade obmedzenia, pozastavenia alebo zrušenia určenia notifikujúci orgán prijme vhodné opatrenia, ktorými zabezpečí, aby sa dokumentácia príslušnej notifikovanej osoby uchovávala, a na požiadanie ju sprístupní notifikujúcim orgánom v iných členských štátoch a orgánom dohľadu nad trhom.

7. V prípade obmedzenia, pozastavenia alebo zrušenia určenia notifikujúci orgán:

   a) posudzuje vplyv na certifikáty vydané notifikovanou osobou;

   b) predkladá Komisii a ostatným členským štátom správu o svojich zisteniach do troch mesiacov po oznámení zmien určenia;

c) požaduje od notifikovanej osoby, aby v primeranej lehote, ktorú tento orgán stanoví, pozastavila alebo stiahla všetky certifikáty, ktoré boli vydané neoprávnene, s cieľom zaistiť pokračujúcu zhodu vysokorizikových systémov AI na trhu;

d) informuje Komisiu a členské štáty o certifikátoch, ktorých pozastavenie alebo stiahnutie požaduje;

e) poskytne vnútroštátnym príslušným orgánom členského štátu, v ktorom má poskytovateľ registrované miesto podnikania, všetky relevantné informácie o certifikátoch, v prípade ktorých požiadal o pozastavenie alebo stiahnutie; ak je to potrebné na zabránenie potenciálnemu riziku pre zdravie, bezpečnosť alebo základné práva, uvedený orgán prijme primerané opatrenia.

8. S výnimkou certifikátov, ktoré boli vydané neoprávnene, a prípadov, keď bolo určenie pozastavené alebo obmedzené, zostávajú certifikáty platné za jednej z týchto okolností:

a) notifikujúci orgán do jedného mesiaca od pozastavenia alebo obmedzenia potvrdil, že vo vzťahu k certifikátom, na ktoré sa pozastavenie alebo obmedzenie vzťahuje, neexistuje riziko pre zdravie, bezpečnosť ani základné práva, a navrhol harmonogram opatrení, ktoré povedú k zrušeniu pozastavenia alebo obmedzenia, alebo

b) notifikujúci orgán potvrdil, že sa počas pozastavenia alebo obmedzenia nebudú vydávať, meniť ani opätovne vydávať žiadne certifikáty, a uvedie, či je notifikovaná osoba spôsobilá naďalej monitorovať existujúce certifikáty vydané na obdobie pozastavenia alebo obmedzenia a zodpovedať za ne; ak notifikujúci orgán zistí, že notifikovaná osoba nie je spôsobilá podporovať existujúce vydané certifikáty, poskytovateľ systému, na ktorý sa certifikát vzťahuje, písomne potvrdí vnútroštátnym príslušným orgánom členského štátu, v ktorom má registrované miesto podnikania, do troch mesiacov od pozastavenia alebo obmedzenia, že iná kvalifikovaná notifikovaná osoba dočasne preberá funkcie notifikovanej osoby v oblasti monitorovania certifikátov a zostáva za ne zodpovedná počas obdobia pozastavenia alebo obmedzenia.

9. S výnimkou certifikátov, ktoré boli vydané neoprávnene, a zrušenia určenia zostávajú certifikáty platné počas obdobia deviatich mesiacov za týchto okolností:

a) vnútroštátny príslušný orgán členského štátu, v ktorom má poskytovateľ vysokorizikového systému AI, na ktorý sa vzťahuje certifikát, registrované miesto podnikania, potvrdil, že v súvislosti s dotknutými vysokorizikovými systémami AI neexistuje žiadne riziko pre zdravie, bezpečnosť alebo základné práva, a

b) iná notifikovaná osoba písomne potvrdila, že okamžite prevezme zodpovednosť za uvedené systémy AI a dokončí svoje posúdenie do 12 mesiacov od zrušenia určenia.

Za okolností uvedených v prvom pododseku môže vnútroštátny príslušný orgán členského štátu, v ktorom má poskytovateľ systému, na ktorý sa certifikát vzťahuje, svoje miesto podnikania, predĺžiť obdobie prechodnej platnosti certifikátov na ďalšie obdobia troch mesiacov, ktoré celkovo neprekročia obdobie 12 mesiacov.

Vnútroštátny príslušný orgán alebo notifikovaná osoba preberajúca úlohy notifikovanej osoby, ktorej sa týka zmena určenia, o tom bezodkladne informuje Komisiu, ostatné členské štáty a ostatné notifikované osoby.

Článok 37

Napadnutie odbornej spôsobilosti notifikovaných osôb

1. Komisia v prípade potreby vyšetrí všetky prípady, v ktorých existujú dôvody pochybovať o odbornej spôsobilosti notifikovanej osoby alebo o pokračujúcom plnení požiadaviek stanovených v článku 31 a uplatniteľných povinností zo strany notifikovanej osoby.

2. Notifikujúci orgán poskytne na požiadanie Komisii všetky relevantné informácie týkajúce sa notifikácie alebo zachovania odbornej spôsobilosti dotknutej notifikovanej osoby.

3. Komisia zabezpečí dôverné zaobchádzanie v súlade s článkom 78 so všetkými citlivými informáciami získanými počas svojich vyšetrovaní podľa tohto článku.

4. Keď Komisia zistí, že notifikovaná osoba nespĺňa alebo prestala spĺňať požiadavky na jej notifikáciu, informuje o tom notifikujúci členský štát a požiada ho, aby prijal potrebné nápravné opatrenia vrátane prípadného pozastavenia alebo zrušenia určenia. Ak daný členský štát neprijme potrebné nápravné opatrenia, Komisia môže prostredníctvom vykonávacieho aktu pozastaviť, obmedziť alebo zrušiť určenie. Uvedený vykonávací akt sa prijme v súlade s postupom preskúmania uvedeným v článku 98 ods. 2.

Článok 38

Koordinácia notifikovaných osôb

1. Komisia zabezpečí, aby sa so zreteľom na vysokorizikové systémy AI, na ktoré sa vzťahuje toto nariadenie, medzi notifikovanými osobami pôsobiacimi v oblasti postupov posudzovania zhody podľa tohto nariadenia zaviedla a riadne vykonávala primeraná koordinácia a spolupráca v podobe odvetvovej skupiny notifikovaných osôb.

2. Každý notifikujúci orgán zabezpečí, aby sa ním notifikované osoby zúčastňovali na práci skupiny uvedenej v odseku 1, a to priamo alebo prostredníctvom určených zástupcov.

3. Komisia zabezpečí výmenu poznatkov a najlepších postupov medzi notifikujúcimi orgánmi.

Článok 39

Orgány posudzovania zhody tretích krajín

Orgány posudzovania zhody zriadené podľa práva tretej krajiny, s ktorou Únia uzavrela dohodu, môžu byť oprávnené vykonávať činnosti notifikovaných osôb podľa tohto nariadenia za predpokladu, že spĺňajú požiadavky stanovené v článku 31 alebo zabezpečujú rovnocennú úroveň súladu.

ODDIEL 5

NORMY, POSUDZOVANIE ZHODY, CERTIFIKÁTY, REGISTRÁCIA

Článok 40

Harmonizované normy a normalizačné produkty

1. Vysokorizikové systémy AI alebo modely AI na všeobecné účely, ktoré sú v zhode s harmonizovanými normami alebo ich časťami, na ktoré boli uverejnené odkazy v *Úradnom vestníku Európskej únie* v súlade s nariadením (EÚ) č. 1025/2012, sa považujú za systémy alebo modely, ktoré sú v zhode s požiadavkami stanovenými v oddiele 2 tejto kapitoly alebo, v relevantnom prípade, s povinnosťami stanovenými v oddieloch 2 a 3 kapitoly V tohto nariadenia, a to v rozsahu, v akom sa tieto normy vzťahujú na uvedené požiadavky alebo povinnosti.

2. Komisia v súlade s článkom 10 nariadenia (EÚ) č. 1025/2012 bez zbytočného odkladu vydá žiadosti o normalizáciu týkajúce sa všetkých požiadaviek stanovených v oddiele 2 tejto kapitoly a v relevantnom prípade žiadosti o normalizáciu týkajúce sa povinností stanovených v oddieloch 2 a 3 kapitoly V tohto nariadenia. V žiadosti o normalizáciu sa žiada aj o produkty týkajúce sa procesov podávania správ a dokumentácie s cieľom zlepšiť výkon systémov AI z hľadiska spotreby zdrojov, ako je zníženie spotreby energie a iných zdrojov vysokorizikového systému AI počas jeho životného cyklu, ako aj produkty týkajúce sa energeticky efektívneho vývoja modelov AI na všeobecné účely. Pri príprave žiadosti o normalizáciu Komisia konzultuje s radou pre AI a relevantnými zainteresovanými stranami vrátane poradného fóra.

Pri vydávaní žiadosti o normalizáciu určenej európskym normalizačným organizáciám Komisia špecifikuje, že normy musia byť jasné, konzistentné, a to aj s normami vypracovanými v rôznych odvetviach pre výrobky, na ktoré sa vzťahujú existujúce harmonizačné právne predpisy Únie uvedené v prílohe I, a s cieľom zabezpečiť, aby vysokorizikové systémy AI alebo modely AI na všeobecné účely uvedené na trh alebo do prevádzky v Únii spĺňali príslušné požiadavky alebo povinnosti stanovené v tomto nariadení.

Komisia požiada európske normalizačné organizácie, aby poskytli dôkazy o svojom najlepšom úsilí pri plnení cieľov uvedených v prvom a druhom pododseku tohto odseku v súlade s článkom 24 nariadenia (EÚ) č. 1025/2012.

3. Účastníci procesu normalizácie sa snažia podporovať investície a inovácie v oblasti AI, okrem iného aj zvyšovaním právnej istoty, ako aj konkurencieschopnosť a rast trhu Únie, prispievať k posilňovaniu globálnej spolupráce v oblasti normalizácie, pričom zohľadňujú existujúce medzinárodné normy v oblasti AI, ktoré sú v súlade s hodnotami, základnými právami a záujmami Únie, a posilňovať správu a riadenie, ktoré vykonáva viacero zainteresovaných strán, čím sa zabezpečuje vyvážené zastúpenie záujmov a efektívna účasť všetkých relevantných zainteresovaných strán v súlade s článkami 5, 6 a 7 nariadenia (EÚ) č. 1025/2012.

Článok 41

Spoločné špecifikácie

1. Komisia môže prijať vykonávacie akty, v ktorých stanoví spoločné špecifikácie pre požiadavky stanovené v oddiele 2 tejto kapitoly alebo v relevantnom prípade pre povinnosti stanovené v oddieloch 2 a 3 kapitoly V, ak sú splnené tieto podmienky:

   a) Komisia podľa článku 10 ods. 1 nariadenia (EÚ) č. 1025/2012 požiadala jednu alebo viacero európskych normalizačných organizácií, aby vypracovali harmonizovanú normu pre požiadavky stanovené v oddiele 2 tejto kapitoly alebo v relevantnom prípade pre povinnosti stanovené v oddieloch 2 a 3 kapitoly V, a:

      i) žiadosť neprijala ani jedna z európskych normalizačných organizácií, alebo

ii) harmonizované normy na riešenie tejto žiadosti neboli doručené v lehote stanovenej v súlade s článkom 10 ods. 1 nariadenia (EÚ) č. 1025/2012, alebo

iii) príslušné harmonizované normy nedostatočne riešia obavy týkajúce sa základných práv, alebo

iv) harmonizované normy nie sú v súlade so žiadosťou, a

b) v *Úradnom vestníku Európskej únie* nie je v súlade s nariadením (EÚ) č. 1025/2012 uverejnený odkaz na harmonizované normy týkajúce sa požiadaviek stanovených v oddiele 2 tejto kapitoly alebo v relevantnom prípade povinností stanovených v oddieloch 2 a 3 kapitoly V a neočakáva sa, že v primeranej lehote bude takýto odkaz uverejnený.

Komisia pri vypracúvaní spoločných špecifikácií vedie konzultácie s poradným fórom uvedeným v článku 67.

Vykonávacie akty uvedené v prvom pododseku tohto odseku sa prijmú v súlade s postupom preskúmania uvedeným v článku 98 ods. 2.

2. Pred vypracovaním návrhu vykonávacieho aktu Komisia informuje výbor uvedený v článku 22 nariadenia (EÚ) č. 1025/2012 o tom, že sa domnieva, že podmienky uvedené v odseku 1 tohto článku sú splnené.

3. Vysokorizikové systémy AI alebo modely AI na všeobecné účely, ktoré sú v zhode so spoločnými špecifikáciami uvedenými v odseku 1 alebo ich časťami, sa považujú za systémy alebo modely, ktoré sú v zhode s požiadavkami stanovenými v oddiele 2 tejto kapitoly, alebo ktoré v relevantnom prípade spĺňajú povinnosti stanovené v oddieloch 2 a 3 kapitoly V, a to v rozsahu, v akom sa uvedené spoločné špecifikácie vzťahujú na uvedené požiadavky alebo uvedené povinnosti.

4. Ak európska normalizačná organizácia prijme harmonizovanú normu a navrhne Komisii, aby uverejnila odkaz na ňu v *Úradnom vestníku Európskej únie*, Komisia túto harmonizovanú normu posúdi v súlade s nariadením (EÚ) č. 1025/2012. Keď sa v *Úradnom vestníku Európskej únie* uverejní odkaz na harmonizovanú normu, Komisia zruší vykonávacie akty uvedené v odseku 1 alebo tie ich časti, ktoré sa vzťahujú na rovnaké požiadavky stanovené v oddiele 2 tejto kapitoly alebo v relevantnom prípade na rovnaké povinnosti stanovené v oddieloch 2 a 3 kapitoly V.

5. Ak poskytovatelia vysokorizikových systémov AI alebo modelov AI na všeobecné účely nedodržiavajú spoločné špecifikácie uvedené v odseku 1, riadne odôvodnia, že prijali technické riešenia, ktoré spĺňajú požiadavky uvedené v oddiele 2 tejto kapitoly alebo v relevantnom prípade spĺňajú povinnosti stanovené v oddieloch 2 a 3 kapitoly V aspoň na rovnakej úrovni.

6. Ak sa členský štát domnieva, že spoločná špecifikácia nespĺňa úplne požiadavky stanovené v oddiele 2 alebo v relevantnom prípade povinnosti stanovené v oddieloch 2 a 3 kapitoly V, informuje o tom Komisiu s podrobným vysvetlením. Komisia posúdi tieto informácie a v prípade potreby zmení vykonávací akt, ktorým sa stanovuje dotknutá spoločná špecifikácia.

Článok 42

Predpoklad zhody s určitými požiadavkami

1. Vysokorizikové systémy AI, ktoré boli trénované a testované na údajoch, ktoré odzrkadľujú konkrétne geografické, behaviorálne, kontextuálne alebo funkčné podmienky, v ktorých sa majú používať, sa považujú za systémy, ktoré sú v súlade s príslušnými požiadavkami stanovenými v článku 10 ods. 4.

2. Vysokorizikové systémy AI, ktoré boli certifikované alebo pre ktoré bolo vydané vyhlásenie o zhode v rámci schémy certifikácie kybernetickej bezpečnosti podľa nariadenia (EÚ) 2019/881, a na ktoré boli uverejnené odkazy v *Úradnom vestníku Európskej únie*, sa považujú za systémy, ktoré sú v súlade s kybernetickobezpečnostnými požiadavkami stanovenými v článku 15 tohto nariadenia, pokiaľ sa certifikát kybernetickej bezpečnosti alebo vyhlásenie o zhode alebo ich časti na tieto požiadavky vzťahujú.

Článok 43

Posudzovanie zhody

1. Ak poskytovateľ pri preukazovaní súladu vysokorizikového systému AI uvedeného v prílohe III bode 1 s požiadavkami stanovenými v oddiele 2 uplatnil harmonizované normy uvedené v článku 40, alebo v relevantnom prípade spoločné špecifikácie uvedené v článku 41, rozhodne sa pre jeden z týchto postupov posudzovania zhody založený na:

   a) vnútornej kontrole uvedenej v prílohe VI, alebo

   b) posudzovaní systému riadenia kvality a posudzovaní technickej dokumentácie so zapojením notifikovanej osoby podľa prílohy VII.

   Pri preukazovaní súladu vysokorizikového systému AI s požiadavkami stanovenými v oddiele 2 poskytovateľ dodržiava postup posudzovania zhody stanovený v prílohe VII, ak:

   a) harmonizované normy uvedené v článku 40 neexistujú a spoločné špecifikácie uvedené v článku 41 nie sú k dispozícii;

   b) poskytovateľ harmonizovanú normu neuplatnil alebo ju uplatnil len čiastočne;

   c) spoločné špecifikácie uvedené v písmene a) existujú, ale poskytovateľ ich neuplatnil;

d) jedna alebo viaceré harmonizované normy uvedené v písmene a) boli uverejnené s obmedzením a len pre tú časť normy, ktorá bola obmedzená.

Na účely postupu posudzovania zhody uvedeného v prílohe VII si poskytovateľ môže vybrať ktorúkoľvek z notifikovaných osôb. Ak však majú vysokorizikový systém AI uviesť do prevádzky orgány presadzovania práva, imigračné alebo azylové orgány, alebo inštitúcie, orgány, úrady alebo agentúry Únie, ako notifikovaná osoba koná orgán dohľadu nad trhom uvedený v článku 74 ods. 8 alebo 9.

2. V prípade vysokorizikových systémov AI uvedených v prílohe III bodoch 2 až 8 poskytovatelia dodržiavajú postup posudzovania zhody na základe vnútornej kontroly uvedený v prílohe VI, v ktorom sa nestanovuje zapojenie notifikovanej osoby.

3. V prípade vysokorizikových systémov AI, na ktoré sa vzťahujú harmonizačné právne predpisy Únie uvedené v prílohe I oddiele A, poskytovateľ dodržiava príslušný postup posudzovania zhody, ako sa vyžaduje v uvedených právnych aktoch. Na uvedené vysokorizikové systémy AI sa vzťahujú požiadavky stanovené v oddiele 2 tejto kapitoly a sú súčasťou tohto posúdenia. Uplatňuje sa aj príloha VII body 4.3, 4.4, 4.5 a bod 4.6 piaty odsek.

Na účely uvedeného posúdenia sú notifikované osoby, ktoré boli notifikované podľa uvedených právnych aktov, oprávnené kontrolovať súlad vysokorizikových systémov AI s požiadavkami stanovenými v oddiele 2 za predpokladu, že v rámci postupu notifikácie podľa uvedených právnych aktov sa posúdil súlad týchto notifikovaných osôb s požiadavkami stanovenými v článku 31 ods. 4, 5, 10 a 11.

Ak právny akt uvedený v prílohe I oddiele A umožňuje výrobcovi výrobku neuplatňovať posudzovanie zhody treťou stranou za predpokladu, že uplatnil všetky harmonizované normy vzťahujúce sa na všetky príslušné požiadavky, môže tento výrobca využiť túto možnosť len vtedy, ak uplatnil aj harmonizované normy alebo v relevantnom prípade spoločné špecifikácie uvedené v článku 41, ktoré sa vzťahujú na všetky požiadavky stanovené v oddiele 2 tejto kapitoly.

4. V prípade, že dôjde k podstatnej zmene vysokorizikových systémov AI, ktoré už prešli postupom posudzovania zhody, podrobia sa novému postupu posudzovania zhody, a to bez ohľadu na to, či je zmenený systém určený na ďalšiu distribúciu alebo či ho ďalej používa súčasný nasadzujúci subjekt.

V prípade vysokorizikových systémov AI, ktoré sa po uvedení na trh alebo do prevádzky ďalej učia, nepredstavujú podstatnú zmenu tie zmeny vysokorizikového systému AI a jeho výkonnosti, ktoré poskytovateľ určil vopred v čase počiatočného posudzovania zhody a ktoré sú zahrnuté v informáciách obsiahnutých v technickej dokumentácii uvedenej v prílohe IV bode 2 písm. f).

5. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 97 na účely zmeny príloh VI a VII ich aktualizáciou vzhľadom na technický pokrok.

6. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 97 na účely zmeny odsekov 1 a 2 tohto článku s cieľom podrobiť vysokorizikové systémy AI uvedené v prílohe III bodoch 2 až 8 postupu posudzovania zhody uvedenému v prílohe VII alebo jeho častiam. Pri prijímaní takýchto delegovaných aktov Komisia zohľadní účinnosť postupu posudzovania zhody na základe vnútornej kontroly uvedeného v prílohe VI pri predchádzaní alebo minimalizácii rizík pre zdravie, bezpečnosť a ochranu základných práv, ktoré takéto systémy predstavujú, ako aj dostupnosť primeraných kapacít a zdrojov notifikovaných osôb.

Článok 44

Certifikáty

1. Certifikáty vydané notifikovanými osobami v súlade s prílohou VII sa vyhotovujú v jazyku, ktorému príslušné orgány v členskom štáte, v ktorom je notifikovaná osoba usadená, bez problémov rozumejú.

2. Certifikáty platia na obdobie, ktoré sa v nich uvádza a ktoré nepresiahne päť rokov v prípade systémov AI, na ktoré sa vzťahuje príloha I, a obdobie štyroch rokov v prípade systémov AI, na ktoré sa vzťahuje príloha III. Na žiadosť poskytovateľa možno platnosť certifikátu predĺžiť na ďalšie obdobia, z ktorých žiadne nepresiahne päť rokov v prípade systémov AI, na ktoré sa vzťahuje príloha I, a štyri roky v prípade systémov AI, na ktoré sa vzťahuje príloha III, a to na základe opätovného posúdenia v súlade s uplatniteľnými postupmi posudzovania zhody. Akýkoľvek dodatok k certifikátu zostáva v platnosti, kým sa neskončí platnosť certifikátu, ktorý dopĺňa.

3. Ak notifikovaná osoba zistí, že systém AI prestal spĺňať požiadavky stanovené v oddiele 2, pozastaví so zreteľom na zásadu primeranosti platnosť vydaného certifikátu alebo ho stiahne, alebo jeho platnosť obmedzí, pokiaľ sa v primeranej lehote stanovenej notifikovanou osobou vhodnými nápravnými opatreniami prijatými poskytovateľom systému nezabezpečí súlad s týmito požiadavkami. Notifikovaná osoba svoje rozhodnutie odôvodní.

Proti rozhodnutiam notifikovaných osôb možno podať odvolanie, a to aj vo veci vydaných certifikátov zhody.

Článok 45

Informačné povinnosti notifikovaných osôb

1. Notifikované osoby informujú notifikujúci orgán:

a) o všetkých certifikátoch Únie o posúdení technickej dokumentácie, všetkých dodatkoch k týmto certifikátom a všetkých schváleniach systémov riadenia kvality vydaných v súlade s požiadavkami prílohy VII;

b) o všetkých zamietnutiach, obmedzeniach platnosti, pozastaveniach platnosti alebo stiahnutiach certifikátov Únie o posúdení technickej dokumentácie alebo schválení systémov riadenia kvality vydaných v súlade s požiadavkami prílohy VII;

c) o všetkých okolnostiach, ktoré majú vplyv na rozsah alebo podmienky notifikácie;

d) o každej žiadosti o informácie, ktorú dostali od orgánov dohľadu nad trhom v súvislosti s činnosťami posudzovania zhody;

e) na požiadanie o činnostiach posudzovania zhody vykonaných v rozsahu ich notifikácie a o akejkoľvek inej vykonanej činnosti vrátane cezhraničných činností a zadávania činností subdodávateľom.

2. Každá notifikovaná osoba informuje ostatné notifikované osoby o:

a) schváleniach systémov riadenia kvality, ktoré zamietla, ktorých platnosť pozastavila alebo ktoré stiahla, a na požiadanie o schváleniach systémov riadenia kvality, ktoré vydala;

b) certifikátoch Únie o posúdení technickej dokumentácie alebo akýchkoľvek ich dodatkoch, ktoré zamietla, stiahla, ktorých platnosť pozastavila alebo inak obmedzila, a na požiadanie o certifikátoch a/alebo ich dodatkoch, ktoré vydala.

3. Každá notifikovaná osoba poskytne ostatným notifikovaným osobám, ktoré vykonávajú podobné činnosti posudzovania zhody vzťahujúce sa na rovnaké typy systémov AI, relevantné informácie o otázkach týkajúcich sa negatívnych a na požiadanie aj pozitívnych výsledkov posudzovania zhody.

4. Notifikované osoby zabezpečia dôvernosť informácií, ktoré získajú, v súlade s článkom 78.

Článok 46

Výnimka z postupu posudzovania zhody

1. Odchylne od článku 43 a na základe riadne odôvodnenej žiadosti môže každý orgán dohľadu nad trhom z výnimočných dôvodov verejnej bezpečnosti alebo ochrany života a zdravia osôb, ochrany životného prostredia a ochrany kľúčových priemyselných a infraštruktúrnych aktív povoliť uvedenie konkrétnych vysokorizikových systémov AI na trh alebo do prevádzky na území dotknutého členského štátu. Toto povolenie sa udelí na obmedzené obdobie, kým sa vykonávajú potrebné postupy posudzovania zhody, pričom sa zohľadnia výnimočné dôvody odôvodňujúce výnimku. Uvedené postupy sa dokončia bez zbytočného odkladu.

2. V riadne odôvodnenej naliehavej situácii z výnimočných dôvodov verejnej bezpečnosti alebo v prípade konkrétneho, závažného a bezprostredného ohrozenia života alebo fyzickej bezpečnosti fyzických osôb môžu orgány presadzovania práva alebo orgány civilnej ochrany uviesť do prevádzky konkrétny vysokorizikový systém AI bez povolenia uvedeného v odseku 1 za predpokladu, že o takéto povolenie sa bez zbytočného odkladu požiada počas jeho používania alebo po ňom. Ak sa povolenie uvedené v odseku 1 zamietne, používanie vysokorizikového systému AI sa s okamžitou účinnosťou zastaví a všetky výsledky a výstupy takéhoto používania sa okamžite zlikvidujú.

3. Povolenie uvedené v odseku 1 sa vydá len vtedy, ak orgán dohľadu nad trhom dospeje k záveru, že vysokorizikový systém AI spĺňa požiadavky oddielu 2. O každom povolení vydanom podľa odsekov 1 a 2 informuje orgán dohľadu nad trhom Komisiu a ostatné členské štáty. Táto povinnosť sa nevzťahuje na citlivé operačné údaje týkajúce sa činností orgánov presadzovania práva.

4. Ak žiaden členský štát ani Komisia do 15 kalendárnych dní od doručenia informácií uvedených v odseku 3 nevznesú námietku proti povoleniu vydanému orgánom dohľadu na trhom členského štátu v súlade s odsekom 1, toto povolenie sa považuje za opodstatnené.

5. Ak do 15 kalendárnych dní od doručenia oznámenia uvedeného v odseku 3 členský štát vznesie námietky proti povoleniu, ktoré vydal orgán dohľadu nad trhom iného členského štátu, alebo ak sa Komisia domnieva, že povolenie je v rozpore s právom Únie alebo že záver členských štátov, pokiaľ ide o súlad systému uvedeného v odseku 3, je neopodstatnený, Komisia začne bezodkladne konzultácie s príslušným členským štátom. S dotknutými prevádzkovateľmi sa vedú konzultácie a majú možnosť vyjadriť svoje stanovisko. So zreteľom na to Komisia rozhodne, či je povolenie opodstatnené. Komisia svoje rozhodnutie oznámi dotknutému členskému štátu a príslušným prevádzkovateľom.

6. Ak Komisia považuje povolenie za neopodstatnené, orgán dohľadu nad trhom dotknutého členského štátu ho stiahne.

7. V prípade vysokorizikových systémov AI súvisiacich s výrobkami, na ktoré sa vzťahujú harmonizačné právne predpisy Únie uvedené v prílohe I oddiele A, sa uplatňujú len výnimky z posudzovania zhody stanovené v uvedených harmonizačných právnych predpisoch Únie.

Článok 47

EÚ vyhlásenie o zhode

1. Pre každý vysokorizikový systém AI vyhotoví poskytovateľ písomné, strojovo čitateľné, fyzicky alebo elektronicky podpísané EÚ vyhlásenie o zhode, ktoré počas 10 rokov po uvedení vysokorizikového systému AI na trh alebo do prevádzky uchováva k dispozícii pre vnútroštátne príslušné orgány. V EÚ vyhlásení o zhode sa uvádza vysokorizikový systém AI, pre ktorý bolo vyhotovené. Na požiadanie sa kópia EÚ vyhlásenia o zhode predloží relevantným vnútroštátnym príslušným orgánom.

2. V EÚ vyhlásení o zhode sa uvedie, že dotknutý vysokorizikový systém AI spĺňa požiadavky stanovené v oddiele 2. EÚ vyhlásenie o zhode obsahuje informácie uvedené v prílohe V a preloží sa do jazyka, ktorému vnútroštátne príslušné orgány členských štátov, v ktorých sa vysokorizikový systém AI uvádza na trh alebo sprístupňuje, bez problémov rozumejú.

3. Ak sa na vysokorizikové systémy AI vzťahujú ďalšie harmonizačné právne predpisy Únie, v ktorých sa takisto vyžaduje EÚ vyhlásenie o zhode, vyhotoví sa vo vzťahu k všetkým právnym predpisom Únie uplatniteľným na daný vysokorizikový systém AI jedno EÚ vyhlásenie o zhode. Toto vyhlásenie obsahuje všetky informácie potrebné na to, aby bolo možné identifikovať harmonizačné právne predpisy Únie, na ktoré sa vyhlásenie vzťahuje.

4. Vypracovaním EÚ vyhlásenia o zhode preberá poskytovateľ zodpovednosť za splnenie požiadaviek stanovených v oddiele 2. Poskytovateľ podľa potreby EÚ vyhlásenie o zhode aktualizuje.

5. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 97 na účely zmeny prílohy V aktualizovaním obsahu EÚ vyhlásenia o zhode stanoveného v uvedenej prílohe s cieľom zaviesť prvky, ktorých potreba vznikne vzhľadom na technický pokrok.

Článok 48

Označenie CE

1. Označenie CE sa riadi všeobecnými zásadami stanovenými v článku 30 nariadenia (ES) č. 765/2008.

2. V prípade digitálne poskytovaných vysokorizikových systémov AI sa digitálne označenie CE používa len vtedy, ak je k nemu možný jednoduchý prístup prostredníctvom rozhrania, z ktorého je prístup k tomuto systému, alebo prostredníctvom ľahko dostupného strojovo čitateľného kódu alebo iných elektronických prostriedkov.

3. Označenie CE sa v prípade vysokorizikových systémov AI umiestni viditeľne, čitateľne a neodstrániteľne. Ak to nie je možné alebo odôvodnené z hľadiska povahy vysokorizikového systému AI, označenie CE sa umiestni na obale alebo v relevantnom prípade na sprievodnej dokumentácii.

4. V relevantných prípadoch za označením CE nasleduje identifikačné číslo notifikovanej osoby zodpovednej za postupy posudzovania zhody stanovené v článku 43. Identifikačné číslo notifikovanej osoby umiestňuje samotná osoba alebo na základe jej pokynov poskytovateľ alebo jeho splnomocnený zástupca. Identifikačné číslo sa uvedie aj v akomkoľvek propagačnom materiáli, v ktorom sa nachádza informácia, že vysokorizikový systém AI spĺňa požiadavky na označenie CE.

5. Ak vysokorizikové systémy AI podliehajú iným právnym predpisom Únie, v ktorých sa takisto vyžaduje umiestňovanie označenia CE, v označení CE sa uvedie, že vysokorizikové systémy AI spĺňajú aj požiadavky uvedených iných právnych predpisov.

Článok 49

Registrácia

1. Pred tým, ako sa na trh alebo do prevádzky uvedie vysokorizikový systém AI uvedený v prílohe III s výnimkou vysokorizikových systémov AI uvedených v prílohe III bode 2, poskytovateľ alebo v relevantnom prípade jeho splnomocnený zástupca sa zaregistruje v databáze Únie uvedenej v článku 71 a zaregistruje aj daný systém.

2. Pred tým, ako sa na trh alebo do prevádzky uvedie systém AI, pri ktorom poskytovateľ dospel podľa článku 6 ods. 3 k záveru, že nie je vysokorizikový, tento poskytovateľ alebo v relevantnom prípade jeho splnomocnený zástupca sa zaregistruje v databáze Únie uvedenej v článku 71 a zaregistruje aj daný systém.

