Rada
Európskej únie

V Bruseli 6. decembra 2022
(OR. en)

15698/22

Medziinštitucionálny spis:
2021/0106(COD)

TELECOM 516
JAI 1633
COPEN 434
CYBER 399
DATAPROTECT 351
EJUSTICE 95
COSI 318
IXIM 291
ENFOPOL 626
RELEX 1674
MI 918
COMPET 1005
CODEC 1940

VÝSLEDOK ROKOVANIA

Od:	Generálny sekretariát Rady
Dátum:	6. decembra 2022
Komu:	Delegácie
Č. predch. dok.:	14954/22 + ADD 1
Č. dok. Kom.:	8115/21
Predmet:	Návrh nariadenia Európskeho parlamentu a Rady, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie (akt o umelej inteligencii) a menia niektoré legislatívne akty Únie – všeobecné smerovanie (6. decembra 2022)

Delegáciám v prílohe zasielame všeobecné smerovanie Rady k uvedenému návrhu, ktoré Rada (doprava, telekomunikácie a energetika) schválila na svojom 3 917. zasadnutí 6. decembra 2022.

Všeobecným smerovaním sa stanovuje predbežná pozícia Rady k tomuto návrhu a vytvára sa základ pre prípravu rokovaní s Európskym parlamentom.

PRÍLOHA

Návrh

NARIADENIE EURÓPSKEHO PARLAMENTU a RADY,

KTORÝM SA STANOVUJÚ HARMONIZOVANÉ PRAVIDLÁ v OBLASTI UMELEJ INTELIGENCIE (AKT o UMELEJ INTELIGENCII) a MENIA NIEKTORÉ LEGISLATÍVNE AKTY ÚNIE

(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 Výboru regiónov[2],

So zreteľom na stanovisko Európskej centrálnej banky[3],

konajúc v súlade s riadnym legislatívnym postupom,

keďže:

[1] Ú. v. EÚ C [...], [...], s. [...].
[2] Ú. v. EÚ C [...], [...], s. [...].
[3] Odkaz na stanovisko ECB.

(1) Účelom tohto nariadenia je zlepšiť fungovanie vnútorného trhu stanovením jednotného právneho rámca, najmä pokiaľ ide o vývoj, uvádzanie na trh a používanie umelej inteligencie v súlade s hodnotami Únie. Toto nariadenie prihliada na viacero naliehavých dôvodov verejného záujmu, ako napr. vysoká úroveň ochrany zdravia, bezpečnosti a základných práv, a zabezpečuje voľný pohyb tovaru a služieb založených na umelej inteligencii cez hranice, čím bráni členským štátom ukladať obmedzenia na vývoj, uvádzanie na trh a používanie systémov umelej inteligencie, pokiaľ sa to týmto nariadením výslovne nepovolí.

(2) Systémy umelej inteligencie (systémy UI) možno ľahko zaviesť vo viacerých odvetviach hospodárstva a spoločnosti, a to aj cezhranične, a môžu sa pohybovať po celej Únii. Niektoré členské štáty už zvažujú prijatie vnútroštátnych pravidiel na zabezpečenie toho, aby bola umelá inteligencia 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 umelej inteligencie. Mala by sa preto zabezpečiť konzistentná a vysoká úroveň ochrany v celej Únii, pričom by sa malo zabrániť rozdielom, ktoré bránia voľnému pohybu systémov umelej inteligencie a súvisiacich výrobkov a služieb v rámci vnútorného trhu, a to stanovením jednotných povinností pre prevádzkovateľov a zaručením jednotnej ochrany naliehavých dôvodov verejného záujmu a práv osôb na celom vnútornom trhu na základe článku 114 Zmluvy o fungovaní Európskej únie (ZFEÚ). Keďže toto nariadenie obsahuje osobitné pravidlá ochrany jednotlivcov v súvislosti so spracúvaním osobných údajov, pokiaľ ide o obmedzenia používania systémov umelej inteligencie na diaľkovú biometrickú identifikáciu v reálnom čase vo verejne dostupných priestoroch na účely presadzovania práva, je vhodné, aby sa tieto osobitné pravidlá uvedené v tomto nariadení zakladali na článku 16 ZFEÚ. Pokiaľ ide o tieto osobitné pravidlá a použitie článku 16 ZFEÚ, je vhodné poradiť sa s Európskym výborom pre ochranu údajov.

(3) Umelá inteligencia je rýchlo sa rozvíjajúca skupina technológií, ktorá môže prispieť k širokému spektru hospodárskych a spoločenských výhod vo všetkých priemyselných odvetviach a spoločenských činnostiach. Zlepšením predpovedí, optimalizáciou operácií a prideľovania zdrojov a personalizáciou digitálnych riešení, ktoré sú k dispozícii jednotlivcom a organizáciám, môže využívanie umelej inteligencie poskytnúť podnikom kľúčové konkurenčné výhody a podporiť sociálne a environmentálne priaznivé výsledky, napríklad v oblasti zdravotnej starostlivosti, poľnohospodárstva, vzdelávania a odbornej prípravy, riadenia infraštruktúry, energetiky, dopravy a logistiky, verejných služieb, bezpečnostnej ochrany, spravodlivosti, efektívneho využívania zdrojov a energie a zmierňovania zmeny klímy a adaptácie na ňu.

(4) Umelá inteligencia môže zároveň v závislosti od okolností týkajúcich sa jej konkrétneho uplatňovania a používania vytvárať riziká a poškodzovať verejné záujmy a práva, ktoré sú chránené právom Únie. Toto poškodenie môže byť hmotné aj nehmotné.

(5) Na podporu rozvoja, využívania a zavádzania umelej inteligencie na vnútornom trhu je preto potrebný právny rámec Únie, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorý zároveň spĺňa vysokú úroveň ochrany verejných záujmov, ako sú zdravie a bezpečnosť, a ochrany základných práv, ako sú uznané a chránené právom Únie. Na dosiahnutie tohto cieľa by sa mali stanoviť pravidlá upravujúce uvádzanie určitých systémov umelej inteligencie na trh a do prevádzky, čím sa zabezpečí hladké fungovanie vnútorného trhu a umožní sa, aby tieto systémy využívali zásadu voľného pohybu tovaru a služieb. Stanovením týchto pravidiel a na základe práce expertnej skupiny na vysokej úrovni pre umelú inteligenciu, ako sa uvádza v usmerneniach pre dôveryhodnú umelú inteligenciu v EÚ, sa týmto nariadením podporuje cieľ Únie stať sa svetovým lídrom v rozvoji bezpečnej, dôveryhodnej a etickej umelej inteligencie, ako to uvádza Európska rada[4], a zabezpečuje sa ním ochrana etických zásad, ako to osobitne požaduje Európsky parlament[5].

---

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

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

5a. Harmonizované pravidlá uvádzania na trh, uvádzania do prevádzky a používania systémov umelej inteligencie stanovené v tomto nariadení by sa mali uplatňovať vo všetkých odvetviach a v súlade s prístupom založeným na novom legislatívnom rámci by nimi nemali byť dotknuté existujúce právne predpisy Únie, najmä pokiaľ ide o ochranu údajov, ochranu spotrebiteľa, základné práva, zamestnanosť a bezpečnosť výrobkov, ktoré toto nariadenie dopĺňa. v dôsledku toho všetky práva a prostriedky nápravy, ktoré takéto právo Únie poskytuje spotrebiteľom a iným osobám, ktoré môžu byť negatívne ovplyvnené systémami umelej inteligencie, a to aj pokiaľ ide o náhradu možných škôd podľa smernice Rady 85/374/EHS z 25. júla 1985 o aproximácii zákonov, iných právnych predpisov a správnych opatrení členských štátov o zodpovednosti za chybné výrobky, zostávajú nedotknuté a plne uplatniteľné. 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 umelej inteligencie. Povinnosti uložené rôznym prevádzkovateľom zapojeným do hodnotového reťazca umelej inteligencie podľa tohto nariadenia by sa zároveň mali uplatňovať bez toho, aby boli dotknuté vnútroštátne právne predpisy, v súlade s právom Únie a s takým účinkom, že v prípadoch, keď uvedené právne predpisy nepatria do rozsahu pôsobnosti tohto nariadenia alebo sú zamerané na iné legitímne ciele verejného záujmu, než sú ciele tohto nariadenia, používanie určitých systémov umelej inteligencie sa obmedzí. Toto nariadenie by napríklad nemalo mať vplyv na vnútroštátne pracovné právo a právne predpisy o ochrane maloletých (t. j. osôb mladších ako 18 rokov) s prihliadnutím na všeobecnú pripomienku Organizácie Spojených národov č. 25 (2021) o právach detí, pokiaľ sa osobitne netýkajú systémov umelej inteligencie a sú zamerané na iné legitímne ciele verejného záujmu.

(6) Pojem „systém umelej inteligencie“ by sa mal jasne vymedziť s cieľom zabezpečiť právnu istotu a zároveň poskytnúť flexibilitu na prispôsobenie sa budúcemu technologickému vývoju. Vymedzenie by malo byť založené na kľúčových funkčných charakteristikách umelej inteligencie, ako sú jej schopnosti učenia sa, uvažovania alebo modelovania, pričom by sa mala odlíšiť od jednoduchších softvérových systémov a programovacích prístupov. Na účely tohto nariadenia by systémy umelej inteligencie mali byť najmä schopné na základe strojových a/alebo ľudských údajov a vstupov odvodiť spôsob, ako dosiahnuť súbor konečných cieľov, ktoré im zadajú ľudia, s využitím strojového učenia a/alebo prístupov založených na logike a poznatkoch, a vytvárať výstupy, ako je obsah v prípade generatívnych systémov umelej inteligencie (napr. text, video alebo obrázky), predpovede, odporúčania alebo rozhodnutia, ktoré ovplyvňujú prostredie, s ktorým systém interaguje, či už vo fyzickom alebo digitálnom rozmere. Systém, ktorý používa pravidlá vymedzené výlučne fyzickými osobami na automatické vykonávanie operácií, by sa nemal považovať za systém umelej inteligencie. Systémy umelej inteligencie môžu byť navrhnuté tak, aby fungovali s rôznymi úrovňami samostatnosti a mohli sa používať samostatne alebo ako komponent určitého výrobku bez ohľadu na to, či je systém do tohto výrobku fyzicky integrovaný (vstavaný) alebo či napomáha funkčnosti tohto výrobku bez toho, aby doň bol integrovaný (nevstavaný). Koncepcia autonómie systému umelej inteligencie sa týka miery, do akej takýto systém funguje bez ľudského zapojenia.

(6a) Prístupy strojového učenia sa zameriavajú na vývoj systémov schopných učiť sa a odvodiť z údajov riešenie aplikačného problému bez toho, aby boli výslovne naprogramované súborom postupných pokynov od vstupu po výstup. Učenie znamená výpočtový proces optimalizácie parametrov modelu z údajov, čo je matematický konštrukt generujúci výstup na základe vstupných údajoch. Rozsah problémov, ktoré sa riešia strojovým učením, zvyčajne zahŕňa úlohy, pri ktorých zlyhajú iné prístupy, a to buď preto, že neexistuje vhodná formalizácia problému, alebo preto, že riešenie problému je neriešiteľné pomocou prístupov bez učenia. Prístupy strojového učenia zahŕňajú napríklad učenie pod dohľadom, bez dohľadu a učenie posilňovaním, pričom sa využívajú rôzne metódy vrátane hĺbkového učenia neurónovými sieťami, štatistických techník učenia a vyvodzovania (vrátane napríklad logistickej regresie, bayesovského odhadu) a metód vyhľadávania a optimalizácie.

(6b) Logické a vedomostné prístupy sa zameriavajú na vývoj systémov so schopnosťami logického uvažovania o znalostiach na riešenie aplikačného problému. Takéto systémy zvyčajne zahŕňajú vedomostnú základňu a inferenčný mechanizmus, ktorý vytvára výstupy na základe uvažovania o vedomostnej základni. Vedomostná základňa, ktorú zvyčajne kódujú ľudskí odborníci, predstavuje subjekty a logické vzťahy relevantné pre aplikačný problém prostredníctvom formalizmov založených na pravidlách, ontológiách alebo vedomostných grafoch. Inferenčný mechanizmus pracuje s vedomostnou základňou a získava nové informácie prostredníctvom operácií, ako je triedenie, vyhľadávanie, párovanie alebo reťazenie. Prístupy založené na logike a poznatkoch zahŕňajú napríklad reprezentáciu poznatkov, induktívne (logické) programovanie, vedomostné základne, inferenčné a deduktívne mechanizmy, (symbolické) uvažovanie, expertné systémy a metódy vyhľadávania a optimalizácie;

(6c) s cieľom zabezpečiť jednotné podmienky vykonávania tohto nariadenia, pokiaľ ide o prístupy strojového učenia s prístupy založené na logike a poznatkoch, a s cieľom zohľadniť vývoj na trhu a technologický vývoj by sa na Komisiu mali preniesť vykonávacie právomoci.

(6d) Pojem „používateľ“ 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 používa systém umelej inteligencie, pod ktorej právomocou sa systém používa. v závislosti od typu systému umelej inteligencie môže mať používanie systému vplyv na iné osoby ako používateľa.

(7) Pojem „biometrické údaje“ použitý v tomto nariadení by sa mal vykladať v súlade s pojmom biometrické údaje vymedzeným v článku 4 bode 14 nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679[6], v článku 3 bode 18 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1725[7] a v článku 3 bode 13 smernice Európskeho parlamentu a Rady (EÚ) 2016/680[8].

[6] 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).

[7] 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).

[8] 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).

(8) Pojem „systém diaľkovej biometrickej identifikácie“, ako sa používa v tomto nariadení, by sa mal vymedziť funkčne ako systém umelej inteligencie určený na identifikáciu fyzických osôb, zvyčajne na diaľku a bez ich aktívnej účasti, porovnávaním biometrických údajov osoby s biometrickými údajmi obsiahnutými v referenčnom registri údajov, a to bez ohľadu na konkrétnu technológiu, procesy alebo typy použitých biometrických údajov. Takéto systémy diaľkovej biometrickej identifikácie sa zvyčajne používajú na vnímanie (skenovanie) viacerých osôb alebo ich správania súčasne s cieľom výrazne uľahčiť identifikáciu určitého počtu osôb bez ich aktívnej účasti. Takéto vymedzenie nezahŕňa systémy overovania/autentifikácie, ktorých jediným účelom by bolo potvrdiť, že konkrétna fyzická osoba je osobou, o ktorej tvrdí, že ňou je, ani systémy, ktoré sa používajú na potvrdenie totožnosti fyzickej osoby výlučne na účely prístupu k službe, zariadeniu alebo 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 spracovanie biometrických údajov veľkého počtu osôb. v prípade systémov „v reálnom čase“ prebieha zachytávanie biometrických údajov, ich porovnávanie a identifikácia okamžite, takmer okamžite alebo v každom prípade bez výrazného oneskorenia. v tejto súvislosti by nemal existovať priestor na obchádzanie pravidiel tohto nariadenia o používaní predmetných systémov umelej inteligencie „v reálnom čase“ tým, že sa stanovia menšie oneskorenia. Systémy v reálnom čase zahŕňajú používanie materiálu „naživo“ alebo „s malým časovým posunom“, ako sú napríklad videozáznamy generované 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 po značnom oneskorení. Ide o materiály, ako sú fotografie alebo videozáznamy generované kamerami s uzavretým televíznym okruhom alebo súkromnými zariadeniami, ktoré boli vytvorené pred použitím tohto systému vo vzťahu k dotknutým fyzickým osobám.

(9) Na účely tohto nariadenia by sa pojem „verejne prístupný priestor“ mal chápať tak, že sa vzťahuje na akékoľvek fyzické miesto, ktoré je prístupné neurčenému počtu fyzických osôb, bez ohľadu na to, či je dané miesto v súkromnom alebo verejnom vlastníctve, a bez ohľadu na činnosť, na ktorú sa miesto používa, ako napríklad obchod (napríklad predajne, reštaurácie, kaviarne), služby (napríklad banky, profesionálne činnosti, ubytovanie a pohostinské služby), šport (napríklad plavecké bazény, telocvične, štadióny), doprava (napríklad autobusové stanice, stanice metra a železničné stanice, letiská, dopravné prostriedky), zábava (napríklad kiná, divadlá, múzeá, koncertné a konferenčné siene), voľný čas alebo iné činnosti (napríklad verejné cesty a námestia, parky, lesy, ihriská). Miesto by sa malo klasifikovať ako verejne prístupné aj vtedy, ak bez ohľadu na potenciálnu kapacitu alebo bezpečnostné obmedzenia podlieha prístup naň určitým vopred určeným podmienkam, ktoré môže splniť neurčený počet osôb, ako je kúpa vstupenky alebo cestovného lístka, registrácia vopred alebo určitá veková hranica. Naopak, miesto by sa nemalo považovať za verejne prístupné, 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 na danom mieste príslušné právomoci. Samotná faktická možnosť prístupu (napr. odomknuté dvere, otvorená brána v oplotení) neznamená, že miesto je verejne prístupné, ak existujú náznaky alebo okolnosti, ktoré naznačujú opak (napr. 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 miesta, ktoré nie sú verejne prístupné. Verejne prístupné priestory by nemali zahŕňať väznice ani oblasti kontroly hraníc. Niektoré ďalšie priestory môžu pozostávať z verejne neprístupných aj verejne prístupných priestorov, ako napríklad hala súkromnej obytnej budovy potrebná na vstup do ordinácie lekára alebo letisko. Nevzťahuje sa ani na 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.

(10) 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 umelej inteligencie nediskriminačným spôsobom bez ohľadu na to, či sú usadení v Únii alebo v tretej krajine, a na používateľov systémov umelej inteligencie usadených v Únii.

(11) Určité systémy umelej inteligencie 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 mimo Únie v súvislosti s činnosťou vykonávanou systémom umelej inteligencie, ktorý by mohol byť označený ako vysokorizikový. Za týchto okolností by systém umelej inteligencie, ktorý používa prevádzkovateľ mimo Únie, mohol spracúvať údaje zákonne zozbierané v Únii a prenášané z Únie a poskytovať zadávajúcemu prevádzkovateľovi v Únii výstup z uvedeného systému umelej inteligencie vyplývajúci z tohto spracovania bez toho, aby sa uvedený systém umelej inteligencie 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 a používateľov systémov umelej inteligencie, ktorí sú usadení v tretej krajine, a to v rozsahu, v akom sa výstup generovaný týmito systémami používa 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 medzinárodných dohôd uzavretých na vnútroštátnej alebo európskej úrovni v oblasti presadzovania práva a justičnej spolupráce s Úniou alebo jej členskými štátmi. Takéto dohody boli uzavreté dvojstranne medzi členskými štátmi a tretími krajinami alebo medzi Európskou úniou, Europolom a inými agentúrami EÚ a tretími krajinami a medzinárodnými organizáciami. Orgány prijímajúcich členských štátov a inštitúcie, úrady a orgány Únie a orgány využívajúce takéto výstupy v Únii sú naďalej zodpovedné za zabezpečenie ich využívania v súlade 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.

(12) Toto nariadenie by sa malo vzťahovať aj na inštitúcie, úrady, orgány a agentúry Únie, ak konajú ako poskytovateľ alebo používateľ systému umelej inteligencie.

(-12a) Ak sa systémy umelej inteligencie uvádzajú na trh, uvádzajú do prevádzky alebo s úpravami alebo bez nich používajú na vojenské alebo obranné účely alebo na účely národnej bezpečnosti, mali by 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 ZEÚ, ako aj osobitosťami obrannej politiky členských štátov a spoločnej obrannej politiky Únie, na ktoré sa vzťahuje hlava v kapitola 2 Zmluvy o Európskej únii (ZEÚ) a ktoré podliehajú medzinárodnému právu verejnému, čo je preto vhodnejším právnym rámcom na reguláciu systémov umelej inteligencie v kontexte používania smrtiacej sily a iných systémov umelej inteligencie 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 ZEÚ, ako aj osobitnou povahou a operačnými potrebami činností v oblasti národnej bezpečnosti a osobitnými vnútroštátnymi pravidlami uplatniteľnými na tieto činnosti. Ak sa však systém umelej inteligencie 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 na iné ako vojenské alebo obranné účely alebo na účely národnej bezpečnosti, mal zabezpečiť súlad systému s týmto nariadením, pokiaľ systém už s ním nie je v súlade. Systémy umelej inteligencie uvedené na trh alebo do prevádzky na vylúčené účely (t. j. vojenské alebo obranné účely alebo účely národnej bezpečnosti) a jeden alebo viacero nevylúčených účelov (napr. civilné účely, 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 umelej inteligencie 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 umelej inteligencie na účely národnej bezpečnosti, na vojenské a obranné účely, ktorých používanie je vylúčené z rozsahu pôsobnosti tohto nariadenia. Systém umelej inteligencie 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.

(12a) Týmto nariadením by nemali byť dotknuté ustanovenia o zodpovednosti poskytovateľov sprostredkovateľských služieb stanovené v smernici Európskeho parlamentu a Rady 2000/31/ES [v znení aktu o digitálnych službách].

(12b) Týmto nariadením by sa nemala narúšať výskumná a vývojová činnosť a mala by sa rešpektovať sloboda vedeckého bádania. Preto je potrebné vylúčiť z rozsahu jeho pôsobnosti systémy umelej inteligencie osobitne vyvinuté a uvedené do prevádzky výlučne na účely vedeckého výskumu a vývoja a zabezpečiť, aby nariadenie inak neovplyvňovalo vedecký výskum a vývoj systémov umelej inteligencie. Ustanovenia tohto nariadenia by sa nemali uplatňovať, ani pokiaľ ide o výskumnú činnosť poskytovateľov zameranú na výrobky. Tým nie je dotknutá povinnosť dodržiavať toto nariadenie, keď sa systém umelej inteligencie patriaci do rozsahu pôsobnosti tohto nariadenia uvádza na trh alebo do prevádzky ako výsledok takejto výskumnej a vývojovej činnosti, ani uplatňovanie ustanovení o experimentálnych regulačných prostrediach a testovaní v reálnych podmienkach. Navyše bez toho, aby bolo dotknuté vyššie uvedené, pokiaľ ide o systémy umelej inteligencie osobitne vyvinuté a uvedené do prevádzky výlučne na účely vedeckého výskumu a vývoja, akýkoľvek iný systém umelej inteligencie, ktorý sa môže používať na vykonávanie akejkoľvek výskumnej a vývojovej činnosti, by mal naďalej podliehať ustanoveniam tohto nariadenia. Za každých okolností by sa každá výskumná a vývojová činnosť mala vykonávať v súlade s uznávanými etickými a odbornými normami pre vedecký výskum.

(12c) Vzhľadom na povahu a zložitosť hodnotového reťazca systémov umelej inteligencie je nevyhnutné objasniť úlohu aktérov, ktorí môžu prispievať k vývoju systémov umelej inteligencie, najmä vysokorizikových systémov umelej inteligencie. Predovšetkým je potrebné objasniť, že systémy umelej inteligencie na všeobecné účely sú systémy umelej inteligencie, ktoré poskytovateľ určil na vykonávanie všeobecne uplatniteľných funkcií, ako je rozpoznávanie obrazu/reči, a to v rôznych kontextoch. Môžu sa používať ako vysokorizikové systémy umelej inteligencie sami osebe alebo môžu byť komponentmi iných vysokorizikových systémov umelej inteligencie. Vzhľadom na svoju osobitnú povahu a s cieľom zabezpečiť spravodlivé rozdelenie zodpovednosti v celom hodnotovom reťazci umelej inteligencie by preto takéto systémy mali podliehať primeraným a špecifickejším požiadavkám a povinnostiam podľa tohto nariadenia a zároveň by mali zaručovať vysokú úroveň ochrany základných práv, zdravia a bezpečnosti. Okrem toho by poskytovatelia systémov umelej inteligencie na všeobecné účely bez ohľadu na to, či ich iní poskytovatelia môžu používať ako vysokorizikové systémy umelej inteligencie ako také alebo ako komponenty vysokorizikových systémov umelej inteligencie, mali podľa potreby spolupracovať s poskytovateľmi príslušných vysokorizikových systémov umelej inteligencie s cieľom umožniť im súlad s príslušnými povinnosťami podľa tohto nariadenia a spolupracovať aj s príslušnými orgánmi zriadenými podľa tohto nariadenia. s cieľom zohľadniť osobitné črty systémov umelej inteligencie na všeobecné účely a rýchlo sa vyvíjajúci trh a technologický vývoj v tejto oblasti by sa mali na Komisiu preniesť vykonávacie právomoci s cieľom špecifikovať a prispôsobiť uplatňovanie požiadaviek stanovených v tomto nariadení na systémy umelej inteligencie na všeobecné účely a špecifikovať informácie, ktoré majú poskytovatelia systémov umelej inteligencie na všeobecné účely zdieľať, aby poskytovatelia príslušných vysokorizikových systémov umelej inteligencie mohli plniť svoje povinnosti podľa tohto nariadenia.

(13) S cieľom zabezpečiť jednotnú a vysokú úroveň ochrany verejných záujmov, pokiaľ ide o zdravie, bezpečnosť a základné práva, by sa mali stanoviť spoločné normatívne štandardy pre všetky vysokorizikové systémy umelej inteligencie. Tieto štandardy by mali byť v súlade s Chartou základných práv Európskej únie (ďalej len „charta“) a mali by byť nediskriminačné a v súlade so záväzkami Únie v oblasti medzinárodného obchodu.