3. Pred uvedením do prevádzky alebo pred začatím používania vysokorizikového systému AI uvedeného v prílohe III, s výnimkou vysokorizikových systémov AI uvedených v prílohe III bode 2, nasadzujúce subjekty, ktoré sú orgánmi verejnej moci, inštitúcie, orgány úrady alebo agentúry Únie, alebo osoby, ktoré konajú v ich mene, sa zaregistrujú v databáze Únie uvedenej v článku 71, vyberú príslušný systém a zaregistrujú jeho používanie.

4. V prípade vysokorizikových systémov AI uvedených v prílohe III bodoch 1, 6 a 7 v oblastiach presadzovania práva, migrácie, azylu a riadenia kontroly hraníc sa registrácia uvedená v odsekoch 1, 2 a 3 tohto článku vykoná v zabezpečenej neverejnej časti databázy Únie uvedenej v článku 71 a podľa potreby zahŕňa len informácie uvedené v:

   a) prílohe VIII oddiele A bodoch 1 až 10 s výnimkou bodov 6, 8 a 9;

   b) prílohe VIII oddiele B bodoch 1 až 5 a 8 a 9;

   c) prílohe VIII oddiele C bodoch 1 až 3;

   d) prílohe IX bodoch 1, 2, 3 a 5.

K príslušným obmedzeným častiam databázy Únie uvedeným v prvom pododseku toho odseku má prístup len Komisia a vnútroštátne orgány uvedené v článku 74 ods. 8.

5. Vysokorizikové systémy AI uvedené v prílohe III bode 2 sa registrujú na vnútroštátnej úrovni.

Kapitola IV
Povinnosti v oblasti transparentnosti pre poskytovateľov a nasadzujúce subjekty určitých systémov AI

Článok 50

Povinnosti v oblasti transparentnosti pre poskytovateľov a nasadzujúce subjekty určitých systémov AI

1. Poskytovatelia zabezpečia, aby systémy AI určené na priamu interakciu s fyzickými osobami boli dizajnované a vyvinuté tak, aby boli dotknuté fyzické osoby informované o tom, že interagujú so systémom AI, pokiaľ to nie je zrejmé z hľadiska fyzickej osoby, ktorá je primerane informovaná, pozorná a obozretná, pričom sa prihliada na okolnosti a kontext používania. Táto povinnosť sa nevzťahuje na systémy AI, ktoré sa podľa zákona môžu používať na odhaľovanie, prevenciu, vyšetrovanie alebo stíhanie trestných činov, a to s výhradou primeraných záruk ochrany práv a slobôd tretích strán, pokiaľ tieto systémy nie sú sprístupnené verejnosti na oznamovanie trestných činov.

2. Poskytovatelia systémov AI vrátane systémov AI na všeobecné účely, ktoré generujú syntetický zvukový, obrazový, video alebo textový obsah, zabezpečia, aby boli výstupy systému AI označené v strojovo čitateľnom formáte a zistiteľné ako umelo vygenerované alebo zmanipulované. Poskytovatelia zabezpečia, aby ich technické riešenia boli účinné, interoperabilné, odolné a spoľahlivé, pokiaľ je to technicky možné, s prihliadnutím na osobitosti a obmedzenia rozličných druhov obsahu, náklady na implementáciu a všeobecne uznávaný aktuálny stav vývoja, ktoré sa môžu odzrkadľovať v príslušných technických normách. Táto povinnosť sa neuplatňuje v rozsahu, v ktorom systémy AI vykonávajú pomocnú funkciu pri štandardných redakčných úpravách alebo pokiaľ podstatne nemenia vstupné údaje poskytnuté nasadzujúcim subjektom alebo ich sémantiku, alebo ak je to zákonom povolené na odhaľovanie, prevenciu, vyšetrovanie alebo stíhanie trestných činov.

3. Nasadzujúce subjekty systému na rozpoznávanie emócií alebo systému biometrickej kategorizácie informujú o prevádzke systému fyzické osoby, ktoré sú mu vystavené, a spracúvajú osobné údaje v súlade s nariadeniami (EÚ) 2016/679 a (EÚ) 2018/1725 a v relevantnom prípade so smernicou (EÚ) 2016/680. Táto povinnosť sa nevzťahuje na systémy AI používané na biometrickú kategorizáciu a rozpoznávanie emócií, ktoré zákon povoľuje na odhaľovanie, prevenciu, vyšetrovanie alebo stíhanie trestných činov, s výhradou primeraných záruk ochrany práv a slobôd tretích strán a v súlade s právom Únie.

4. Subjekty nasadzujúce systém AI, ktorý generuje alebo manipuluje obrazový, zvukový alebo video obsah, ktorý predstavuje deep fake, zverejnia, že obsah bol umelo vytvorený alebo manipulovaný. Táto povinnosť sa neuplatňuje, ak je použitie povolené zákonom na odhaľovanie, prevenciu, vyšetrovanie alebo stíhanie trestných činov. Ak je obsah súčasťou zjavne umeleckého, kreatívneho, satirického, fiktívneho alebo analogického diela alebo programu, povinnosti týkajúce sa transparentnosti stanovené v tomto odseku sa obmedzujú na zverejnenie existencie takéhoto vygenerovaného alebo zmanipulovaného obsahu, a to primeraným spôsobom, ktorý nebráni zobrazeniu diela a zážitku z neho.

   Subjekty nasadzujúce systém AI, ktorý generuje alebo manipuluje text uverejnený s cieľom informovať verejnosť o záležitostiach verejného záujmu, zverejnia, že text bol umelo vygenerovaný alebo manipulovaný. Táto povinnosť sa neuplatňuje, ak je použitie povolené zákonom na odhaľovanie, prevenciu, vyšetrovanie alebo stíhanie trestných činov alebo ak obsah vygenerovaný AI prešiel procesom ľudskej alebo redakčnej kontroly a ak za uverejnenie obsahu nesie redakčnú zodpovednosť fyzická alebo právnická osoba.

5. Informácie uvedené v odsekoch 1 až 4 sa dotknutým fyzickým osobám poskytnú jasným a rozlíšiteľným spôsobom najneskôr v čase prvej interakcie alebo vystavenia sa systému. Informácie musia byť v súlade s uplatniteľnými požiadavkami na prístupnosť.

6. Odseky 1 až 4 nemajú vplyv na požiadavky a povinnosti stanovené v kapitole III a nie sú nimi dotknuté iné povinnosti týkajúce sa transparentnosti stanovené pre subjekty nasadzujúce systémy AI v práve Únie alebo vo vnútroštátnom práve.

7. Úrad pre AI podporuje a uľahčuje vypracúvanie kódexov postupov na úrovni Únie s cieľom uľahčiť účinné vykonávanie povinností týkajúcich sa odhaľovania a označovania umelo vygenerovaného alebo zmanipulovaného obsahu. Komisia môže prijať vykonávacie akty na schválenie uvedených kódexov postupov v súlade s postupom stanoveným v článku 56 ods. 6. Ak sa Komisia domnieva, že kódex nie je primeraný, môže prijať vykonávací akt, v ktorom stanoví spoločné pravidlá vykonávania týchto povinností v súlade s postupom preskúmania stanoveným v článku 98 ods. 2.

Kapitola V
Modely AI na všeobecné účely

ODDIEL 1
PRAVIDLÁ KLASIFIKÁCIE

Článok 51

Klasifikácia modelov AI na všeobecné účely ako modelov AI na všeobecné účely so systémovým rizikom

1. Model AI na všeobecné účely sa klasifikuje ako model AI na všeobecné účely so systémovým rizikom, ak spĺňa ktorúkoľvek z týchto podmienok:

   a) má spôsobilosti s veľkým dopadom vyhodnotené na základe vhodných technických nástrojov a metodík vrátane ukazovateľov a referenčných hodnôt;

b) na základe rozhodnutia Komisie, z úradnej moci alebo na základe kvalifikovaného upozornenia vedeckého panelu má so zreteľom na kritériá stanovené v prílohe XIII spôsobilosti alebo dopad rovnocenný s tými, ktoré sú stanovené v písmene a).

2. Model AI na všeobecné účely sa považuje za model, ktorý má spôsobilosti s veľkým dopadom podľa odseku 1 písm. a), ak je kumulatívny počet výpočtov použitých na jeho trénovanie meraný v operáciách s pohyblivou rádovou čiarkou vyššia ako 1025.

3. Komisia prijme delegované akty v súlade s článkom 97 s cieľom zmeniť prahové hodnoty uvedené v odsekoch 1 a 2 tohto článku, ako aj doplniť referenčné hodnoty a ukazovatele vzhľadom na technologický vývoj, ako sú algoritmické zlepšenia alebo zvýšená efektívnosť hardvéru, ak je to potrebné, aby tieto prahové hodnoty odrážali aktuálny stav vývoja.

Článok 52

Postup

1. Ak model AI na všeobecné účely spĺňa podmienku uvedenú v článku 51 ods. 1 písm. a), príslušný poskytovateľ to oznámi Komisii, a to bezodkladne a v každom prípade do dvoch týždňov od splnenia uvedenej požiadavky alebo od zistenia, že bude splnená. Toto oznámenie obsahuje informácie potrebné na preukázanie splnenia príslušnej požiadavky. Ak sa Komisia dozvie o modeli AI na všeobecné účely predstavujúcom systémové riziká, o ktorom nebola informovaná, môže sa rozhodnúť označiť ho za model so systémovým rizikom.

2. Poskytovateľ modelu AI na všeobecné účely, ktorý spĺňa podmienku uvedenú v článku 51 ods. 1 písm. a), môže spolu so svojim oznámením predložiť dostatočne podložené argumenty na preukázanie toho, že model AI na všeobecné účely, hoci spĺňa uvedenú požiadavku, vzhľadom na svoje osobitné vlastnosti výnimočne nepredstavuje systémové riziká, a preto by sa nemal klasifikovať ako model AI na všeobecné účely so systémovým rizikom.

3. Ak Komisia dospeje k záveru, že argumenty predložené podľa odseku 2 nie sú dostatočne podložené a príslušný poskytovateľ nebol schopný preukázať, že model AI na všeobecné účely vzhľadom na svoje osobitné vlastnosti nepredstavuje systémové riziká, zamietne tieto argumenty a model AI na všeobecné účely sa považuje za model AI na všeobecné účely so systémovým rizikom.

4. Komisia môže označiť model AI na všeobecné účely za model predstavujúci systémové riziká, a to z úradnej moci alebo na základe kvalifikovaného upozornenia vedeckého panelu podľa článku 90 ods. 1 písm. a) na základe kritérií stanovených v prílohe XIII.

   Komisia je splnomocnená prijímať delegované akty v súlade s článkom 97 s cieľom zmeniť prílohu XIII spresnením a aktualizovaním kritérií stanovených v uvedenej prílohe.

5. Na základe odôvodnenej žiadosti poskytovateľa, ktorého model bol označený za model AI na všeobecné účely so systémovým rizikom podľa odseku 4, Komisia žiadosť zohľadní a môže rozhodnúť o prehodnotení, či model AI na všeobecné účely možno stále považovať za model predstavujúci systémové riziká na základe kritérií stanovených v prílohe XIII. Takáto žiadosť obsahuje objektívne, podrobné a nové dôvody, ktoré vznikli od rozhodnutia o označení. Poskytovatelia môžu požiadať o opätovné posúdenie najskôr šesť mesiacov po rozhodnutí o označení. Ak sa Komisia po svojom opätovnom posúdení rozhodne zachovať označenie modelu AI na všeobecné účely so systémovým rizikom, poskytovatelia môžu požiadať o opätovné posúdenie najskôr šesť mesiacov po uvedenom rozhodnutí.

6. Komisia zabezpečí, aby sa uverejnil zoznam modelov AI na všeobecné účely so systémovým rizikom, a tento zoznam priebežne aktualizuje bez toho, aby bola dotknutá potreba dodržiavať a chrániť práva duševného vlastníctva a dôverné obchodné informácie alebo obchodné tajomstvá v súlade s právom Únie a vnútroštátnym právom.

ODDIEL 2

POVINNOSTI POSKYTOVATEĽOV MODELOV AI NA VŠEOBECNÉ ÚČELY

Článok 53

Povinnosti poskytovateľov modelov AI na všeobecné účely

1. Poskytovatelia modelov AI na všeobecné účely:

a) vypracúvajú a aktualizujú technickú dokumentáciu modelu vrátane procesu jeho trénovania a testovania a výsledkov jeho hodnotenia, ktorá obsahuje aspoň informácie stanovené v prílohe XI, aby ju mohli na požiadanie poskytnúť úradu pre AI a vnútroštátnym príslušným orgánom;

b) vypracúvajú, aktualizujú a sprístupňujú informácie a dokumentáciu poskytovateľom systémov AI, ktorí majú v úmysle integrovať model AI na všeobecné účely do svojich systémov AI. Bez toho, aby bola dotknutá potreba dodržiavať a chrániť práva duševného vlastníctva a dôverné obchodné informácie alebo obchodné tajomstvá v súlade s právom Únie a vnútroštátnym právom, informácie a dokumentácia:

i) umožnia poskytovateľom systémov AI dobre pochopiť spôsobilosti a obmedzenia modelu AI na všeobecné účely a plniť si povinnosti podľa tohto nariadenia, a

ii) obsahujú aspoň prvky stanovené v prílohe XII;

c) zavedú politiku dodržiavania práva Únie v oblasti autorského práva a s ním súvisiacich práv, najmä s cieľom identifikovať a dodržiavať výslovné vyhradenie práv podľa článku 4 ods. 3 smernice (EÚ) 2019/790, a to aj prostredníctvom najmodernejších technológií;

d) vypracujú a zverejnia dostatočne podrobné zhrnutie obsahu použitého na trénovanie modelu AI na všeobecné účely podľa vzoru, ktorý poskytne úrad pre AI.

2. Povinnosti stanovené v odseku 1 písm. a) a b) sa nevzťahujú na poskytovateľov modelov AI, ktoré sa vydávajú na základe bezplatnej licencie s otvoreným zdrojovým kódom, ktorá umožňuje prístup k modelu, jeho používanie, úpravu a distribúciu, a ktorých parametre vrátane váh, informácií o architektúre modelu a informácií o používaní modelu sú verejne dostupné. Táto výnimka sa nevzťahuje na modely AI na všeobecné účely so systémovými rizikami.

3. Poskytovatelia modelov AI na všeobecné účely podľa potreby spolupracujú s Komisiou a vnútroštátnymi príslušnými orgánmi pri výkone svojich kompetencií a právomocí podľa tohto nariadenia.

4. Poskytovatelia modelov AI na všeobecné účely sa môžu na účely preukázania splnenia povinností stanovených v odseku 1 tohto článku do uverejnenia harmonizovanej normy odvolávať na kódexy postupov v zmysle článku 56. Spĺňanie európskych harmonizovaných noriem dáva poskytovateľom predpoklad zhody v rozsahu, v akom sa uvedené normy vzťahujú na uvedené povinnosti. Poskytovatelia modelov AI na všeobecné účely, ktorí nedodržiavajú schválený kódex postupov alebo nespĺňajú európsku harmonizovanú normu, použijú na účely posúdenia Komisiou alternatívne primerané prostriedky preukázania súladu.

5. Na účely uľahčenia súladu s prílohou XI, najmä bodom 2 písm. d) a e) je Komisia splnomocnená prijímať delegované akty v súlade s článkom 97 na podrobné uvedenie metodík merania a výpočtu s cieľom umožniť porovnateľnú a overiteľnú dokumentáciu.

6. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 97 ods. 2 s cieľom meniť prílohy XI a XII vzhľadom na technologický vývoj.

7. So všetkými informáciami alebo dokumentáciou získanou v súlade s týmto článkom vrátane obchodných tajomstiev sa zaobchádza v súlade s povinnosťami zachovávania dôvernosti podľa článku 78.

Článok 54

Splnomocnení zástupcovia poskytovateľov modelov AI na všeobecné účely

1. Poskytovatelia usadení v tretích krajinách pred sprístupnením modelu AI na všeobecné účely na trhu Únie písomným splnomocnením vymenujú splnomocneného zástupcu usadeného v Únii.

2. Poskytovateľ umožní svojmu splnomocnenému zástupcovi vykonávať úlohy uvedené v splnomocnení, ktoré mu udelil poskytovateľ.

3. Splnomocnený zástupca vykonáva úlohy uvedené v splnomocnení, ktoré mu udelil poskytovateľ. Na požiadanie poskytne kópiu splnomocnenia úradu pre AI v jednom z úradných jazykov inštitúcií Únie. Na účely tohto nariadenia sa splnomocnený zástupca splnomocnením poveruje vykonávaním týchto úloh:

   a) overenie, či poskytovateľ vypracoval technickú dokumentáciu uvedenú v prílohe XI a či splnil všetky povinnosti uvedené v článku 53 a v relevantnom prípade v článku 55;

   b) uchovávanie kópie technickej dokumentácie uvedenej v prílohe XI, aby bola k dispozícii úradu pre AI a vnútroštátnym príslušným orgánom počas obdobia 10 rokov po uvedení modelu AI na všeobecné účely na trh, ako aj kontaktných údajov poskytovateľa, ktorý vymenoval splnomocneného zástupcu;

   c) poskytuje úradu pre AI na jeho odôvodnenú žiadosť všetky informácie a dokumentáciu vrátane tých, ktoré sú uvedené v písmene b), ktoré sú potrebné na preukázanie súladu s povinnosťami v tejto kapitole;

   d) spolupracuje s úradom pre AI a príslušnými orgánmi na základe odôvodnenej žiadosti pri akomkoľvek opatrení, ktoré prijmú v súvislosti s modelom AI na všeobecné účely, a to aj vtedy, keď je model integrovaný do systémov AI uvádzaných na trh alebo do prevádzky v Únii.

4. Splnomocnenie splnomocňuje splnomocneného zástupcu, aby sa okrem poskytovateľa, alebo namiesto neho, naň obracal úrad pre AI alebo príslušné orgány vo všetkých otázkach týkajúcich sa zabezpečenia súladu s týmto nariadením.

5. Splnomocnený zástupca splnomocnenie vypovie, ak sa domnieva alebo má dôvod domnievať sa, že poskytovateľ koná v rozpore so svojimi povinnosťami podľa tohto nariadenia. V takom prípade bezodkladne informuje úrad pre AI o vypovedaní splnomocnenia a jeho dôvodoch.

6. Povinnosť stanovená v tomto článku sa nevzťahuje na poskytovateľov modelov AI na všeobecné účely, ktoré sa vydávajú na základe bezplatnej licencie s otvoreným zdrojovým kódom, ktorá umožňuje prístup k modelu, jeho používanie, zmenu a distribúciu, a ktorých parametre vrátane váh, informácií o architektúre modelu a informácií o používaní modelu sú verejne dostupné, pokiaľ daný model AI na všeobecné účely nepredstavuje systémové riziká.

ODDIEL 3

POVINNOSTI POSKYTOVATEĽOV MODELOV AI NA VŠEOBECNÉ ÚČELY SO SYSTÉMOVÝM RIZIKOM

Článok 55

Povinnosti poskytovateľov modelov AI na všeobecné účely so systémovým rizikom

1. Okrem povinností uvedených v článkoch 53 a 54 poskytovatelia modelov AI na všeobecné účely so systémovým rizikom:

   a) vykonávajú hodnotenie modelu v súlade s normalizovanými protokolmi a nástrojmi odrážajúcimi aktuálny stav vývoja vrátane vykonávania a zdokumentovania testovania modelu na nepriateľské útoky s cieľom identifikovať a zmierniť systémové riziká;

   b) posudzujú a zmierňujú prípadné systémové riziká na úrovni Únie vrátane ich zdrojov, ktoré môžu vyplývať z vývoja, uvádzania na trh alebo používania modelov AI na všeobecné účely so systémovým rizikom;

   c) sledujú relevantné informácie o závažných incidentoch a možných nápravných opatrenia na ich riešenie, dokumentujú ich a bez zbytočného odkladu ich oznamujú úradu pre AI a v prípade potreby vnútroštátnym príslušným orgánom;

   d) zabezpečujú primeranú úroveň kybernetickobezpečnostnej ochrany pre model AI na všeobecné účely so systémovým rizikom a fyzickú infraštruktúru modelu.

2. Poskytovatelia modelov AI na všeobecné účely so systémovým rizikom sa môžu na účely preukázania splnenia povinností stanovených v odseku 1 tohto článku do uverejnenia harmonizovanej normy odvolávať na kódexy postupov v zmysle článku 56. Spĺňanie európskych harmonizovaných noriem dáva poskytovateľom predpoklad zhody v rozsahu, v akom sa uvedené normy vzťahujú na uvedené povinnosti. Poskytovatelia modelov AI na všeobecné účely so systémovými rizikami, ktorí nedodržiavajú schválený kódex postupov alebo nespĺňajú európsku harmonizovanú normu, použijú na účely posúdenia Komisiou alternatívne primerané prostriedky preukázania súladu.

3. So všetkými informáciami alebo dokumentáciou získanou v súlade s týmto článkom vrátane obchodných tajomstiev sa zaobchádza v súlade s povinnosťami zachovávania dôvernosti podľa článku 78.

ODDIEL 4

KÓDEXY POSTUPOV

Článok 56

Kódexy postupov

1. Úrad pre AI podporuje a uľahčuje vypracúvanie kódexov postupov na úrovni Únie s cieľom prispievať k riadnemu uplatňovaniu tohto nariadenia, pričom zohľadňuje medzinárodné prístupy.

2. Úrad pre AI a rada pre AI sa zameriavajú na zabezpečenie toho, aby kódexy postupov zahŕňali aspoň povinnosti stanovené v článkoch 53 a 55 vrátane týchto záležitostí:

a) prostriedky na zabezpečenie toho, aby sa informácie uvedené v článku 53 ods. 1 písm. a) a b) aktualizovali vzhľadom na vývoj na trhu a technologický vývoj;

b) primeraná úroveň podrobnosti zhrnutia obsahu použitého na trénovanie;

c) identifikácia druhu a povahy systémových rizík na úrovni Únie vrátane ich prípadných zdrojov;

d) opatrenia, postupy a spôsoby posudzovania a riadenia systémových rizík na úrovni Únie vrátane ich dokumentácie, ktoré musia byť primerané rizikám, zohľadňovať ich závažnosť a pravdepodobnosť a prihliadať na osobitné výzvy spojené s riešením týchto rizík vzhľadom na možné spôsoby, akými sa takéto riziká môžu objaviť a prejaviť v celom hodnotovom reťazci AI.

3. Úrad pre AI môže vyzvať všetkých poskytovateľov modelov AI na všeobecné účely, ako aj vnútroštátne príslušné orgány, aby sa zúčastnili na vypracúvaní kódexov postupov. Tento proces môžu podporovať organizácie občianskej spoločnosti, predstavitelia priemyslu, akademická obec a iné príslušné zainteresované strany, ako sú nadväzujúci poskytovatelia a nezávislí experti.

4. Úrad pre AI a rada pre AI sa usilujú zabezpečiť, aby sa v kódexoch postupov jasne stanovili ich špecifické ciele a aby obsahovali záväzky alebo opatrenia vrátane prípadných kľúčových ukazovateľov výkonu, aby sa zabezpečilo dosiahnutie týchto cieľov a aby sa náležite zohľadnili potreby a záujmy všetkých zainteresovaných strán vrátane dotknutých osôb na úrovni Únie.

5. Cieľom úradu pre AI je zabezpečiť, aby mu účastníci kódexov postupov pravidelne podávali správy o plnení záväzkov a prijatých opatreniach a ich výsledkoch, vo vhodných prípadoch formou ich porovnania s kľúčovými ukazovateľmi výkonu. Pri kľúčových ukazovateľoch výkonu a záväzkoch týkajúcich sa podávania správ sa zohľadňujú rozdiely vo veľkosti a kapacite rozličných účastníkov.

6. Úrad pre AI a rada pre AI pravidelne monitorujú a hodnotia, ako účastníci plnia ciele kódexov postupov a ako prispievajú k riadnemu uplatňovaniu tohto nariadenia. Úrad pre AI a rada pre AI posúdia, či sa kódexy postupov vzťahujú na povinnosti stanovené v článkoch 53 a 55, a pravidelne monitorujú a hodnotia plnenie svojich cieľov. Uverejnia svoje posúdenie primeranosti kódexov postupov.

   Komisia môže prostredníctvom vykonávacieho aktu schváliť kódex postupov a udeliť mu všeobecnú platnosť v rámci Únie. Uvedený vykonávací akt sa prijme v súlade s postupom preskúmania uvedeným v článku 98 ods. 2.

7. Úrad pre AI môže vyzvať všetkých poskytovateľov modelov AI na všeobecné účely, aby kódexy postupov dodržiavali. V prípade poskytovateľov modelov AI na všeobecné účely, ktoré nepredstavujú systémové riziká, možno takéto dodržiavanie obmedziť na povinnosti stanovené v článku 53, pokiaľ výslovne neprejavia záujem pripojiť sa k celému kódexu.

8. Úrad pre AI podľa vhodnosti podporuje a uľahčuje aj preskúmanie a úpravu kódexov postupov, najmä vzhľadom na nové normy. Úrad pre AI pomáha pri posudzovaní dostupných noriem.

9. Kódexy postupov sa pripravia najneskôr do ... [deväť mesiacov odo dňa nadobudnutia účinnosti tohto nariadenia]. Úrad pre AI prijme potrebné kroky vrátane vyzvania poskytovateľov podľa odseku 7.

   Ak sa kódex postupov nepodarí dokončiť do ... [12 mesiacov odo dňa nadobudnutia účinnosti tohto nariadenia] alebo ak ho úrad pre AI po tom, ako ho posúdi podľa odseku 6 tohto článku, považuje za neprimeraný, Komisia môže prostredníctvom vykonávacích aktov stanoviť spoločné pravidlá vykonávania povinností stanovených v článkoch 53 a 55 vrátane záležitostí stanovených v odseku 2 tohto článku. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 98 ods. 2.

Kapitola VI
Opatrenia na podporu inovácií

Článok 57

Regulačné experimentálne prostredia pre AI

1. Členské štáty zabezpečia, aby ich príslušné orgány zriadili aspoň jedno regulačné experimentálne prostredie pre AI na vnútroštátnej úrovni, ktoré bude uvedené do prevádzky do ... [24 mesiacov odo dňa nadobudnutia účinnosti tohto nariadenia]. Toto experimentálne prostredie sa môže zriadiť aj spoločne s príslušnými orgánmi iných členských štátov. Komisia môže poskytovať technickú podporu, poradenstvo a nástroje na zriadenie a prevádzku regulačných experimentálnych prostredí pre AI.

   Povinnosť stanovenú v prvom pododseku možno splniť aj účasťou v existujúcom experimentálnom prostredí, pokiaľ táto účasť poskytuje zúčastneným členským štátom rovnocennú úroveň vnútroštátneho pokrytia.

2. Môžu sa zriadiť aj ďalšie regulačné experimentálne prostredia pre AI na regionálnej alebo miestnej úrovni, alebo sa môžu zriadiť spoločne s príslušnými orgánmi iných členských štátov.

3. Európsky dozorný úradník pre ochranu údajov môže takisto zriadiť regulačné experimentálne prostredie pre AI pre inštitúcie, orgány, úrady a agentúry Únie a môže vykonávať úlohy vnútroštátnych príslušných orgánov v súlade s touto kapitolou.

4. Členské štáty zabezpečia, aby príslušné orgány uvedené v odsekoch 1 a 2 vyčlenili dostatočné zdroje na účinné a včasné dodržiavanie tohto článku. Vnútroštátne príslušné orgány v prípade potreby spolupracujú s inými relevantnými orgánmi a môžu umožniť zapojenie ďalších aktérov v rámci ekosystému AI. Tento článok nemá vplyv na iné regulačné experimentálne prostredia zriadené podľa práva Únie alebo vnútroštátneho práva. Členské štáty zabezpečia primeranú úroveň spolupráce medzi orgánmi vykonávajúcimi dohľad nad týmito inými experimentálnymi prostrediami a vnútroštátnymi príslušnými orgánmi.

5. Regulačné experimentálne prostredia pre AI zriadené podľa odseku 1 poskytujú kontrolované prostredie, ktoré podporuje inovácie a uľahčuje vývoj, trénovanie, testovanie a validáciu inovačných systémov AI na obmedzený čas pred ich uvedením na trh alebo do prevádzky podľa konkrétneho plánu experimentálneho prostredia dohodnutého medzi poskytovateľmi alebo potenciálnymi poskytovateľmi a príslušným orgánom. Takéto experimentálne prostredia môžu zahŕňať testovanie v reálnych podmienkach, na ktoré sa v nich dohliada.

6. Príslušné orgány poskytujú vo vhodných prípadoch usmernenia, dohľad a podporu v rámci regulačného experimentálneho prostredia pre AI s cieľom identifikovať riziká, najmä pre základné práva, zdravie a bezpečnosť, testovať, prijímať zmierňujúce opatrenia a zabezpečiť ich účinnosť vo vzťahu k povinnostiam a požiadavkám podľa tohto nariadenia a v relevantnom prípade iných právnych predpisov Únie a vnútroštátnych právnych predpisov, nad ktorými sa v rámci experimentálneho prostredia vykonáva dohľad.

7. Príslušné orgány poskytnú poskytovateľom a potenciálnym poskytovateľom, ktorí sú účastníkmi regulačného experimentálneho prostredia pre AI, usmernenia týkajúce sa regulačných očakávaní a spôsobu plnenia požiadaviek a povinností stanovených v tomto nariadení.

Na žiadosť poskytovateľa alebo potenciálneho poskytovateľa systému AI poskytne príslušný orgán písomný dôkaz o činnostiach, ktoré boli v experimentálnom prostredí úspešne vykonané. Príslušný orgán poskytne aj výstupnú správu, v ktorej podrobne opíše činnosti vykonané v experimentálnom prostredí a súvisiace výsledky a vzdelávacie výstupy. Poskytovatelia môžu použiť takúto dokumentáciu na preukázanie ich súladu s týmto nariadením prostredníctvom postupu posudzovania zhody alebo príslušných činností dohľadu nad trhom. Orgány dohľadu nad trhom a notifikované osoby v tejto súvislosti pozitívne zohľadnia výstupné správy a písomný dôkaz, ktoré poskytol vnútroštátny príslušný orgán, aby sa v primeranom rozsahu urýchlili postupy posudzovania zhody.

8. S výhradou ustanovení o dôvernosti v článku 78 a so súhlasom poskytovateľa alebo potenciálneho poskytovateľa majú Komisia a rada pre AI právo na prístup k výstupným správam, ktoré vo vhodných prípadoch zohľadňujú pri vykonávaní svojich úloh podľa tohto nariadenia. Ak s tým poskytovateľ alebo potenciálny poskytovateľ a vnútroštátny príslušný orgán výslovne súhlasia, výstupná správa sa môže zverejniť prostredníctvom jednotnej informačnej platformy uvedenej v tomto článku.

9. Zriaďovaním regulačných experimentálnych prostredí pre AI sa má prispieť k dosiahnutiu týchto cieľov:

   a) zlepšiť právnu istotu s cieľom dosiahnuť regulačný súlad s týmto nariadením alebo v relevantnom prípade s inými uplatniteľnými právnymi predpismi Únie a vnútroštátnymi právnymi predpismi;

   b) podporovať výmenu najlepších postupov prostredníctvom spolupráce s orgánmi, ktoré sa podieľajú na regulačných experimentálnych prostrediach pre AI;

c) podporovať inovácie a konkurencieschopnosť a uľahčovať vývoj ekosystému AI;

d) prispievať k regulačnému učeniu založenému na dôkazoch;

e) uľahčiť a urýchliť prístup systémov AI na trh Únie, najmä ak ich poskytujú MSP vrátane startupov.

10. Vnútroštátne príslušné orgány zabezpečia, že pokiaľ inovačné systémy AI spracúvajú osobné údaje alebo na inom základe podliehajú dohľadu ďalších vnútroštátnych orgánov alebo príslušných orgánov, ktoré poskytujú alebo podporujú prístup k údajom, aby do prevádzky regulačného experimentálneho prostredia pre AI a do dohľadu nad jeho aspektmi boli zapojené vnútroštátne orgány na ochranu údajov a takéto ďalšie vnútroštátne alebo príslušné orgány v rozsahu svojich príslušných úloh a právomocí.