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

(15) Využívanie umelej inteligencie má síce mnoho výhod, túto technológiu však možno zneužiť a môže sa stať zdrojom nových a výkonných nástrojov umožňujúcich manipulatívne a zneužívajúce praktiky a praktiky v oblasti sociálnej kontroly. Takéto praktiky sú mimoriadne škodlivé 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 Únie vrátane práva na nediskrimináciu, ochranu údajov a súkromia a práv dieťaťa.

(16) Manipulačné techniky, ktoré umožňuje umelá inteligencia, sa môžu použiť na presviedčanie osôb, aby sa správali neželaným spôsobom, alebo na ich oklamanie nabádaním na rozhodnutia spôsobom, ktorý narúša a oslabuje ich samostatnosť, rozhodovacie schopnosti a slobodnú voľbu. Malo by sa preto zakázať uvádzanie na trh, do prevádzky alebo používanie určitých systémov umelej inteligencie, ktoré podstatne deformujú ľudské správanie a pri ktorých je pravdepodobné, že spôsobia fyzickú alebo psychickú ujmu. Takéto systémy umelej inteligencie využívajú podprahové komponenty, ako sú zvukové a obrazové podnety alebo videopodnety, ktoré osoby nemôžu vnímať, keďže sú mimo ľudského vnímania, alebo iné podprahové techniky, ktoré narúšajú alebo oslabujú samostatnosť, rozhodovacie schopnosti a slobodnú voľbu osôb spôsobmi, ktoré ľudia vedome nevnímajú, a keď vnímajú, nie sú schopní ich ovládať alebo im odolávať, napríklad v prípade rozhraní stroj – mozog alebo virtuálnej reality. Systémy umelej inteligencie môžu aj inak zneužívať zraniteľnosti osobitnej skupiny osôb z dôvodu ich veku, zdravotného postihnutia v zmysle smernice (EÚ) 2019/882 alebo osobitnej sociálnej alebo ekonomickej situácie, čo pravdepodobne spôsobuje, že tieto osoby sú zraniteľnejšie voči zneužívaniu, ako napríklad osoby žijúce v extrémnej chudobe, etnické alebo náboženské menšiny. Takéto systémy umelej inteligencie sa môžu uvádzať na trh, uvádzať do prevádzky alebo používať s cieľom alebo účinkom podstatnej deformácie správania osoby a spôsobom, ktorý spôsobuje alebo pri ktorom je odôvodnene pravdepodobné, že spôsobí fyzickú alebo psychickú ujmu tejto alebo inej osobe alebo skupinám osôb vrátane škôd, ktoré sa môžu časom kumulovať. Úmysel deformovať správanie nemožno predpokladať, ak deformácia vyplýva z faktorov mimo systému umelej inteligencie, ktoré sú mimo kontroly poskytovateľa alebo používateľa, čo znamená faktory, ktoré poskytovateľ alebo používateľ systému umelej inteligencie nemôže dôvodne predpokladať a zmierňovať. v každom prípade nie je potrebné, aby poskytovateľ alebo používateľ mal úmysel spôsobiť fyzickú alebo psychickú ujmu, pokiaľ takáto ujma vyplýva z manipulatívnych alebo zneužívajúcich praktík, ktoré umožňuje umelá inteligencia. Zákazmi takýchto praktík umelej inteligencie sa dopĺňajú ustanovenia uvedené v smernici 2005/29/ES, 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 umelej inteligencie 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. Okrem toho by sa bežné a legitímne obchodné praktiky, ktoré sú v súlade s uplatniteľným právom, nemali samy osebe považovať za škodlivé manipulatívne praktiky umelej inteligencie.

(17) Systémy umelej inteligencie, ktoré poskytujú sociálne hodnotenie fyzických osôb vykonávané orgánmi verejnej moci, môžu viesť k diskriminačným výsledkom a vylúčeniu určitých skupín. Môžu porušovať právo na dôstojnosť a nediskrimináciu a hodnoty rovnosti a spravodlivosti. Takéto systémy umelej inteligencie hodnotia alebo klasifikujú fyzické osoby na základe ich spoločenského správania vo viacerých kontextoch alebo známych či predpokladaných osobných alebo osobnostných charakteristík. Sociálne skóre získané na základe takýchto systémov umelej inteligencie môže viesť k poškodzujúcemu 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 sociálneho správania. Systémy umelej inteligencie, ktoré zahŕňajú takéto neprijateľné postupy hodnotenia, by sa preto mali zakázať. Tento zákaz by nemal mať vplyv na zákonné postupy hodnotenia fyzických osôb vykonávané na jeden alebo viacero konkrétnych účelov v súlade so zákonom.

(18) Používanie systémov umelej inteligencie 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 súkromný život veľkej časti obyvateľstva, vyvoláva pocit neustáleho sledovania a nepriamo odrádza od využívania slobody zhromažďovania a iných základných práv. 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 osôb, ktorých sa týkajú činnosti v oblasti presadzovania práva.

(19) Používanie týchto systémov na účely presadzovania práva by sa preto malo zakázať s výnimkou podrobne opísaných a úzko vymedzených situácií, keď je toto použitie nevyhnutne potrebné na dosiahnutie podstatného verejného záujmu, ktorého význam prevažuje nad rizikami. Tieto situácie zahŕňajú pátranie po potenciálnych obetiach trestných činov vrátane nezvestných detí, niektoré prípady ohrozenia života alebo fyzickej bezpečnosti fyzických osôb alebo hrozby teroristického útoku a odhaľovanie, lokalizáciu, identifikáciu alebo stíhanie páchateľov trestných činov uvedených v rámcovom rozhodnutí Rady 2002/584/SVV[9], ak za ne podľa právnych predpisov dotknutého členského štátu možno v danom členskom štáte uložiť trest odňatia slobody alebo ochranné opatrenie spojené s odňatím slobody s hornou hranicou trestnej sadzby najmenej tri roky, alebo podozrivých zo spáchania takýchto trestných činov. Takáto hranica trestu odňatia slobody alebo ochranného opatrenia spojeného s odňatím 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 je pravdepodobné, že niektoré z 32 trestných činov uvedených v rámcovom rozhodnutí Rady 2002/584/SVV sú v praxi relevantnejšie ako iné, keďže nevyhnutnosť a primeranosť použitia diaľkovej biometrickej identifikácie „v reálnom čase“ budú pravdepodobne veľmi rôznorodé jednak z hľadiska praktického vykonávania odhaľovania, lokalizácie, identifikácie alebo stíhania páchateľa jednotlivých uvedených trestných činov alebo osôb podozrivých z ich spáchania a zároveň vzhľadom na pravdepodobné rozdiely v závažnosti, pravdepodobnosti a rozsahu spôsobenej ujmy alebo možných negatívnych dôsledkov. Okrem toho by sa týmto nariadením mala zachovať schopnosť 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 osoby, ktorá sa počas kontroly totožnosti buď odmietne identifikovať, alebo nie je schopná 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 nehody alebo zdravotného stavu nie je schopná uviesť svoju totožnosť orgánom presadzovania práva.

[9] 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).

(20) S cieľom zabezpečiť, aby sa tieto systémy používali zodpovedným a primeraným spôsobom, je tiež dôležité stanoviť, že v každej z týchto podrobne opísaných 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 používanie systému diaľkovej biometrickej identifikácie „v reálnom čase“ vo verejne prístupných priestoroch na účely presadzovania práva by malo podliehať primeraným časovým a priestorovým obmedzeniam, najmä so zreteľom na dôkazy alebo náznaky týkajúce sa daných hrozieb, obetí alebo páchateľa. Referenčná databáza osôb by mala byť vhodná pre každý prípad použitia v každej z uvedených situácií.

(21) Každé použitie systému diaľkovej biometrickej identifikácie „v reálnom čase“ vo verejne prístupných priestoroch na účely presadzovania práva by malo podliehať výslovnému a osobitnému povoleniu súdneho orgánu alebo nezávislého správneho orgánu členského štátu. Takéto povolenie by sa v zásade malo získať pred použitím systému s cieľom identifikovať osobu alebo osoby. Výnimky z tohto pravidla by mali byť povolené v riadne odôvodnených naliehavých situáciách, t. j. situáciách, v ktorých je potreba použiť predmetné systémy tak naliehavá, že je naozaj objektívne nemožné získať povolenie pred začatím tohto použitia. v takýchto naliehavých situáciách by sa používanie 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 sa orgán presadzovania práva mal v takýchto situáciách snažiť získať povolenie čo najskôr, pričom uvedie dôvody, pre ktoré ho nemohol požadovať skôr.

(22) 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 daný 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.

(23) Používanie systémov umelej inteligencie 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 2016/680. Na používanie systémov umelej inteligencie 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 môže vykonávať.

(24) Každé spracovanie biometrických údajov a iných osobných údajov súvisiace s používaním systémov umelej inteligencie na biometrickú identifikáciu, okrem spracovania v súvislosti s používaním systémov umelej inteligencie 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. Na účely iné ako účely presadzovania práva sa v článku 9 ods. 1 nariadenia (EÚ) 2016/679 a v článku 10 ods. 1 nariadenia (EÚ) 2018/1725 zakazuje spracúvanie biometrických údajov na účely individuálnej identifikácie fyzickej osoby, pokiaľ nenastala jedna zo situácií uvedených v príslušných druhých odsekoch uvedených dvoch článkov.

(25) 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 ZEÚ a ZFEÚ, nie je Írsko viazané pravidlami stanovenými v článku 5 ods. 1 písm. d) a článku 5 ods. 2, 3 a 4 tohto nariadenia prijatého na základe článku 16 Zmluvy o fungovaní EÚ, 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.

(26) V súlade s článkami 2 a 2a Protokolu č. 22 o postavení Dánska, ktorý je pripojený k ZEÚ a ZFEÚ, nie je Dánsko viazané pravidlami stanovenými v článku 5 ods. 1 písm. d) a článku 5 ods. 2, 3 a 4 tohto nariadenia prijatého 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.

(27) Vysokorizikové systémy umelej inteligencie by sa mali uviesť na trh Únie alebo do prevádzky len vtedy, ak spĺňajú určité povinné požiadavky. Týmito požiadavkami by sa malo zabezpečiť, aby vysokorizikové systémy umelej inteligencie, 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. Systémy umelej inteligencie 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 minimalizuje akékoľvek prípadné obmedzenie medzinárodného obchodu.

(28) Systémy umelej inteligencie by mohli mať nepriaznivé účinky na zdravie a bezpečnosť osôb, najmä ak takéto systémy fungujú ako 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 umelej inteligencie, 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. Pri klasifikácii systému umelej inteligencie ako vysokorizikového je obzvlášť dôležitý rozsah nepriaznivého vplyvu systému umelej inteligencie 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, nediskriminácia, ochrana spotrebiteľa, základné pracovné práva, práva osôb so zdravotným postihnutím, právo na účinný prostriedok nápravy a na spravodlivý proces, právo na obhajobu a prezumpcia neviny, právo na dobrú správu vecí verejných. Okrem týchto práv je dôležité zdôrazniť, že deti majú osobitné práva zakotvené v článku 24 Charty EÚ a v Dohovore Organizácie Spojených národov o právach dieťaťa (ďalej rozpracované vo všeobecnej poznámke č. 25 Dohovoru OSN o právach dieťaťa, pokiaľ ide o digitálne prostredie), 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 umelej inteligencie 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.

(29) Pokiaľ ide o vysokorizikové systémy umelej inteligencie, 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[10], nariadenia Európskeho parlamentu a Rady (EÚ) č. 167/2013[11], nariadenia Európskeho parlamentu a Rady (EÚ) č. 168/2013[12], smernice Európskeho parlamentu a Rady 2014/90/EÚ[13], smernice Európskeho parlamentu a Rady (EÚ) 2016/797[14], nariadenia Európskeho parlamentu a Rady (EÚ) 2018/858[15], nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1139[16] a nariadenia Európskeho parlamentu a Rady (EÚ) 2019/2144[17], je vhodné uvedené akty zmeniť s cieľom zaistiť, aby Komisia pri prijímaní akýchkoľvek budúcich relevantných delegovaných alebo vykonávacích aktov na základe uvedených aktov zohľadňovala povinné požiadavky na vysokorizikové systémy umelej inteligencie 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.

---

10 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).

11 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).

12 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).

13 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).

14 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).

15 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).

16 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).

17 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)

(30) Pokiaľ ide o systémy umelej inteligencie, ktoré sú bezpečnostnými komponentmi výrobkov alebo ktoré sú samy výrobkami, ktoré patria do rozsahu pôsobnosti určitých harmonizačných právnych predpisov Únie, je vhodné klasifikovať ich podľa tohto nariadenia ako vysokorizikové, pokiaľ v prípade daného 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 prostredí s nebezpečím výbuchu, rádiové zariadenia, tlakové zariadenia, vybavenie rekreačných plavidiel, lanovkové zariadenia, spotrebiče spaľujúce plynné palivá, zdravotnícke pomôcky a diagnostické zdravotnícke pomôcky in vitro.