11. Regulačné experimentálne prostredia pre AI nemajú vplyv na právomoci v oblasti dohľadu a nápravných opatrení, ktoré majú príslušné orgány vykonávajúce dohľad nad experimentálnymi prostrediami vrátane na regionálnej alebo miestnej úrovni. Akékoľvek významné riziká pre zdravie a bezpečnosť, ako aj pre základné práva, ktoré sa zistia počas vývoja a testovania takýchto systémov AI, musia viesť k primeranému zmierneniu rizík. Ak nemožno prijať účinné zmierňujúce opatrenia, vnútroštátne príslušné orgány majú právomoc dočasne alebo natrvalo pozastaviť testovanie alebo účasť v experimentálnom prostredí a o takomto rozhodnutí informujú úrad pre AI. Vnútroštátne príslušné orgány vykonávajú svoje právomoci v oblasti dohľadu v medziach príslušných právnych predpisov, pričom pri vykonávaní právnych ustanovení v prípade konkrétneho projektu regulačného experimentálneho prostredia pre AI využívajú svoje diskrečné právomoci s cieľom podporovať inovácie v oblasti AI v Únii.

12. Poskytovatelia a potenciálni poskytovatelia, ktorí sú účastníkmi regulačného experimentálneho prostredia pre AI, sú podľa uplatniteľných právnych predpisov Únie a vnútroštátnych právnych predpisov týkajúcich sa zodpovednosti zodpovední za akúkoľvek škodu spôsobenú tretím stranám v dôsledku experimentov, ktoré sa v takomto experimentálnom prostredí uskutočňujú. Ak však potenciálni poskytovatelia dodržiavajú konkrétny plán a podmienky svojej účasti a v dobrej viere sa riadia usmerneniami vnútroštátneho príslušného orgánu, za porušenie tohto nariadenia neuložia orgány žiadne správne pokuty. V prípadoch, keď sa iné príslušné orgány zodpovedné za iné právne predpisy Únie a vnútroštátne právne predpisy aktívne podieľali na dohľade nad systémom AI v experimentálnom prostredí a poskytli usmernenia na zabezpečenie súladu, za tieto právne predpisy sa správne pokuty neukladajú.

13. Regulačné experimentálne prostredia pre AI sa dizajnujú a implementujú tak, aby v relevantných prípadoch uľahčovali cezhraničnú spoluprácu medzi vnútroštátnymi príslušnými orgánmi.

14. Vnútroštátne príslušné orgány koordinujú svoje činnosti a spolupracujú v rámci rady pre AI.

15. Vnútroštátne príslušné orgány informujú úrad pre AI a radu pre AI o zriadení experimentálneho prostredia a môžu ich požiadať o podporu a usmernenie. Úrad pre AI zverejní zoznam plánovaných a existujúcich experimentálnych prostredí a aktualizuje ho s cieľom podporiť väčšiu interakciu v regulačných experimentálnych prostrediach pre AI a cezhraničnú spoluprácu.

16. Vnútroštátne príslušné orgány predkladajú úradu pre AI a rade pre AI výročné správy počnúc jeden rok po zriadení regulačného experimentálneho prostredia pre AI a potom každý rok až do jeho ukončenia, a záverečnú správu. Tieto správy poskytujú informácie o pokroku a výsledkoch implementácie experimentálnych prostredí vrátane najlepších postupov, incidentov, získaných skúseností a odporúčaní týkajúcich sa ich nastavenia a v relevantnom prípade aj uplatňovania a prípadnej revízie tohto nariadenia vrátane jeho delegovaných a vykonávacích aktov, a uplatňovania iných právnych predpisov Únie, nad ktorými v rámci experimentálneho prostredia vykonávajú dohľad príslušné orgány. Vnútroštátne príslušné orgány zverejnia tieto výročné správy alebo ich zhrnutia online. Komisia v prípade potreby zohľadní výročné správy pri vykonávaní svojich úloh podľa tohto nariadenia.

17. Komisia vytvorí jednotné a vyhradené rozhranie, ktoré bude obsahovať všetky relevantné informácie týkajúce sa regulačných experimentálnych prostredí pre AI, s cieľom umožniť zainteresovaným stranám interagovať s regulačnými experimentálnymi prostrediami pre AI a klásť otázky príslušným orgánom a žiadať nezáväzné usmernenia o zhode inovačných produktov, služieb a obchodných modelov zahŕňajúcich technológie AI v súlade s článkom 62 ods. 1 písm. c). Komisia svoju činnosť v relevantných prípadoch aktívne koordinuje s vnútroštátnymi príslušnými orgánmi.

Článok 58

Podrobné dojednania pre regulačné experimentálne prostredia pre AI a ich fungovanie

1. S cieľom zabrániť fragmentácii v rámci Únie Komisia prijme vykonávacie akty, v ktorých uvedie podrobné dojednania týkajúce sa zriadenia regulačných experimentálnych prostredí pre AI, ich vývoja, implementácie, prevádzky a dohľadu nad nimi. Uvedené vykonávacie akty zahŕňajú spoločné zásady v týchto otázkach:

   a) oprávnenosť a výberové kritériá na účasť v regulačnom experimentálnom prostredí pre AI;

   b) postupy na podávanie žiadostí, účasť, monitorovanie, odchod z regulačného experimentálneho prostredia pre AI a jeho ukončenie vrátane plánu experimentálneho prostredia a výstupnej správy;

   c) podmienky vzťahujúce sa na účastníkov.

   Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 98 ods. 2.

2. Vykonávacími aktmi uvedenými v odseku 1 sa zabezpečí, aby:

   a) regulačné experimentálne prostredia pre AI boli otvorené pre každého žiadajúceho poskytovateľa alebo potenciálneho poskytovateľa systému AI, ktorý spĺňa kritériá oprávnenosti a výberové kritériá, ktoré musia byť transparentné a spravodlivé, a aby vnútroštátne príslušné orgány informovali žiadateľov o svojom rozhodnutí do troch mesiacov od podania žiadosti;

b) regulačné experimentálne prostredia pre AI umožňovali široký a spravodlivý prístup za rovnakých podmienok a udržiavali krok s dopytom po účasti; poskytovatelia a potenciálni poskytovatelia môžu predkladať žiadosti aj v partnerstve s nasadzujúcimi subjektmi a inými relevantnými tretími stranami;

c) podrobné dojednania a podmienky týkajúce sa regulačných experimentálnych prostredí pre AI v najväčšej možnej miere podporovali flexibilitu vnútroštátnych príslušných orgánov pri zriaďovaní a prevádzkovaní ich regulačných experimentálnych prostredí pre AI;

d) bol prístup MSP vrátane startupov do regulačných experimentálnych prostredí pre AI bezplatný bez toho, aby bola dotknutá možnosť vnútroštátnych príslušných orgánov spravodlivo a primerane vymáhať mimoriadne náklady;

e) poskytovateľom a potenciálnym poskytovateľom prostredníctvom vzdelávacích výstupov regulačných experimentálnych prostredí pre AI uľahčovali plnenie povinností posudzovania zhody podľa tohto nariadenia a dobrovoľné uplatňovanie kódexov správania uvedených v článku 95;

f) regulačné experimentálne prostredia pre AI uľahčovali zapojenie ďalších relevantných aktérov do ekosystému AI, ako sú notifikované osoby a normalizačné organizácie, MSP vrátane startupov, podniky, inovátori, testovacie a experimentálne zariadenia, výskumné a experimentálne laboratóriá, európske centrá digitálnych inovácií, centrá excelentnosti a výskumní pracovníci, s cieľom umožniť a uľahčiť spoluprácu s verejným a súkromným sektorom;

g) postupy, procesy a administratívne požiadavky na podávanie žiadostí, výber, účasť a odchod z regulačného experimentálneho prostredia pre AI boli jednoduché, ľahko zrozumiteľné a jasne komunikované s cieľom uľahčiť účasť MSP vrátane startupov s obmedzenými právnymi a administratívnymi kapacitami, a aby boli zosúladené v celej Únii s cieľom zabrániť fragmentácii a aby sa účasť v regulačnom experimentálnom prostredí pre AI zriadenom členským štátom alebo európskym dozorným úradníkom pre ochranu údajov vzájomne a jednotne uznávala a mala rovnaké právne účinky v celej Únii;

h) účasť v regulačnom experimentálnom prostredí pre AI bola obmedzená na obdobie, ktoré je primerané zložitosti a rozsahu projektu a ktoré môže vnútroštátny príslušný orgán predĺžiť;

i) regulačné experimentálne prostredia pre AI uľahčovali vývoj nástrojov a infraštruktúry na testovanie, referenčné porovnávanie, posudzovanie a vysvetľovanie rozmerov systémov AI, ktoré sú relevantné pre regulačné vzdelávanie, ako sú presnosť, odolnosť a kybernetická bezpečnosť, ako aj nástrojov na zmierňovanie rizík pre základné práva a spoločnosť ako celok.

3. Potenciálni poskytovatelia v regulačných experimentálnych prostrediach pre AI, najmä MSP a startupy, sa v relevantných prípadoch nasmerujú k službám pred nasadením, ako sú usmernenia týkajúce sa vykonávania tohto nariadenia, k iným službám s pridanou hodnotou, ako je pomoc s normalizačnými dokumentmi a certifikáciou, testovacie a experimentálne zariadenia, európske centrá digitálnych inovácií a centrá excelentnosti.

4. Ak vnútroštátne príslušné orgány zvažujú povolenie testovania v reálnych podmienkach, nad ktorým sa vykonáva dohľad v rámci regulačného experimentálneho prostredia pre AI zriadeného podľa tohto článku, osobitne sa s účastníkmi dohodnú na podmienkach takéhoto testovania a najmä na primeraných zárukách s cieľom chrániť základné práva, zdravie a bezpečnosť. Vo vhodných prípadoch spolupracujú s inými vnútroštátnymi príslušnými orgánmi s cieľom zabezpečiť jednotné postupy v celej Únii.

Článok 59

Ďalšie spracúvanie osobných údajov na účely vývoja určitých systémov AI vo verejnom záujme v regulačných experimentálnych prostrediach pre AI

1. V regulačnom experimentálnom prostredí pre AI sa môžu osobné údaje zákonne zozbierané na iné účely spracúvať výlučne na účely vývoja, trénovania a testovania určitých systémov AI v experimentálnom prostredí, ak sú splnené všetky tieto podmienky:

   a) systémy AI sa vyvíjajú na ochranu významného verejného záujmu orgánom verejnej moci alebo inou fyzickou alebo právnickou osobou v jednej alebo viacerých z týchto oblastí:

      i) verejná bezpečnosť a verejné zdravie vrátane odhaľovania, diagnostiky, prevencie, kontroly a liečby chorôb a zlepšovania systémov zdravotnej starostlivosti;

      ii) vysoká úroveň ochrany životného prostredia a zlepšovanie jeho kvality, ochrana biodiverzity, ochrana pred znečistením, opatrenia zelenej transformácie, opatrenia na zmierňovanie zmeny klímy a adaptáciu na ňu;

iii) energetická udržateľnosť;

iv) bezpečnosť a odolnosť dopravných systémov a mobility, kritickej infraštruktúry a sietí;

v) efektívnosť a kvalita verejnej správy a verejných služieb;

b) spracúvané údaje sú potrebné na splnenie jednej alebo viacerých požiadaviek uvedených v kapitole III oddiele 2, ak tieto požiadavky nie je možné účinne splniť spracúvaním anonymizovaných, syntetických alebo iných ako osobných údajov;

c) existujú účinné mechanizmy monitorovania umožňujúce zistiť, či počas experimentovania v experimentálnych prostrediach môžu vznikať vysoké riziká pre práva a slobody dotknutých osôb, ako sa uvádzajú v článku 35 nariadenia (EÚ) 2016/679 a v článku 39 nariadenia (EÚ) 2018/1725, ako aj mechanizmy reakcie na rýchle zmiernenie týchto rizík a v prípade potreby na zastavenie spracúvania;

d) všetky osobné údaje, ktoré sa majú spracúvať v kontexte experimentálneho prostredia, sú vo funkčne oddelenom, izolovanom a chránenom prostredí spracúvania údajov pod kontrolou potenciálneho poskytovateľa a prístup k uvedeným údajom majú len oprávnené osoby;

e) poskytovatelia môžu pôvodne zozbierané údaje ďalej zdieľať len v súlade s právnymi predpismi Únie v oblasti ochrany údajov; žiadne osobné údaje vytvorené v experimentálnom prostredí nemožno zdieľať mimo neho;

f) spracúvanie osobných údajov v kontexte experimentálneho prostredia nevedie k opatreniam alebo rozhodnutiam, ktoré majú vplyv na dotknuté osoby, ani nemá vplyv na uplatňovanie ich práv stanovených v právnych predpisoch Únie v oblasti ochrany osobných údajov;

g) všetky osobné údaje spracúvané v kontexte experimentálneho prostredia sa chránia prostredníctvom vhodných technických a organizačných opatrení a po ukončení účasti v experimentálnom prostredí alebo po skončení obdobia uchovávania osobných údajov sa vymažú;

h) logy o spracúvaní osobných údajov v kontexte experimentálneho prostredia sa uchovávajú počas trvania účasti v experimentálnom prostredí, pokiaľ sa v práve Únie alebo vo vnútroštátnom práve nestanovuje inak;

i) ako súčasť technickej dokumentácie podľa prílohy IV sa spolu s výsledkami testovania uchováva úplný a podrobný opis procesu a dôvodov trénovania, testovania a validácie systému AI;

j) na webovom sídle príslušných orgánov sa zverejní krátke zhrnutie projektu AI vyvinutého v experimentálnom prostredí, jeho cieľov a očakávaných výsledkov; táto povinnosť sa nevzťahuje na citlivé operačné údaje týkajúce sa činností orgánov presadzovania práva, orgánov kontroly hraníc a imigračných alebo azylových orgánov.

2. Na účely prevencie, vyšetrovania, odhaľovania alebo stíhania trestných činov alebo na účely výkonu trestných sankcií vrátane ochrany pred ohrozením verejnej bezpečnosti a predchádzania takémuto ohrozeniu pod kontrolou a v rámci zodpovednosti orgánov presadzovania práva sa spracúvanie osobných údajov v regulačných experimentálnych prostrediach pre AI zakladá na osobitnom práve Únie alebo vnútroštátnom práve a podlieha rovnakým kumulatívnym podmienkam, ako sa uvádzajú v odseku 1.

3. Odsekom 1 nie je dotknuté právo Únie alebo vnútroštátne právo, ktorým sa vylučuje spracúvanie na iné účely, ako sú účely výslovne stanovené v uvedenom práve, ani právo Únie alebo vnútroštátne právo, ktorým sa stanovuje základ pre spracúvanie osobných údajov, ktoré je potrebné na účely vývoja, testovania alebo trénovania inovačných systémov AI, ani akýkoľvek iný právny základ v súlade s právom Únie v oblasti ochrany osobných údajov.

Článok 60

Testovanie vysokorizikových systémov AI v reálnych podmienkach mimo regulačných experimentálnych prostredí pre AI

1. Poskytovatelia alebo potenciálni poskytovatelia vysokorizikových systémov AI uvedených v prílohe III môžu vykonávať testovanie vysokorizikových systémov AI v reálnych podmienkach mimo regulačných experimentálnych prostredí pre AI v súlade s týmto článkom a plánom testovania v reálnych podmienkach uvedeným v tomto článku bez toho, aby boli dotknuté zákazy podľa článku 5.

   Komisia prostredníctvom vykonávacích aktov stanoví podrobné prvky plánu testovania v reálnych podmienkach. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 98 ods. 2.

Týmto odsekom nie je dotknuté právo Únie ani vnútroštátne právo týkajúce sa testovania v reálnych podmienkach, pokiaľ ide o vysokorizikové systémy AI súvisiace s výrobkami, na ktoré sa vzťahujú harmonizačné právne predpisy Únie uvedené v prílohe I.

2. Poskytovatelia alebo potenciálni poskytovatelia môžu vykonávať testovanie vysokorizikových systémov AI uvedených v prílohe III v reálnych podmienkach kedykoľvek pred uvedením systému AI na trh alebo do prevádzky samostatne alebo v partnerstve s jedným alebo viacerými nasadzujúcimi subjektmi alebo potenciálnymi nasadzujúcimi subjektmi.

3. Testovaním vysokorizikových systémov AI v reálnych podmienkach podľa tohto článku nie je dotknuté etické preskúmanie, ktoré sa vyžaduje podľa práva Únie alebo vnútroštátneho práva.

4. Poskytovatelia alebo potenciálni poskytovatelia môžu vykonávať testovanie v reálnych podmienkach, len ak sú splnené všetky tieto podmienky:

   a) poskytovateľ alebo potenciálny poskytovateľ vypracoval plán testovania v reálnych podmienkach a predložil ho orgánu dohľadu nad trhom v členskom štáte, v ktorom sa má testovanie v reálnych podmienkach vykonať;

   b) orgán dohľadu nad trhom v členskom štáte, v ktorom sa má testovanie v reálnych podmienkach vykonať, schválil testovanie v reálnych podmienkach a plán testovania v reálnych podmienkach; ak orgán dohľadu nad trhom neposkytol odpoveď do 30 dní, testovanie v reálnych podmienkach a plán testovania v reálnych podmienkach sa považujú za schválené; ak sa vo vnútroštátnom práve nestanovuje konkludentný súhlas, testovanie v reálnych podmienkach podlieha povoleniu;

c) poskytovateľ alebo potenciálny poskytovateľ s výnimkou poskytovateľov alebo potenciálnych poskytovateľov vysokorizikových systémov AI uvedených v prílohe III bodoch 1, 6 a 7 v oblastiach presadzovania práva, migrácie, azylu a riadenia kontroly hraníc a vysokorizikových systémov AI uvedených v prílohe III bode 2 zaregistroval testovanie v reálnych podmienkach v súlade s článkom 71 ods. 4 s jedinečným jednotným identifikačným číslom pre celú Úniu a s informáciami uvedenými v prílohe IX; poskytovateľ alebo potenciálny poskytovateľ vysokorizikových systémov AI uvedených v prílohe III bodoch 1, 6 a 7 v oblastiach presadzovania práva, migrácie, azylu a riadenia kontroly hraníc zaregistroval testovanie v reálnych podmienkach v neverejnej časti databázy Únie podľa článku 49 ods. 4 písm. d) s jedinečným jednotným identifikačným číslom pre celú Úniu a s informáciami v ňom uvedenými; poskytovateľ alebo potenciálny poskytovateľ vysokorizikových systémov AI uvedených v prílohe III bode 2 zaregistroval testovanie v reálnych podmienkach v súlade s článkom 49 ods. 5;

d) poskytovateľ alebo potenciálny poskytovateľ vykonávajúci testovanie v reálnych podmienkach je usadený v Únii alebo vymenoval právneho zástupcu, ktorý je usadený v Únii;

e) údaje zozbierané a spracúvané na účely testovania v reálnych podmienkach sa prenášajú do tretích krajín len za predpokladu, že sa implementujú primerané a uplatniteľné záruky podľa práva Únie;

f) testovanie v reálnych podmienkach netrvá dlhšie, ako je potrebné na dosiahnutie jeho cieľov, a v žiadnom prípade nie dlhšie ako šesť mesiacov, ktoré možno predĺžiť o ďalších šesť mesiacov, ak o tom poskytovateľ alebo potenciálny poskytovateľ vopred informoval orgán dohľadu nad trhom spolu s vysvetlením potreby takéhoto predĺženia;

g) účastníci testovania v reálnych podmienkach, ktorí sú osobami patriacimi do zraniteľných skupín z dôvodu ich veku alebo zdravotného postihnutia, sú primerane chránení;

h) ak poskytovateľ alebo potenciálny poskytovateľ organizuje testovanie v reálnych podmienkach v spolupráci s jedným alebo viacerými nasadzujúcimi subjektmi alebo potenciálnymi nasadzujúcimi subjektmi, poskytnú sa takýmto subjektom informácie o všetkých aspektoch testovania, ktoré sú relevantné pre ich rozhodnutie zúčastniť sa, ako aj príslušný návod na použitie systému AI uvedený v článku 13; poskytovateľ alebo potenciálny poskytovateľ a nasadzujúci subjekt alebo potenciálny nasadzujúci subjekt uzavrú dohodu, v ktorej sa stanovia ich úlohy a povinnosti s cieľom zabezpečiť súlad s ustanoveniami o testovaní v reálnych podmienkach podľa tohto nariadenia a iného uplatniteľného práva Únie a vnútroštátneho práva;

i) účastníci testovania v reálnych podmienkach poskytli informovaný súhlas v súlade s článkom 61 alebo, v prípade presadzovania práva, ak by získanie informovaného súhlasu bránilo testovaniu systému AI, samotné testovanie a výsledok testovania v reálnych podmienkach nesmú mať žiaden negatívny vplyv na účastníkov a osobné údaje účastníkov sa po vykonaní testovania vymažú;

j) na testovanie v reálnych podmienkach účinne dohliada poskytovateľ alebo potenciálny poskytovateľ a nasadzujúce subjekty alebo potenciálne nasadzujúce subjekty prostredníctvom osôb, ktoré sú primerane kvalifikované v príslušnej oblasti a majú potrebnú kapacitu, odbornú prípravu a právomoc na vykonávanie svojich úloh;

k) predpovede, odporúčania alebo rozhodnutia systému AI možno účinne zvrátiť a nezohľadniť.

5. Ktorýkoľvek účastník testovania v reálnych podmienkach alebo v relevantnom prípade jeho zákonne určený zástupca, sa môže kedykoľvek stiahnuť z testovania odvolaním svojho informovaného súhlasu bez akejkoľvek následnej ujmy a bez toho, aby musel poskytnúť akékoľvek odôvodnenie, a požiadať o bezodkladné a trvalé vymazanie svojich osobných údajov. Odvolanie informovaného súhlasu nemá vplyv na činnosti, ktoré už boli vykonané.

6. V súlade s článkom 75 členské štáty prenesú na svoje orgány dohľadu nad trhom právomoc požadovať informácie od poskytovateľov a potenciálnych poskytovateľov, vykonávať neohlásené kontroly na diaľku alebo na mieste a vykonávať kontroly vykonávania testovania v reálnych podmienkach a súvisiacich vysokorizikových systémov AI. Orgány dohľadu nad trhom využívajú túto právomoc na zaistenie bezpečného vývoja testovania v reálnych podmienkach.

7. Každý závažný incident zistený počas testovania v reálnych podmienkach sa oznamuje vnútroštátnemu orgánu dohľadu nad trhom v súlade s článkom 73. Poskytovateľ alebo potenciálny poskytovateľ prijme okamžité opatrenia na zmiernenie dôsledkov incidentu, alebo ak to nie je možné, pozastaví testovanie v reálnych podmienkach dovtedy, kým nedôjde k takémuto zmierneniu, alebo ho v opačnom prípade ukončí. Poskytovateľ alebo potenciálny poskytovateľ stanoví postup rýchleho stiahnutia systému AI od používateľa pri takomto ukončení testovania v reálnych podmienkach.

8. Poskytovatelia alebo potenciálni poskytovatelia informujú vnútroštátny orgán dohľadu nad trhom v členskom štáte, v ktorom sa vykonáva testovanie v reálnych podmienkach, o pozastavení alebo ukončení testovania v reálnych podmienkach a o konečných výsledkoch.

9. Poskytovateľ alebo potenciálny poskytovateľ je zodpovedný za všetky škody, ktoré vzniknú počas testovania v reálnych podmienkach, podľa uplatniteľného práva Únie a vnútroštátneho práva v oblasti zodpovednosti.

Článok 61

Informovaný súhlas s účasťou na testovaní v reálnych podmienkach mimo regulačných experimentálnych prostredí pre AI

1. Na účely testovania v reálnych podmienkach podľa článku 60 účastníci testovania slobodne udelia informovaný súhlas pred svojou účasťou na takomto testovaní a po tom, ako im boli riadne poskytnuté stručné, jasné, relevantné a zrozumiteľné informácie, ktoré sa týkajú:

   a) povahy a cieľov testovania v reálnych podmienkach a možných nepríjemností, ktoré môžu byť spojené s ich účasťou;

   b) podmienok, za ktorých sa má vykonávať testovanie v reálnych podmienkach, vrátane očakávaného trvania zapojenia účastníka alebo účastníkov;

   c) práv a záruk pre účastníkov v súvislosti s ich účasťou, najmä ich práva odmietnuť účasť a práva kedykoľvek sa stiahnuť z testovania v reálnych podmienkach bez akejkoľvek následnej ujmy a bez nutnosti poskytnúť akékoľvek odôvodnenie;

   d) možností ako žiadať o zvrátenie alebo nezohľadnenie predpovedí, odporúčaní alebo rozhodnutí systému AI;

   e) jedinečného jednotného identifikačného čísla testovania v reálnych podmienkach pre celú Úniu v súlade s článkom 60 ods. 4 písm. c) a kontaktných údajov poskytovateľa alebo jeho právneho zástupcu, od ktorého možno získať ďalšie informácie.

2. Informovaný súhlas sa označí dátumom a zdokumentuje a kópia sa poskytne účastníkom testovania alebo ich právnemu zástupcovi.

Článok 62

Opatrenia pre poskytovateľov a nasadzujúce subjekty, najmä MSP vrátane startupov

1. Členské štáty prijmú tieto opatrenia:

   a) poskytnú MSP vrátane startupov so sídlom alebo pobočkou v Únii prednostný prístup do regulačných experimentálnych prostredí pre AI za predpokladu, že spĺňajú podmienky oprávnenosti a výberové kritériá; prednostný prístup nebráni iným MSP vrátane startupov, ktoré nie sú uvedené v tomto odseku, v prístupe do regulačného experimentálneho prostredia pre AI za predpokladu, že tiež spĺňajú podmienky oprávnenosti a výberové kritériá;

   b) organizujú osobitné činnosti na zvyšovanie informovanosti a činnosti odbornej prípravy o uplatňovaní tohto nariadenia prispôsobené potrebám MSP vrátane startupov, nasadzujúcich subjektov a v relevantnom prípade miestnych orgánov verejnej správy;

   c) využívajú existujúce osobitné kanály a v prípade potreby zriadia nové na komunikáciu s MSP vrátane startupov, nasadzujúcimi subjektmi, inými inovátormi a v relevantnom prípade s miestnymi orgánmi verejnej správy s cieľom poskytovať poradenstvo a odpovedať na otázky týkajúce sa vykonávania tohto nariadenia, a to aj pokiaľ ide o účasť v regulačných experimentálnych prostrediach pre AI;

d) uľahčujú účasť MSP a iných relevantných zainteresovaných strán na procese tvorby noriem.

2. Pri stanovovaní poplatkov za posudzovanie zhody podľa článku 43 sa zohľadnia osobitné záujmy a potreby poskytovateľov, ktorí sú MSP, vrátane startupov tak, že sa tieto poplatky znížia úmerne k ich veľkosti, veľkosti trhu a iným relevantným ukazovateľom.

3. Úrad pre AI prijme tieto opatrenia:

a) poskytuje štandardizované vzory pre oblasti, na ktoré sa vzťahuje toto nariadenie, ako uvádza rada pre AI vo svojej žiadosti;

b) vytvorí a udržiava jednotnú informačnú platformu poskytujúcu ľahko použiteľné informácie v súvislosti s týmto nariadením pre všetkých prevádzkovateľov v celej Únii;

c) organizuje vhodné komunikačné kampane na zvýšenie povedomia o povinnostiach vyplývajúcich z tohto nariadenia;

d) hodnotí a podporuje zbližovanie najlepších postupov, pokiaľ ide o postupy verejného obstarávania v súvislosti so systémami AI.

Článok 63

Výnimky pre špecifických prevádzkovateľov

1. Mikropodniky v zmysle odporúčania 2003/361/ES môžu dodržiavať určité prvky systému riadenia kvality vyžadovaného v článku 17 tohto nariadenia zjednodušeným spôsobom za predpokladu, že nemajú partnerské podniky alebo prepojené podniky v zmysle uvedeného odporúčania. Komisia na tento účel vypracuje usmernenia o prvkoch systému riadenia kvality, ktoré možno vzhľadom na potreby mikropodnikov dodržiavať zjednodušeným spôsobom bez toho, aby to malo vplyv na úroveň ochrany alebo potrebu splnenia požiadaviek v súvislosti s vysokorizikovými systémami AI.

2. Odsek 1 tohto článku sa nevykladá tak, že by sa ním títo prevádzkovatelia oslobodzovali od plnenia akýchkoľvek iných požiadaviek alebo povinností stanovených v tomto nariadení vrátane tých, ktoré sú stanovené v článkoch 9, 10, 11, 12, 13, 14, 15, 72 a 73.

Kapitola VII
Správa a riadenie

ODDIEL 1
SPRÁVA A RIADENIE NA ÚROVNI ÚNIE

Článok 64
Úrad pre AI

1. Komisia vyvíja odborné znalosti a spôsobilosti Únie v oblasti AI prostredníctvom úradu pre AI.

2. Členské štáty uľahčujú úlohy zverené úradu pre AI, ako sa uvádza v tomto nariadení.

Článok 65
Zriadenie a štruktúra Európskej rady pre umelú inteligenciu

1. Týmto sa zriaďuje Európska rada pre umelú inteligenciu (ďalej len „rada pre AI“).

2. Rada pre AI sa skladá z jedného zástupcu za každý členský štát. Európsky dozorný úradník pre ochranu údajov sa zúčastňuje ako pozorovateľ. Úrad pre AI sa tiež zúčastňuje na zasadnutiach rady pre AI bez toho, aby sa zúčastňoval na hlasovaní. Rada pre AI môže v jednotlivých prípadoch prizvať na zasadnutia iné orgány, subjekty alebo expertov členských štátov a Únie, ak sa prerokúvajú otázky, ktoré sú pre nich relevantné.

3. Každého zástupcu určí členský štát na obdobie troch rokov, ktoré možno raz obnoviť.

4. Členské štáty zabezpečia, aby ich zástupcovia v rade pre AI:

   a) mali vo svojom členskom štáte príslušné kompetencie a právomoci na to, aby aktívne prispievali k plneniu úloh rady pre AI uvedených v článku 66;

   b) boli určení ako jednotné kontaktné miesto vo vzťahu k rade pre AI a v prípade potreby s prihliadnutím na potreby členských štátov ako jednotné kontaktné miesto pre zainteresované strany;

   c) boli splnomocnení uľahčovať konzistentnosť a koordináciu medzi vnútroštátnymi príslušnými orgánmi vo svojom členskom štáte, pokiaľ ide o vykonávanie tohto nariadenia, a to aj prostredníctvom zberu relevantných údajov a informácií na účely plnenia svojich úloh v rade pre AI.

5. Určení zástupcovia členských štátov prijmú rokovací poriadok rady pre AI dvojtretinovou väčšinou. V rokovacom poriadku sa stanovujú najmä postupy výberového konania, trvanie mandátu a špecifikácie úloh predsedu, podrobnosti o hlasovaní a organizácia činností rady pre AI a jej podskupín.

6. Rada pre AI zriadi dve stále podskupiny s cieľom poskytnúť platformu na spoluprácu a výmenu informácií medzi orgánmi dohľadu nad trhom a notifikujúcimi orgánmi v otázkach týkajúcich sa dohľadu nad trhom, ako aj v otázkach týkajúcich sa notifikovaných osôb.

   Stála podskupina pre dohľad nad trhom by mala konať ako skupina pre administratívnu spoluprácu (ADCO) pre toto nariadenie v zmysle článku 30 nariadenia (EÚ) 2019/1020.

   Na účely preskúmania konkrétnych otázok môže rada pre AI podľa potreby zriaďovať ďalšie stále alebo dočasné podskupiny. V prípade potreby môžu byť do takýchto podskupín alebo na osobitné zasadnutia týchto podskupín prizvaní ako pozorovatelia predstavitelia poradného fóra uvedeného v článku 67.

7. Rada pre AI je organizovaná a funguje tak, aby sa zabezpečila objektivita a nestrannosť jej činností.

8. Rade pre AI predsedá jeden zo zástupcov členských štátov. Úrad pre AI zabezpečuje sekretariát rady pre AI, na žiadosť predsedu zvoláva zasadnutia a pripravuje program v súlade s úlohami rady pre AI podľa tohto nariadenia a s jej rokovacím poriadkom.

Článok 66

Úlohy rady pre AI

Rada pre AI poskytuje poradenstvo a pomoc Komisii a členským štátom s cieľom uľahčiť konzistentné a účinné uplatňovanie tohto nariadenia. Na tento účel môže rada pre AI najmä:

a) prispievať ku koordinácii medzi vnútroštátnymi príslušnými orgánmi zodpovednými za uplatňovanie tohto nariadenia a v spolupráci a so súhlasom dotknutých orgánov dohľadu nad trhom podporovať spoločné činnosti orgánov dohľadu nad trhom uvedené v článku 74 ods. 11;

b) zhromažďovať technické a regulačné znalosti a najlepšie postupy a poskytovať ich členským štátom;

c) poskytovať poradenstvo pri vykonávaní tohto nariadenia, najmä pokiaľ ide o presadzovanie pravidiel týkajúcich sa modelov AI na všeobecné účely;

d) prispievať k harmonizácii administratívnych postupov v členských štátoch, a to aj pokiaľ ide o výnimku z postupov posudzovania zhody uvedenú v článku 46, fungovanie regulačných experimentálnych prostredí pre AI a testovanie v reálnych podmienkach uvedené v článkoch 57, 59 a 60;

e) na žiadosť Komisie alebo z vlastnej iniciatívy vydávať odporúčania a písomné stanoviská ku všetkým relevantným záležitostiam týkajúcim sa vykonávania tohto nariadenia a jeho konzistentného a účinného uplatňovania, a to aj:

i) k vypracúvaniu a uplatňovaniu kódexov správania a kódexu postupov podľa tohto nariadenia, ako aj usmernení Komisie;

ii) k hodnoteniu a preskúmavaniu tohto nariadenia podľa článku 112, a to aj pokiaľ ide o správy o závažných incidentoch uvedené v článku 73 a fungovanie databázy Únie uvedenej v článku 71, prípravu delegovaných alebo vykonávacích aktov a možné zosúladenia tohto nariadenia s harmonizačnými právnymi predpismi Únie uvedenými v prílohe I;

iii) k technickým špecifikáciám alebo existujúcim normám v súvislosti s požiadavkami stanovenými v kapitole III oddiele 2;

iv) k používaniu harmonizovaných noriem alebo spoločných špecifikácií uvedených v článkoch 40 a 41;

v) k trendom, ako sú európska globálna konkurencieschopnosť v oblasti AI, zavádzanie AI v Únii a rozvoj digitálnych zručností;

vi) k trendom týkajúcim sa vyvíjajúcej sa typológie hodnotových reťazcov AI, najmä pokiaľ ide o konečné dôsledky z hľadiska zodpovednosti;

vii) k prípadnej potrebe zmeniť prílohu III v súlade s článkom 7 a k prípadnej potrebe možnej revízie článku 5 podľa článku 112, pričom zohľadňuje relevantné dostupné dôkazy a najnovší technologický vývoj;

f) podporovať Komisiu pri presadzovaní gramotnosti v oblasti AI, informovanosti verejnosti a chápaní prínosov, rizík, záruk, práv a povinností v súvislosti s používaním systémov AI;

g) uľahčovať vypracovanie spoločných kritérií a spoločné chápanie relevantných koncepcií stanovených v tomto nariadení organizátormi trhu a príslušnými orgánmi, a to aj príspevkami k zavedeniu referenčných hodnôt;

h) podľa potreby spolupracovať s ostatnými inštitúciami, orgánmi, úradmi a agentúrami Únie, ako aj s relevantnými expertnými skupinami a sieťami Únie, najmä v oblasti bezpečnosti výrobkov, kybernetickej bezpečnosti, hospodárskej súťaže, digitálnych a mediálnych služieb, finančných služieb, ochrany spotrebiteľa, ochrany údajov a ochrany základných práv;

i) prispievať k účinnej spolupráci s príslušnými orgánmi tretích krajín a s medzinárodnými organizáciami;

j) pomáhať vnútroštátnym príslušným orgánom a Komisii pri rozvoji organizačných a technických odborných znalostí potrebných na vykonávanie tohto nariadenia, a to aj prispievaním k posudzovaniu potrieb odbornej prípravy zamestnancov členských štátov zapojených do vykonávania tohto nariadenia;

k) pomáhať úradu pre AI pri podpore vnútroštátnych príslušných orgánov pri zriaďovaní a rozvoji regulačných experimentálnych prostredí pre AI a uľahčovať spoluprácu a výmenu informácií medzi regulačnými experimentálnymi prostrediami pre AI;

l) prispievať k vypracúvaniu usmerňovacích dokumentov a poskytovať pri tom relevantné poradenstvo;

m) poskytovať Komisii poradenstvo v súvislosti s medzinárodnými záležitosťami týkajúcimi sa AI;

n) poskytovať Komisii stanoviská ku kvalifikovaným upozorneniam týkajúcim sa modelov AI na všeobecné účely;

o) prijímať stanoviská členských štátov ku kvalifikovaným upozorneniam týkajúcim sa modelov AI na všeobecné účely a k vnútroštátnym skúsenostiam a postupom v oblasti monitorovania a presadzovania systémov AI, najmä systémov, do ktorých sa integrovali modely AI na všeobecné účely.

Článok 67

Poradné fórum

1. Zriadi sa poradné fórum na poskytovanie technických odborných znalostí a poradenstva rade pre AI a Komisii s cieľom prispievať k plneniu ich úloh podľa tohto nariadenia.

2. Členovia poradného fóra predstavujú vyvážený výber zainteresovaných strán vrátane predstaviteľov priemyslu, startupov, MSP, občianskej spoločnosti a akademickej obce. Zloženie členov poradného fóra musí byť vyvážené, pokiaľ ide o komerčné a nekomerčné záujmy, a v rámci kategórie komerčných záujmov, pokiaľ ide o MSP a iné podniky.

3. Komisia spomedzi zainteresovaných strán s uznávanými odbornými znalosťami v oblasti AI vymenuje členov poradného fóra v súlade s kritériami stanovenými v odseku 2.

4. Funkčné obdobie členov poradného fóra je dva roky a môže sa predĺžiť najviac o štyri roky.

5. Stálymi členmi poradného fóra sú Agentúra pre základné práva, ENISA, Európsky výbor pre normalizáciu (CEN), Európsky výbor pre normalizáciu v elektrotechnike (CENELEC) a Európsky inštitút pre telekomunikačné normy (ETSI).

6. Poradné fórum vypracuje svoj rokovací poriadok. Spomedzi svojich členov zvolí v súlade s kritériami stanovenými v odseku 2 dvoch spolupredsedov. Funkčné obdobie spolupredsedov je dva roky a možno ho raz obnoviť.

7. Zasadnutia poradného fóra sa konajú aspoň dvakrát do roka. Poradné fórum môže na svoje zasadnutia pozvať expertov a iné zainteresované strany.

8. Poradné fórum môže na žiadosť rady pre AI alebo Komisie vypracúvať stanoviská, odporúčania a písomné príspevky.

9. Poradné fórum môže podľa potreby zriadiť stále alebo dočasné podskupiny na účely preskúmania špecifických otázok súvisiacich s cieľmi tohto nariadenia.

10. Poradné fórum vypracúva výročnú správu o svojej činnosti. Táto správa sa sprístupňuje verejnosti.

Článok 68

Vedecký panel nezávislých expertov

1. Komisia prostredníctvom vykonávacieho aktu prijme ustanovenia o zriadení vedeckého panelu nezávislých expertov (ďalej len „vedecký panel“) určeného na podporu činností presadzovania podľa tohto nariadenia. Uvedený vykonávací akt sa prijme v súlade s postupom preskúmania uvedeným v článku 98 ods. 2.

2. Vedecký panel pozostáva z expertov vybraných Komisiou na základe aktuálnych vedeckých alebo technických odborných znalostí v oblasti AI, ktoré sú potrebné na plnenie úloh stanovených v odseku 3, a musí byť schopný preukázať splnenie všetkých týchto podmienok:

   a) osobitné odborné znalosti a spôsobilosti a vedecké alebo technické odborné znalosti v oblasti AI;

   b) nezávislosť od akéhokoľvek poskytovateľa systémov AI alebo modelov AI na všeobecné účely;

   c) schopnosť vykonávať činnosti dôsledne, presne a objektívne.

   Komisia po konzultácii s radou pre AI určí počet expertov v paneli v súlade s požadovanými potrebami a zabezpečí spravodlivé rodové a geografické zastúpenie.

3. Vedecký panel poskytuje poradenstvo a podporu úradu pre AI, najmä pokiaľ ide o tieto úlohy:

a) podpora vykonávania a presadzovania tohto nariadenia, pokiaľ ide o modely a systémy AI na všeobecné účely, najmä:

i) upozorňovanie úradu pre AI na možné systémové riziká na úrovni Únie súvisiace s modelmi AI na všeobecné účely v súlade s článkom 90;

ii) príspevky k vývoju nástrojov a metodík na hodnotenie spôsobilostí modelov a systémov AI na všeobecné účely, a to aj prostredníctvom referenčných hodnôt;

iii) poskytovanie poradenstva o klasifikácii modelov AI na všeobecné účely so systémovým rizikom;

iv) poskytovanie poradenstva o klasifikácii rôznych modelov a systémov AI na všeobecné účely;

v) prispievanie k vývoju nástrojov a vzorov;

b) podpora práce orgánov dohľadu nad trhom na ich žiadosť;

c) podpora činností cezhraničného dohľadu nad trhom podľa článku 74 ods. 11 bez toho, aby boli dotknuté právomoci orgánov dohľadu nad trhom;

d) podpora úradu pre AI pri plnení jeho povinností v súvislosti s ochranným postupom Únie podľa článku 81.

4. Experti vedeckého panelu vykonávajú svoje úlohy nestranne a objektívne a zabezpečujú dôvernosť informácií a údajov získaných pri vykonávaní svojich úloh a činností. Pri plnení svojich úloh podľa odseku 3 od nikoho nežiadajú ani neprijímajú pokyny. Každý expert vypracuje vyhlásenie o záujmoch, ktoré sa zverejní. Úrad pre AI zavedie systémy a postupy na aktívne riadenie možných konfliktov záujmov a na predchádzanie týmto konfliktom.

5. Vykonávací akt uvedený v odseku 1 obsahuje ustanovenia o podmienkach, postupoch a podrobných dojednaniach týkajúcich sa vedeckého panelu a jeho členov pri vydávaní upozornení a pri žiadostiach o pomoc určených úradu pre AI pri plnení úloh vedeckého panelu.

Článok 69

Prístup členských štátov k skupine expertov

1. Členské štáty môžu vyzvať expertov vedeckého panelu, aby podporili ich činnosti v oblasti presadzovania podľa tohto nariadenia.

2. Od členských štátov sa môže vyžadovať, aby za poradenstvo a podporu expertov platili poplatky. Štruktúra a výška poplatkov, ako aj rozsah a štruktúra nahraditeľných nákladov sa stanovia prostredníctvom vykonávacieho aktu uvedeného v článku 68 ods. 1, pričom sa zohľadnia ciele primeraného vykonávania tohto nariadenia, nákladová efektívnosť a potreba zabezpečiť účinný prístup všetkých členských štátov k expertom.

3. Komisia podľa potreby uľahčuje členským štátom včasný prístup k expertom a zabezpečí, aby sa kombinácia podporných činností vykonávaných štruktúrami Únie na podporu testovania AI podľa článku 84 a expertmi podľa tohto článku organizovala efektívne a poskytovala najlepšiu možnú pridanú hodnotu.

ODDIEL 2

VNÚTROŠTÁTNE PRÍSLUŠNÉ ORGÁNY

Článok 70

Určenie vnútroštátnych príslušných orgánov a jednotných kontaktných miest

1. Každý členský štát zriadi alebo určí aspoň jeden notifikujúci orgán a aspoň jeden orgán dohľadu nad trhom na účely tohto nariadenia ako vnútroštátne príslušné orgány. Tieto vnútroštátne príslušné orgány vykonávajú svoje právomoci nezávisle, nestranne a bez zaujatosti s cieľom chrániť objektivitu svojich činností a úloh a zabezpečiť uplatňovanie a vykonávanie tohto nariadenia. Členovia týchto orgánov sa zdržia akéhokoľvek konania nezlučiteľného s ich funkciou. Za predpokladu, že sa tieto zásady dodržiavajú, takéto činnosti a úlohy môže vykonávať jeden alebo viacero určených orgánov v súlade s organizačnými potrebami členského štátu.

2. Členské štáty oznámia Komisii totožnosť notifikujúcich orgánov a orgánov dohľadu nad trhom a úlohy týchto orgánov, ako aj všetky ich následné zmeny. Členské štáty zverejnia informácie o tom, ako možno kontaktovať príslušné orgány a jednotné kontaktné miesta, a to prostriedkami elektronickej komunikácie do ... [12 mesiacov odo dňa nadobudnutia účinnosti tohto nariadenia]. Členské štáty určia orgán dohľadu nad trhom, ktorý bude pôsobiť ako jednotné kontaktné miesto pre toto nariadenie, a oznámia Komisii totožnosť jednotného kontaktného miesta. Komisia zverejní zoznam jednotných kontaktných miest.

3. Členské štáty zabezpečia, aby ich vnútroštátne príslušné orgány mali na účinné plnenie svojich úloh podľa tohto nariadenia k dispozícii primerané technické, finančné a ľudské zdroje a infraštruktúru. Vnútroštátne príslušné orgány musia mať predovšetkým k dispozícii dostatočný počet zamestnancov, ktorých spôsobilosti a odborné znalosti zahŕňajú dôkladné pochopenie technológií AI, údajov a výpočtu údajov, ochrany osobných údajov, kybernetickej bezpečnosti, základných práv, zdravotných a bezpečnostných rizík a znalosť existujúcich noriem a právnych požiadaviek. Členské štáty každoročne posudzujú a v prípade potreby aktualizujú požiadavky na spôsobilosť a zdroje uvedené v tomto odseku.

4. Vnútroštátne príslušné orgány prijmú primerané opatrenia na zabezpečenie primeranej úrovne kybernetickej bezpečnosti.

5. Vnútroštátne príslušné orgány pri plnení svojich úloh konajú v súlade s povinnosťami zachovávania dôvernosti podľa článku 78.

6. Členské štáty do ... [jeden rok odo dňa nadobudnutia účinnosti tohto nariadenia] a potom každé dva roky informujú Komisiu o stave finančných a ľudských zdrojov vnútroštátnych príslušných orgánov spolu s posúdením ich primeranosti. Komisia tieto informácie postúpi rade pre AI na prerokovanie a prípadné odporúčania.

7. Komisia podporuje výmenu skúseností medzi vnútroštátnymi príslušnými orgánmi.

8. Vnútroštátne príslušné orgány môžu poskytovať usmernenia a poradenstvo týkajúce sa vykonávania tohto nariadenia, a to najmä MSP vrátane startupov, pričom podľa okolností zohľadňujú usmernenia a poradenstvo rady pre AI a Komisie. Keď vnútroštátne príslušné orgány zamýšľajú poskytnúť usmernenia a poradenstvo v súvislosti so systémom AI v oblastiach, na ktoré sa vzťahuje iné právo Únie, uskutočnia sa podľa potreby konzultácie s vnútroštátnymi príslušnými orgánmi podľa uvedeného práva Únie.

9. Pokiaľ do rozsahu pôsobnosti tohto nariadenia spadajú inštitúcie, orgány, úrady alebo agentúry Únie, koná ako príslušný orgán pre dohľad nad nimi európsky dozorný úradník pre ochranu údajov.

Kapitola VIII
Databáza Únie pre vysokorizikové systémy AI

Článok 71

Databáza Únie pre vysokorizikové systémy AI uvedené v prílohe III

1. Komisia v spolupráci s členskými štátmi zriadi a spravuje databázu Únie obsahujúcu informácie uvedené v odsekoch 2 a 3 tohto článku týkajúce sa vysokorizikových systémov AI uvedených v článku 6 ods. 2, ktoré sú registrované v súlade s článkami 49 a 60, a systémov AI, ktoré sa nepovažujú za vysokorizikové podľa článku 6 ods. 3 a ktoré sú registrované v súlade s článkom 6 ods. 4 a článkom 49. Pri stanovovaní funkčných špecifikácií takejto databázy Komisia konzultuje s príslušnými expertmi a pri aktualizácii funkčných špecifikácií takejto databázy konzultuje s radou pre AI.

2. Údaje uvedené v prílohe VIII oddieloch A a B vkladá do databázy Únie poskytovateľ alebo v relevantnom prípade splnomocnený zástupca.

3. Údaje uvedené v prílohe VIII oddiele C vkladá do databázy Únie nasadzujúci subjekt, ktorý je orgánom verejnej moci, verejnou agentúrou alebo verejným subjektom alebo ktorý koná v ich mene, v súlade s článkom 49 ods. 3 a 4.

4. S výnimkou oddielu uvedeného v článku 49 ods. 4 a článku 60 ods. 4 písm. c) sú informácie obsiahnuté v databáze Únie registrované v súlade s článkom 49 prístupné a zverejnené používateľsky ústretovým spôsobom. Informácie by mali byť prehľadné a strojovo čitateľné. Informácie zaregistrované v súlade s článkom 60 sú prístupné len orgánom dohľadu nad trhom a Komisii, pokiaľ potenciálny poskytovateľ alebo poskytovateľ neudelil súhlas aj so zverejnením týchto informácií.

5. Databáza Únie obsahuje osobné údaje, len ak je to nutné na zber a spracúvanie informácií v súlade s týmto nariadením. Súčasťou týchto informácií sú mená a kontaktné údaje fyzických osôb, ktoré sú zodpovedné za registráciu systému a majú právomoc zastupovať poskytovateľa alebo v relevantnom prípade nasadzujúci subjekt.

6. Prevádzkovateľom databázy Únie je Komisia. Poskytovateľom, potenciálnym poskytovateľom a nasadzujúcim subjektom poskytuje primeranú technickú a administratívnu podporu. Databáza Únie musí byť v súlade s uplatniteľnými požiadavkami na prístupnosť.

Kapitola IX
Monitorovanie po uvedení na trh, výmena informácií a dohľad nad trhom

ODDIEL 1
MONITOROVANIE PO UVEDENÍ NA TRH

Článok 72

Monitorovanie po uvedení na trh vykonávané poskytovateľmi a plán monitorovania vysokorizikových systémov AI po uvedení na trh

1. Poskytovatelia zavedú a zdokumentujú systém monitorovania po uvedení na trh spôsobom, ktorý je primeraný povahe technológií AI a rizikám vysokorizikového systému AI.

2. Systémom monitorovania po uvedení na trh sa aktívne a systematicky zbierajú, dokumentujú a analyzujú relevantné údaje o výkonnosti vysokorizikových systémov AI počas celej ich životnosti, ktoré môžu poskytovať nasadzujúce subjekty alebo ktoré možno zbierať prostredníctvom iných zdrojov a ktoré umožňujú poskytovateľovi hodnotiť nepretržitý súlad systémov AI s požiadavkami stanovenými v kapitole III oddiele 2. V prípade potreby monitorovanie po uvedení na trh zahŕňa analýzu interakcie s inými systémami AI. Táto povinnosť sa nevzťahuje na citlivé operačné údaje nasadzujúcich subjektov, ktoré sú orgánmi presadzovania práva.

3. Systém monitorovania po uvedení na trh sa zakladá na pláne monitorovania po uvedení na trh. Plán monitorovania po uvedení na trh tvorí súčasť technickej dokumentácie uvedenej v prílohe IV. Komisia prijme do ... [18 mesiacov od nadobudnutia účinnosti tohto nariadenia] vykonávací akt, v ktorom sa uvedú podrobné ustanovenia pre zavedenie vzoru plánu monitorovania po uvedení na trh a zoznam prvkov, ktoré sa majú do plánu zahrnúť. Uvedený vykonávací akt sa prijme v súlade s postupom preskúmania uvedeným v článku 98 ods. 2.

4. V prípade vysokorizikových systémov AI, na ktoré sa vzťahujú harmonizačné právne predpisy Únie uvedené v prílohe I oddiele A, ak je systém a plán monitorovania po uvedení na trh už zavedený podľa uvedených právnych predpisov, s cieľom zabezpečiť konzistentnosť, zabrániť duplicitám a minimalizovať dodatočné zaťaženie, majú poskytovatelia možnosť podľa potreby začleniť potrebné prvky opísané v odsekoch 1, 2 a 3 použitím vzoru uvedeného v odseku 3 do už existujúcich systémov a plánov podľa uvedených právnych predpisov za predpokladu, že sa tým dosiahne rovnocenná úroveň ochrany.

   Prvý pododsek tohto odseku sa uplatňuje aj na vysokorizikové systémy AI uvedené v prílohe III bode 5, ktoré uvádzajú na trh alebo do prevádzky finančné inštitúcie, na ktoré sa vzťahujú požiadavky týkajúce sa ich vnútornej správy a riadenia, dojednaní alebo postupov podľa práva Únie v oblasti finančných služieb.

ODDIEL 2

ZDIEĽANIE INFORMÁCIÍ O ZÁVAŽNÝCH INCIDENTOCH

Článok 73

Podávanie správ o závažných incidentoch

1. Poskytovatelia vysokorizikových systémov AI uvedených na trh Únie podávajú správu o každom závažnom incidente orgánom dohľadu nad trhom členských štátov, v ktorých k tomuto závažnému incidentu došlo.

2. Správa uvedená v odseku 1 sa podáva ihneď po tom, ako poskytovateľ zistí príčinnú súvislosť medzi systémom AI a závažným incidentom alebo logickú pravdepodobnosť takejto súvislosti, najneskôr však do 15 dní po tom, ako sa poskytovateľ alebo v relevantnom prípade nasadzujúci subjekt o závažnom incidente dozvedel.

   Lehota pre podanie správy uvedenej v prvom pododseku zohľadňuje stupeň závažnosti incidentu.

3. Bez ohľadu na odsek 2 tohto článku sa v prípade rozsiahleho porušenia právnych predpisov alebo závažného incidentu v zmysle vymedzenia v článku 3 bode 49 písm. b) správa uvedená v odseku 1 tohto článku podá ihneď, najneskôr však do dvoch dní po tom, ako sa poskytovateľ alebo v relevantnom prípad nasadzujúci subjekt o tomto incidente dozvedel.

4. Bez ohľadu na odsek 2 sa v prípade úmrtia osoby správa podá ihneď po tom, ako poskytovateľ alebo nasadzujúci subjekt zistí príčinný vzťah medzi vysokorizikovým systémom AI a závažným incidentom, alebo hneď, ako má podozrenie na takýto príčinný vzťah, najneskôr však do 10 dní odo dňa, keď sa poskytovateľ alebo v relevantnom prípade nasadzujúci subjekt o závažnom incidente dozvedel.

5. Ak je to potrebné na zabezpečenie včasného podania správy, poskytovateľ alebo v relevantnom prípade nasadzujúci subjekt môže predložiť prvotnú neúplnú správu, po ktorej nasleduje úplná správa.

6. Po podaní správy o závažnom incidente podľa odseku 1 poskytovateľ bezodkladne vykoná potrebné vyšetrenie závažného incidentu a dotknutého systému AI. To zahŕňa posúdenie rizika incidentu a nápravné opatrenia.

   Poskytovateľ počas vyšetrovania uvedeného v prvom pododseku spolupracuje s príslušnými orgánmi v relevantnom prípade s dotknutou notifikovanou osobou a nevykonáva žiadne vyšetrovanie, ktoré zahŕňa úpravu dotknutého systému AI spôsobom, ktorý môže mať vplyv na akékoľvek následné hodnotenie príčin incidentu, pred informovaním príslušných orgánov o takomto kroku.

7. Po doručení oznámenia týkajúceho sa závažného incidentu uvedeného v článku 3 bode 49 písm. c) príslušný orgán dohľadu nad trhom informuje vnútroštátne orgány verejnej moci alebo subjekty uvedené v článku 77 ods. 1. Na uľahčenie plnenia povinností stanovených v odseku 1 tohto článku vypracuje Komisia osobitné usmernenia. Tieto usmernenia sa vydajú do ... [12 mesiacov od nadobudnutia účinnosti tohto nariadenia] a pravidelne sa posudzujú.

8. Orgán dohľadu nad trhom prijme vhodné opatrenia, ako sa stanovuje v článku 19 nariadenia (EÚ) 2019/1020, do siedmych dní od dátumu doručenia oznámenia uvedeného v odseku 1 tohto článku a dodržiava postupy oznamovania stanovené v uvedenom nariadení.

9. V prípade vysokorizikových systémov AI uvedených v prílohe III, ktoré uvádzajú na trh alebo do prevádzky poskytovatelia, na ktorých sa vzťahujú právne nástroje Únie, v ktorých sa stanovujú povinnosti týkajúce sa podávania správ rovnocenné s povinnosťami stanovenými v tomto nariadení, sa podávanie správ o závažných incidentoch obmedzuje na tie, ktoré sú uvedené v článku 3 bode 49 písm. c).

10. V prípade vysokorizikových systémov AI, ktoré sú bezpečnostnými komponentmi zariadení alebo sú samy zariadeniami, na ktoré sa vzťahujú nariadenia (EÚ) 2017/745 a (EÚ) 2017/746, sa podávanie správ o závažných incidentoch obmedzuje na tie, ktoré sú uvedené v článku 3 bode 49 písm. c) tohto nariadenia, a správa sa podáva vnútroštátnemu príslušnému orgánu, ktorý na tento účel určili členské štáty, v ktorých k tomuto incidentu došlo.

11. Vnútroštátne príslušné orgány ihneď informujú Komisiu o každom závažnom incidente bez ohľadu na to, či v súvislosti s ním prijali nejaké opatrenie, v súlade s článkom 20 nariadenia (EÚ) 2019/1020.

ODDIEL 3

PRESADZOVANIE

Článok 74

Dohľad nad trhom a kontrola systémov AI na trhu Únie

1. Na systémy AI v rozsahu pôsobnosti tohto nariadenia sa vzťahuje nariadenie (EÚ) 2019/1020. Na účely účinného presadzovania tohto nariadenia sa:

   a) každý odkaz na hospodársky subjekt podľa nariadenia (EÚ) 2019/1020 vykladá tak, že zahŕňa všetkých prevádzkovateľov uvedených v článku 2 ods. 1 tohto nariadenia;

   b) každý odkaz na výrobok podľa nariadenia (EÚ) 2019/1020 vykladá tak, že zahŕňa všetky systémy AI, ktoré patria do rozsahu pôsobnosti tohto nariadenia.

2. V rámci svojich oznamovacích povinností podľa článku 34 ods. 4 nariadenia (EÚ) 2019/1020 orgány dohľadu nad trhom každoročne oznamujú Komisii a vnútroštátnym príslušným orgánom na ochranu hospodárskej súťaže všetky informácie zistené počas činností dohľadu nad trhom, ktoré môžu mať potenciálny význam pre uplatňovanie práva Únie v oblasti pravidiel hospodárskej súťaže. Takisto každoročne podávajú Komisii správu o používaní zakázaných praktík, ku ktorým došlo počas daného roka, a o prijatých opatreniach.

3. V prípade vysokorizikových systémov AI súvisiacich s výrobkami, na ktoré sa vzťahujú harmonizačné právne predpisy Únie uvedené v prílohe I oddiele A, je orgánom dohľadu nad trhom na účely tohto nariadenia orgán zodpovedný za činnosti dohľadu nad trhom určený podľa uvedených právnych aktov.

Odchylne od prvého pododseku a za vhodných okolností môžu členské štáty určiť iný relevantný orgán, ktorý bude konať ako orgán dohľadu nad trhom, a to za predpokladu, že zabezpečia koordináciu s relevantnými odvetvovými orgánmi dohľadu nad trhom zodpovednými za presadzovanie harmonizačných právnych predpisov Únie uvedených v prílohe I.

4. Postupy uvedené v článkoch 79 až 83 tohto nariadenia sa neuplatňujú na systémy AI súvisiace s výrobkami, na ktoré sa vzťahujú harmonizačné právne predpisy Únie uvedené v prílohe I oddiele A, ak sa v takýchto právnych aktoch už stanovujú postupy, ktoré zaručujú rovnocennú úroveň ochrany a majú rovnaký cieľ. V takých prípadoch sa namiesto toho uplatnia príslušné odvetvové postupy.

5. Bez toho, aby boli dotknuté právomoci orgánov dohľadu nad trhom podľa článku 14 nariadenia (EÚ) 2019/1020, môžu orgány dohľadu nad trhom na účely zabezpečenia účinného presadzovania tohto nariadenia podľa potreby vykonávať právomoci, ktoré sú uvedené v článku 14 ods. 4 písm. d) a j) uvedeného nariadenia, na diaľku.

6. V prípade vysokorizikových systémov AI, ktoré uvádzajú na trh, do prevádzky alebo používajú finančné inštitúcie regulované právnymi predpismi Únie v oblasti finančných služieb, je orgánom dohľadu nad trhom na účely tohto nariadenia relevantný vnútroštátny orgán zodpovedný za finančný dohľad nad týmito inštitúciami podľa uvedených právnych predpisov, pokiaľ uvádzanie na trh, uvádzanie do prevádzky alebo používanie systému AI priamo súvisí s poskytovaním týchto finančných služieb.

7. Odchylne od odseku 6 môže členský štát za vhodných okolností a za predpokladu, že je zabezpečená koordinácia, určiť za orgán dohľadu nad trhom na účely tohto nariadenia iný relevantný orgán.

Vnútroštátne orgány dohľadu nad trhom, ktoré vykonávajú dohľad nad regulovanými úverovými inštitúciami regulovanými podľa smernice 2013/36/EÚ a ktoré sa zúčastňujú na jednotnom mechanizme dohľadu zriadenom nariadením (EÚ) č. 1024/2013, by mali Európskej centrálnej banke bezodkladne oznamovať všetky informácie zistené v priebehu svojich činností dohľadu nad trhom, ktoré môžu byť potenciálne zaujímavé pre úlohy Európskej centrálnej banky v oblasti prudenciálneho dohľadu, ako sa uvádzajú v uvedenom nariadení.

8. V prípade vysokorizikových systémov AI uvedených v prílohe III bode 1 tohto nariadenia, pokiaľ sa tieto systémy používajú na účely presadzovania práva, riadenia hraníc a spravodlivosti a demokracie, a v prípade vysokorizikových systémov AI uvedených v prílohe III bodoch 6, 7 a 8 tohto nariadenia, členské štáty určia za orgány dohľadu nad trhom na účely tohto nariadenia buď príslušné dozorné orgány pre ochranu údajov podľa nariadenia (EÚ) 2016/679 alebo smernice (EÚ) 2016/680 alebo akýkoľvek iný orgán určený podľa rovnakých podmienok stanovených v článkoch 41 až 44 smernice (EÚ) 2016/680. Činnosti dohľadu nad trhom nesmú žiadnym spôsobom ovplyvňovať nezávislosť justičných orgánov ani inak zasahovať do ich činnosti pri výkone ich súdnej právomoci.

9. Pokiaľ do rozsahu pôsobnosti tohto nariadenia spadajú inštitúcie, orgány, úrady alebo agentúry Únie, koná ako ich orgán pre dohľad nad trhom európsky dozorný úradník pre ochranu údajov s výnimkou Súdneho dvora Európskej únie konajúceho v rámci svojej súdnej právomoci.

10. Členské štáty podporujú koordináciu medzi orgánmi dohľadu nad trhom určenými podľa tohto nariadenia a inými vnútroštátnymi príslušnými orgánmi alebo subjektmi, ktoré vykonávajú dohľad nad uplatňovaním harmonizačných právnych predpisov Únie uvedených v prílohe I alebo v iných právnych predpisoch Únie, ktoré by mohli byť relevantné pre vysokorizikové systémy AI uvedené v prílohe III.