(31) Klasifikácia systému umelej inteligencie ako vysokorizikového podľa tohto nariadenia by nemala nevyhnutne znamenať, že výrobok, ktorého bezpečnostným komponentom je systém umelej inteligencie, alebo samotný systém umelej inteligencie ako výrobok sa považuje za „vysokorizikový“ podľa kritérií stanovených v príslušných harmonizačných právnych predpisoch Únie, ktoré sa vzťahujú na daný výrobok. Platí to najmä pre nariadenie Európskeho parlamentu a Rady (EÚ) 2017/745[18] a nariadenie Európskeho parlamentu a Rady (EÚ) 2017/746[19], kde sa pre výrobky so stredným a vysokým rizikom vyžaduje posudzovanie zhody treťou stranou.

---

18 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).

19 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).

(32) Iné vysokorizikové systémy umelej inteligencie ako tie, ktoré sú bezpečnostnými komponentmi výrobkov alebo ktoré sú samy výrobkami, je vhodné klasifikovať 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 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 umelej inteligencie. Takisto je dôležité objasniť, že v rámci vysokorizikových scenárov uvedených v prílohe III môžu existovať systémy, ktoré vzhľadom na výstupy, ktoré vytvárajú, nevedú k významnému riziku pre právne záujmy chránené v rámci týchto scenárov. Systém umelej inteligencie by sa mal preto za vysokorizikový považovať len vtedy, keď sa ním vytvára výstup, ktorý má vysoký stupeň dôležitosti (t. j. nie je čisto doplnkový) vo vzťahu k príslušnému konaniu alebo rozhodnutiu, a tvorí tak významné riziko pre chránené právne záujmy. Ak napríklad informácie, ktoré systémy umelej inteligencie poskytujú ľuďom, pozostávajú z profilovania fyzických osôb v zmysle článku 4 ods. 4 nariadenia (EÚ) 2016/679, článku 3 ods. 4 smernice (EÚ) 2016/680 a článku 3 ods. 5 nariadenia (EÚ) 2018/1725, takéto informácie by sa v kontexte vysokorizikových systémov umelej inteligencie, ako sa uvádzajú v prílohe III, zvyčajne nemali považovať za doplnkové. Ak má však výstup systému umelej inteligencie len zanedbateľný alebo malý význam pre ľudské konanie alebo rozhodnutie, môže sa považovať za čisto doplnkový, napríklad vrátane systémov umelej inteligencie používaných na preklad na informatívne účely alebo na správu dokumentov.

(33) Technické nepresnosti systémov umelej inteligencie určených na diaľkovú biometrickú identifikáciu fyzických osôb môžu viesť k skresleným výsledkom a mať diskriminačné účinky. Platí to najmä v prípade veku, etnického pôvodu, rasy, pohlavia alebo zdravotných postihnutí. Preto by sa systémy diaľkovej biometrickej identifikácie „v reálnom čase“ a „následnej“ diaľkovej biometrickej identifikácie mali klasifikovať ako vysokorizikové. Vzhľadom na riziká, ktoré predstavujú, by oba typy systémov diaľkovej biometrickej identifikácie mali podliehať osobitným požiadavkám týkajúcim sa schopností logovania a ľudského dohľadu.

(34) Pokiaľ ide o riadenie a prevádzku kritickej infraštruktúry, je vhodné klasifikovať ako vysokorizikové také systémy umelej inteligencie, ktoré sú určené na používanie ako bezpečnostné komponenty pri riadení a prevádzke kritickej digitálnej infraštruktúry uvedenej v prílohe I bode 8 smernice o odolnosti kritických subjektov, cestnej premávky a pri dodávkach vody, plynu, tepla a elektrickej energie, keďže ich zlyhanie alebo porucha môže ohroziť život a zdravie osôb vo veľkom rozsahu a viesť k značným narušeniam bežného vykonávania sociálnych 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.

(35) Za vysokorizikové by sa mali považovať systémy umelej inteligencie používané vo vzdelávaní alebo odbornej príprave, najmä na určovanie prístupu, prijatia alebo pridelenia osôb do inštitúcií alebo programov vzdelávania a odbornej prípravy na akejkoľvek úrovni alebo na hodnotenie vzdelávacích výstupov osôb, pretože môžu určovať vzdelávací a profesionálny priebeh života osoby, a tým ovplyvňovať jej schopnosť zabezpečiť si živobytie. Ak sú takéto systémy navrhnuté a používané nesprávne, môžu porušovať právo na vzdelanie a odbornú prípravu, ako aj právo nebyť diskriminovaný a tým zachovávať zaužívané formy diskriminácie.

(36) Ako vysokorizikové by sa mali klasifikovať aj systémy umelej inteligencie používané pri zamestnávaní, riadení pracovníkov a prístupe k samostatnej zárobkovej činnosti, najmä pri nábore a výbere osôb, pri rozhodovaní o povýšení a ukončení pracovného pomeru a pri prideľovaní úloh na základe individuálneho správania sa alebo osobných čŕt či vlastností, monitorovaní alebo hodnotení osôb v zmluvných pracovnoprávnych vzťahoch, pretože tieto systémy môžu významne ovplyvniť budúce kariérne vyhliadky a živobytie týchto osôb. Príslušné zmluvné pracovnoprávne vzťahy by mali zahŕňať zamestnancov a osoby, ktorí poskytujú služby prostredníctvom platforiem, ako sa uvádza v pracovnom programe Komisie na rok 2021. Takéto osoby by sa v zásade nemali považovať za používateľov v zmysle tohto nariadenia. Takéto systémy môžu počas celého procesu prijímania do zamestnania a počas hodnotenia, povyšovania alebo udržiavania osôb v zmluvných pracovnoprávnych vzťahoch zachovávať zaužívané formy diskriminácie, napríklad žien, určitých vekových skupín, osôb so zdravotným postihnutím alebo osôb určitého rasového alebo etnického pôvodu alebo sexuálnej orientácie. Systémy umelej inteligencie používané na monitorovanie výkonnosti a správania týchto osôb môžu mať vplyv aj na ich práva na ochranu údajov a súkromia.

(37) Ďalšou oblasťou, v ktorej si využívanie systémov umelej inteligencie 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. Ako vysokorizikové by sa mali klasifikovať najmä systémy umelej inteligencie 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 umelej inteligencie používané na tento účel môžu viesť k diskriminácii osôb alebo skupín a zachovávať zaužívané formy diskriminácie, napríklad na základe rasového alebo etnického pôvodu, zdravotných postihnutí, veku, sexuálnej orientácie, alebo môžu vytvárať nové formy diskriminačných vplyvov. Vzhľadom na veľmi obmedzený rozsah vplyvu a dostupné alternatívy na trhu je vhodné stanoviť výnimku pre systémy umelej inteligencie na účely posudzovania úverovej bonity a bodového hodnotenia kreditného rizika, pokiaľ ich uvedú do prevádzky mikropodniky a malé podniky v zmysle prílohy k odporúčaniu Komisie 2003/361/ES, a to na vlastné použitie. Fyzické osoby, ktoré žiadajú o základné dávky a služby verejnej pomoci alebo ktoré od orgánov verejnej moci prijímajú tieto dávky a služby, sú zvyčajne od týchto dávok a služieb závislé a nachádzajú sa v zraniteľnom postavení vo vzťahu k zodpovedným orgánom. Ak sa systémy umelej inteligencie používajú na určenie toho, či by orgány mali takéto dávky a služby zamietnuť, znížiť, zrušiť alebo žiadať o ich vrátenie, vrátane toho, či majú poberatelia oprávnený nárok na takéto dávky a 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. Preto by sa tieto systémy mali klasifikovať ako vysokorizikové. Toto nariadenie by však nemalo brániť rozvoju a využívaniu inovačných prístupov vo verejnej správe, pre ktorú by mohlo byť širšie využívanie vyhovujúcich a bezpečných systémov umelej inteligencie prospešné, za predpokladu, že tieto systémy nepredstavujú vysoké riziko pre právnické a fyzické osoby. v konečnom dôsledku by sa ako vysokorizikové mali klasifikovať aj systémy umelej inteligencie používané na vysielanie záchranných služieb prvej reakcie alebo na stanovovanie priority ich vysielania, pretože prijímajú rozhodnutia v situáciách, ktoré sú veľmi kritické z hľadiska života a zdravia osôb a ich majetku. Systémy umelej inteligencie sa takisto čoraz častejšie používajú na posudzovanie rizík v súvislosti s fyzickými osobami a cenotvorbou v prípade životného a zdravotného poistenia, ktoré, ak nie sú riadne navrhnuté, vyvinuté a používané, môže mať vážne dôsledky pre život a zdravie ľudí vrátane finančného vylúčenia a diskriminácie. s cieľom zabezpečiť jednotný prístup v sektore finančných služieb by sa uvedená výnimka pre mikropodniky alebo malé podniky na ich vlastné použitie mala uplatňovať, pokiaľ systém umelej inteligencie poskytujú a uvádzajú do prevádzky tieto podniky samotné, a to na účely predaja svojich vlastných poistných produktov.

(38) Opatrenia orgánov presadzovania práva zahŕňajúce určité použitia systémov umelej inteligencie sa vyznačujú značným stupňom nerovnováhy právomocí a môžu viesť k sledovaniu, zatknutiu alebo pozbaveniu slobody fyzickej osoby, ako aj k iným nepriaznivým vplyvom na základné práva zaručené chartou. Najmä ak systém umelej inteligencie nie je trénovaný na vysokokvalitných údajoch, nespĺňa primerané požiadavky, pokiaľ ide o jeho presnosť alebo spoľahlivosť, alebo nie je pred uvedením na trh alebo do prevádzky riadne koncipovaný a otestovaný, môže ľudí vylúčiť 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 umelej inteligencie nie sú dostatočne transparentné, vysvetliteľné a zdokumentované. Preto je vhodné klasifikovať ako vysokorizikové viaceré systémy umelej inteligencie 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 súvisiace riziká by tieto vysokorizikové systémy umelej inteligencie mali zahŕňať najmä systémy umelej inteligencie, ktoré majú orgány presadzovania práva používať na individuálne posúdenia rizika, ako detektory lži a podobné nástroje, alebo na zisťovanie emocionálneho stavu fyzickej osoby, na hodnotenie spoľahlivosti dôkazov v trestnom konaní, na predpovedanie výskytu alebo opätovného výskytu skutočného alebo potenciálneho trestného činu na základe profilovania fyzických osôb alebo posudzovania osobnostných a povahových rysov alebo trestnej činnosti fyzických osôb alebo skupín v minulosti, na profilovanie v priebehu odhaľovania, vyšetrovania alebo stíhania trestných činov. Systémy umelej inteligencie, ktoré sú osobitne určené na používanie v správnych konaniach daňovými a colnými orgánmi, ako aj finančnými spravodajskými jednotkami vykonávajúcimi administratívne úlohy analyzujúce informácie podľa právnych predpisov Únie v oblasti boja proti praniu špinavých peňazí, by sa nemali považovať za vysokorizikové systémy umelej inteligencie používané orgánmi presadzovania práva na účely predchádzania trestným činom, ich odhaľovania, vyšetrovania a stíhania.

(39) Systémy umelej inteligencie používané v oblastiach migrácie, azylu a riadenia kontroly hraníc majú vplyv na ľudí, ktorí sú často v mimoriadne zraniteľnom postavení a ktorí sú závislí od výsledku činností príslušných orgánov verejnej moci. Presnosť, nediskriminačný charakter a transparentnosť systémov umelej inteligencie používaných v tomto kontexte sú preto mimoriadne dôležité na zaručenie dodržiavania základných práv dotknutých osôb, najmä ich práva na voľný pohyb, nediskrimináciu, ochranu súkromného života a osobných údajov, medzinárodnú ochranu a dobrú správu vecí verejných. Je preto vhodné klasifikovať ako vysokorizikové tie systémy umelej inteligencie, ktoré majú používať príslušné orgány verejnej moci poverené úlohami v oblasti migrácie, azylu a riadenia kontroly hraníc, ako napríklad detektory lži a podobné nástroje, alebo na zisťovanie emocionálneho stavu fyzickej osoby, posudzovanie určitých rizík, ktoré predstavujú fyzické osoby vstupujúce na územie členského štátu alebo žiadajúce o vízum alebo azyl, pomoc príslušným orgánom verejnej moci pri posudzovaní žiadostí o azyl, víza a povolenia na pobyt a súvisiacich sťažností, pokiaľ ide o cieľ zistiť oprávnenosť fyzických osôb žiadajúcich o určitý status. Systémy umelej inteligencie v oblasti migrácie, azylu a riadenia kontroly hraníc, na ktoré sa vzťahuje toto nariadenie, by mali spĺňať príslušné procedurálne požiadavky stanovené v smernici Európskeho parlamentu a Rady 2013/32/EÚ[20], nariadení Európskeho parlamentu a Rady (ES) č. 810/2009[21] a iných príslušných právnych predpisoch.

[20] 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).

[21] 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).

(40) Niektoré systémy umelej inteligencie 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 umelej inteligencie určené na pomoc justičným orgánom pri výklade skutočností a práva a pri uplatňovaní práva na konkrétny súbor skutočností, najmä z dôvodu riešenia rizík možných skreslení, chýb a nepriehľadnosti. Takáto kvalifikácia by sa však nemala vzťahovať na systémy umelej inteligencie určené na čisto pomocné administratívne činnosti, ktoré nemajú vplyv na skutočný výkon spravodlivosti v jednotlivých prípadoch, ako napr. anonymizácia alebo pseudonymizácia súdnych rozhodnutí, dokumentov alebo údajov, komunikácia medzi zamestnancami alebo administratívne úlohy.

(41) Skutočnosť, že systém umelej inteligencie sa podľa tohto nariadenia klasifikuje ako vysokorizikový, by sa nemala vykladať tak, že používanie tohto systému je zákonné podľa iných aktov práva Únie alebo vnútroštátneho práva zlučiteľného s právom Únie, ako napr. v oblasti ochrany osobných údajov, používania detektorov lži 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 chápať 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.

(42) S cieľom zmierniť riziká, ktoré vyplývajú z vysokorizikových systémov umelej inteligencie uvedených na trh Únie alebo inak uvedených do prevádzky na trhu Únie, by sa mali uplatňovať určité povinné požiadavky, pričom by sa mal zohľadniť zamýšľaný účel používania tohto systému a systém riadenia rizík, ktorý zavedie poskytovateľ. Systém riadenia rizík by mal pozostávať najmä z nepretržitého iteratívneho procesu plánovaného a používaného počas celého životného cyklu vysokorizikového systému umelej inteligencie. Týmto procesom by sa malo zabezpečiť, aby poskytovateľ identifikoval a analyzoval riziká pre zdravie, bezpečnosť a základné práva osôb, ktoré môžu byť ovplyvnené systémom vzhľadom na jeho zamýšľaný účel, vrátane možných rizík vyplývajúcich zo vzájomného pôsobenia medzi systémom umelej inteligencie a prostredím, v ktorom funguje, a aby zodpovedajúcim spôsobom prijal vhodné opatrenia na riadenie rizík vzhľadom na najnovší technologický vývoj.

(43) Požiadavky by sa mali vzťahovať na vysokorizikové systémy umelej inteligencie, pokiaľ ide o kvalitu použitých súborov údajov, technickú dokumentáciu a uchovávanie záznamov, transparentnosť a poskytovanie informácií používateľom, ľudský dohľad a spoľahlivosť, presnosť a kybernetickú bezpečnosť. Tieto požiadavky sú potrebné na účinné zmiernenie rizík pre zdravie, bezpečnosť a základné práva, ktoré sa uplatňujú vzhľadom na zamýšľaný účel systému, a nie sú primerane dostupné žiadne iné opatrenia menej obmedzujúce obchod, takže nedochádza k neodôvodneným obmedzeniam obchodu.

(44) Pre výkonnosť mnohých systémov umelej inteligencie je kľúčová vysoká kvalita údajov, najmä ak sa využívajú techniky zahŕňajúce trénovanie modelov, aby vysokorizikový systém umelej inteligencie 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 trénovacích, validačných a testovacích údajov by mali byť dostatočne relevantné a reprezentatívne a mali by mať aj primerané štatistické vlastnosti, a to aj pokiaľ ide o osoby alebo skupiny osôb, v prípade ktorých sa má vysokorizikový systém umelej inteligencie používať. Tieto súbory údajov by takisto mali byť bez chýb a mali by byť čo najúplnejšie vzhľadom na zamýšľaný účel systému umelej inteligencie, pričom by sa primeraným spôsobom mala zohľadniť technická uskutočniteľnosť a najnovší technologický vývoj, dostupnosť údajov a vykonávanie vhodných opatrení na riadenie rizík, aby sa možné nedostatky súborov údajov náležite riešili. Požiadavka, aby boli súbory údajov úplné a bez chýb, by nemala mať v súvislosti s vývojom a testovaním systémov umelej inteligencie vplyv na používanie techník na zachovanie súkromia. Súbory trénovacích, validačných a testovacích údajov by mali v rozsahu, v akom si to vyžaduje zamýšľaný účel, zohľadňovať vlastnosti, charakteristiky alebo prvky, ktoré sú špecifické pre konkrétne geografické, behaviorálne alebo funkčné podmienky alebo súvislosti, v ktorých sa má systém umelej inteligencie používať. Na ochranu práva iných osôb pred diskrimináciou, ktorá by mohla vyplynúť zo skreslenia systémov umelej inteligencie, by poskytovatelia mali mať vzhľadom na významný verejný záujem v zmysle článku 9 ods. 2 písm. g) nariadenia (EÚ) 2016/679 a článku 10 ods. 2 písm. g) nariadenia (EÚ) 2018/1725 možnosť spracúvať aj osobitné kategórie osobných údajov s cieľom zabezpečiť monitorovanie, odhaľovanie a nápravu tohto skreslenia vo vzťahu k vysokorizikovým systémom umelej inteligencie.

(44a) Pri uplatňovaní zásad uvedených v článku 5 ods. 1 písm. c) nariadenia 2016/679 a článku 4 ods. 1 písm. c) nariadenia 2018/1725, najmä zásady minimalizácie údajov, pokiaľ ide o súbory trénovacích, validačných a testovacích údajov podľa tohto nariadenia, by sa mal náležite zohľadniť celý životný cyklus systému umelej inteligencie.

(45) Pokiaľ ide o vývoj vysokorizikových systémov umelej inteligencie, niektorí aktéri, ako sú poskytovatelia, notifikované osoby a iné príslušné subjekty, ako napr. centrá digitálnych inovácií, testovacie experimentačné zariadenia a výskumní pracovníci, by mali mať prístup k súborom vysokokvalitných údajov a využívať ich v rámci svojich príslušných oblastí činností, ktoré súvisia s týmto nariadením. Pri poskytovaní dôveryhodného, zodpovedného a nediskriminačného prístupu k vysokokvalitným údajom na účely trénovania, validácie a testovania systémov umelej inteligencie budú mať zásadný význam európske spoločné 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 umelej inteligencie 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 umelej inteligencie.

(46) Na overenie súladu s požiadavkami podľa tohto nariadenia je nevyhnutné mať informácie o tom, ako boli vyvinuté vysokorizikové systémy umelej inteligencie a ako fungujú počas celého svojho životného cyklu. Preto sa vyžaduje uchovávanie záznamov a dostupnosť technickej dokumentácie obsahujúcej informácie, ktoré sú potrebné na posúdenie súladu systému umelej inteligencie s príslušnými požiadavkami. Takéto informácie by mali zahŕňať všeobecné charakteristiky, schopnosti a obmedzenia systému, použité algoritmy, údaje, postupy trénovania, testovania a validácie, ako aj dokumentáciu o príslušnom systéme riadenia rizík. Technická dokumentácia by sa mala priebežne aktualizovať. Poskytovatelia alebo používatelia by okrem toho mali uchovávať logy automaticky generované vysokorizikovým systémom umelej inteligencie, napríklad vrátane výstupných údajov, dátumu a času začiatku atď., pokiaľ sú takýto systém a súvisiace logy pod ich kontrolou, a to počas obdobia, ktoré je primerané na to, aby si mohli plniť svoje povinnosti.

(47) Pre vysokorizikové systémy umelej inteligencie by sa mal vyžadovať určitý stupeň transparentnosti, aby sa vyriešila nepriehľadnosť, ktorá môže spôsobiť, že niektoré systémy umelej inteligencie budú pre fyzické osoby nezrozumiteľné alebo príliš zložité. Používatelia by mali byť schopní interpretovať výstup systému a vhodne ho používať. K vysokorizikovým systémom umelej inteligencie by preto mala byť pripojená príslušná dokumentácia a návod na použitie, ktoré by mali obsahovať stručné a jasné informácie, a to prípadne aj v súvislosti s možnými rizikami týkajúcimi sa základných práv a diskriminácie osôb, na ktoré môže mať systém vplyv vzhľadom na jeho zamýšľaný účel. Aby sa používateľom uľahčilo pochopenie návodu na použitie, mal by podľa potreby obsahovať ilustračné príklady.

(48) Vysokorizikové systémy umelej inteligencie by mali byť koncipované a vyvinuté tak, aby fyzické osoby mohli dohliadať na ich fungovanie. Na tento účel by mal poskytovateľ systému určiť pred jeho uvedením na trh alebo do prevádzky vhodné opatrenia 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. Vzhľadom na významné dôsledky pre osoby v prípade nesprávnych zhôd prostredníctvom určitých systémov biometrickej identifikácie je vhodné stanoviť požiadavku posilneného ľudského dohľadu nad týmito systémami, aby používateľ nemohol prijať žiadne opatrenie ani rozhodnutie na základe identifikácie vyplývajúcej zo systému, pokiaľ ju 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 rôznymi osobami automaticky zaznamenávali do logov generovaných systémom.

(49) Vysokorizikové systémy umelej inteligencie by mali fungovať konzistentne počas celého svojho životného cyklu a mali by spĺňať primeranú úroveň presnosti, spoľahlivosti a kybernetickej bezpečnosti v súlade so všeobecne uznávaným stavom techniky. Používatelia by mali byť informovaní o úrovni a metrikách na meranie presnosti.

(50) Technická spoľahlivosť je kľúčovou požiadavkou pre vysokorizikové systémy umelej inteligencie. Mali by byť odolné voči škodlivému alebo inak nežiaducemu správaniu, ktoré môže vyplynúť z obmedzení systémov alebo prostredia, v ktorom systémy fungujú (napr. chyby, poruchy, nezrovnalosti, neočakávané situácie). Vysokorizikové systémy umelej inteligencie by sa preto mali navrhovať a vyvíjať s primeranými technickými riešeniami na prevenciu alebo minimalizáciu takéhoto škodlivého alebo inak nežiaduceho správania sa, ako sú napríklad mechanizmy, ktoré systému umožňujú bezpečne prerušiť svoju prevádzku (plány zaistenia v prípade zlyhania), ak dôjde k určitým anomáliám alebo keď 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 umelej inteligencie.

(51) Kybernetická bezpečnosť zohráva kľúčovú úlohu pri zabezpečovaní odolnosti systémov umelej inteligencie 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 umelej inteligencie môžu využívať aktíva špecifické pre umelú inteligenciu, ako sú súbory trénovacích údajov (napr. otrávenie údajov) alebo trénované modely (napr. nepriateľské útoky), alebo zneužívať zraniteľné miesta digitálnych aktív systému umelej inteligencie alebo základnej infraštruktúry IKT. Na zabezpečenie úrovne kybernetickej bezpečnosti primeranej rizikám by preto poskytovatelia vysokorizikových systémov umelej inteligencie mali prijať vhodné opatrenia a náležite pritom zohľadniť základnú infraštruktúru IKT.

(52) Ako súčasť harmonizačných právnych predpisov Únie by sa pravidlá uplatniteľné na uvádzanie vysokorizikových systémov umelej inteligencie na trh, do prevádzky a na ich používanie mali stanoviť v súlade s nariadením Európskeho parlamentu a Rady (ES) č. 765/2008[22], ktorým sa stanovujú požiadavky akreditácie výrobkov a dohľadu nad trhom s nimi, rozhodnutím Európskeho parlamentu a Rady č. 768/2008/ES[23] o spoločnom rámci na uvádzanie výrobkov na trh a s nariadením Európskeho parlamentu a Rady (EÚ) 2019/1020[24] o dohľade nad trhom a súlade výrobkov („nový legislatívny rámec pre uvádzanie výrobkov na trh“).

(52a) Mali by sa stanoviť osobitné povinnosti pre príslušných prevádzkovateľov v rámci hodnotového reťazca umelej inteligencie v súlade so zásadami nového legislatívneho rámca, aby sa zabezpečila právna istota a uľahčil súlad s týmto nariadením. 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.

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

---

22 Nariadenie Európskeho parlamentu a Rady (ES) č. 765/2008 z 9. júla 2008, ktorým sa stanovujú požiadavky akreditácie a dohľadu nad trhom v súvislosti s uvádzaním výrobkov na trh a ktorým sa zrušuje nariadenie (EHS) č. 339/93 (Ú. v. EÚ L 218, 13.8.2008, s. 30).

23 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).

24 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 (Text s významom pre EHP) (Ú. v. EÚ L 169, 25.6.2019, s. 1 – 44).