11. Orgány dohľadu nad trhom a Komisia majú možnosť navrhovať spoločné činnosti vrátane spoločných vyšetrovaní, ktoré majú vykonávať buď orgány dohľadu nad trhom alebo orgány dohľadu nad trhom spoločne s Komisiou a ktorých cieľom je podpora dodržiavania predpisov, zisťovanie nesúladu, zvyšovanie informovanosti alebo poskytovanie usmernení v súvislosti s týmto nariadením, pokiaľ ide o konkrétne kategórie vysokorizikových systémov AI, o ktorých sa zistilo, že predstavujú závažné riziko v dvoch alebo viacerých členských štátoch v súlade s článkom 9 nariadenia (EÚ) 2019/1020. Úrad pre AI poskytuje koordinačnú podporu pre spoločné vyšetrovania.

12. Poskytovatelia poskytnú orgánom dohľadu nad trhom v relevantných prípadoch a do miery, ktorá je potrebná na plnenie ich úloh, úplný prístup k dokumentácii, ako aj súborom trénovacích, validačných a testovacích údajov používaných na vývoj vysokorizikových systémov AI, v prípade potreby a s výhradou bezpečnostných záruk aj prostredníctvom aplikačných programovacích rozhraní alebo iných relevantných technických prostriedkov a nástrojov umožňujúcich diaľkový prístup, a to bez toho, aby boli dotknuté právomoci stanovené v nariadení (EÚ) 2019/1020.

13. Orgánom dohľadu nad trhom sa udelí prístup k zdrojovému kódu vysokorizikového systému AI na základe odôvodnenej žiadosti a len vtedy, ak sú splnené obe tieto podmienky:

    a) prístup k zdrojovému kódu je potrebný na posúdenie súladu vysokorizikového systému AI s požiadavkami stanovenými v kapitole III oddiele 2; a

    b) postupy testovania alebo auditu a overovania založené na údajoch a dokumentácii, ktoré poskytol poskytovateľ, boli vyčerpané alebo sa ukázali ako nedostatočné.

14. Orgány dohľadu nad trhom zaobchádzajú so všetkými získanými informáciami alebo dokumentáciou v súlade s povinnosťou zachovávania dôvernosti podľa článku 78.

Článok 75

Vzájomná pomoc, dohľad nad trhom a kontrola systémov AI na všeobecné účely

1. Ak je systém AI založený na modeli AI na všeobecné účely a tento model a systém vyvíja ten istý poskytovateľ, úrad pre AI má právomoc monitorovať súlad tohto systému AI s povinnosťami vyplývajúcimi z tohto nariadenia a dohliadať na tento súlad.
Na vykonávanie svojich úloh monitorovania a dohľadu má úrad pre AI všetky právomoci orgánu dohľadu nad trhom stanovené v tomto oddiele a v nariadení (EÚ) 2019/1020.

2. Ak majú relevantné orgány dohľadu nad trhom dostatočné dôvody domnievať sa, že systémy AI na všeobecné účely, ktoré môžu nasadzujúce subjekty priamo používať aspoň na jeden účel, ktorý je podľa tohto nariadenia klasifikovaný ako vysokorizikový, nie sú v súlade s požiadavkami stanovenými v tomto nariadení, spolupracujú s úradom pre AI s cieľom vykonať hodnotenie súladu a zodpovedajúcim spôsobom o tom informujú radu pre AI a ostatné orgány dohľadu nad trhom.

3. Ak orgán dohľadu nad trhom nie je schopný uzavrieť vyšetrovanie vysokorizikového systému AI z dôvodu, že nemá prístup k určitým informáciám týkajúcim sa modelu AI na všeobecné účely napriek tomu, že vynaložil všetko primerané úsilie na získanie týchto informácií, môže úradu pre AI predložiť odôvodnenú žiadosť, ktorou sa vymôže prístup k týmto informáciám. V tomto prípade úrad pre AI bezodkladne, najneskôr však do 30 dní, poskytne žiadajúcemu orgánu všetky informácie, ktoré úrad pre AI považuje za podstatné, aby mohol zistiť, či je vysokorizikový systém AI v nesúlade. Orgány dohľadu nad trhom zabezpečia dôvernosť informácií, ktoré získajú v súlade s článkom 78 tohto nariadenia. Postup stanovený v kapitole VI nariadenia (EÚ) 2019/1020 sa uplatňuje primerane.

Článok 76

Dohľad orgánov dohľadu nad trhom nad testovaním v reálnych podmienkach

1. Orgány dohľadu nad trhom majú kompetencie a právomoci na zabezpečenie toho, aby testovanie v reálnych podmienkach bolo v súlade s týmto nariadením.

2. Ak sa testovanie v reálnych podmienkach vykonáva v prípade systémov AI, nad ktorými sa vykonáva dohľad v rámci regulačného experimentálneho prostredia pre AI podľa článku 58, orgány dohľadu nad trhom overia súlad s článkom 60 ako súčasť svojej úlohy dohľadu nad regulačným experimentálnym prostredím pre AI. Uvedené orgány môžu v prípade potreby povoliť, aby poskytovateľ alebo potenciálny poskytovateľ vykonal testovanie v reálnych podmienkach odchylne od podmienok stanovených v článku 60 ods. 4 písm. f) a g).

3. Ak potenciálny poskytovateľ, poskytovateľ alebo akákoľvek tretia strana informovali orgán dohľadu nad trhom o závažnom incidente alebo má tento orgán iné dôvody domnievať sa, že podmienky stanovené v článkoch 60 a 61 nie sú splnené, môže na svojom území podľa potreby prijať ktorékoľvek z týchto rozhodnutí:

   a) pozastaviť alebo ukončiť testovanie v reálnych podmienkach;

   b) požadovať od poskytovateľa alebo potenciálneho poskytovateľa a nasadzujúceho subjektu alebo potenciálneho nasadzujúceho subjektu, aby zmenili akýkoľvek aspekt testovania v reálnych podmienkach.

4. Ak orgán dohľadu nad trhom prijal rozhodnutie uvedené v odseku 3 tohto článku alebo vzniesol námietku v zmysle článku 60 ods. 4 písm. b), v rozhodnutí alebo námietke sa uvedú dôvody tohto rozhodnutia alebo námietky, ako aj to, ako môže poskytovateľ alebo potenciálny poskytovateľ toto rozhodnutie alebo námietku napadnúť.

5. Ak orgán dohľadu nad trhom prijal rozhodnutie uvedené v odseku 3, v náležitých prípadoch oznámi dôvody tohto rozhodnutia orgánom dohľadu nad trhom ostatných členských štátov, v ktorých bol systém AI testovaný v súlade s plánom testovania.

Článok 77

Právomoci orgánov chrániacich základné práva

1. Vnútroštátne orgány verejnej moci alebo subjekty, ktoré dohliadajú na dodržiavanie povinností podľa právnych predpisov Únie na ochranu základných práv vrátane práva na nediskrimináciu v súvislosti s používaním vysokorizikových systémov AI uvedených v prílohe III alebo dodržiavanie týchto povinností presadzujú, majú právomoc požadovať akúkoľvek dokumentáciu vytvorenú alebo uchovávanú podľa tohto nariadenia v zrozumiteľnom jazyku a prístupnom formáte a mať k nej prístup, ak je prístup k tejto dokumentácii potrebný na účinné vykonávanie ich mandátu v rámcoch ich jurisdikcie. O každej takejto žiadosti príslušný orgán verejnej moci alebo subjekt informuje orgán dohľadu nad trhom dotknutého členského štátu.

2. Do ... [tri mesiace od nadobudnutia účinnosti tohto nariadenia] každý členský štát určí orgány verejnej moci alebo subjekty uvedené v odseku 1 a ich zoznam zverejní. Členské štáty oznámia uvedený zoznam Komisii a ostatným členským štátom a udržujú ho v aktuálnom stave.

3. Ak dokumentácia uvedená v odseku 1 nepostačuje na zistenie toho, či došlo k porušeniu povinností vyplývajúcich z právnych predpisov Únie na ochranu základných práv, orgán verejnej moci alebo subjekt uvedený v odseku 1 môže orgánu dohľadu nad trhom predložiť odôvodnenú žiadosť, aby zorganizoval testovanie vysokorizikového systému AI technickými prostriedkami. Orgán dohľadu nad trhom zorganizuje testovanie v primeranom čase od podania žiadosti v úzkej spolupráci so žiadajúcim orgánom verejnej moci alebo subjektom.

4. So všetkými informáciami alebo s dokumentáciou, ktoré vnútroštátne orgány verejnej moci alebo subjekty uvedené v odseku 1 tohto článku získali podľa tohto článku, sa zaobchádza v súlade s povinnosťami zachovávania dôvernosti podľa článku 78.

Článok 78

Dôvernosť

1. Komisia, orgány dohľadu nad trhom a notifikované osoby a akékoľvek iné fyzické alebo právnické osoby podieľajúce sa na uplatňovaní tohto nariadenia zachovávajú v súlade s právom Únie alebo vnútroštátnym právom dôvernosť informácií a údajov získaných pri vykonávaní svojich úloh a činností takým spôsobom, aby chránili najmä:

   a) práva duševného vlastníctva a dôverné obchodné informácie alebo obchodné tajomstvo fyzickej alebo právnickej osoby vrátane zdrojového kódu, s výnimkou prípadov uvedených v článku 5 smernice Európskeho parlamentu a Rady (EÚ) 2016/943[57];

   b) účinné vykonávanie tohto nariadenia, najmä na účely inšpekcií, vyšetrovaní alebo auditov;

   c) verejné záujmy a záujmy národnej bezpečnosti;

   d) vykonávanie trestného alebo správneho konania;

[57] Smernica Európskeho parlamentu a Rady (EÚ) 2016/943 z 8. júna 2016 o prístupnosti webových sídel a mobilných aplikácií subjektov verejného sektora (Ú. v. EÚ L 157, 15.6.2016, s. 1).

e) informácie utajované podľa práva Únie alebo vnútroštátneho práva.

2. Orgány zapojené do uplatňovania tohto nariadenia podľa odseku 1 požadujú len údaje, ktoré sú nevyhnutne potrebné na posúdenie rizika, ktoré systém AI predstavuje, a na výkon svojich právomocí v súlade s týmto nariadením a s nariadením (EÚ) 2019/1020. V súlade s platným právom Únie alebo vnútroštátnym právom zavedú primerané a účinné opatrenia v oblasti kybernetickej bezpečnosti na ochranu bezpečnosti a dôvernosti získaných informácií a údajov a zozbierané údaje vymažú hneď, ako prestanú byť potrebné na účel, na ktorý boli získané.

3. Bez toho, aby boli dotknuté odseky 1 a 2, sa informácie, ktoré sa vymieňajú na dôvernom základe medzi vnútroštátnymi príslušnými orgánmi navzájom alebo medzi vnútroštátnymi príslušnými orgánmi a Komisiou, neposkytujú bez predchádzajúcej konzultácie s vnútroštátnym príslušným orgánom, od ktorého pochádzajú, a nasadzujúcim subjektom, ak vysokorizikové systémy AI uvedené v prílohe III bode 1, 6 alebo 7 používajú orgány presadzovania práva, kontroly hraníc, imigračné alebo azylové orgány, a ak by takéto poskytnutie ohrozilo verejné záujmy a záujmy národnej bezpečnosti. Táto výmena informácií sa nevzťahuje na citlivé operačné údaje týkajúce sa činností orgánov presadzovania práva, kontroly hraníc, imigračných alebo azylových orgánov.

Ak sú poskytovateľmi vysokorizikových systémov AI uvedených v prílohe III bode 1, 6 alebo 7 orgány presadzovania práva, imigračné alebo azylové orgány, technická dokumentácia uvedená v prílohe IV zostáva v priestoroch týchto orgánov. Tieto orgány zabezpečia, aby orgány dohľadu nad trhom uvedené v článku 74 ods. 8 a 9 mali na požiadanie okamžitý prístup k dokumentácii alebo aby okamžite dostali jej kópiu. Prístup k dokumentácii alebo akejkoľvek jej kópii majú len zamestnanci orgánu dohľadu nad trhom, ktorí sú držiteľmi bezpečnostnej previerky na primeranej úrovni.

4. Odsekmi 1, 2 a 3 nie sú dotknuté práva ani povinnosti Komisie, členských štátov a ich relevantných orgánov, ani práva alebo povinnosti notifikovaných osôb, pokiaľ ide o výmenu informácií a šírenie upozornení, a to aj v kontexte cezhraničnej spolupráce, ani povinnosti dotknutých strán poskytovať informácie podľa trestného práva členských štátov.

5. Komisia a členské štáty si v prípade, že je to potrebné, a v súlade s príslušnými ustanoveniami medzinárodných a obchodných dohôd, môžu vymieňať dôverné informácie s regulačnými orgánmi tretích krajín, s ktorými uzavreli bilaterálne alebo multilaterálne dohody o zachovávaní dôvernosti zaručujúce primeranú úroveň dôvernosti.

Článok 79

Postup vnútroštátneho zaobchádzania so systémami AI predstavujúcimi riziko

1. Systémy AI predstavujúce riziko sa považujú za výrobky predstavujúce riziko v zmysle vymedzenia v článku 3 bode 19 nariadenia (EÚ) 2019/1020, pokiaľ predstavujú riziká pre zdravie, bezpečnosť alebo základné práva osôb.

2. Ak má orgán dohľadu nad trhom členského štátu dostatočné dôvody domnievať sa, že systém AI predstavuje riziko uvedené v odseku 1 tohto článku, vykoná hodnotenie dotknutého systému AI, pokiaľ ide o jeho súlad so všetkými požiadavkami a povinnosťami stanovenými v tomto nariadení. Osobitná pozornosť sa venuje systémom AI predstavujúcim riziko pre zraniteľné skupiny. V prípade identifikácie rizík pre základné práva orgán dohľadu nad trhom informuje aj relevantné vnútroštátne orgány verejnej moci alebo subjekty uvedené v článku 77 ods. 1 a v plnej miere s nimi spolupracuje. Príslušní prevádzkovatelia podľa potreby spolupracujú s orgánom dohľadu nad trhom a ostatnými vnútroštátnymi orgánmi verejnej moci alebo subjektmi uvedenými v článku 77 ods. 1.

Ak v priebehu uvedeného hodnotenia orgán dohľadu nad trhom alebo v relevantných prípadoch orgán dohľadu nad trhom v spolupráci s vnútroštátnym orgánom verejnej moci uvedeným v článku 77 ods. 1 zistí, že systém AI nespĺňa požiadavky a povinnosti stanovené v tomto nariadení, bez zbytočného odkladu vyžaduje od príslušného prevádzkovateľa prijatie všetkých primeraných nápravných opatrení na dosiahnutie súladu systému AI s uvedenými požiadavkami a povinnosťami, jeho stiahnutie z trhu alebo od používateľa, a to v lehote, ktorú môže orgán dohľadu nad trhom stanoviť, a v každom prípade najneskôr do 15 pracovných dní, alebo ako je stanovené v príslušných harmonizačných právnych predpisov Únie.

Orgán dohľadu nad trhom o tom informuje príslušnú notifikovanú osobu. Na opatrenia uvedené v druhom pododseku tohto odseku sa uplatňuje článok 18 nariadenia (EÚ) 2019/1020.

3. Ak sa orgán dohľadu nad trhom domnieva, že nesúlad sa neobmedzuje na územie jeho štátu, bez zbytočného odkladu informuje Komisiu a ostatné členské štáty o výsledkoch hodnotenia a o opatreniach, ktorých prijatie od prevádzkovateľa vyžaduje.

4. Prevádzkovateľ zabezpečí prijatie všetkých primeraných nápravných opatrení v súvislosti so všetkými dotknutými systémami AI, ktoré sprístupnil na trhu Únie.

5. Ak prevádzkovateľ systému AI v lehote uvedenej v odseku 2 neprijme primerané nápravné opatrenia, orgán dohľadu nad trhom prijme všetky primerané predbežné opatrenia s cieľom zakázať alebo obmedziť sprístupňovanie systému AI na svojom vnútroštátnom trhu alebo jeho uvedenie do prevádzky, výrobok alebo samostatný systém AI z uvedeného trhu stiahnuť alebo ho stiahnuť od používateľa. Uvedený orgán oznámi tieto opatrenia bez zbytočného odkladu Komisii a ostatným členským štátom.

6. Oznámenie uvedené v odseku 5 obsahuje všetky podrobné údaje, ktoré sú k dispozícii, najmä informácie potrebné na identifikáciu systému AI, ktorý nie je v súlade, pôvod systému AI a dodávateľský reťazec, povahu údajného nesúladu a z neho vyplývajúce riziko, povahu a trvanie prijatých vnútroštátnych opatrení a vyjadrenie, ktoré predložil príslušný prevádzkovateľ. Orgány dohľadu nad trhom predovšetkým uvedú, či k nesúladu došlo v dôsledku jedného alebo viacerých z týchto dôvodov:

   a) nedodržiavanie zákazu praktík využívajúcich AI uvedených v článku 5;

   b) vysokorizikový systém AI nespĺňa požiadavky stanovené v kapitole III oddiele 2;

c) nedostatky v harmonizovaných normách alebo spoločných špecifikáciách uvedených v článkoch 40 a 41, ktoré sú základom pre predpoklad zhody;

d) nesúlad s článkom 50.

7. Iné orgány dohľadu nad trhom než orgán dohľadu nad trhom členského štátu, ktorý postup inicioval, bez zbytočného odkladu oznámia Komisii a ostatným členským štátom všetky prijaté opatrenia a akékoľvek dodatočné informácie týkajúce sa nesúladu dotknutého systému AI, ktoré majú k dispozícii, a v prípade, že nesúhlasia s oznámeným vnútroštátnym opatrením, aj svoje námietky.

8. Ak do troch mesiacov od doručenia oznámenia uvedeného v odseku 5 tohto článku žiaden orgán dohľadu nad trhom členského štátu ani Komisia nevznesú námietku proti predbežnému opatreniu prijatému orgánom dohľadu nad trhom iného členského štátu, opatrenie sa považuje za opodstatnené. Týmto nie sú dotknuté procesné práva dotknutého prevádzkovateľa v súlade s článkom 18 nariadenia (EÚ) 2019/1020. V prípade nedodržania zákazu praktík využívajúcich AI uvedených v článku 5 tohto nariadenia sa trojmesačné lehota uvedená v tomto odseku skráti na 30 dní.

9. Orgány dohľadu nad trhom zabezpečia, aby sa vo vzťahu k dotknutému výrobku alebo systému AI bez zbytočného odkladu prijali primerané reštriktívne opatrenia, ako je napríklad stiahnutie výrobku alebo systému AI z ich trhu.

Článok 80

Postup zaobchádzania so systémami AI, ktoré poskytovateľ uplatnením prílohy III klasifikoval ako nie vysokorizikové

1. Ak má orgán dohľadu nad trhom dostatočné dôvody domnievať sa, že systém AI, ktorý poskytovateľ podľa článku 6 ods. 3 klasifikoval ako nie vysokorizikový, je v skutočnosti vysokorizikový, orgán dohľadu nad trhom vykoná hodnotenie dotknutého systému AI, pokiaľ ide o jeho klasifikáciu ako vysokorizikového systému AI na základe podmienok stanovených v článku 6 ods. 3 a usmerneniach Komisie.

2. Ak v rámci tohto hodnotenia orgán dohľadu nad trhom zistí, že dotknutý systém AI je vysokorizikový, bez zbytočného odkladu požiada príslušného poskytovateľa, aby prijal všetky potrebné opatrenia na zosúladenie systému AI s požiadavkami a povinnosťami stanovenými v tomto nariadení a aby v lehote, ktorú orgán dohľadu nad trhom môže stanoviť, prijal vhodné nápravné opatrenia.

3. Ak sa orgán dohľadu nad trhom domnieva, že používanie dotknutého systému AI sa neobmedzuje na územie jeho štátu, bez zbytočného odkladu informuje Komisiu a ostatné členské štáty o výsledkoch hodnotenia a opatreniach, ktorých prijatie požadoval od prevádzkovateľa.

4. Poskytovateľ zabezpečí, aby sa prijali všetky opatrenia potrebné na zosúladenie systému AI s požiadavkami a povinnosťami stanovenými v tomto nariadení. Ak poskytovateľ dotknutého systému AI neuvedie systém AI do súladu s uvedenými požiadavkami a povinnosťami v lehote uvedenej v odseku 2 tohto článku, poskytovateľovi sa uložia pokuty v súlade s článkom 99.

5. Poskytovateľ zabezpečí prijatie všetkých primeraných nápravných opatrení v súvislosti so všetkými dotknutými systémami AI, ktoré sprístupnil na trhu Únie.

6. Ak poskytovateľ dotknutého systému AI neprijme primerané nápravné opatrenia v lehote uvedenej v odseku 2 tohto článku, uplatňuje sa článok 79 ods. 5 až 9.

7. Ak v priebehu hodnotenia podľa odseku 1 tohto článku orgán dohľadu nad trhom zistí, že poskytovateľ nesprávne klasifikoval systém AI ako nie vysokorizikový s cieľom obísť uplatňovanie požiadaviek uvedených v kapitole III oddiele 2, poskytovateľovi sa uložia pokuty v súlade s článkom 99.

8. Orgány dohľadu nad trhom môžu pri výkone svojej právomoci monitorovať uplatňovanie tohto článku a v súlade s článkom 11 nariadenia (EÚ) 2019/1020 vykonávať primerané kontroly, pričom zohľadnia najmä informácie uložené v databáze Únie uvedenej v článku 71 tohto nariadenia.

Článok 81

Ochranný postup Únie

1. Ak do troch mesiacov od doručenia oznámenia uvedeného v článku 79 ods. 5 alebo do 30 dní v prípade nedodržania zákazu praktík využívajúcich AI uvedených v článku 5 orgán dohľadu nad trhom členského štátu vznesie námietky proti opatreniu prijatému iným orgánom dohľadu nad trhom, alebo ak sa Komisia domnieva, že toto opatrenie je v rozpore s právom Únie, začne Komisia bez zbytočného odkladu konzultácie s orgánom dohľadu nad trhom príslušného členského štátu a prevádzkovateľom alebo prevádzkovateľmi a vyhodnotí vnútroštátne opatrenie. Na základe výsledkov tohto hodnotenia Komisia do šiestich mesiacov od doručenia oznámenia uvedeného v článku 79 ods. 5 alebo do 60 dní v prípade nedodržania zákazu praktík využívajúcich AI uvedených v článku 5 rozhodne, či je vnútroštátne opatrenie opodstatnené, a svoje rozhodnutie oznámi orgánu dohľadu nad trhom dotknutého členského štátu. Komisia o svojom rozhodnutí informuje aj všetky ostatné orgány dohľadu nad trhom.

2. Ak sa Komisia domnieva, že opatrenie prijaté príslušným členským štátom je opodstatnené, všetky členské štáty zabezpečia, aby vo vzťahu k dotknutému systému AI prijali primerané reštriktívne opatrenia, ako je požiadavka na stiahnutie systému AI z ich trhu bez zbytočného odkladu, a informujú o tom Komisiu. Ak Komisia považuje vnútroštátne opatrenie za neopodstatnené, dotknutý členský štát toto opatrenie vezme späť a informuje o tom Komisiu.

3. Ak sa vnútroštátne opatrenie považuje za opodstatnené a nesúlad systému AI sa pripisuje nedostatkom v harmonizovaných normách alebo spoločných špecifikáciách uvedených v článkoch 40 a 41 tohto nariadenia, Komisia uplatní postup stanovený v článku 11 nariadenia (EÚ) č. 1025/2012.

Článok 82

Vyhovujúce systémy AI, ktoré predstavujú riziko

1. Ak po vykonaní hodnotenia podľa článku 79 po konzultácii s príslušným vnútroštátnym orgánom verejnej moci uvedeným v článku 77 ods. 1 orgán dohľadu nad trhom členského štátu zistí, že hoci je vysokorizikový systém AI v súlade s týmto nariadením, napriek tomu predstavuje riziko pre zdravie alebo bezpečnosť osôb, pre základné práva alebo pre iné aspekty ochrany verejného záujmu, požiada príslušného prevádzkovateľa, aby bez zbytočného odkladu, v lehote, ktorú môže orgán stanoviť, prijal všetky primerané opatrenia, ktorými sa zabezpečí, aby dotknutý systém AI pri uvedení na trh alebo do prevádzky už takéto riziko nepredstavoval.

2. Poskytovateľ alebo iný relevantný prevádzkovateľ v lehote stanovenej orgánom dohľadu nad trhom členského štátu v zmysle odseku 1 zabezpečí prijatie nápravných opatrení v súvislosti so všetkými dotknutými systémami AI, ktoré sprístupnil na trhu Únie.

3. Členské štáty o zistení podľa odseku 1 okamžite informujú Komisiu a ostatné členské štáty. Tieto informácie obsahujú všetky podrobnosti, ktoré sú k dispozícii, najmä údaje potrebné na identifikáciu dotknutého systému AI, jeho pôvod a dodávateľský reťazec, povahu z neho vyplývajúceho rizika a povahu a trvanie prijatých vnútroštátnych opatrení.

4. Komisia začne bez zbytočného odkladu konzultovať s dotknutými členskými štátmi a príslušnými prevádzkovateľmi a vyhodnotí prijaté vnútroštátne opatrenia. Na základe výsledkov tohto hodnotenia Komisia rozhodne, či je opatrenie opodstatnené, a podľa potreby navrhne iné primerané opatrenia.

5. Komisia svoje rozhodnutie bezodkladne oznámi dotknutým členským štátom a príslušným prevádzkovateľom. Informuje aj ostatné členské štáty.

Článok 83

Formálny nesúlad

1. Orgán dohľadu na trhom členského štátu požiada príslušného prevádzkovateľa o odstránenie predmetného nesúladu v lehote, ktorú môže určiť, ak dospeje k jednému z týchto zistení:

   a) označenie CE bolo umiestnené v rozpore s článkom 48;

   b) označenie CE nebolo umiestnené;

   c) nebolo vyhotovené EÚ vyhlásenie o zhode uvedené v článku 47;

d) EÚ vyhlásenie o zhode uvedené v článku 47 nebolo vyhotovené správne;

e) nebola vykonaná registrácia v databáze Únie uvedenej v článku 71;

f) v relevantných prípadoch nebol vymenovaný splnomocnený zástupca;

g) technická dokumentácia nie je k dispozícii.

2. Ak nesúlad uvedený v odseku 1 pretrváva, orgán dohľadu nad trhom dotknutého členského štátu prijme náležité a primerané opatrenia na obmedzenie alebo zákaz sprístupňovania vysokorizikového systému AI na trhu alebo zabezpečí jeho bezodkladné stiahnutie od používateľa alebo z trhu.

Článok 84

Podporné štruktúry Únie na testovanie AI

1. Komisia určí jednu alebo viacero podporných štruktúr Únie na testovanie AI na plnenie úloh uvedených v článku 21 ods. 6 nariadenia (EÚ) 2019/1020 v oblasti AI.

2. Bez toho, aby boli dotknuté úlohy uvedené v odseku 1, na žiadosť rady pre AI, Komisie alebo orgánov dohľadu nad trhom poskytujú podporné štruktúry Únie na testovanie AI aj nezávislé technické alebo vedecké poradenstvo.

ODDIEL 4

PROSTRIEDKY NÁPRAVY

Článok 85

Právo podať sťažnosť orgánu dohľadu nad trhom

Bez toho, aby boli dotknuté iné správne alebo súdne prostriedky nápravy, každá fyzická alebo právnická osoba, ktorá má dôvody domnievať sa, že došlo k porušeniu ustanovení tohto nariadenia, môže podať sťažnosť príslušnému orgánu dohľadu nad trhom.

V súlade s nariadením (EÚ) 2019/1020 sa takéto sťažnosti zohľadňujú na účel vykonávania činností dohľadu nad trhom a vybavujú sa v súlade so špecializovanými postupmi, ktoré na to stanovili orgány dohľadu nad trhom.

Článok 86

Právo na vysvetlenie individuálneho rozhodovania

1. Každá dotknutá osoba, na ktorú sa vzťahuje rozhodnutie prijaté nasadzujúcim subjektom na základe výstupu z vysokorizikového systému AI uvedeného v prílohe III, s výnimkou systémov uvedených v jej bode 2, ktoré má právne účinky alebo má na dotknutú osobu podobne významný vplyv, ktorý podľa danej osoby nepriaznivo ovplyvňuje jej zdravie, bezpečnosť alebo základné práva, má právo získať od nasadzujúceho subjektu jasné a zmysluplné vysvetlenie úlohy systému AI v rozhodovacom postupe a hlavných prvkoch prijatého rozhodnutia.

2. Odsek 1 sa nevzťahuje na používanie systémov AI, v prípade ktorých výnimky z povinnosti podľa uvedeného odseku alebo obmedzenia tejto povinnosti vyplývajú z práva Únie alebo vnútroštátneho práva, ktoré je v súlade s právom Únie.

3. Tento článok sa uplatňuje len v rozsahu, v akom právo uvedené v odseku 1 nie je inak stanovené v práve Únie.

Článok 87

Nahlasovanie porušení a ochrana nahlasujúcich osôb

Pri nahlasovaní porušení tohto nariadenia a na ochranu osôb nahlasujúcich takéto porušenia sa uplatňuje smernica (EÚ) 2019/1937.

ODDIEL 5

DOHĽAD, VYŠETROVANIE, PRESADZOVANIE A MONITOROVANIE V SÚVISLOSTI S POSKYTOVATEĽMI MODELOV AI NA VŠEOBECNÉ ÚČELY

Článok 88

Presadzovanie plnenia povinností poskytovateľov modelov AI na všeobecné účely

1. Komisia má výlučnú právomoc vykonávať dohľad nad kapitolou V a presadzovať ju, pričom zohľadňuje procesné záruky podľa článku 94. Komisia poverí vykonávaním týchto úloh úrad pre AI bez toho, aby boli dotknuté organizačné právomoci Komisie a rozdelenie právomocí medzi členské štáty a Úniu na základe zmlúv.

2. Bez toho, aby bol dotknutý článok 75 ods. 3, môžu orgány dohľadu nad trhom požiadať Komisiu o výkon právomocí stanovených v tomto oddiele, ak je to potrebné a primerané na pomoc pri plnení ich úloh podľa tohto nariadenia.

Článok 89

Monitorovacie opatrenia

1. Úrad pre AI môže v záujme plnenia úloh, ktoré mu prislúchajú podľa tohto oddielu, prijať opatrenia potrebné na monitorovanie účinného vykonávania a dodržiavania tohto nariadenia zo strany poskytovateľov modelov AI na všeobecné účely vrátane dodržiavania schválených kódexov postupov.

2. Nadväzujúci poskytovatelia majú právo podať sťažnosť na údajné porušenie tohto nariadenia. Sťažnosť musí byť riadne odôvodnená a musí obsahovať aspoň:

   a) kontaktné miesto poskytovateľa dotknutého modelu AI na všeobecné účely;

   b) opis relevantných skutočností, príslušné ustanovenia tohto nariadenia a dôvod, prečo sa nadväzujúci poskytovateľ domnieva, že poskytovateľ dotknutého modelu AI na všeobecné účely porušil toto nariadenie;

   c) akékoľvek ďalšie informácie, ktoré nadväzujúci poskytovateľ, ktorý podáva sťažnosť, považuje za relevantné, vrátane prípadných informácií, ktoré zhromaždil z vlastnej iniciatívy.

Článok 90

Upozornenia vedeckého panelu na systémové riziká

1. Vedecký panel môže úradu pre AI poskytnúť kvalifikované upozornenie, ak má dôvodné podozrenie, že:

   a) model AI na všeobecné účely predstavuje konkrétne identifikovateľné riziko na úrovni Únie; alebo

   b) model AI na všeobecné účely spĺňa podmienky uvedené v článku 51.

2. Po takomto kvalifikovanom upozornení môže Komisia prostredníctvom úradu pre AI a po informovaní rady pre AI vykonať právomoci stanovené v tomto oddiele na účely posúdenia danej záležitosti. Úrad pre AI informuje radu pre AI o každom opatrení podľa článkov 91 až 94.

3. Kvalifikované upozornenie musí byť riadne odôvodnené a musí obsahovať aspoň:

   a) kontaktné miesto poskytovateľa dotknutého modelu AI na všeobecné účely so systémovým rizikom;

   b) opis relevantných skutočností a odôvodnenie upozornenia vedeckého panelu;

   c) akékoľvek ďalšie informácie, ktoré vedecký panel považuje za relevantné, vrátane prípadných informácií, ktoré zhromaždil z vlastnej iniciatívy.

Článok 91

Právomoc požadovať dokumentáciu a informácie

1. Komisia môže požiadať poskytovateľa dotknutého modelu AI na všeobecné účely, aby poskytol dokumentáciu, ktorú vypracoval v súlade s článkami 53 a 55 alebo akékoľvek dodatočné informácie, ktoré sú potrebné na účely posúdenia súladu poskytovateľa s týmto nariadením.

2. Úrad pre AI môže pred odoslaním žiadosti o informácie iniciovať štruktúrovaný dialóg s poskytovateľom modelu AI na všeobecné účely.

3. Komisia môže na základe riadne odôvodnenej žiadosti vedeckého panelu predložiť poskytovateľovi modelu AI na všeobecné účely žiadosť o informácie, ak je prístup k informáciám potrebný a primeraný na plnenie úloh vedeckého panelu podľa článku 68 ods. 2.

4. V žiadosti o informácie sa uvedie právny základ a účel žiadosti, upresní sa, aké informácie sa požadujú, stanoví sa lehota, v ktorej sa majú informácie poskytnúť, a uvedú sa pokuty stanovené v článku 101 za poskytnutie nesprávnych, neúplných alebo zavádzajúcich informácií.

5. Požadované informácie poskytne poskytovateľ dotknutého modelu AI na všeobecné účely alebo jeho zástupca. V prípade právnických osôb, spoločností alebo firiem, alebo ak poskytovateľ nemá právnu subjektivitu, poskytnú v mene poskytovateľa dotknutého modelu AI na všeobecné účely požadované informácie osoby oprávnenej na ich zastupovanie podľa zákona alebo v súlade s ich stanovami. V mene svojich klientov môžu poskytovať informácie riadne splnomocnení právnici. Za poskytnutie neúplných, nesprávnych alebo zavádzajúcich informácií však ostávajú plne zodpovední klienti.

Článok 92

Právomoc vykonávať hodnotenia

1. Úrad pre AI môže po konzultácii s radou pre AI vykonať hodnotenia dotknutého modelu AI na všeobecné účely s cieľom:

   a) posúdiť, či poskytovateľ dodržiava povinnosti podľa tohto nariadenia, ak informácie zhromaždené podľa článku 91 nie sú dostatočné; alebo

   b) vyšetrovať na úrovni Únie systémové riziká modelov AI na všeobecné účely so systémovým rizikom, najmä na základe kvalifikovaného upozornenia vedeckého panelu v súlade s článkom 90 ods. 1 písm. a).

2. Komisia môže rozhodnúť o vymenovaní nezávislých expertov na vykonávanie hodnotení v jej mene, a to aj z vedeckého panelu zriadeného podľa článku 68. Nezávislí experti vymenovaní na túto úlohu musia spĺňať kritériá uvedené v článku 68 ods. 2.

3. Na účely odseku 1 môže Komisia požiadať o prístup k dotknutému modelu AI na všeobecné účely prostredníctvom aplikačných programovacích rozhraní alebo ďalších vhodných technických prostriedkov a nástrojov, a to aj zdrojového kódu.

4. V žiadosti o prístup sa uvedie právny základ, účel a dôvody žiadosti a stanoví sa lehota na poskytnutie prístupu, ako aj pokuty stanovené v článku 101 za neposkytnutie prístupu.

5. Poskytovatelia dotknutého modelu AI na všeobecné účely alebo ich zástupcovia poskytnú požadované informácie. V prípade právnických osôb, spoločností alebo firiem, alebo ak poskytovateľ nemá právnu subjektivitu, osoby oprávnené zastupovať ich podľa zákona alebo v súlade s ich stanovami poskytnú požadovaný prístup v mene poskytovateľa dotknutého modelu AI na všeobecné účely.

6. Komisia prijme vykonávacie akty, v ktorých stanoví podrobné dojednania a podmienky týkajúce sa hodnotení vrátane podrobných dojednaní na zapojenie nezávislých expertov a postup ich výberu. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 98 ods. 2.

7. Úrad pre AI môže pred požiadaním o prístup k dotknutému modelu AI na všeobecné účely iniciovať štruktúrovaný dialóg s jeho poskytovateľom s cieľom zhromaždiť viac informácií o vnútornom testovaní modelu, vnútorných zárukách na predchádzanie systémovým rizikám a iných vnútorných postupoch a opatreniach, ktoré poskytovateľ prijal na zmiernenie takýchto rizík.

Článok 93

Právomoc požadovať opatrenia

1. Ak je to potrebné a vhodné, Komisia môže od poskytovateľov požadovať, aby:

   a) prijali vhodné opatrenia na splnenie povinností stanovených v článkoch 53 a 54;

   b) vykonali zmierňujúce opatrenia, ak hodnotenie vykonané v súlade s článkom 92 vyvolalo vážne a odôvodnené obavy zo systémového rizika na úrovni Únie;

   c) obmedzili sprístupnenie modelu na trhu alebo ho stiahli z trhu alebo od používateľa.

2. Úrad pre AI môže pred požadovaním opatrenia iniciovať štruktúrovaný dialóg s poskytovateľom modelu AI na všeobecné účely.

3. Ak poskytovateľ modelu AI na všeobecné účely so systémovým rizikom počas štruktúrovaného dialógu uvedeného v odseku 2 ponúkne, že sa zaviaže vykonať zmierňujúce opatrenia na riešenie systémového rizika na úrovni Únie, Komisia môže rozhodnutím vyhlásiť uvedené záväzky za záväzné a vyhlásiť, že neexistujú žiadne ďalšie dôvody na prijatie opatrení.

Článok 94

Procesné práva hospodárskych subjektov prevádzkujúcich model AI na všeobecné účely

Článok 18 nariadenia (EÚ) 2019/1020 sa primerane uplatňuje na poskytovateľov modelu AI na všeobecné účely bez toho, aby boli dotknuté konkrétnejšie procesné práva stanovené v tomto nariadení.

Kapitola X

Kódexy správania a usmernenia

Článok 95

Kódex správania pre dobrovoľné uplatňovanie osobitných požiadaviek

1. Úrad pre AI a členské štáty podporujú a uľahčujú vypracúvanie kódexov správania vrátane súvisiacich mechanizmov správy a riadenia určených na podporu dobrovoľného uplatňovania niektorých alebo všetkých požiadaviek stanovených v kapitole III oddiele 2 na iné systémy AI ako vysokorizikové systémy AI, pričom zohľadnia dostupné technické riešenia a najlepšie postupy v príslušnom odvetví umožňujúce uplatňovanie takýchto požiadaviek.

2. Úrad pre AI a členské štáty uľahčujú vypracúvanie kódexov správania týkajúcich sa dobrovoľného uplatňovania, a to aj zo strany nasadzujúcich subjektov, osobitných požiadaviek na všetky systémy AI na základe jasných cieľov a kľúčových ukazovateľov výkonu na meranie dosahovania týchto cieľov vrátane prvkov, ako sú okrem iného:

a) uplatniteľné prvky stanovené v etických usmerneniach Únie pre dôveryhodnú AI;

b) posudzovanie a minimalizácia vplyvu systémov AI na životné prostredie, a to aj pokiaľ ide o energeticky účinné programovanie a techniky efektívneho dizajnu, trénovania a používania AI;

c) podpora gramotnosti v oblasti AI, najmä osôb, ktoré sa zaoberajú vývojom, prevádzkovaním a používaním AI;

d) uľahčenie inkluzívnych a rôznorodých dizajnov systémov AI, a to aj prostredníctvom zriaďovania inkluzívnych a rôznorodých vývojárskych tímov a podpora účasti zainteresovaných strán na tomto procese;

e) posudzovanie a predchádzanie negatívnemu vplyvu systémov AI na zraniteľné osoby alebo skupiny zraniteľných osôb, a to aj pokiaľ ide o prístupnosť pre osoby so zdravotným postihnutím, ako aj ich vplyvu na rodovú rovnosť.

3. Kódexy správania môžu vypracúvať jednotliví poskytovatelia alebo nasadzujúce subjekty systémov AI alebo organizácie, ktoré ich zastupujú, a to aj v spolupráci s akýmikoľvek zainteresovanými stranami a organizáciami, ktoré ich zastupujú, vrátane organizácií občianskej spoločnosti a akademickej obce. Kódexy správania sa môžu vzťahovať na jeden alebo viacero systémov AI, pričom sa zohľadní podobnosť zamýšľaného účelu príslušných systémov.

4. Úrad pre AI a členské štáty pri podpore a uľahčovaní vypracúvania kódexov správania zohľadňujú osobitné záujmy a potreby MSP vrátane startupov.

Článok 96

Usmernenia Komisie k vykonávaniu tohto nariadenia

1. Komisia vypracuje usmernenia o praktickom vykonávaní tohto nariadenia, a to najmä o:

   a) uplatňovaní požiadaviek a povinností uvedených v článkoch 8 až 15 a v článku 25;

   b) zakázaných praktikách uvedených v článku 5;

   c) praktickom vykonávaní ustanovení týkajúcich sa podstatnej zmeny;

   d) praktickom plnení povinností v oblasti transparentnosti stanovených v článku 50;

e) podrobných informáciách o vzťahu tohto nariadenia s harmonizačnými právnymi predpismi Únie uvedenými v prílohe I, ako aj s inými príslušnými právnymi predpismi Únie, a to aj pokiaľ ide o konzistentnosť pri ich presadzovaní;

f) uplatňovaní vymedzenia pojmu „systém AI“, ako sa uvádza v článku 3 bode 1.

Pri vydávaní takýchto usmernení Komisia venuje osobitnú pozornosť potrebám MSP vrátane startupov, miestnych orgánov verejnej správy a odvetví, ktoré budú s najväčšou pravdepodobnosťou ovplyvnené týmto nariadením.

V usmerneniach uvedených v prvom pododseku tohto odseku sa náležite zohľadní všeobecne uznávaný aktuálny stav vývoja v oblasti AI, ako aj príslušné harmonizované normy a spoločné špecifikácie, ktoré sú uvedené v článkoch 40 a 41, alebo harmonizované normy alebo technické špecifikácie, ktoré sú stanovené podľa harmonizačného práva Únie.

2. Komisia na žiadosť členských štátov, úradu pre AI alebo z vlastnej iniciatívy v prípade potreby aktualizuje usmernenia, ktoré prijala v minulosti.

Kapitola XI
Delegovanie právomoci a postup výboru

Článok 97

Vykonávanie delegovania právomoci

1. Komisii sa udeľuje právomoc prijímať delegované akty za podmienok stanovených v tomto článku.

2. Právomoc prijímať delegované akty uvedené v článku 6 ods. 6 a 7, článku 7 ods. 1 a 3, článku 11 ods. 3, článku 43 ods. 5 a 6, článku 47 ods. 5, článku 51 ods. 3, článku 52 ods. 4 a článku 53 ods. 5 a 6 sa Komisii udeľuje na obdobie piatich rokov od ... [deň nadobudnutia účinnosti tohto nariadenia]. Komisia vypracuje správu týkajúcu sa delegovania právomoci najneskôr deväť mesiacov pred uplynutím tohto päťročného obdobia. Delegovanie právomoci sa automaticky predlžuje o rovnako dlhé obdobia, pokiaľ Európsky parlament alebo Rada nevznesú voči takémuto predĺženiu námietku najneskôr tri mesiace pred koncom každého obdobia.

3. Delegovanie právomoci uvedené v článku 6 ods. 6 a 7, článku 7 ods. 1 a 3, článku 11 ods. 3, článku 43 ods. 5 a 6, článku 47 ods. 5, článku 51 ods. 3, článku 52 ods. 4 a článku 53 ods. 5 a 6 môže Európsky parlament alebo Rada kedykoľvek odvolať. Rozhodnutím o odvolaní sa ukončuje delegovanie právomoci, ktoré sa v ňom uvádza. Rozhodnutie nadobúda účinnosť dňom nasledujúcim po jeho uverejnení v *Úradnom vestníku Európskej únie* alebo k neskoršiemu dátumu, ktorý je v ňom určený. Nie je ním dotknutá platnosť delegovaných aktov, ktoré už nadobudli účinnosť.

4. Komisia pred prijatím delegovaného aktu konzultuje s expertmi určenými jednotlivými členskými štátmi v súlade so zásadami stanovenými v Medziinštitucionálnej dohode z 13. apríla 2016 o lepšej tvorbe práva.

5. Komisia oznamuje delegovaný akt hneď po jeho prijatí súčasne Európskemu parlamentu a Rade.

6. Delegovaný akt prijatý podľa článku 6 ods. 6 alebo 7, článku 7 ods. 1 alebo 3, článku 11 ods. 3, článku 43 ods. 5 alebo 6, článku 47 ods. 5, článku 51 ods. 3, článku 52 ods. 4 alebo článku 53 ods. 5 alebo 6 nadobudne účinnosť, len ak Európsky parlament alebo Rada voči nemu nevzniesli námietku v lehote troch mesiacov odo dňa oznámenia uvedeného aktu Európskemu parlamentu a Rade alebo ak pred uplynutím uvedenej lehoty Európsky parlament a Rada informovali Komisiu o svojom rozhodnutí nevzniesť námietku.
Na podnet Európskeho parlamentu alebo Rady sa táto lehota predĺži o tri mesiace.

Článok 98

Postup výboru

1. Komisii pomáha výbor. Uvedený výbor je výborom v zmysle nariadenia (EÚ) č. 182/2011.

2. Ak sa odkazuje na tento odsek, uplatňuje sa článok 5 nariadenia (EÚ) č. 182/2011.

Kapitola XII
Sankcie

Článok 99
Sankcie

1. Členské štáty v súlade s podmienkami stanovenými v tomto nariadení stanovia pravidlá, pokiaľ ide o sankcie a iné opatrenia presadzovania, ktoré môžu zahŕňať varovania a nepeňažné opatrenia a sú uplatniteľné pri porušeniach tohto nariadenia zo strany prevádzkovateľov, a prijmú všetky opatrenia potrebné na zabezpečenie ich riadneho a účinného vykonávania, pričom zohľadnia usmernenia vydané Komisiou podľa článku 96. Stanovené sankcie musia byť účinné, primerané a odrádzajúce. Musia zohľadňovať záujmy MSP vrátane startupov a ich ekonomickú životaschopnosť.

2. Členské štáty o pravidlách týkajúcich sa sankcií a iných opatreniach presadzovania uvedených v odseku 1 bezodkladne a najneskôr do dňa začatia uplatňovania informujú Komisiu a bezodkladne jej oznámia každú ich nasledujúcu zmenu.

3. Za nedodržanie zákazov praktík využívajúcich AI uvedených v článku 5 sa ukladajú správne pokuty až do výšky 35 000 000 EUR, alebo ak je páchateľom podnik, až do výšky 7 % jeho celkového celosvetového ročného obratu za predchádzajúci finančný rok, podľa toho, ktorá suma je vyššia.

4. Správne pokuty až do výšky 15 000 000 EUR, alebo ak je páchateľom podnik, až do výšky 3 % jeho celkového celosvetového ročného obratu za predchádzajúci finančný rok, podľa toho, ktorá suma je vyššia, sa ukladajú za nesúlad s ktorýmkoľvek z týchto ustanovení týkajúcich sa prevádzkovateľov alebo notifikovaných osôb iných ako stanovených v článku 5:

a) povinnosti poskytovateľov podľa článku 16;

b) povinnosti splnomocnených zástupcov podľa článku 22;

c) povinnosti dovozcov podľa článku 23;

d) povinnosti distribútorov podľa článku 24;

e) povinnosti nasadzujúcich subjektov podľa článku 26;

f) požiadavky a povinnosti notifikovaných osôb podľa článku 31, článku 33 ods. 1, 3 a 4 alebo článku 34;

g) povinnosti v oblasti transparentnosti pre poskytovateľov a nasadzujúce subjekty podľa článku 50.

5. Za poskytnutie nesprávnych, neúplných alebo zavádzajúcich informácií v odpovedi na žiadosť notifikovaných osôb alebo vnútroštátnych príslušných orgánov sa ukladajú správne pokuty až do výšky 7 500 000 EUR, alebo ak je páchateľom podnik, až do výšky 1 % jeho celkového celosvetového ročného obratu za predchádzajúci finančný rok, podľa toho, ktorá suma je vyššia.

6. V prípade MSP vrátane startupov sa každá pokuta uvedená v tomto článku ukladá až do percentuálneho podielu alebo sumy uvedenej v odsekoch 3, 4 a 5, podľa toho, ktorá suma je nižšia.

7. Pri rozhodovaní o uložení správnej pokuty a o jej výške sa v každom jednotlivom prípade zohľadnia všetky relevantné okolnosti konkrétnej situácie a vo vhodných prípadoch sa vezme do úvahy:

a) povaha, závažnosť a trvanie porušenia a jeho dôsledkov s prihliadnutím na účel systému AI a vo vhodných prípadoch aj na počet dotknutých jednotlivcov a rozsah škody, ktorú utrpeli;

b) či už tomu istému prevádzkovateľovi uložili za to isté porušenie správne pokuty iné orgány dohľadu nad trhom;

c) či už iné orgány uložili správne pokuty tomu istému prevádzkovateľovi za porušenia iných právnych predpisov Únie alebo vnútroštátnych právnych predpisov, ak takéto porušenia vyplývajú z tej istej činnosti alebo opomenutia predstavujúceho relevantné porušenie tohto nariadenia;

d) veľkosť, ročný obrat a trhový podiel prevádzkovateľa, ktorý sa dopustil porušenia;

e) akékoľvek iné priťažujúce alebo poľahčujúce okolnosti prípadu, ako napríklad získané finančné výhody alebo straty, ktorým sa zabránilo, priamo alebo nepriamo v súvislosti s porušením;

f) miera spolupráce s vnútroštátnymi príslušnými orgánmi pri náprave porušenia a zmiernení možných nepriaznivých dôsledkov porušenia;

g) miera zodpovednosti prevádzkovateľa s prihliadnutím na technické a organizačné opatrenia, ktoré vykonal;

h) spôsob, akým sa vnútroštátne príslušné orgány o porušení dozvedeli, a najmä to, či prevádzkovateľ porušenie oznámil, a ak áno, v akom rozsahu;

i) úmyselný alebo nedbanlivostný charakter porušenia;

j) všetky opatrenia prijaté prevádzkovateľom na zmiernenie ujmy, ktorú utrpeli dotknuté osoby.

8. Každý členský štát stanoví pravidlá o tom, v akom rozsahu sa môžu správne pokuty uložiť orgánom verejnej moci a subjektom zriadeným v danom členskom štáte.

9. V závislosti od právneho systému členských štátov sa pravidlá o správnych pokutách môžu uplatňovať tak, aby pokuty podľa pravidiel uplatniteľných v daných členských štátoch ukladali príslušné vnútroštátne súdy alebo iné orgány. Uplatňovanie takýchto pravidiel v uvedených členských štátoch má rovnocenný účinok.

10. Výkon právomocí podľa tohto článku podlieha primeraným procesným zárukám v súlade s právom Únie a vnútroštátnym právom vrátane účinného súdneho prostriedku nápravy a riadneho procesu.

11. Členské štáty každoročne podávajú Komisii správu o správnych pokutách, ktoré počas daného roka uložili v súlade s týmto článkom, a o všetkých súvisiacich sporoch alebo súdnych konaniach.

Článok 100

Správne pokuty ukladané inštitúciám, orgánom, úradom a agentúram Únie

1. Európsky dozorný úradník pre ochranu údajov môže uložiť správne pokuty inštitúciám, orgánom, úradom a agentúram Únie, ktoré patria do rozsahu pôsobnosti tohto nariadenia. Pri rozhodovaní o uložení správnej pokuty a o jej výške sa v každom jednotlivom prípade zohľadnia všetky relevantné okolnosti konkrétnej situácie a náležite sa vezme do úvahy:

   a) povaha, závažnosť a trvanie porušenia a jeho dôsledky, pričom sa zohľadní účel dotknutého systému AI, ako aj v prípade potreby počet dotknutých osôb a rozsah škody, ktorú utrpeli;

   b) miera zodpovednosti inštitúcie, orgánu, úradu alebo agentúry Únie s prihliadnutím na technické a organizačné opatrenia, ktoré vykonali;

   c) akékoľvek opatrenie, ktoré inštitúcia, orgán, úrad alebo agentúra Únie prijali na zmiernenie škody, ktorú utrpeli dotknuté osoby;

   d) miera spolupráce s európskym dozorným úradníkom pre ochranu údajov s cieľom napraviť porušenie a zmierniť možné nepriaznivé účinky porušenia vrátane dodržiavania všetkých opatrení, ktoré predtým nariadil európsky dozorný úradník pre ochranu údajov dotknutej inštitúcii, orgánu, úradu alebo agentúre Únie v rovnakej veci;

e) akékoľvek podobné predchádzajúce porušenia zo strany inštitúcie, orgánu, úradu alebo agentúry Únie;

f) spôsob, akým sa európsky dozorný úradník pre ochranu údajov o porušení dozvedel, najmä to, či inštitúcia, orgán, úrad alebo agentúra Únie porušenie oznámili, a ak áno, v akom rozsahu;

g) ročný rozpočet inštitúcie, orgánu, úradu alebo agentúry Únie.

2. Za nedodržanie zákazu praktík využívajúcich AI, ktoré sa uvádzajú v článku 5, sa ukladajú správne pokuty až do výšky 1 500 000 EUR.

3. Za nesúlad systému AI s inými požiadavkami alebo povinnosťami podľa tohto nariadenia než s tými, ktoré sú stanovené v článku 5, sa ukladajú správne pokuty až do výšky 750 000 EUR.

4. Pred prijatím rozhodnutí podľa tohto článku európsky dozorný úradník pre ochranu údajov poskytne inštitúcii, orgánu, úradu alebo agentúre Únie, voči ktorým vedie konanie, možnosť vyjadriť sa k záležitostiam týkajúcim sa možného porušenia. Európsky dozorný úradník pre ochranu údajov pri svojich rozhodnutiach vychádza len zo skutočností a okolností, ku ktorým sa dotknuté strany mohli vyjadriť. Prípadní sťažovatelia sú do konania úzko zapojení.

5. V konaní sa v plnej miere rešpektuje právo dotknutých strán na obhajobu. S výhradou oprávneného záujmu fyzických osôb alebo podnikov na ochrane ich osobných údajov alebo obchodného tajomstva majú dotknuté strany právo na prístup k spisu európskeho dozorného úradníka pre ochranu údajov.

6. Prostriedky získané z pokút uložených podľa tohto článku sú príspevkom do všeobecného rozpočtu Únie. Pokuty nesmú ovplyvniť účinné fungovanie inštitúcie, orgánu, úradu alebo agentúry Únie, ktorej boli uložené.

7. Európsky dozorný úradník pre ochranu údajov každoročne informuje Komisiu o správnych pokutách, ktoré uložil podľa tohto článku, a akýchkoľvek sporoch alebo súdnych konaniach, ktoré inicioval.

Článok 101

Pokuty ukladané poskytovateľom modelov AI na všeobecné účely

1. Komisia môže poskytovateľom modelov AI na všeobecné účely uložiť pokuty nepresahujúce 3 % ich celkového ročného celosvetového obratu v predchádzajúcom finančnom roku alebo 15 000 000 EUR, podľa toho, ktorá suma je vyššia, keď zistí, že poskytovateľ úmyselne alebo z nedbanlivosti:

   a) porušil relevantné ustanovenia tohto nariadenia;

   b) nevyhovel žiadosti o dokument alebo informácie podľa článku 91 alebo poskytol nesprávne, neúplné alebo zavádzajúce informácie;

c) nesplnil opatrenie požadované podľa článku 93;

d) neumožnil Komisii prístup k modelu AI na všeobecné účely alebo k modelu AI na všeobecné účely so systémovým rizikom, aby mohla vykonať hodnotenie podľa článku 92.

Pri určovaní výšky pokuty alebo pravidelného penále sa prihliada na povahu, závažnosť a trvanie porušenia, pričom sa náležitým spôsobom zohľadňujú zásady proporcionality a vhodnosti. Komisia zohľadní aj záväzky prijaté v súlade s článkom 93 ods. 3 alebo v príslušných kódexoch postupov v súlade s článkom 56.

2. Komisia pred prijatím rozhodnutia podľa odseku 1 oznámi poskytovateľovi modelu AI na všeobecné účely svoje predbežné zistenia a poskytne mu príležitosť na vypočutie.

3. Pokuty uložené v súlade s týmto článkom musia byť účinné, primerané a odrádzajúce.

4. Informácie o pokutách uložených podľa tohto článku sa podľa potreby oznámia aj rade pre AI.

5. Súdny dvor Európskej únie má neobmedzenú súdnu právomoc na preskúmanie rozhodnutí Komisie, v ktorých stanovila pokutu podľa tohto článku. Uloženú pokutu môže zrušiť, znížiť alebo zvýšiť.

6. Komisia prijme vykonávacie akty obsahujúce podrobné dojednania a procesné záruky pre konanie na účely prípadného prijatia rozhodnutí podľa odseku 1 tohto článku. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 98 ods. 2.

Kapitola XIII
Záverečné ustanovenia

Článok 102

Zmena nariadenia (ES) č. 300/2008

V článku 4 ods. 3 nariadenia (ES) č. 300/2008 sa dopĺňa tento pododsek:

„Pri prijímaní podrobných opatrení súvisiacich s technickými špecifikáciami a postupmi schvaľovania a používania bezpečnostných zariadení týkajúcich sa systémov AI v zmysle nariadenia Európskeho parlamentu a Rady (EÚ) 2024/...*+ sa zohľadňujú požiadavky stanovené v kapitole III oddiele 2 uvedeného nariadenia.

---

* Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/... z ..., ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii) (Ú. v. EÚ L, ..., ELI: ...).“

\+ Ú. v.: vložte do textu číslo tohto nariadenia (2021/0106 (COD)) a doplňte príslušnú poznámku pod čiarou.

Článok 103

Zmena nariadenia (EÚ) č. 167/2013

V článku 17 ods. 5 nariadenia (EÚ) č. 167/2013 sa dopĺňa tento pododsek:

„Pri prijímaní delegovaných aktov podľa prvého pododseku týkajúcich sa systémov AI, ktoré sú bezpečnostnými komponentmi v zmysle nariadenia Európskeho parlamentu a Rady (EÚ) 2024/...[*+], sa zohľadňujú požiadavky stanovené v kapitole III oddiele 2 uvedeného nariadenia.

---

[*] Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/... z ..., ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii) (Ú. v. EÚ L, ..., ELI: ...).“

[+] Ú. v.: vložte do textu číslo tohto nariadenia 2021/0106 (COD)) a doplňte príslušnú poznámku pod čiarou.

Článok 104

Zmena nariadenia (EÚ) č. 168/2013

V článku 22 ods. 5 nariadenia (EÚ) č. 168/2013 sa dopĺňa tento pododsek:

„Pri prijímaní delegovaných aktov podľa prvého pododseku týkajúcich sa systémov AI, ktoré sú bezpečnostnými komponentmi v zmysle nariadenia Európskeho parlamentu a Rady (EÚ) 2024/...[*+], sa zohľadňujú požiadavky stanovené v kapitole III oddiele 2 uvedeného nariadenia.

---

[*] Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/... z ..., ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii) (Ú. v. EÚ L, ..., ELI: ...).“

[+] Ú. v.: vložte do textu číslo tohto nariadenia 2021/0106 (COD)) a doplňte príslušnú poznámku pod čiarou.

Článok 105

Zmena smernice 2014/90/EÚ

V článku 8 smernice 2014/90/EÚ sa dopĺňa tento odsek:

„5. V prípade systémov AI, ktoré sú bezpečnostnými komponentmi v zmysle nariadenia Európskeho parlamentu a Rady (EÚ) 2024/..[*+], Komisia pri vykonávaní svojich činností podľa odseku 1 a pri prijímaní technických špecifikácií a skúšobných noriem v súlade s odsekmi 2 a 3 zohľadní požiadavky stanovené v kapitole III oddiele 2 uvedeného nariadenia.

---

[*] Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/... z ..., ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii) (Ú. v. EÚ L, ..., ELI: ...).“

[+] Ú. v.: vložte do textu číslo tohto nariadenia 2021/0106 (COD)) a doplňte príslušnú poznámku pod čiarou.

Článok 106

Zmena smernice (EÚ) 2016/797

V článku 5 smernice (EÚ) 2016/797 sa dopĺňa tento odsek:

„12. Pri prijímaní delegovaných aktov podľa odseku 1 a vykonávacích aktov podľa odseku 11 týkajúcich sa systémov AI, ktoré sú bezpečnostnými komponentmi v zmysle nariadenia Európskeho parlamentu a Rady (EÚ) 2024/...*+, sa zohľadňujú požiadavky stanovené v kapitole III oddiele 2 uvedeného nariadenia.

---

* Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/... z ..., ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii) (Ú. v. EÚ L, ..., ELI: ...).“

\+ Ú. v.: vložte do textu číslo tohto nariadenia[2021/0106 (COD)) a doplňte príslušnú poznámku pod čiarou.

Článok 107

Zmena nariadenia (EÚ) 2018/858

V článku 5 nariadenia (EÚ) 2018/858 sa dopĺňa tento odsek:

„4. „Pri prijímaní delegovaných aktov podľa odseku 3 týkajúcich sa systémov AI, ktoré sú bezpečnostnými komponentmi v zmysle nariadenia Európskeho parlamentu a Rady (EÚ) 2024/...[*+], sa zohľadňujú požiadavky stanovené v kapitole III oddiele 2 uvedeného nariadenia.

---

[*] Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/... z ..., ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii) (Ú. v. EÚ L, ..., ELI: ...).“

[+] Ú. v.: vložte do textu číslo tohto nariadenia 2021/0106 (COD)) a doplňte príslušnú poznámku pod čiarou.

Článok 108

Zmeny nariadenia (EÚ) 2018/1139

Nariadenie (EÚ) 2018/1139 sa mení takto:

1. V článku 17 sa dopĺňa tento odsek:

„3. Bez toho, aby bol dotknutý odsek 2, pri prijímaní vykonávacích aktov podľa odseku 1 týkajúcich sa systémov AI, ktoré sú bezpečnostnými komponentmi v zmysle nariadenia Európskeho parlamentu a Rady (EÚ) 2024/...[*+], sa zohľadňujú požiadavky stanovené v kapitole III oddiele 2 uvedeného nariadenia.

---

[*] Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/... z ..., ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii) (Ú. v. EÚ L, ..., ELI: ...).“

2. V článku 19 sa dopĺňa tento odsek:

„4. Pri prijímaní delegovaných aktov podľa odsekov 1 a 2 týkajúcich sa systémov AI, ktoré sú bezpečnostnými komponentmi v zmysle nariadenia (EÚ) 2024/...[++], sa zohľadňujú požiadavky stanovené v kapitole III oddiele 2 uvedeného nariadenia.“

[+] Ú. v.: vložte, prosím, do textu číslo tohto nariadenia 2021/0106 (COD)) a doplňte príslušnú poznámku pod čiarou.

[++] Ú. v.: vložte, prosím, číslo tohto nariadenia 2021/0106 (COD)).

3. V článku 43 sa dopĺňa tento odsek:

„4. Pri prijímaní vykonávacích aktov podľa odseku 1 týkajúcich sa systémov AI, ktoré sú bezpečnostnými komponentmi v zmysle nariadenia (EÚ) 2024/...[+], sa zohľadňujú požiadavky stanovené v kapitole III oddiele 2 uvedeného nariadenia.“

4. V článku 47 sa dopĺňa tento odsek:

„3. Pri prijímaní delegovaných aktov podľa odsekov 1 a 2 týkajúcich sa systémov AI, ktoré sú bezpečnostnými komponentmi v zmysle nariadenia (EÚ) 2024/...[+], sa zohľadňujú požiadavky stanovené v kapitole III oddiele 2 uvedeného nariadenia.“

5. V článku 57 sa dopĺňa tento pododsek:

„Pri prijímaní uvedených vykonávacích aktov týkajúcich sa systémov AI, ktoré sú bezpečnostnými komponentmi v zmysle nariadenia (EÚ) 2024/...[+], sa zohľadňujú požiadavky stanovené v kapitole III oddiele 2 uvedeného nariadenia.“

6. V článku 58 sa dopĺňa tento odsek:

„3. Pri prijímaní delegovaných aktov podľa odsekov 1 a 2 týkajúcich sa systémov AI, ktoré sú bezpečnostnými komponentmi v zmysle nariadenia (EÚ) 2024/...[+], sa zohľadňujú požiadavky stanovené v kapitole III oddiele 2 uvedeného nariadenia.“

[+] Ú. v.: vložte, prosím, číslo tohto nariadenia 2021/0106 (COD)).