(54) 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. Orgány verejnej moci, ktoré uvádzajú do prevádzky vysokorizikové systémy umelej inteligencie 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 príslušného orgánu verejnej moci.

(54a) V záujme zabezpečenia právnej istoty je potrebné objasniť, že za určitých osobitných podmienok by sa každá fyzická alebo právnická osoba mala považovať za poskytovateľa nového vysokorizikového systému umelej inteligencie, a preto by mala prevziať všetky príslušné povinnosti. Bolo by to tak napríklad v prípade, ak daná osoba umiestni svoje meno alebo ochrannú známku na vysokorizikový systém umelej inteligencie, ktorý už bol uvedený na trh alebo do prevádzky, alebo ak táto osoba zmení zamýšľaný účel systému umelej inteligencie, ktorý nie je vysokorizikový a ktorý je už uvedený na trh alebo do prevádzky, takým spôsobom, že zmenený systém sa stane vysokorizikovým systémom umelej inteligencie. Tieto ustanovenia by sa mali uplatňovať bez toho, aby nimi boli dotknuté konkrétnejšie ustanovenia zavedené v určitých odvetvových právnych predpisoch nového legislatívneho rámca, s ktorými by sa toto nariadenie malo uplatňovať spoločne. Napríklad článok 16 ods. 2 nariadenia č. 745/2017, 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 umelej inteligencie, ktoré sú zdravotníckymi pomôckami v zmysle uvedeného nariadenia.

(55) Ak sa vysokorizikový systém umelej inteligencie, ktorý je bezpečnostným komponentom výrobku, na ktorý sa vzťahujú príslušné odvetvové právne predpisy nového legislatívneho rámca, neuvádza na trh ani do prevádzky nezávisle od daného výrobku, výrobca výrobku, ako sa vymedzuje v príslušných právnych predpisoch nového legislatívneho rámca, by mal dodržiavať povinnosti poskytovateľa stanovené v tomto nariadení, a najmä zabezpečiť, aby systém umelej inteligencie zabudovaný do konečného výrobku spĺňal požiadavky tohto nariadenia.

(56) 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 umelej inteligencie. Preto ak nie je možné identifikovať dovozcu, poskytovatelia usadení mimo Únie vymenujú písomným splnomocnením pred sprístupnením svojich systémov umelej inteligencie na trhu Únie splnomocneného zástupcu usadeného v Únii.

(56a) V prípade poskytovateľov, ktorí nie sú usadení v Únii, zohráva splnomocnený zástupca kľúčovú úlohu pri zabezpečovaní súladu vysokorizikových systémov umelej inteligencie uvedených na trh alebo do prevádzky v Únii týmito poskytovateľmi a slúži ako ich kontaktná osoba usadená v Únii. Vzhľadom na túto kľúčovú úlohu a s cieľom zabezpečiť prevzatie zodpovednosti na účely presadzovania tohto nariadenia je vhodné, aby bol splnomocnený zástupca zodpovedný za chybné vysokorizikové systémy umelej inteligencie spoločne a nerozdielne s poskytovateľom. Zodpovednosťou splnomocneného zástupcu ustanovenou v tomto nariadení nie sú dotknuté ustanovenia smernice 85/374/EHS o zodpovednosti za chybné výrobky.

(57) [vypúšťa sa]

(58) Vzhľadom na povahu systémov umelej inteligencie a riziká pre bezpečnosť a základné práva, ktoré môžu súvisieť s ich používaním, a to aj pokiaľ ide o potrebu zabezpečiť riadne monitorovanie výkonnosti systému umelej inteligencie v reálnom prostredí, je vhodné stanoviť osobitné povinnosti používateľov. Používatelia by hlavne mali používať vysokorizikové systémy umelej inteligencie v súlade s návodom na použitie a mali by sa stanoviť určité ďalšie povinnosti, pokiaľ ide o monitorovanie fungovania systémov umelej inteligencie a prípadne aj uchovávanie záznamov. Týmito povinnosťami by nemali byť dotknuté iné povinnosti používateľov v súvislosti s vysokorizikovými systémami umelej inteligencie podľa práva Únie alebo vnútroštátneho práva a nemali by sa uplatňovať, ak sa systémy používajú v rámci osobnej neprofesionálnej činnosti.

(58a) Je vhodné objasniť, že týmto nariadením nie sú dotknuté povinnosti poskytovateľov a používateľov systémov umelej inteligencie v ich úlohe prevádzkovateľov alebo sprostredkovateľov vyplývajúce z práva Únie o ochrane osobných údajov, pokiaľ návrh, vývoj alebo používanie systémov umelej inteligencie 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 umelej inteligencie ustanovené podľa tohto nariadenia 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.

(59) [vypúšťa sa]

(60) [vypúšťa sa]

(61) Kľúčovú úlohu pri poskytovaní technických riešení poskytovateľom na zabezpečenie súladu s týmto nariadením v súlade s najnovším technologickým vývojom by mala zohrávať normalizácia. Dodržiavanie harmonizovaných noriem vymedzených v nariadení Európskeho parlamentu a Rady (EÚ) č. 1025/2012[25], ktoré by za bežných okolností mali odzrkadľovať stav najnovšieho technologického vývoja, by malo byť pre poskytovateľov prostriedkom na preukázanie zhody s požiadavkami tohto nariadenia. Ak však neexistujú relevantné odkazy na harmonizované normy, Komisia by mala mať možnosť stanoviť prostredníctvom vykonávacích aktov spoločné špecifikácie pre určité požiadavky podľa tohto nariadenia ako výnimočné núdzové riešenie na uľahčenie povinnosti poskytovateľa dodržiavať požiadavky tohto nariadenia, ak je proces normalizácie zablokovaný alebo keď dôjde k oneskoreniu pri vypracúvaní vhodnej harmonizovanej normy. Ak je takéto oneskorenie spôsobené technickou zložitosťou príslušnej normy, Komisia by to mala zohľadniť pred tým, ako zváži ustanovenie spoločných špecifikácií. Na podporu inovácie a konkurencieschopnosti v oblasti umelej inteligencie v Únii je nevyhnutné primerané zapojenie malých a stredných podnikov do vypracúvania noriem na podporu vykonávania tohto nariadenia. Takéto zapojenie by sa malo primerane zabezpečiť v súlade s článkami 5 a 6 nariadenia 1025/2012.

[25] 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).

(61a) Bez toho, aby bolo dotknuté používanie harmonizovaných noriem a spoločných špecifikácií, je vhodné, aby poskytovatelia využívali predpoklad zhody s príslušnou požiadavkou na údaje, ak bol ich vysokorizikový systém umelej inteligencie trénovaný a testovaný na údajoch odrážajúcich konkrétne geografické, behaviorálne alebo funkčné prostredie, v ktorom sa má systém umelej inteligencie používať. Podobne by sa v súlade s článkom 54 ods. 3 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 mali vysokorizikové systémy umelej inteligencie, ktoré boli certifikované alebo pre ktoré bolo vydané vyhlásenie o zhode v rámci systému kybernetickej bezpečnosti podľa uvedeného nariadenia a na ktoré boli uverejnené odkazy v Úradnom vestníku Európskej únie, považovať za systémy, ktoré sú v súlade s požiadavkou na kybernetickú bezpečnosť podľa tohto nariadenia. Tým nie je dotknutá dobrovoľná povaha uvedeného systému kybernetickej bezpečnosti.

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

(63) S cieľom minimalizovať zaťaženie prevádzkovateľov a predchádzať prípadnej duplicite je vhodné, aby sa v prípade vysokorizikových systémov umelej inteligencie súvisiacich s výrobkami, na ktoré sa vzťahujú existujúce harmonizačné právne predpisy Únie na základe prístupu nového legislatívneho rámca, posudzoval súlad týchto systémov umelej inteligencie s požiadavkami tohto nariadenia v rámci posudzovania zhody, ktoré sa už upravuje na základe uvedených právnych predpisov. Uplatniteľnosť požiadaviek tohto nariadenia by preto nemala mať vplyv na konkrétnu logiku, metodiku ani všeobecnú štruktúru posudzovania zhody podľa príslušných osobitných právnych predpisov nového legislatívneho rámca. Tento prístup sa plne odráža v súhre tohto nariadenia s [nariadením o strojových zariadeniach]. Zatiaľ čo požiadavky tohto nariadenia sa zaoberajú bezpečnostnými rizikami systémov umelej inteligencie, ktoré zaisťujú bezpečnostné funkcie v strojových zariadeniach, [nariadenie o strojových zariadeniach] obsahuje určité osobitné požiadavky, ktorými sa zaručí bezpečné zakomponovanie systémov umelej inteligencie do celého strojového zariadenia tak, aby nebola ohrozená bezpečnosť strojového zariadenia ako celku. v [nariadení o strojových zariadeniach] sa uplatňuje rovnaké vymedzenie pojmu systému umelej inteligencie ako v tomto nariadení. Pokiaľ ide o vysokorizikové systémy umelej inteligencie súvisiace s výrobkami, na ktoré sa vzťahujú nariadenia č. 745/2017 a 746/2017 o zdravotníckych pomôckach, uplatniteľnosť požiadaviek tohto nariadenia by nemala mať vplyv na logiku riadenia rizík a posúdenie pomeru prínosu a rizika vykonávané podľa rámca pre zdravotnícke pomôcky, ktoré by sa v nej mali zohľadniť.

(64) Vzhľadom na rozsiahlejšie skúsenosti profesionálnych certifikačných subjektov pred uvedením na trh v oblasti bezpečnosti výrobkov a na rozličnú povahu súvisiacich rizík je vhodné aspoň v počiatočnej fáze uplatňovania tohto nariadenia obmedziť rozsah uplatňovania posudzovania zhody treťou stranou v prípade vysokorizikových systémov umelej inteligencie iných ako tých, ktoré sa týkajú výrobkov. Posudzovanie zhody takýchto systémov by mal preto spravidla vykonávať poskytovateľ na vlastnú zodpovednosť s jedinou výnimkou, ktorú tvoria systémy umelej inteligencie určené na používanie na diaľkovú biometrickú identifikáciu osôb, v prípade ktorých by sa malo predpokladať zapojenie notifikovanej osoby do posudzovania zhody, pokiaľ tieto systémy nie sú zakázané.

(65) S cieľom vykonávať posudzovanie zhody treťou stranou v prípade systémov umelej inteligencie, ktoré sa majú používať na diaľkovú biometrickú identifikáciu osôb, by podľa tohto nariadenia mali byť notifikované osoby notifikované príslušnými vnútroštátnymi orgánmi za predpokladu, že spĺňajú súbor požiadaviek, najmä pokiaľ ide o nezávislosť, spôsobilosť a neexistenciu konfliktu záujmov. Notifikáciu týchto osôb by mali príslušné vnútroštátne orgány zasielať Komisii a ostatným členským štátom prostredníctvom elektronického nástroja notifikácie vyvinutého a riadeného Komisiou podľa článku R23 rozhodnutia 768/2008.

(66) 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 umelej inteligencie s týmto nariadením (napr. zmena operačného systému alebo softvérovej architektúry), alebo ak sa zmení zamýšľaný účel systému, tento systém umelej inteligencie považoval za nový systém umelej inteligencie, ktorý by sa mal podrobiť novému posudzovaniu zhody. Zmeny algoritmu a výkonnosti systémov umelej inteligencie, ktoré sa po uvedení na trh alebo do prevádzky ďalej „učia“ (t. j. 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.

(67) Vysokorizikové systémy umelej inteligencie by mali niesť označenie CE, ktoré by preukazovalo ich súlad s týmto nariadením, aby im bol umožnený voľný pohyb v rámci vnútorného trhu. Členské štáty by nemali vytvárať neodôvodnené prekážky uvedeniu na trh ani do prevádzky v prípade vysokorizikových systémov umelej inteligencie, ktoré spĺňajú požiadavky stanovené v tomto nariadení a majú označenie CE.

(68) Rýchla dostupnosť inovačných technológií môže mať za určitých podmienok zásadný význam pre zdravie a bezpečnosť osôb a pre spoločnosť ako celok. Je preto vhodné, aby členské štáty mohli z výnimočných dôvodov verejnej bezpečnosti alebo ochrany života a zdravia fyzických osôb a ochrany priemyselného a obchodného vlastníctva povoliť uvedenie na trh alebo do prevádzky v prípade systémov umelej inteligencie, ktoré neboli podrobené posudzovaniu zhody.