Článok 109

Zmena nariadenia (EÚ) 2019/2144

V článku 11 nariadenia (EÚ) 2019/2144 sa dopĺňa tento odsek:

„3. Pri prijímaní vykonávacích aktov podľa odseku 2 týkajúcich sa systémov AI, ktoré sú bezpečnostnými komponentmi v zmysle nariadenia Európskeho parlamentu a Rady (EÚ) 2024/...[*+], sa zohľadňujú požiadavky stanovené v kapitole III oddiele 2 uvedeného nariadenia.

---

[*] Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/... z ..., ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii) (Ú. v. EÚ L, ..., ELI: ...).“

[+] Ú. v.: vložte, prosím, do textu číslo tohto nariadenia 2021/0106 (COD)) a doplňte príslušnú poznámku pod čiarou.

Článok 110

Zmena smernice (EÚ) 2020/1828

V prílohe I k smernici Európskeho parlamentu a Rady (EÚ) 2020/1828[58] sa dopĺňa tento bod:

„68. Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/... z ..., ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii) (Ú. v. EÚ L, ..., ELI: ...).[+]“

Článok 111

Systémy AI, ktoré už boli uvedené na trh alebo do prevádzky a modely AI na všeobecné účely, ktoré už boli uvedené na trh

1. Bez toho, aby bolo dotknuté uplatňovanie článku 5, ako sa uvádza v článku 113 ods. 3 písm. a), systémy AI, ktoré sú komponentmi rozsiahlych informačných systémov zriadených právnymi aktmi uvedenými v prílohe X, ktoré boli uvedené na trh alebo do prevádzky pred ... [36 mesiacov odo dňa nadobudnutia účinnosti tohto nariadenia], sa uvedú do súladu s týmto nariadením do 31. decembra 2030.

---

58 Smernica Európskeho parlamentu a Rady (EÚ) 2020/1828 z 25. novembra 2020 o žalobách v zastúpení na ochranu kolektívnych záujmov spotrebiteľov a o zrušení smernice 2009/22/ES (Ú. v. EÚ L 409, 4.12.2020, s. 1).

\+ Ú. v.: vložte, prosím, do textu číslo, dátum prijatia a odkaz na uverejnenie tohto nariadenia 2021/0106 (COD)).

Pri hodnotení každého rozsiahleho informačného systému zriadeného právnymi aktmi uvedenými v prílohe X, ktoré sa má vykonať podľa uvedených právnych aktov a vtedy, keď sa uvedené právne akty nahradia alebo zmenia, sa zohľadnia požiadavky stanovené v tomto nariadení.

2. Bez toho, aby bolo dotknuté uplatňovanie článku 5, ako sa uvádza v článku 113 ods. 3 písm. a), sa toto nariadenie uplatňuje na prevádzkovateľov iných vysokorizikových systémov AI, než sú systémy uvedené v odseku 1 tohto článku, ktoré boli uvedené na trh alebo do prevádzky pred ... [24 mesiacov odo dňa nadobudnutia účinnosti tohto nariadenia], len vtedy, ak v týchto systémoch došlo od uvedeného dátumu k významným zmenám dizajnu. V každom prípade poskytovatelia vysokorizikových systémov AI a subjekty nasadzujúce vysokorizikové systémy AI, ktoré majú používať orgány verejnej moci, prijmú potrebné kroky na dosiahnutie súladu s požiadavkami a povinnosťami podľa tohto nariadenia do ... [šesť rokov odo dňa nadobudnutia účinnosti tohto nariadenia].

3. Poskytovatelia modelov AI na všeobecné účely, ktoré boli uvedené na trh pred ... [12 mesiacov odo dňa nadobudnutia účinnosti tohto nariadenia], prijmú potrebné kroky na splnenie povinností stanovených v tomto nariadení do ... [36 mesiacov odo dňa nadobudnutia účinnosti tohto nariadenia].

Článok 112

Hodnotenie a preskúmanie

1. Komisia každý rok po nadobudnutí účinnosti tohto nariadenia a až do konca obdobia delegovania právomoci stanoveného v článku 97 posúdi potrebu zmeny zoznamu v prílohe III a zoznamu zakázaných praktík využívajúcich AI v článku 5. Komisia predloží zistenia tohto posúdenia Európskemu parlamentu a Rade.

2. Komisia do ... [štyri roky odo dňa nadobudnutia účinnosti tohto nariadenia] a potom každé štyri roky vyhodnotí nasledovné skutočnosti a predloží správu Európskemu parlamentu a Rade:

   a) potrebu zmien, ktorými sa rozširujú existujúce oblasti alebo dopĺňajú nové oblasti v prílohe III;

   b) zmeny zoznamu systémov AI, ktoré si vyžadujú dodatočné opatrenia v oblasti transparentnosti podľa článku 50;

   c) zmeny, ktorými sa zvyšuje účinnosť systému dohľadu a správy a riadenia.

3. Komisia do ... [päť rokov odo dňa nadobudnutia účinnosti tohto nariadenia] a potom každé štyri roky predloží Európskemu parlamentu a Rade správu o hodnotení a preskúmaní tohto nariadenia. Táto správa obsahuje posúdenie štruktúry presadzovania a prípadnej potreby, aby zistené nedostatky odstránila agentúra Únie. Na základe zistení sa k uvedenej správe v prípade potreby pripojí návrh na zmenu tohto nariadenia. Správy sa uverejňujú.

4. V správach uvedených v odseku 2 sa venuje osobitná pozornosť:

a) stavu finančných, technických a ľudských zdrojov vnútroštátnych príslušných orgánov na účinné vykonávanie úloh, ktoré im boli pridelené podľa tohto nariadenia;

b) stavu sankcií, najmä správnych pokút uvedených v článku 99 ods. 1, ktoré členské štáty ukladajú za porušenie tohto nariadenia;

c) prijatým harmonizovaným normám a spoločným špecifikáciám vypracovaným na podporu tohto nariadenia;

d) počtu podnikov, ktoré vstúpia na trh po začatí uplatňovania tohto nariadenia, a tomu, koľko z nich sú MSP.

5. Komisia do ... [štyri roky odo dňa nadobudnutia účinnosti tohto nariadenia] vyhodnotí fungovanie úradu pre AI, to, či mu boli udelené dostatočné právomoci na plnenie jeho úloh a či by na riadne vykonávanie a presadzovanie tohto nariadenia bolo vhodné a potrebné posilniť úrad pre AI a jeho právomoci v oblasti presadzovania a navýšiť jeho zdroje. Komisia správu o svojom hodnotení predloží Európskemu parlamentu a Rade.

6. Komisia do ... [štyri roky odo dňa nadobudnutia účinnosti tohto nariadenia] a potom každé štyri roky predloží správu o preskúmaní pokroku pri vývoji normalizačných produktov týkajúcich sa energeticky efektívneho vývoja modelov AI na všeobecné účely a posúdi potrebu ďalších opatrení alebo krokov vrátane záväzných opatrení alebo krokov. Táto správa sa predloží Európskemu parlamentu a Rade a zverejní sa.

7. Komisia do ... [štyri roky odo dňa nadobudnutia účinnosti tohto nariadenia] a potom každé tri roky vyhodnotí vplyv a účinnosť dobrovoľných kódexov správania na podporu uplatňovania požiadaviek stanovených v kapitole III oddiele 2 na systémy AI, ktoré nie sú vysokorizikové, a prípadne ďalších dodatočných požiadaviek na systémy AI, ktoré nie sú vysokorizikové, a to aj pokiaľ ide o environmentálnu udržateľnosť.

8. Rada pre AI, členské štáty a vnútroštátne príslušné orgány bez zbytočného odkladu poskytnú Komisii na jej žiadosť informácie na účely odsekov 1 až 7.

9. Pri hodnoteniach a preskúmaniach uvedených v odsekoch 1 až 7 Komisia zohľadní stanoviská a zistenia rady pre AI, Európskeho parlamentu, Rady a iných relevantných subjektov alebo zdrojov.

10. Komisia v prípade potreby predloží vhodné návrhy na zmenu tohto nariadenia, pričom zohľadní najmä vývoj v oblasti technológií a vplyv systémov AI na zdravie a bezpečnosť a na základné práva a vezme do úvahy aktuálny stav pokroku v informačnej spoločnosti.

11. S cieľom usmerniť hodnotenia a preskúmania uvedené v odsekoch 1 až 7 tohto článku vypracuje úrad pre AI objektívnu a participatívnu metodiku hodnotenia úrovní rizika na základe kritérií uvedených v príslušných článkoch a začlenenia nových systémov do:

a) zoznamu uvedeného v prílohe III vrátane rozšírenia existujúcich oblastí alebo pridania nových oblastí do uvedenej prílohy;

b) zoznamu zakázaných praktík uvedených v článku 5; a

c) zoznamu systémov AI, ktoré si vyžadujú dodatočné opatrenia v oblasti transparentnosti podľa článku 50.

12. Pri každej zmene tohto nariadenia podľa odseku 10 alebo príslušných delegovaných alebo vykonávacích aktov, ktoré sa týkajú odvetvových harmonizačných právnych predpisov Únie uvedených v prílohe I oddiele B, sa zohľadňujú regulačné osobitosti jednotlivých odvetví, existujúce mechanizmy správy a riadenia, posudzovania zhody a presadzovania a orgány, ktorú sú nimi zriadené.

13. Komisia do ... [sedem rokov odo dňa nadobudnutia účinnosti tohto nariadenia] posúdi presadzovanie tohto nariadenia a podá o ňom správu Európskemu parlamentu, Rade a Európskemu hospodárskemu a sociálnemu výboru, pričom zohľadní prvé roky uplatňovania tohto nariadenia. Na základe zistení sa k správe v prípade potreby pripojí návrh na zmenu tohto nariadenia, pokiaľ ide o štruktúru presadzovania a potrebu, aby všetky zistené nedostatky odstránila agentúra Únie.

Článok 113

Nadobudnutie účinnosti a uplatňovanie

Toto nariadenie nadobúda účinnosť dvadsiatym dňom nasledujúcim po jeho uverejnení v *Úradnom vestníku Európskej únie*.

Uplatňuje sa od ... [24 mesiacov odo dňa nadobudnutia účinnosti tohto nariadenia].

Avšak:

a) kapitoly I a II sa uplatňujú od ... [šesť mesiacov odo dňa nadobudnutia účinnosti tohto nariadenia];

b) kapitola III oddiel 4, kapitola V, kapitola VII, kapitola XII a článok 78 sa uplatňujú od ... [12 mesiacov odo dňa nadobudnutia účinnosti tohto nariadenia], s výnimkou článku 101;

c) článok 6 ods. 1 a zodpovedajúce povinnosti stanovené v tomto nariadení sa uplatňujú od ... [36 mesiacov odo dňa nadobudnutia účinnosti tohto nariadenia].

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V ...

Za Európsky parlament	*Za Radu*
predsedníčka	*predseda/predsedníčka*

PRÍLOHA I

Zoznam harmonizačných právnych predpisov Únie

Oddiel A. Zoznam harmonizačných právnych predpisov Únie na základe nového legislatívneho rámca

1. Smernica Európskeho parlamentu a Rady 2006/42/ES zo 17. mája 2006 o strojových zariadeniach a o zmene a doplnení smernice 95/16/ES (Ú. v. EÚ L 157, 9.6.2006, s. 24) [zrušená nariadením o strojových zariadeniach];

2. smernica Európskeho parlamentu a Rady 2009/48/ES z 18. júna 2009 o bezpečnosti hračiek (Ú. v. EÚ L 170, 30.6.2009, s. 1);

3. smernica Európskeho parlamentu a Rady 2013/53/EÚ z 20. novembra 2013 o rekreačných plavidlách a vodných skútroch a o zrušení smernice 94/25/ES (Ú. v. EÚ L 354, 28.12.2013, s. 90);

4. smernica Európskeho parlamentu a Rady 2014/33/EÚ z 26. februára 2014 o harmonizácii právnych predpisov členských štátov týkajúcich sa výťahov a bezpečnostných komponentov do výťahov (Ú. v. EÚ L 96, 29.3.2014, s. 251);

5. smernica Európskeho parlamentu a Rady 2014/34/EÚ z 26. februára 2014 o harmonizácii právnych predpisov členských štátov týkajúcich sa zariadení a ochranných systémov určených na použitie v potenciálne výbušnej atmosfére (Ú. v. EÚ L 96, 29.3.2014, s. 309);

6. smernica Európskeho parlamentu a Rady 2014/53/EÚ zo 16. apríla 2014 o harmonizácii právnych predpisov členských štátov týkajúcich sa sprístupňovania rádiových zariadení na trhu, ktorou sa zrušuje smernica 1999/5/ES (Ú. v. EÚ L 153, 22.5.2014, s. 62);

7. smernica Európskeho parlamentu a Rady 2014/68/EÚ z 15. mája 2014 o harmonizácii právnych predpisov členských štátov týkajúcich sa sprístupňovania tlakových zariadení na trhu (Ú. v. EÚ L 189, 27.6.2014, s. 164);

8. nariadenie Európskeho parlamentu a Rady (EÚ) 2016/424 z 9. marca 2016 o lanovkových zariadeniach a zrušení smernice 2000/9/ES (Ú. v. EÚ L 81, 31.3.2016, s. 1);

9. nariadenie Európskeho parlamentu a Rady (EÚ) 2016/425 z 9. marca 2016 o osobných ochranných prostriedkoch a o zrušení smernice Rady 89/686/EHS (Ú. v. EÚ L 81, 31.3.2016, s. 51);

10. nariadenie Európskeho parlamentu a Rady (EÚ) 2016/426 z 9. marca 2016 o spotrebičoch spaľujúcich plynné palivá a zrušení smernice 2009/142/ES (Ú. v. EÚ L 81, 31.3.2016, s. 99);

11. nariadenie Európskeho parlamentu a Rady (EÚ) 2017/745 z 5. apríla 2017 o zdravotníckych pomôckach, zmene smernice 2001/83/ES, nariadenia (ES) č. 178/2002 a nariadenia (ES) č. 1223/2009 a o zrušení smerníc Rady 90/385/EHS a 93/42/EHS (Ú. v. EÚ L 117, 5.5.2017, s. 1);

12. nariadenie Európskeho parlamentu a Rady (EÚ) 2017/746 z 5. apríla 2017 o diagnostických zdravotníckych pomôckach in vitro a o zrušení smernice 98/79/ES a rozhodnutia Komisie 2010/227/EÚ (Ú. v. EÚ L 117, 5.5.2017, s. 176).

Oddiel B. Zoznam iných harmonizačných právnych predpisov Únie

13. Nariadenie Európskeho parlamentu a Rady (ES) č. 300/2008 z 11. marca 2008 o spoločných pravidlách v oblasti bezpečnostnej ochrany civilného letectva a o zrušení nariadenia (ES) č. 2320/2002 (Ú. v. EÚ L 97, 9.4.2008, s. 72);

14. nariadenie Európskeho parlamentu a Rady (EÚ) č. 168/2013 z 15. januára 2013 o schvaľovaní a dohľade nad trhom dvoj- alebo trojkolesových vozidiel a štvorkoliek (Ú. v. EÚ L 60, 2.3.2013, s. 52);

15. nariadenie Európskeho parlamentu a Rady (EÚ) č. 167/2013 z 5. februára 2013 o schvaľovaní poľnohospodárskych a lesných vozidiel a o dohľade nad trhom s týmito vozidlami (Ú. v. EÚ L 60, 2.3.2013, s. 1);

16. smernica Európskeho parlamentu a Rady 2014/90/EÚ z 23. júla 2014 o vybavení námorných lodí a o zrušení smernice Rady 96/98/ES (Ú. v. EÚ L 257, 28.8.2014, s. 146);

17. smernica Európskeho parlamentu a Rady (EÚ) 2016/797 z 11. mája 2016 o interoperabilite železničného systému v Európskej únii (Ú. v. EÚ L 138, 26.5.2016, s. 44);

18. nariadenie Európskeho parlamentu a Rady (EÚ) 2018/858 z 30. mája 2018 o schvaľovaní motorových vozidiel a ich prípojných vozidiel, ako aj systémov, komponentov a samostatných technických jednotiek určených pre takéto vozidlá a o dohľade nad trhom s nimi, ktorým sa menia nariadenia (ES) č. 715/2007 a (ES) č. 595/2009 a zrušuje smernica 2007/46/ES (Ú. v. EÚ L 151, 14.6.2018, s. 1);

19. nariadenie Európskeho parlamentu a Rady (EÚ) 2019/2144 z 27. novembra 2019 o požiadavkách na typové schvaľovanie motorových vozidiel a ich prípojných vozidiel a systémov, komponentov a samostatných technických jednotiek určených pre tieto vozidlá, pokiaľ ide o ich všeobecnú bezpečnosť a ochranu cestujúcich vo vozidle a zraniteľných účastníkov cestnej premávky, ktorým sa mení nariadenie Európskeho parlamentu a Rady (EÚ) 2018/858 a ktorým sa zrušujú nariadenia Európskeho parlamentu a Rady (ES) č. 78/2009, (ES) č. 79/2009 a (ES) č. 661/2009 a nariadenia Komisie (ES) č. 631/2009, (EÚ) č. 406/2010, (EÚ) č. 672/2010, (EÚ) č. 1003/2010, (EÚ) č. 1005/2010, (EÚ) č. 1008/2010, (EÚ) č. 1009/2010, (EÚ) č. 19/2011, (EÚ) č. 109/2011, (EÚ) č. 458/2011, (EÚ) č. 65/2012, (EÚ) č. 130/2012, (EÚ) č. 347/2012, (EÚ) č. 351/2012, (EÚ) č. 1230/2012 a (EÚ) 2015/166 (Ú. v. EÚ L 325, 16.12.2019, s. 1);

20. nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1139 zo 4. júla 2018 o spoločných pravidlách v oblasti civilného letectva, ktorým sa zriaďuje Agentúra Európskej únie pre bezpečnosť letectva a ktorým sa menia nariadenia Európskeho parlamentu a Rady (ES) č. 2111/2005, (ES) č. 1008/2008, (EÚ) č. 996/2010, (EÚ) č. 376/2014 a smernice Európskeho parlamentu a Rady 2014/30/EÚ a 2014/53/EÚ a zrušujú nariadenia Európskeho parlamentu a Rady (ES) č. 552/2004 a (ES) č. 216/2008 a nariadenie Rady (EHS) č. 3922/91 (Ú. v. EÚ L 212, 22.8.2018, s. 1), pokiaľ ide o projektovanie a výrobu lietadiel uvedených v článku 2 ods. 1 písm. a) a b) a ich umiestňovanie na trh, ak sa týka bezpilotných lietadiel, a ich motorov, vrtúľ, súčastí a vybavenia na ich diaľkové ovládanie.

PRÍLOHA II

Zoznam trestných činov podľa článku 5 ods. 1 prvého pododseku písm. h) bodu iii)

Trestné činy podľa článku 5 ods. 1 prvého pododseku písm. h) bodu iii):

– terorizmus,

– obchodovanie s ľuďmi,

– sexuálne vykorisťovanie detí a detská pornografia,

– nedovolené obchodovanie s omamnými alebo psychotropnými látkami,

– nedovolené obchodovanie so zbraňami, strelivom alebo s výbušninami,

– vražda, ťažká ujma na zdraví,

– nedovolené obchodovanie s ľudskými orgánmi alebo tkanivami,

– nedovolené obchodovanie s jadrovými alebo rádioaktívnymi materiálmi,

– únos, obmedzovanie osobnej slobody alebo branie rukojemníka,

– trestné činy podliehajúce právomoci Medzinárodného trestného súdu,

– nezákonné ovládnutie lietadla alebo plavidla,

– znásilnenie,

– trestné činy proti životnému prostrediu,

– organizovaná alebo ozbrojená lúpež,

– sabotáž,

– účasť v zločineckej organizácii zapojenej do jedného alebo viacerých vyššie uvedených trestných činov.

PRÍLOHA III

Vysokorizikové systémy AI podľa článku 6 ods. 2

Vysokorizikové systémy AI podľa článku 6 ods. 2 sú systémy AI uvedené v ktorejkoľvek z týchto oblastí:

1. Biometria, pokiaľ je jej použitie povolené podľa príslušných právnych predpisov Únie alebo vnútroštátnych právnych predpisov:

   a) systémy diaľkovej biometrickej identifikácie.

      Nie sú tu zahrnuté systémy AI určené na používanie na biometrické overenie, ktorých jediným účelom je potvrdiť, že konkrétna fyzická osoba je osobou, za ktorú sa vydáva;

   b) systémy AI určené na použitie na biometrickú kategorizáciu podľa citlivých alebo chránených atribútov alebo charakteristík na základe odvodenia týchto atribútov alebo charakteristík;

   c) systémy AI určené na rozpoznávanie emócií.

2. Kritická infraštruktúra: systémy AI, ktoré sa majú používať ako bezpečnostné komponenty pri riadení a prevádzke kritickej digitálnej infraštruktúry, cestnej premávky alebo pri dodávkach vody, plynu, tepla alebo elektriny.

3. Vzdelávanie a odborná príprava:

a) systémy AI, ktoré sa majú používať na určenie prístupu alebo prijatia alebo pridelenia fyzických osôb do inštitúcií vzdelávania a odbornej prípravy na všetkých úrovniach;

b) systémy AI, ktoré sa majú používať na hodnotenie vzdelávacích výstupov, a to aj vtedy, keď sa tieto výstupy používajú na riadenie procesu učenia fyzických osôb v inštitúciách vzdelávania a odbornej prípravy na všetkých úrovniach;

c) systémy AI, ktoré sa majú používať na účely posúdenia primeranej úrovne vzdelania, ktoré fyzická osoba získa alebo ku ktorému bude mať prístup, v kontexte alebo v rámci inštitúcie vzdelávania a odbornej prípravy na všetkých úrovniach;

d) systémy AI, ktoré sa majú používať na monitorovanie a zisťovanie zakázaného správania študentov počas skúšok v kontexte alebo v rámci inštitúcií vzdelávania a odbornej prípravy na všetkých úrovniach.

4. Zamestnanosť, riadenie pracovníkov a prístup k samostatnej zárobkovej činnosti:

a) systémy AI, ktoré sa majú používať na nábor alebo výber fyzických osôb, najmä na umiestňovanie cielených inzerátov na pracovné miesta, na analýzu a filtrovanie žiadostí o zamestnanie a na hodnotenie uchádzačov;

b) systémy AI, ktoré sa majú používať pri rozhodovaní o podmienkach pracovnoprávnych vzťahov, o kariérnom postupe v zamestnaní alebo ukončení zmluvných pracovnoprávnych vzťahov, pri prideľovaní úloh na základe individuálneho správania alebo osobných čŕt alebo charakteristických znakov alebo pri monitorovaní a hodnotení výkonnosti a správania osôb v rámci takýchto vzťahov.

5. Prístup k základným súkromným službám a základným verejným službám a dávkam a ich využívanie:

a) systémy AI, ktoré majú používať orgány verejnej moci alebo ktoré sa majú používať v ich mene na hodnotenie oprávnenosti fyzických osôb na základné dávky a služby verejnej pomoci vrátane služieb zdravotnej starostlivosti, ako aj na poskytovanie, zníženie či zrušenie takýchto dávok a služieb alebo uplatnenie nároku na ich vrátenie;

b) systémy AI, ktoré sa majú používať na hodnotenie úverovej bonity fyzických osôb alebo stanovenie ich bodového hodnotenia kreditného rizika, s výnimkou systémov AI používaných na účely odhaľovania finančných podvodov;

c) systémy AI, ktoré sa majú používať na hodnotenie rizika a stanovovanie cien vo vzťahu k fyzickým osobám v prípade životného a zdravotného poistenia;

d) systémy AI určené na hodnotenie a klasifikáciu tiesňových volaní fyzických osôb alebo na vysielanie záchranných služieb prvej reakcie vrátane zo strany polície, hasičov a zdravotníckej pomoci alebo na stanovovanie priority ich vysielania, ako aj pokiaľ ide o systémy triedenia pacientov v rámci pohotovostnej zdravotnej starostlivosti.

6. Presadzovanie práva, pokiaľ je ich použitie povolené podľa príslušných právnych predpisov Únie alebo vnútroštátnych právnych predpisov:

a) systémy AI, ktoré majú používať orgány presadzovania práva alebo ktoré sa majú používať v ich mene alebo ktoré majú používať inštitúcie, orgány, úrady alebo agentúry Únie na podporu orgánov presadzovania práva alebo ktoré sa majú používať v ich mene na posudzovanie rizika, že sa fyzická osoba stane obeťou trestných činov;

b) systémy AI, ktoré majú používať orgány presadzovania práva alebo ktoré sa majú používať v ich mene alebo ktoré majú používať inštitúcie, orgány, úrady alebo agentúry Únie na podporu orgánov presadzovania práva ako polygrafy alebo podobné nástroje;

c) systémy AI, ktoré majú používať orgány presadzovania práva alebo ktoré sa majú používať v ich mene alebo ktoré majú používať inštitúcie, orgány, úrady alebo agentúry Únie na podporu orgánov presadzovania práva na hodnotenie spoľahlivosti dôkazov v priebehu vyšetrovania alebo stíhania trestných činov;

d) systémy AI, ktoré majú používať orgány presadzovania práva alebo ktoré sa majú používať v ich mene alebo ktoré majú používať inštitúcie, orgány, úrady alebo agentúry Únie na podporu orgánov presadzovania práva na posudzovanie rizika, že fyzická osoba spácha alebo opätovne spácha trestný čin, a to nielen na základe profilovania fyzických osôb uvedeného v článku 3 bode 4 smernice (EÚ) 2016/680, alebo na posúdenie osobnostných čŕt a charakteristických znakov alebo trestnej činnosti fyzických osôb alebo skupín v minulosti;

e) systémy AI, ktoré majú používať orgány presadzovania práva alebo ktoré sa majú používať v ich mene alebo ktoré majú používať inštitúcie, orgány, úrady alebo agentúry Únie na podporu orgánov presadzovania práva na profilovanie fyzických osôb uvedené v článku 3 bode 4 smernice (EÚ) 2016/680 v priebehu odhaľovania, vyšetrovania alebo stíhania trestných činov.

7. Migrácia, azyl a riadenie kontroly hraníc, pokiaľ je ich použitie povolené podľa príslušných právnych predpisov Únie alebo vnútroštátnych právnych predpisov:

a) systémy AI, ktoré majú používať príslušné orgány verejnej moci alebo ktoré sa majú používať v ich mene alebo ktoré majú používať inštitúcie, orgány, úrady alebo agentúry Únie ako polygrafy alebo podobné nástroje;

b) systémy AI, ktoré majú používať príslušné orgány verejnej moci alebo ktoré sa majú používať v ich mene alebo ktoré majú používať inštitúcie, orgány, úrady alebo agentúry Únie na posúdenie rizika vrátane bezpečnostného rizika, rizika neoprávnenej migrácie alebo zdravotného rizika, ktoré predstavuje fyzická osoba, ktorá má v úmysle vstúpiť na územie členského štátu alebo naň už vstúpila;

c) systémy AI, ktoré majú používať príslušné orgány verejnej moci alebo ktoré sa majú používať v ich mene alebo ktoré majú používať inštitúcie, orgány, úrady alebo agentúry Únie na pomoc príslušným orgánom verejnej moci na preskúmanie žiadostí o azyl, víza alebo povolenia na pobyt a súvisiacich sťažností týkajúcich sa oprávnenosti fyzických osôb žiadajúcich o určitý status vrátane súvisiaceho posudzovania spoľahlivosti dôkazov;

d) systémy AI, ktoré majú používať príslušné orgány verejnej moci alebo ktoré sa majú používať v ich mene alebo ktoré majú používať inštitúcie, orgány, úrady alebo agentúry Únie v súvislosti s migráciou, azylom a riadením kontroly hraníc na účely odhaľovania, uznávania alebo identifikácie fyzických osôb s výnimkou overovania cestovných dokladov.

8. Výkon spravodlivosti a demokratické procesy:

a) systémy AI, ktoré má používať justičný orgán alebo ktoré sa majú používať v jeho mene na pomoc justičnému orgánu pri skúmaní a interpretácii skutkových okolností a práva a pri uplatňovaní práva na konkrétny súbor skutkových okolností alebo ktoré sa majú používať obdobným spôsobom pri alternatívnom riešení sporov;

b) systémy AI určené na ovplyvňovanie výsledku volieb alebo referenda alebo volebného správania fyzických osôb pri hlasovaní vo voľbách alebo v referende; nepatria sem systémy AI, ktorých výstupom nie sú fyzické osoby priamo vystavené, ako sú nástroje používané na organizovanie, optimalizáciu alebo tvorbu štruktúry politických kampaní z administratívneho a logistického hľadiska.