(69) S cieľom uľahčiť prácu Komisie a členských štátov v oblasti umelej inteligencie, ako aj zvýšiť transparentnosť voči verejnosti by sa od poskytovateľov vysokorizikových systémov umelej inteligencie, ktoré nesúvisia s výrobkami patriacimi do rozsahu pôsobnosti príslušných existujúcich harmonizačných právnych predpisov Únie, malo vyžadovať, aby seba a informácie o svojom vysokorizikovom systéme umelej inteligencie zaregistrovali v databáze EÚ, ktorú má zriadiť a spravovať Komisia. Pred použitím vysokorizikového systému umelej inteligencie uvedeného v prílohe III sa používatelia vysokorizikových systémov umelej inteligencie, ktorí sú orgánmi verejnej moci, verejnými agentúrami alebo verejnými subjektmi, s výnimkou orgánov presadzovania práva, kontroly hraníc, imigračných alebo azylových orgánov a orgánov, ktoré sú používateľmi vysokorizikových systémov umelej inteligencie v oblasti kritickej infraštruktúry, takisto zaregistrujú v tejto databáze a vyberú si systém, ktorý plánujú používať. Prevádzkovateľom uvedenej databázy by v súlade s nariadením Európskeho parlamentu a Rady (EÚ) 2018/1725[26] mala byť Komisia. Aby sa zaistila plná funkčnosť tejto databázy pri jej zavedení, by postup pri vytváraní databázy mal zahŕňať funkčné špecifikácie vypracované Komisiou a nezávislú audítorskú správu.

[26] 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).

(70) Určité systémy umelej inteligencie určené na interakciu s fyzickými osobami alebo generovanie obsahu môžu predstavovať osobitné riziko podvodu predstieraním identity alebo podvodného konania bez ohľadu na to, či sú klasifikované ako vysokorizikové alebo nie. Preto by používanie týchto systémov malo za určitých okolností podliehať osobitným povinnostiam transparentnosti bez toho, aby boli dotknuté požiadavky a povinnosti týkajúce sa vysokorizikových systémov umelej inteligencie. Konkrétne by fyzické osoby mali byť informované o tom, že komunikujú so systémom umelej inteligencie, pokiaľ to nie je zrejmé z hľadiska fyzickej osoby, ktorá je primerane dobre informovaná, pozorná a obozretná s prihliadnutím na okolnosti a kontext používania. Pri vykonávaní tejto povinnosti by sa mali zohľadniť vlastnosti jednotlivcov, ktorí patria do zraniteľných skupín vzhľadom na ich vek alebo zdravotné postihnutie, a to v rozsahu, v akom je systém umelej inteligencie určený aj na interakciu s týmito skupinami. Okrem toho by fyzické osoby mali byť informované, keď sú vystavené systémom, ktoré spracovaním ich biometrických údajov dokážu identifikovať alebo odvodiť emócie alebo zámery týchto osôb alebo ich zaradiť do konkrétnych kategórií. Takéto osobitné kategórie sa môžu týkať aspektov ako pohlavie, vek, farba vlasov, farba očí, tetovania, osobné črty, etnický pôvod, osobné preferencie a záujmy alebo iné aspekty, ako je sexuálna alebo politická orientácia. Takéto informácie a oznámenia by sa mali poskytovať vo formátoch prístupných pre osoby so zdravotným postihnutím. Používatelia, ktorí používajú systém umelej inteligencie na vytváranie obrazového, zvukového alebo video obsahu alebo na manipuláciu s ním a tento obsah sa očividne podobá existujúcim osobám, miestam alebo udalostiam a nepravdivo na človeka pôsobí ako autentický obsah, by mali zverejniť, že tento obsah bol umelo vytvorený alebo zmanipulovaný, tak, že výstup umelej inteligencie zodpovedajúcim spôsobom označia a zverejnia jeho umelý pôvod. Dodržiavanie uvedených informačných povinností by sa nemalo vykladať tak, že používanie systému alebo jeho výstupov je zákonné podľa tohto nariadenia alebo iných právnych predpisov Únie a členských štátov, a nemali by ním byť dotknuté iné povinnosti týkajúce sa transparentnosti pre používateľov systémov umelej inteligencie stanovené v práve Únie alebo vo vnútroštátnom práve. Nemalo by sa vykladať ani tak, že používanie systému alebo jeho výstupov bráni právu na slobodu prejavu a právu na slobodu umenia a vedeckého bádania, ktoré sú zaručené Chartou základných práv EÚ, najmä ak je obsah súčasťou zjavne kreatívneho, satirického, umeleckého alebo fiktívneho diela alebo programu, s výhradou primeraných záruk pre práva a slobody tretích strán.

(71) Umelá inteligencia je rýchlo sa rozvíjajúca skupina technológií, ktorá si vyžaduje nové formy regulačného dohľadu a bezpečný priestor na experimentovanie, pričom sa musí zabezpečiť, aby inovácia bola zodpovedná a aby boli integrované primerané záruky a opatrenia na zmiernenie rizika. Na zabezpečenie právneho rámca, ktorý bude priaznivý pre inovácie, nadčasový a odolný voči narušeniu, by bolo potrebné podporiť príslušné vnútroštátne orgány jedného alebo viacerých členských štátov, aby zriadili experimentálne regulačné prostredia pre umelú inteligenciu s cieľom uľahčiť vývoj a testovanie inovačných systémov umelej inteligencie pod prísnym regulačným dohľadom skôr, než sa tieto systémy uvedú na trh alebo inak uvedú do prevádzky.

(72) Cieľmi experimentálnych regulačných prostredí pre umelú inteligenciu by mala byť podpora inovácií v oblasti umelej inteligencie vytvorením kontrolovaného experimentačného a testovacieho prostredia vo fáze vývoja a pred uvedením na trh s cieľom zabezpečiť súlad inovačných systémov umelej inteligencie s týmto nariadením a inými príslušnými právnymi predpismi Únie a členských štátov, zvýšiť právnu istotu pre inovátorov, skvalitniť dohľad príslušných orgánov a ich chápanie príležitostí, vznikajúcich rizík a vplyvov používania umelej inteligencie a urýchliť prístup na trhy, a to aj odstránením prekážok pre malé a stredné podniky (MSP) vrátane startupov. Účasť v experimentálnom regulačnom prostredí pre umelú inteligenciu by sa mala zamerať na otázky, ktoré vyvolávajú právnu neistotu pre poskytovateľov a potenciálnych poskytovateľov pri inováciách, experimentovaní s umelou inteligenciou v Únii a prispievaní k regulačnému vzdelávaniu založenému na dôkazoch. Dohľad nad systémami umelej inteligencie v experimentálnom regulačnom prostredí pre umelú inteligenciu by sa preto mal vzťahovať na ich vývoj, trénovanie, testovanie a validáciu pred uvedením systémov na trh alebo do prevádzky, ako aj na pojem podstatnej zmeny a jej výskyty, ktoré si môžu vyžadovať nový postup posudzovania zhody. Príslušné vnútroštátne orgány, ktoré zriaďujú experimentálne regulačné prostredia pre umelú inteligenciu, by mali v prípade potreby spolupracovať s inými príslušnými orgánmi vrátane tých, ktoré dohliadajú na ochranu základných práv, a mohli by umožniť zapojenie ďalších aktérov v rámci ekosystému umelej inteligencie, ako sú vnútroštátne alebo európske normalizačné organizácie, notifikované osoby, testovacie a experimentačné zariadenia, výskumné a experimentačné laboratóriá, inovačné centrá 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 experimentálnych regulačných prostredí a rámec pre spoluprácu medzi príslušnými orgánmi zapojenými do dohľadu nad experimentálnymi prostrediami. Experimentálne regulačné prostredia pre umelú inteligenciu zriadené podľa tohto nariadenia by nemali mať vplyv na iné právne predpisy umožňujúce zriadenie iných experimentálnych prostredí zameraných na zabezpečenie súladu s inými právnymi predpismi, ako je toto nariadenie. v prípade potreby by relevantné príslušné orgány zodpovedné za tieto iné experimentálne regulačné prostredia mali zvážiť výhody používania týchto experimentálnych prostredí aj na účely zabezpečenia súladu systémov umelej inteligencie s týmto nariadením. Na základe dohody medzi príslušnými vnútroštátnymi orgánmi a účastníkmi experimentálneho regulačného prostredia pre umelú inteligenciu sa testovanie v reálnych podmienkach môže vykonávať a môže sa naň dohliadať aj v rámci experimentálneho regulačného prostredia pre umelú inteligenciu.

(-72a) Toto nariadenie by malo poskytnúť právny základ pre používanie osobných údajov, ktoré boli zozbierané na iné účely, účastníkmi experimentálneho regulačného prostredia pre umelú inteligenciu na vývoj určitých systémov umelej inteligencie vo verejnom záujme v rámci experimentálneho regulačného prostredia pre umelú inteligenciu v súlade s článkom 6 ods. 4 a článkom 9 ods. 2 písm. g) nariadenia (EÚ) 2016/679 a článkami 5 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 v platnosti. 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. Účastníci experimentálneho prostredia 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 zmierniť akékoľvek vysoké riziko pre bezpečnosť a základné práva, ktoré môže vzniknúť počas vývoja a experimentovania v experimentálnom prostredí. Pri rozhodovaní o uložení správnej pokuty podľa článku 83 ods. 2 nariadenia 2016/679 a článku 57 smernice 2016/680 by sa malo zohľadniť správanie účastníkov v experimentálnom prostredí.

(72a) S cieľom urýchliť proces vývoja a uvádzania vysokorizikových systémov umelej inteligencie uvedených v prílohe III na trh 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 experimentálneho regulačného prostredia pre umelú inteligenciu. v takýchto prípadoch a pri zohľadnení možných dôsledkov takéhoto testovania na jednotlivcov by sa však 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 získanie informovaného súhlasu bránilo testovaniu systému umelej inteligencie. Súhlas subjektov s účasťou na takomto testovaní podľa tohto nariadenia je odlišný od súhlasu dotknutých osôb so spracúvaním ich osobných údajov podľa príslušných právnych predpisov o ochrane údajov a nemá naň vplyv.

(73) V záujme podpory a ochrany inovácií je dôležité, aby sa osobitne prihliadalo na záujmy poskytovateľov a používateľov systémov umelej inteligencie spomedzi MSP. Na tento účel by členské štáty mali vyvíjať iniciatívy zamerané na týchto prevádzkovateľov vrátane zvyšovania informovanosti a informačnej komunikácie. Aj notifikované osoby zohľadnia pri stanovovaní poplatkov za posudzovanie zhody osobitné záujmy a potreby poskytovateľov spomedzi MSP. Značné náklady pre poskytovateľov a iných, 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 príslušných poskytovateľov a komunikácie s prevádzkovateľmi, bol jazyk, ktorému vo všeobecnosti rozumie čo najväčší počet cezhraničných používateľov.

(73a) S cieľom podporovať a chrániť inovácie by k dosiahnutiu cieľov tohto nariadenia mala prispievať platforma umelej inteligencie na požiadanie a všetky príslušné programy a projekty financovania zo strany EÚ, ako je program Digitálna Európa alebo Horizont Európa, ktoré vykonáva Komisia a členské štáty na vnútroštátnej úrovni alebo na úrovni EÚ.

(74) S cieľom najmä minimalizovať riziká spojené s vykonávaním vyplývajúce z nedostatku poznatkov a odborných znalostí na trhu, ako aj uľahčiť poskytovateľom, najmä MSP, a notifikovaným osobám plnenie ich povinností podľa tohto nariadenia by k vykonávaniu tohto nariadenia mali podľa možnosti prispievať platforma umelej inteligencie na požiadanie, európske centrá digitálnych inovácií a testovacie a experimentačné zariadenia zriadené Komisiou a členskými štátmi na vnútroštátnej úrovni alebo na úrovni EÚ. v rámci svojho príslušného poslania a oblastí pôsobnosti môžu poskytovať najmä technickú a vedeckú podporu poskytovateľom a notifikovaným osobám.

(74a) Okrem toho s cieľom zabezpečiť proporcionalitu vzhľadom na veľmi malú veľkosť niektorých prevádzkovateľov, pokiaľ ide o náklady na inovácie, je vhodné oslobodiť mikropodniky od najnákladnejších povinností, ako je napríklad zavedenie systému riadenia kvality, 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 umelej inteligencie.

(75) Je vhodné, aby Komisia v čo najväčšej možnej miere uľahčila prístup k testovacím a experimentačným 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 nariadenia (EÚ) 2017/745 a nariadenia (EÚ) 2017/746.