PRÍLOHA IV

Technická dokumentácia podľa článku 11 ods. 1

Technická dokumentácia podľa článku 11 ods. 1 obsahuje v závislosti od príslušného systému AI aspoň tieto informácie:

1. všeobecný opis systému AI vrátane týchto prvkov:

   a) jeho zamýšľaný účel, meno poskytovateľa a verziu systému odrážajúcu jeho vzťah k predchádzajúcim verziám;

   b) spôsob interakcie systému AI s hardvérom alebo softvérom vrátane iných systémov AI, ktoré nie sú súčasťou samotného systému AI, alebo ako ho prípadne možno na takúto interakciu použiť;

   c) verzie príslušného softvéru alebo firmvéru a všetky požiadavky týkajúce sa aktualizácií verzií;

   d) opis všetkých foriem, v ktorých sa systém AI uvádza na trh alebo do prevádzky, ako sú softvérové balíky zabudované do hardvéru, stiahnuteľná forma alebo aplikačné programovacie rozhrania;

   e) opis hardvéru, na ktorom má systém AI fungovať;

   f) ak je systém AI komponentom výrobkov, fotografií alebo ilustrácií znázorňujúcich vonkajšie znaky, označenie a vnútorné usporiadanie týchto výrobkov;

g) základný opis používateľského rozhrania poskytnutého nasadzujúcemu subjektu;

h) návod na použitie pre nasadzujúci subjekt a prípadný základný opis používateľského rozhrania poskytnutého nasadzujúcemu subjektu;

2. podrobný opis prvkov systému AI a procesu jeho vývoja, vrátane:

a) metód a krokov vykonaných pri vývoji systému AI vrátane prípadného využívania vopred natrénovaných systémov alebo nástrojov poskytnutých tretími stranami a spôsobu, akým ich poskytovateľ používal, integroval alebo zmenil;

b) špecifikácií dizajnu systému, konkrétne všeobecnej logiky systému AI a algoritmov; kľúčových rozhodnutí o riešeniach dizajnu vrátane odôvodnenia a predpokladov, a to aj so zreteľom na osoby alebo skupiny osôb, vo vzťahu ku ktorým sa má systém používať; hlavných možností klasifikácie; čo má systém optimalizovať a relevantnosť jednotlivých parametrov; opisu očakávaného výstupu systému a kvality tohto výstupu; rozhodnutí o akomkoľvek možnom kompromise vykonanom v súvislosti s technickými riešeniami prijatými na dosiahnutie súladu s požiadavkami stanovenými v kapitole III oddiele 2;

c) opisu architektúry systému, v ktorom sa vysvetľuje, ako softvérové komponenty na seba nadväzujú alebo ako sa navzájom dopĺňajú a integrujú do celkového spracúvania; výpočtových zdrojov používaných na vývoj, trénovanie, testovanie a validáciu systému AI;

d) v príslušnom prípade požiadaviek na údaje, pokiaľ ide o údajové hárky s opisom trénovacích metodík a techník a použitých súborov trénovacích údajov vrátane všeobecného opisu týchto súborov údajov, informácií o ich pôvode, rozsahu a hlavných charakteristikách; spôsobu získavania a výberu údajov; postupov označovania (napr. pre učenie pod dohľadom), metodík čistenia údajov (napr. zisťovanie odľahlých hodnôt);

e) posúdenia potrebných opatrení na zabezpečenie ľudského dohľadu v súlade s článkom 14 vrátane posúdenia technických opatrení potrebných na uľahčenie interpretácie výstupov systémov AI nasadzujúcimi subjektmi v súlade s článkom 13 ods. 3 písm. d);

f) v náležitom prípade podrobného opisu vopred určených zmien systému AI a jeho výkonnosti spolu so všetkými relevantnými informáciami týkajúcimi sa technických riešení prijatých na zabezpečenie trvalého súladu systému AI s príslušnými požiadavkami stanovenými v kapitole III oddiele 2;

g) použitých postupov validácie a testovania vrátane informácií o použitých validačných a testovacích údajoch a ich hlavných charakteristikách; metrík používaných na meranie presnosti, spoľahlivosti a dosiahnutia súladu s inými relevantnými požiadavkami stanovenými v kapitole III oddiele 2, ako aj potenciálne diskriminačných vplyvov; testovacích log a všetkých správ o testoch s dátumom a podpisom zodpovedných osôb, a to aj pokiaľ ide o vopred určené zmeny uvedené v písmene f);

h) zavedených opatrení v oblasti kybernetickej bezpečnosti;

3. podrobné informácie o monitorovaní, fungovaní a kontrole systému AI, najmä pokiaľ ide o: jeho spôsobilosti a obmedzenia výkonnosti vrátane miery presnosti v prípade konkrétnych osôb alebo skupín osôb, v prípade ktorých sa má systém používať, a celkovú očakávanú úroveň presnosti vo vzťahu k zamýšľanému účelu; predvídateľné nezamýšľané výsledky a zdroje rizík pre zdravie a bezpečnosť, základné práva a diskrimináciu vzhľadom na zamýšľaný účel systému AI; opatrenia na zabezpečenie ľudského dohľadu potrebné v súlade s článkom 14 vrátane technických opatrení zavedených na uľahčenie interpretácie výstupov systémov AI nasadzujúcimi subjektmi; prípadné špecifikácie vstupných údajov;

4. opis vhodnosti ukazovateľov výkonnosti pre konkrétny systém AI;

5. podrobný opis systému riadenia rizík v súlade s článkom 9;

6. opis relevantných zmien systému, ktoré vykonal poskytovateľ počas jeho životného cyklu;

7. zoznam harmonizovaných, úplne alebo čiastočne uplatnených noriem, na ktoré boli uverejnené odkazy v *Úradnom vestníku Európskej únie*; ak sa žiadne takéto harmonizované normy neuplatnili, podrobný opis riešení prijatých na splnenie požiadaviek stanovených v kapitole III oddiele 2 vrátane zoznamu iných príslušných noriem a technických špecifikácií, ktoré sa uplatnili;

8. kópiu EÚ vyhlásenia o zhode uvedeného v článku 47;

9. podrobný opis systému zavedeného na hodnotenie výkonnosti systému AI vo fáze po uvedení na trh v súlade s článkom 72 vrátane plánu monitorovania po uvedení na trh v zmysle článku 72 ods. 3.

PRÍLOHA V

EÚ vyhlásenie o zhode

EÚ vyhlásenie o zhode uvedené v článku 47 obsahuje všetky tieto informácie:

1. názov a typ systému AI a akýkoľvek ďalší jednoznačný odkaz umožňujúci identifikáciu a vysledovateľnosť systému AI;

2. meno a adresa poskytovateľa alebo v náležitom prípade jeho splnomocneného zástupcu;

3. vyhlásenie o tom, že EÚ vyhlásenie o zhode uvedené v článku 47 sa vydáva na výhradnú zodpovednosť poskytovateľa;

4. vyhlásenie, že systém AI je v zhode s týmto nariadením a prípadne aj s akýmikoľvek iným príslušným právom Únie, ktorým sa stanovuje vydávanie EÚ vyhlásenia o zhode uvedeného v článku 47;

5. ak systém AI zahŕňa spracúvanie osobných údajov, vyhlásenie, že tento systém AI je v súlade s nariadeniami (EÚ) 2016/679 a (EÚ) 2018/1725 a so smernicou (EÚ) 2016/680;

6. odkazy na všetky príslušné použité harmonizované normy alebo akékoľvek iné spoločné špecifikácie, v súvislosti s ktorými sa vyhlasuje zhoda;

7. v náležitom prípade meno a identifikačné číslo notifikovanej osoby, opis použitého postupu posudzovania zhody a identifikácia vydaného certifikátu;

8. miesto a dátum vydania vyhlásenia, meno a funkcia osoby, ktorá ho podpísala, ako aj informácia o tom, pre koho alebo v mene koho daná osoba vyhlásenie podpísala, a podpis.

PRÍLOHA VI

Postup posudzovania zhody na základe vnútornej kontroly

1. Postup posudzovania zhody na základe vnútornej kontroly je postup posudzovania zhody založený na bodoch 2, 3 a 4.

2. Poskytovateľ overí, či je zavedený systém riadenia kvality v súlade s požiadavkami článku 17.

3. Poskytovateľ preskúma informácie obsiahnuté v technickej dokumentácii s cieľom posúdiť súlad systému AI s príslušnými základnými požiadavkami stanovenými v kapitole III oddiele 2.

4. Poskytovateľ takisto overí, či je proces dizajnu a vývoja systému AI a jeho monitorovanie po uvedení na trh v zmysle článku 72 v súlade s technickou dokumentáciou.

PRÍLOHA VII

Zhoda založená na posúdení systému riadenia kvality a na posúdení technickej dokumentácie

1. Úvod

Zhoda založená na posúdení systému riadenia kvality a na posúdení technickej dokumentácie je postup posudzovania zhody založený na bodoch 2 až 5.

2. Prehľad

Schválený systém riadenia kvality pre dizajn, vývoj a testovanie systémov AI podľa článku 17 sa preskúma v súlade s bodom 3 a podlieha dohľadu v zmysle bodu 5. Technická dokumentácia systému AI sa preskúma v súlade s bodom 4.

3. Systém riadenia kvality

3.1. Žiadosť poskytovateľa obsahuje:

a) meno a adresu poskytovateľa, a ak žiadosť podáva splnomocnený zástupca, aj jeho meno a adresu;

b) zoznam systémov AI, na ktoré sa vzťahuje ten istý systém riadenia kvality;

c) technickú dokumentáciu pre každý systém AI, na ktorý sa vzťahuje ten istý systém riadenia kvality;

d) dokumentáciu týkajúcu sa systému riadenia kvality, ktorá zahŕňa všetky aspekty uvedené v článku 17;

e) opis zavedených postupov na zabezpečenie zachovania primeranosti a účinnosti systému riadenia kvality;

f) písomné vyhlásenie, že tá istá žiadosť nebola podaná inej notifikovanej osobe.

3.2. Systém riadenia kvality posudzuje notifikovaná osoba, ktorá určí, či systém spĺňa požiadavky uvedené v článku 17.

Rozhodnutie sa oznámi poskytovateľovi alebo jeho splnomocnenému zástupcovi.

Oznámenie obsahuje závery posúdenia systému riadenia kvality a odôvodnené rozhodnutie o posúdení.

3.3. Schválený systém riadenia kvality poskytovateľ naďalej uplatňuje a udržiava tak, aby bol aj naďalej primeraný a účinný.

3.4. Poskytovateľ informuje notifikovanú osobu o každej zamýšľanej zmene schváleného systému riadenia kvality alebo zmene zoznamu systémov AI, na ktoré sa tento systém vzťahuje.

Notifikovaná osoba navrhované zmeny preskúma a rozhodne, či zmenený systém riadenia kvality naďalej spĺňa požiadavky uvedené v bode 3.2, alebo či je potrebné opätovné posúdenie.

Notifikovaná osoba oznámi svoje rozhodnutie poskytovateľovi. Oznámenie obsahuje závery preskúmania zmien a odôvodnené rozhodnutie o posúdení.

4. Kontrola technickej dokumentácie

4.1. Okrem žiadosti uvedenej v bode 3 predkladá poskytovateľ notifikovanej osobe podľa svojho výberu žiadosť o posúdenie technickej dokumentácie vzťahujúcej sa na systém AI, ktorý plánuje uviesť na trh alebo do prevádzky a na ktorý sa vzťahuje systém riadenia kvality uvedený v bode 3.

4.2. Žiadosť obsahuje:

a) meno a adresu poskytovateľa;

b) písomné vyhlásenie, že tá istá žiadosť nebola podaná inej notifikovanej osobe;

c) technickú dokumentáciu uvedenú v prílohe IV.

4.3. Notifikovaná osoba technickú dokumentáciu preskúma. Notifikovanej osobe sa v relevantných prípadoch a s obmedzením na to, čo je potrebné na plnenie jej úloh, poskytne úplný prístup k použitým súborom trénovacích, validačných a testovacích údajov, v prípade potreby a s výhradou bezpečnostných záruk aj prostredníctvom aplikačného programovacieho rozhrania alebo iných relevantných technických prostriedkov a nástrojov umožňujúcich diaľkový prístup.

4.4. Pri skúmaní technickej dokumentácie môže notifikovaná osoba požadovať, aby poskytovateľ predložil ďalšie dôkazy alebo vykonal ďalšie testy s cieľom umožniť riadne posúdenie zhody systému AI s požiadavkami stanovenými v kapitole III oddiele 2. Ak notifikovaná osoba nie je s testmi, ktoré vykonal poskytovateľ, spokojná, zodpovedajúce testy vykoná v prípade potreby priamo samotná notifikovaná osoba.

4.5. Ak je to potrebné na posúdenie zhody vysokorizikového systému AI s požiadavkami stanovenými v kapitole III oddiele 2, po vyčerpaní všetkých ostatných primeraných prostriedkov overenia zhody, ktoré sa ukázali ako nedostatočné, a na základe odôvodnenej žiadosti sa notifikovanej osobe udelí prístup aj k trénovacím a trénovaným modelom systému AI vrátane jeho relevantných parametrov. Takýto prístup podlieha platným právnym predpisom Únie o ochrane duševného vlastníctva a obchodného tajomstva.

4.6. Rozhodnutie notifikovanej osoby sa oznámi poskytovateľovi alebo jeho splnomocnenému zástupcovi. Oznámenie obsahuje závery posúdenia technickej dokumentácie a odôvodnené rozhodnutie o posúdení.

Ak je systém AI v zhode s požiadavkami stanovenými v kapitole III oddiele 2, notifikovaná osoba vydá certifikát Únie o posúdení technickej dokumentácie. V certifikáte sa uvádza meno a adresa poskytovateľa, závery preskúmania, podmienky jeho platnosti (ak existujú) a potrebné údaje na identifikáciu systému AI.

Certifikát a jeho prílohy obsahujú všetky relevantné informácie, ktoré umožňujú vyhodnotiť zhodu systému AI a v prípade potreby kontrolu systému AI počas jeho používania.

Ak systém AI nie je v zhode s požiadavkami stanovenými v kapitole III oddiele 2, notifikovaná osoba zamietne vydanie certifikátu Únie o posúdení technickej dokumentácie a následne o tom informuje žiadateľa, pričom uvedie podrobné dôvody zamietnutia.

Ak systém AI nespĺňa požiadavku týkajúcu sa údajov použitých na jeho trénovanie, pred podaním žiadosti o nové posúdenie zhody bude potrebné opätovné trénovanie systému AI. V tomto prípade odôvodnené rozhodnutie notifikovanej osoby o posúdení, ktorým sa zamieta vydanie certifikátu Únie o posúdení technickej dokumentácie, obsahuje konkrétne vyjadrenia o kvalite údajov použitých na trénovanie systému AI, najmä o dôvodoch nesúladu.

4.7. Každú zmenu systému AI, ktorá by mohla ovplyvniť súlad systému AI s požiadavkami alebo jeho zamýšľaným účelom, posudzuje notifikovaná osoba, ktorá vydala certifikát Únie o posúdení technickej dokumentácie. Poskytovateľ takúto notifikovanú osobu informuje o svojom zámere zaviesť ktorúkoľvek z uvedených zmien, alebo ak sa o výskyte takýchto zmien dozvedel inak. Plánované zmeny posudzuje notifikovaná osoba, ktorá rozhoduje, či si tieto zmeny vyžadujú nové posúdenie zhody v súlade s článkom 43 ods. 4, alebo či by sa na ne mohol vzťahovať dodatok k certifikátu Únie o posúdení technickej dokumentácie. V druhom prípade notifikovaná osoba tieto zmeny posúdi, svoje rozhodnutie oznámi poskytovateľovi a v prípade schválenia zmien mu vydá dodatok k certifikátu Únie o posúdení technickej dokumentácie.

5. Dohľad nad schváleným systémom riadenia kvality

5.1. Účelom dohľadu vykonávaného notifikovanou osobou v zmysle bodu 3 je zabezpečiť, aby poskytovateľ riadne dodržiaval podmienky schváleného systému riadenia kvality.

5.2. Na účely posúdenia poskytovateľ umožní notifikovanej osobe prístup do priestorov, v ktorých sa uskutočňuje dizajn, vývoj alebo testovanie systémov AI. Poskytovateľ ďalej notifikovanej osobe poskytuje všetky potrebné informácie.

5.3. Notifikovaná osoba vykonáva pravidelné audity s cieľom zabezpečiť, aby poskytovateľ zachovával a uplatňoval systém riadenia kvality, a poskytovateľovi predkladá správu o audite. V rámci týchto auditov môže notifikovaná osoba vykonať dodatočné testy systémov AI, pre ktoré bol vydaný certifikát Únie o posúdení technickej dokumentácie.

PRÍLOHA VIII

Informácie, ktoré sa majú predložiť pri registrácii vysokorizikových systémov AI v súlade s článkom 49

Oddiel A – Informácie, ktoré majú predkladať poskytovatelia vysokorizikových systémov AI v súlade s článkom 49 ods. 1

V súvislosti s vysokorizikovými systémami AI, ktoré sa majú registrovať v súlade s článkom 49 ods. 1, sa poskytujú a následne aktualizujú tieto informácie:

1. názov, adresa a kontaktné údaje poskytovateľa;

2. v prípade, že informácie za poskytovateľa predkladá iná osoba, meno, adresa a kontaktné údaje danej osoby;

3. v náležitom prípade meno, adresa a kontaktné údaje splnomocneného zástupcu;

4. obchodný názov systému AI a akýkoľvek ďalší jednoznačný odkaz umožňujúci identifikáciu a vysledovateľnosť systému AI;

5. opis zamýšľaného účelu systému AI a komponentov a funkcií podporovaných prostredníctvom tohto systému AI;

6. základný a stručný opis informácií, ktoré systémom používa (údaje, vstupy), a jeho prevádzkovej logiky;

7. status systému AI (na trhu alebo v prevádzke; už nie je na trhu/v prevádzke, stiahnutý od používateľa);

8. typ, číslo a dátum skončenia platnosti certifikátu vydaného notifikovanou osobou a v náležitom prípade meno alebo identifikačné číslo tejto notifikovanej osoby;

9. v náležitom prípade naskenovaná kópia certifikátu uvedeného v bode 8;

10. všetky členské štáty, v ktorých bol systém AI uvedený na trh, uvedený do prevádzky alebo sprístupnený v Únii;

11. kópia EÚ vyhlásenia o zhode uvedeného v článku 47;

12. elektronický návod na použitie; tieto informácie sa neposkytujú v prípade vysokorizikových systémov AI v oblastiach presadzovania práva alebo migrácie, azylu a riadenia kontroly hraníc v zmysle prílohy III bodov 1, 6 a 7;

13. adresa URL pre doplňujúce informácie (nepovinné).

Oddiel B – Informácie, ktoré majú predkladať poskytovatelia vysokorizikových systémov AI v súlade s článkom 49 ods. 2

V súvislosti so systémami AI, ktoré sa majú registrovať v súlade s článkom 49 ods. 2, sa poskytujú a následne aktualizujú tieto informácie:

1. názov, adresa a kontaktné údaje poskytovateľa;

2. v prípade, že informácie za poskytovateľa predkladá iná osoba, meno, adresa a kontaktné údaje danej osoby;

3. v náležitom prípade meno, adresa a kontaktné údaje splnomocneného zástupcu;

4. obchodný názov systému AI a akýkoľvek ďalší jednoznačný odkaz umožňujúci identifikáciu a vysledovateľnosť systému AI;

5. opis zamýšľaného účelu systému AI;

6. podmienka alebo podmienky podľa článku 6 ods. 3, na základe ktorých sa systém AI nepovažuje za vysokorizikový;

7. stručné zhrnutie dôvodov, na základe ktorých sa systém AI nepovažuje za vysokorizikový pri uplatňovaní postupu podľa článku 6 ods. 3;

8. status systému AI (na trhu alebo v prevádzke; už nie je na trhu/v prevádzke, stiahnutý od používateľa);

9. všetky členské štáty, v ktorých bol systém AI uvedený na trh, uvedený do prevádzky alebo sprístupnený v Únii.

Oddiel C – Informácie, ktoré majú predkladať subjekty nasadzujúce vysokorizikové systémy AI v súlade s článkom 49 ods. 3

V súvislosti s vysokorizikovými systémami AI, ktoré sa majú registrovať v súlade s článkom 49, sa poskytujú a následne aktualizujú tieto informácie:

1. meno, adresa a kontaktné údaje nasadzujúceho subjektu;

2. meno, adresa a kontaktné údaje osoby predkladajúcej informácie v mene nasadzujúceho subjektu;

3. adresa URL zápisu systému AI do databázy Únie jeho poskytovateľom;

4. zhrnutie zistení posúdenia vplyvu na základné práva vykonaného v súlade s článkom 27;

5. v náležitých prípadoch zhrnutie posúdenia vplyvu na ochranu údajov vykonaného v súlade s článkom 35 nariadenia (EÚ) 2016/679 alebo článkom 27 smernice (EÚ) 2016/680, ako sa uvádza v článku 26 ods. 8 tohto nariadenia.

PRÍLOHA IX

Informácie, ktoré sa majú predkladať pri registrácii vysokorizikových systémov AI uvedených v prílohe III vo vzťahu k testovaniu v reálnych podmienkach v súlade s článkom 60

V súvislosti s testovaním v reálnych podmienkach, ktoré sa má zaregistrovať v súlade s článkom 60, sa poskytujú a následne aktualizujú tieto informácie:

1. jedinečné jednotné identifikačné číslo testovania v reálnych podmienkach pre celú Úniu;

2. meno a kontaktné údaje poskytovateľa alebo potenciálneho poskytovateľa a nasadzujúcich subjektov zapojených do testovania v reálnych podmienkach;

3. stručný opis systému AI, jeho zamýšľaný účel a ďalšie informácie potrebné na identifikáciu systému;

4. súhrn hlavných charakteristík plánu testovania v reálnych podmienkach;

5. informácie o pozastavení alebo ukončení testovania v reálnych podmienkach.

PRÍLOHA X

Legislatívne akty Únie o rozsiahlych informačných systémoch v priestore slobody, bezpečnosti a spravodlivosti

1. Schengenský informačný systém

   a) nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1860 z 28. novembra 2018 o využívaní Schengenského informačného systému na účely návratu neoprávnene sa zdržiavajúcich štátnych príslušníkov tretích krajín (Ú. v. EÚ L 312, 7.12.2018, s. 1);

   b) nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1861 z 28. novembra 2018 o zriadení, prevádzke a využívaní Schengenského informačného systému (SIS) v oblasti hraničných kontrol, o zmene Dohovoru, ktorým sa vykonáva Schengenská dohoda, a o zmene a zrušení nariadenia (ES) č. 1987/2006 (Ú. v. EÚ L 312, 7.12.2018, s. 14);

   c) nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1862 z 28. novembra 2018 o zriadení, prevádzke a využívaní Schengenského informačného systému (SIS) v oblasti policajnej spolupráce a justičnej spolupráce v trestných veciach, o zmene a zrušení rozhodnutia Rady 2007/533/SVV a o zrušení nariadenia Európskeho parlamentu a Rady (ES) č. 1986/2006 a rozhodnutia Komisie 2010/261/EÚ (Ú. v. EÚ L 312, 7.12.2018, s. 56).

2. Vízový informačný systém

a) nariadenie Európskeho parlamentu a Rady (EÚ) 2021/1133 zo 7. júla 2021, ktorým sa menia nariadenia (EÚ) č. 603/2013, (EÚ) 2016/794, (EÚ) 2018/1862, (EÚ) 2019/816 a (EÚ) 2019/818, pokiaľ ide o stanovenie podmienok prístupu k ostatným informačným systémom EÚ na účely vízového informačného systému (Ú. v. EÚ L 248, 13.7.2021, s. 1);

b) nariadenie Európskeho parlamentu a Rady (EÚ) 2021/1134 zo 7. júla 2021, ktorým sa na účely reformy vízového informačného systému menia nariadenia Európskeho parlamentu a Rady (ES) č. 767/2008, (ES) č. 810/2009, (EÚ) 2016/399, (EÚ) 2017/2226, (EÚ) 2018/1240, (EÚ) 2018/1860, (EÚ) 2018/1861, (EÚ) 2019/817 a (EÚ) 2019/1896 a zrušujú rozhodnutia Rady 2004/512/ES a 2008/633/SVV (Ú. v. EÚ L 248, 13.7.2021, s. 11).

3. Systém Eurodac

nariadenie Európskeho parlamentu a Rady (EÚ) 2024/... z ... o zriadení systému Eurodac na porovnávanie biometrických údajov s cieľom účinne uplatňovať nariadenia Európskeho parlamentu a Rady (EÚ) 2024/… a (EÚ) 2024/… a smernicu Rady 2001/55/ES a identifikovať neoprávnene sa zdržiavajúcich štátnych príslušníkov tretích krajín a osoby bez štátnej príslušnosti, o žiadostiach orgánov presadzovania práva členských štátov a Europolu o porovnanie s údajmi v systéme Eurodac na účely presadzovania práva, o zmene nariadení Európskeho parlamentu a Rady (EÚ) 2018/1240 a (EÚ) 2019/818 a o zrušení nariadenia Európskeho parlamentu a Rady (EÚ) č. 603/2013[+].

4. Systém vstup/výstup

nariadenie Európskeho parlamentu a Rady (EÚ) 2017/2226 z 30. novembra 2017, ktorým sa zriaďuje systém vstup/výstup na zaznamenávanie údajov o vstupe a výstupe štátnych príslušníkov tretích krajín prekračujúcich vonkajšie hranice členských štátov a o odopretí ich vstupu a stanovujú podmienky prístupu do systému vstup/výstup na účely presadzovania práva, a ktorým sa mení Dohovor, ktorým sa vykonáva Schengenská dohoda, a nariadenia (ES) č. 767/2008 a (EÚ) č. 1077/2011 (Ú. v. EÚ L 327, 9.12.2017, s. 20).

[+] Ú. v.: vložte, prosím, do textu číslo nariadenia, ktoré sa nachádza v dokumente PE-CONS 15/24 (2016/0132 (COD)) a do poznámky pod čiarou číslo, dátum a názov uvedeného nariadenia a odkaz na jeho uverejnenie v úradnom vestníku.

5. Európsky systém pre cestovné informácie a povolenia

a) nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1240 z 12. septembra 2018, ktorým sa zriaďuje Európsky systém pre cestovné informácie a povolenia (ETIAS) a ktorým sa menia nariadenia (EÚ) č. 1077/2011, (EÚ) č. 515/2014, (EÚ) 2016/399, (EÚ) 2016/1624 a (EÚ) 2017/2226 (Ú. v. EÚ L 236, 19.9.2018, s. 1);

b) nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1241 z 12. septembra 2018, ktorým sa mení nariadenie (EÚ) 2016/794 na účely zriadenia Európskeho systému cestovných informácií a povolení (ETIAS) (Ú. v. EÚ L 236, 19.9.2018, s. 72).

6. Európsky informačný systém registrov trestov pre štátnych príslušníkov tretích krajín a osoby bez štátnej príslušnosti

nariadenie Európskeho parlamentu a Rady (EÚ) 2019/816 zo 17. apríla 2019, ktorým sa zriaďuje centralizovaný systém na identifikáciu členských štátov, ktoré majú informácie o odsúdeniach štátnych príslušníkov tretích krajín a osôb bez štátnej príslušnosti (ECRIS-TCN), s cieľom doplniť Európsky informačný systém registrov trestov, a ktorým sa mení nariadenie (EÚ) 2018/1726 (Ú. v. EÚ L 135, 22.5.2019, s. 1).

7. Interoperabilita

a) nariadenie Európskeho parlamentu a Rady (EÚ) 2019/817 z 20. mája 2019 o stanovení rámca pre interoperabilitu medzi informačnými systémami EÚ v oblasti hraníc a víz a o zmene nariadení Európskeho parlamentu a Rady (ES) č. 767/2008, (EÚ) 2016/399, (EÚ) 2017/2226, (EÚ) 2018/1240, (EÚ) 2018/1726 a (EÚ) 2018/1861 a rozhodnutí Rady 2004/512/ES a 2008/633/SVV (Ú. v. EÚ L 135, 22.5.2019, s. 27);

b) nariadenie Európskeho parlamentu a Rady (EÚ) 2019/818 z 20. mája 2019 o stanovení rámca pre interoperabilitu medzi informačnými systémami EÚ v oblasti policajnej a justičnej spolupráce, azylu a migrácie a o zmene nariadení (EÚ) 2018/1726, (EÚ) 2018/1862 a (EÚ) 2019/816 (Ú. v. EÚ L 135, 22.5.2019, s. 85).

PRÍLOHA XI

Technická dokumentácia podľa článku 53 ods. 1 písm. a) – technická dokumentácia pre poskytovateľov modelov AI na všeobecné účely

Oddiel 1

Informácie, ktoré majú poskytnúť všetci poskytovatelia modelov AI na všeobecné účely

Technická dokumentácia podľa článku 53 ods. 1 písm. a) obsahuje v závislosti od veľkosti a rizikového profilu modelu aspoň tieto informácie:

1. všeobecný opis modelu AI na všeobecné účely vrátane týchto prvkov:

   a) úlohy, ktoré má model plniť, a typ a povaha systémov AI, do ktorých ho možno integrovať;

   b) uplatniteľné politiky prijateľného použitia;

   c) dátum vydania a spôsoby distribúcie;

   d) architektúra a počet parametrov;

   e) modality (napr. text, obrázok) a formát vstupov a výstupov;

   f) licencia.

2. Podrobný opis prvkov modelu uvedeného v bode 1 a relevantné informácie o procese vývoja vrátane týchto prvkov:

a) technické prostriedky (napr. návod na použitie, infraštruktúra, nástroje) potrebné na integráciu modelu AI na všeobecné účely do systémov AI;

b) špecifikácie dizajnu modelu a procesu trénovania vrátane metodík a techník trénovania, kľúčové rozhodnutia prijaté počas dizajnovania vrátane odôvodnenia a predpokladov; čo má model optimalizovať a relevantnosť jednotlivých parametrov, podľa prípadu;

c) informácie o údajoch použitých na trénovanie, testovanie a prípadne validáciu vrátane typu a pôvodu údajov a metodík spracovania (napr. čistenie, filtrovanie atď.), o počte údajových bodov, ich rozsahu a hlavných charakteristikách; spôsob, akým sa údaje získali a vybrali, ako aj všetky ostatné opatrenia na zistenie nevhodnosti zdrojov údajov a metód na zistenie identifikovateľných skreslení, podľa prípadu;

d) výpočtové zdroje použité na trénovanie modelu (napr. počet operácií s pohyblivou rádovou čiarkou), dĺžka trénovania a iné relevantné podrobnosti týkajúce sa trénovania;

e) známa alebo odhadovaná spotreba energie modelu.

Pokiaľ ide o písmeno e), ak spotreba energie modelu nie je známa, spotreba energie môže byť založená na informáciách o použitých výpočtových zdrojoch.

Oddiel 2

Ďalšie informácie, ktoré majú poskytovať poskytovatelia modelov AI na všeobecné účely so systémovým rizikom

1. Podrobný opis stratégií hodnotenia vrátane výsledkov hodnotenia na základe dostupných protokolov a nástrojov verejného hodnotenia alebo iných metodík hodnotenia. Stratégie hodnotenia zahŕňajú hodnotiace kritériá, metriky a metodiku identifikácie obmedzení.

2. Ak je to relevantné, podrobný opis opatrení zavedených na účely vykonávania interného a/alebo externého testovania na nepriateľské útoky (napr. červené tímy), úpravy modelu vrátane zosúlaďovania a dolaďovania.

3. Ak je to relevantné, podrobný opis architektúry systému, v ktorom sa vysvetľuje, ako softvérové komponenty na seba nadväzujú alebo ako sa navzájom dopĺňajú a ako sú integrované do celkového spracúvania.

PRÍLOHA XII

Informácie o transparentnosti podľa článku 53 ods. 1 písm. b) – technická dokumentácia pre poskytovateľov modelov AI na všeobecné účely pre nadväzujúcich poskytovateľov, ktorí integrujú model do svojho systému AI

Informácie podľa článku 53 ods. 1 písm. b) zahŕňajú aspoň:

1. všeobecný opis modelu AI na všeobecné účely vrátane týchto prvkov:

   a) úlohy, ktoré má model plniť, a typ a povaha systémov AI, do ktorých ho možno integrovať;

   b) uplatniteľné politiky prijateľného použitia;

   c) dátum vydania a spôsoby distribúcie;

   d) spôsob interakcie modelu s hardvérom alebo softvérom, ktorý nie je súčasťou samotného modelu, alebo ako ho prípadne možno na takúto interakciu použiť;

   e) ak je to relevantné, verzie relevantného softvéru súvisiaceho s používaním modelu AI na všeobecné účely;

   f) architektúra a počet parametrov;

   g) modality (napr. text, obrázok) a formát vstupov a výstupov;

   h) licencia na model.

2. Opis prvkov modelu a procesu jeho vývoja vrátane:

a) technických prostriedkov (napr. návod na použitie, infraštruktúra, nástroje) potrebných na integráciu modelu AI na všeobecné účely do systémov AI;

b) modality (napr. text, obrázok atď.) a formátu vstupov a výstupov a ich maximálnej veľkosti (napr. dĺžka kontextového okna atď.);

c) informácií o údajoch použitých na trénovanie, testovanie a prípadne validáciu vrátane druhu a pôvodu údajov a metodík spracovania.

PRÍLOHA XIII

Kritériá na určenie modelov AI na všeobecné účely so systémovým rizikom podľa článku 51

S cieľom určiť, či má model AI na všeobecné účely spôsobilosti alebo vplyv rovnocenné s tými, ktoré sú stanovené v článku 51 ods. 1 písm. a), Komisia zohľadní tieto kritériá:

a) počet parametrov modelu;

b) kvalita alebo veľkosť dátového súboru, napríklad meraná prostredníctvom tokenov;

c) výpočtová sila použitá na trénovanie modelu, meraná v operáciách s pohyblivou rádovou čiarkou alebo uvedená kombináciou iných premenných, ako sú odhadované náklady na trénovanie, odhadovaný čas potrebný na trénovanie alebo odhadovaná spotreba energie na trénovanie;

d) vstupné a výstupné modality modelu, ako sú text na text (veľké jazykové modely), text na obraz, multimodalita a najmodernejšie prahové hodnoty na určenie spôsobilostí s veľkým vplyvom pre každú modalitu a konkrétny typ vstupov a výstupov (napr. biologické sekvencie);

e) referenčné hodnoty a hodnotenia spôsobilostí modelu vrátane zváženia počtu úloh bez dodatočného trénovania, prispôsobivosť na učenie sa nových, odlišných úloh, úroveň jeho autonómnosti a škálovateľnosti, nástroje, ku ktorým má prístup;

f) či má veľký vplyv na vnútorný trh z dôvodu svojho dosahu, ktorý sa predpokladá, po sprístupnení najmenej 10 000 registrovaným komerčným používateľom usadeným v Únii;

g) počet registrovaných koncových používateľov.