(76) Na uľahčenie bezproblémového, účinného a harmonizovaného vykonávania tohto nariadenia by sa mala zriadiť Európska rada pre umelú inteligenciu. Rada by mala odrážať rôzne záujmy ekosystému umelej inteligencie a mala by byť zložená zo zástupcov členských štátov. s cieľom zabezpečiť zapojenie príslušných zainteresovaných strán by sa mala vytvoriť stála podskupina rady. Táto rada by mala byť zodpovedná za niekoľko poradných úloh vrátane vydávania stanovísk, odporúčaní a poradenstva alebo prispievania k usmerneniam v záležitostiach týkajúcich sa vykonávania tohto nariadenia vrátane záležitostí presadzovania, technických špecifikácií alebo existujúcich noriem týkajúcich sa požiadaviek stanovených v tomto nariadení a poskytovania poradenstva Komisii a členským štátom a ich príslušným orgánom v konkrétnych otázkach súvisiacich s umelou inteligenciou. s cieľom poskytnúť členským štátom určitú flexibilitu pri určovaní ich zástupcov v rade pre umelú inteligenciu 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. Výbor by mal 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 a 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 poslaním a úlohami Komisie podľa článku 33 nariadenia (EÚ) 2019/1020 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 podľa potreby zriaďovať ďalšie stále alebo dočasné podskupiny. Rada by mala podľa potreby spolupracovať aj s príslušnými orgánmi EÚ, expertnými skupinami a sieťami pôsobiacimi v kontexte príslušných právnych predpisov EÚ, a to najmä s tými, ktoré sú aktívne podľa príslušných predpisov EÚ o údajoch, digitálnych produktoch a službách.

(76a) Komisia by mala aktívne podporovať členské štáty a prevádzkovateľov pri vykonávaní a presadzovaní tohto nariadenia. v tejto súvislosti by mala vypracovať usmernenia ku konkrétnym témam zamerané na uľahčenie uplatňovania tohto nariadenia, pričom by mala venovať osobitnú pozornosť potrebám MSP a startupov v odvetviach, ktoré budú s najväčšou pravdepodobnosťou ovplyvnené. s cieľom podporiť primerané presadzovanie a kapacity členských štátov by sa mali zriadiť testovacie zariadenia Únie pre umelú inteligenciu a rezerva príslušných expertov, ktoré by sa mali sprístupniť členským štátom.

(77) Pri uplatňovaní a presadzovaní tohto nariadenia zohrávajú kľúčovú úlohu členské štáty. v tejto súvislosti by mal na účely dohľadu nad uplatňovaním a vykonávaním tohto nariadenia každý členský štát určiť jeden alebo viac príslušných vnútroštátnych orgánov. Členské štáty môžu rozhodnúť o vymenovaní akéhokoľvek druhu verejného subjektu na plnenie úloh príslušných vnútroštátnych orgánov v zmysle tohto nariadenia v súlade s ich osobitnými vnútroštátnymi organizačnými charakteristikami a potrebami.

(78) Všetci poskytovatelia vysokorizikových systémov umelej inteligencie by mali mať zavedený systém monitorovania po uvedení na trh, aby zabezpečili, že budú schopní zohľadniť skúsenosti s používaním vysokorizikových systémov umelej inteligencie na zlepšenie svojich systémov a procesu koncipovania a vývoja, alebo aby mohli včas prijať akékoľvek možné nápravné opatrenia. Tento systém je takisto kľúčový na zabezpečenie toho, aby sa možné riziká vyplývajúce zo systémov umelej inteligencie, ktoré sa po uvedení na trh alebo do prevádzky ďalej učia, mohli účinnejšie a včas riešiť. v tejto súvislosti by sa od poskytovateľov malo vyžadovať, aby mali zavedený systém, prostredníctvom ktorého by príslušným orgánom nahlasovali všetky závažné incidenty vyplývajúce z používania ich systémov umelej inteligencie.

(79) S cieľom zabezpečiť primerané a účinné presadzovanie požiadaviek a povinností stanovených v tomto nariadení, ktoré predstavuje harmonizačné právne predpisy 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 podľa tohto nariadenia a nariadenia (EÚ) 2019/1020 a mali by vykonávať svoje právomoci a povinnosti nezávisle, nestranne a bez zaujatosti. Hoci väčšina systémov umelej inteligencie nepodlieha osobitným požiadavkám ani povinnostiam podľa tohto nariadenia, orgány dohľadu nad trhom môžu prijať opatrenia vo vzťahu ku všetkým systémom umelej inteligencie, ak predstavujú riziko v súlade s týmto nariadením. 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 príslušných vnútroštátnych 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.

(79a) 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 nutné pre ich mandát. Na zabezpečenie primeraného a včasného presadzovania v prípade systémov umelej inteligencie, ktoré predstavujú riziko pre zdravie, bezpečnosť a základné práva, by sa mal stanoviť osobitný ochranný postup. Postup pre takéto systémy umelej inteligencie predstavujúce riziko by sa mal uplatňovať na vysokorizikové systémy umelej inteligencie predstavujúce riziko, zakázané systémy, ktoré boli uvedené na trh, do prevádzky alebo používané v rozpore so zakázanými praktikami stanovenými v tomto nariadení, a na systémy umelej inteligencie, ktoré boli sprístupnené v rozpore s požiadavkami na transparentnosť stanovenými v tomto nariadení a predstavujú riziko.

(80) Právne predpisy Únie o finančných službách zahŕňajú pravidlá a požiadavky vnútornej správy a riadenia rizík, ktoré sa vzťahujú na regulované finančné inštitúcie počas poskytovania týchto služieb vrátane prípadov, keď využívajú systémy umelej inteligencie. s cieľom zabezpečiť jednotné uplatňovanie a presadzovanie povinností podľa tohto nariadenia a príslušných pravidiel a požiadaviek právnych predpisov Únie v oblasti finančných služieb by mali byť orgány zodpovedné za dohľad nad právnymi predpismi v oblasti finančných služieb a za ich presadzovanie určené za príslušné orgány na účely dohľadu nad vykonávaním tohto nariadenia vrátane činností dohľadu nad trhom, pokiaľ ide o systémy umelej inteligencie, ktoré poskytujú alebo používajú regulované finančné inštitúcie a finančné inštitúcie podliehajúce dohľadu, pokiaľ členské štáty nerozhodnú o určení iného orgánu na plnenie týchto úloh dohľadu nad trhom. Tieto príslušné orgány by mali mať všetky právomoci podľa tohto nariadenia a nariadenia (EÚ) 2019/1020 o dohľade nad trhom 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 č. 1024/2013, 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 posilnenia súladu medzi týmto nariadením a pravidlami, ktoré sa vzťahujú na úverové inštitúcie regulované podľa smernice Európskeho parlamentu a Rady 2013/36/EÚ[27], je takisto vhodné začleniť niektoré procesné povinnosti poskytovateľov v súvislosti s riadením rizík, monitorovaním po uvedení na trh a dokumentáciou do existujúcich povinností a postupov na základe 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 používateľom vysokorizikových systémov umelej inteligencie, pokiaľ sa vzťahujú na

[27] 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).

úverové inštitúcie regulované smernicou 2013/36/EÚ. Rovnaký režim by sa mal uplatňovať na poisťovne a zaisťovne a holdingové poisťovne podľa smernice 2009/138/EÚ (Solventnosť II) a sprostredkovateľov poistenia podľa smernice (EÚ) 2016/97 a na iné druhy finančných inštitúcií, na ktoré sa vzťahujú požiadavky týkajúce sa vnútornej správy a riadenia spoločnosti, dojednaní alebo postupov stanovených podľa príslušných právnych predpisov Únie v oblasti finančných služieb s cieľom zabezpečiť konzistentnosť a rovnaké zaobchádzanie vo finančnom sektore.

(81) Vývoj systémov umelej inteligencie iných ako vysokorizikových systémov umelej inteligencie v súlade s požiadavkami tohto nariadenia môže viesť k rozsiahlejšiemu využívaniu dôveryhodnej umelej inteligencie v Únii. Poskytovatelia systémov umelej inteligencie, ktoré nie sú vysokorizikové, by sa mali nabádať k tomu, aby vypracúvali kódexy správania určené na podporu dobrovoľného uplatňovania požiadaviek uplatniteľných na vysokorizikové systémy umelej inteligencie prispôsobené zamýšľanému účelu systémov a nižšiemu súvisiacemu riziku. Ďalej by mali byť poskytovatelia povzbudzovaní k tomu, aby dobrovoľne uplatňovali ďalšie požiadavky týkajúce sa napríklad environmentálnej udržateľnosti, prístupnosti pre osoby so zdravotným postihnutím, účasti zainteresovaných strán na koncipovaní a vývoji systémov umelej inteligencie a rozmanitosti vývojových tímov. Komisia môže vypracovať iniciatívy, a to aj odvetvovej povahy, na uľahčenie odstraňovania technických prekážok, ktoré bránia cezhraničnej výmene údajov na účely rozvoja umelej inteligencie, a to aj v oblasti infraštruktúry prístupu k údajom, sémantickej a technickej interoperability rôznych typov údajov.

(82) Je dôležité, aby systémy umelej inteligencie týkajúce sa výrobkov, ktoré nie sú vysokorizikové v súlade s týmto nariadením, a preto sa od nich nevyžaduje, aby spĺňali požiadavky stanovené v tomto nariadení, však boli pri uvádzaní na trh alebo do prevádzky bezpečné. s cieľom prispieť k dosiahnutiu tohto cieľa by sa ako bezpečnostná sieť uplatňovala smernica Európskeho parlamentu a Rady 2001/95/ES[28].

(83) Na zabezpečenie dôveryhodnej a konštruktívnej spolupráce príslušných orgánov na úrovni Únie a na vnútroštátnej úrovni by mali všetky strany zapojené do uplatňovania tohto nariadenia rešpektovať dôvernosť informácií a údajov získaných pri plnení svojich úloh v súlade s právom Únie alebo vnútroštátnym právom.

---

[28] Smernica Európskeho parlamentu a Rady 2001/95/ES z 3. decembra 2001 o všeobecnej bezpečnosti výrobkov (Ú. v. ES L 11, 15.1.2002, s. 4).

(84) 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 to pri dodržaní zásady *ne bis in idem*. v prípade určitých konkrétnych porušení by členské štáty mali zohľadniť rozpätia a kritériá stanovené v tomto nariadení. 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.

(85) 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 harmonizačných právnych predpisov Únie uvedených v prílohe II, vysokorizikových systémov umelej inteligencie uvedených v prílohe III, ustanovení týkajúcich sa technickej dokumentácie uvedených v prílohe IV, obsahu EÚ vyhlásenia o zhode v prílohe V, ustanovení týkajúcich sa postupov posudzovania zhody v prílohách VI a VII a ustanovení, ktorými sa stanovujú systémy umelej inteligencie, na ktoré by sa mal vzťahovať postup posudzovania zhody založený na posúdení systému riadenia kvality a posúdení technickej dokumentácie. Je osobitne dôležité, aby Komisia počas prípravných prác uskutočnila príslušné konzultácie, a to aj na úrovni odborníkov, a aby tieto konzultácie vykonávala v súlade so zásadami stanovenými v Medziinštitucionálnej dohode z 13. apríla 2016 o lepšej tvorbe práva[29]. Predovšetkým, v záujme rovnakého zastúpenia pri príprave delegovaných aktov, sa všetky dokumenty doručujú Európskemu parlamentu a Rade v rovnakom čase ako odborníkom z členských štátov, a odborníci Európskeho parlamentu a Rady majú systematický prístup na zasadnutia skupín odborníkov Komisie, ktoré sa zaoberajú prípravou delegovaných aktov. Takéto konzultácie a poradenská podpora by sa mali vykonávať aj v rámci činností rady pre umelú inteligenciu a jej podskupín.

[29] Ú. v. EÚ L 123, 12.5.2016, s. 1.

(86) 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[30]. Je osobitne dôležité, aby Komisia v súlade so zásadami stanovenými v Medziinštitucionálnej dohode z 13. apríla 2016 o lepšej tvorbe práva vždy, keď sú pri včasnej príprave návrhov vykonávacích aktov potrebné širšie odborné znalosti, podľa potreby využívala expertné skupiny, konzultovala s cieľovými zainteresovanými stranami alebo uskutočnila verejné konzultácie. Takéto konzultácie a poradenská podpora by sa mali vykonávať aj v rámci činností rady pre umelú inteligenciu a jej podskupín vrátane prípravy vykonávacích aktov v súvislosti s článkami 4, 4b a 6.

(87) Keďže cieľ tohto nariadenia nie je možné uspokojivo dosiahnuť na úrovni samotných členských štátov a z dôvodov rozsahu alebo dôsledkov činnosti ho možno lepšie dosiahnuť na úrovni Únie, môže Únia prijať opatrenia v súlade so zásadou subsidiarity podľa článku 5 ZEÚ. v súlade so zásadou proporcionality podľa uvedeného článku toto nariadenie neprekračuje rámec nevyhnutný na dosiahnutie tohto cieľa.

(87a) S cieľom zabezpečiť právnu istotu a primerané adaptačné obdobie pre prevádzkovateľov a zabrániť narušeniu trhu, a to aj zabezpečením kontinuity používania systémov umelej inteligencie, je vhodné, aby sa toto nariadenie uplatňovalo na vysokorizikové systémy umelej inteligencie, ktoré boli uvedené na trh alebo do prevádzky pred všeobecným dátumom jeho uplatňovania, len ak od uvedeného dátumu tieto systémy prešli významnými zmenami ich koncepcie alebo zamýšľaného účelu. Je vhodné spresniť, že v tejto súvislosti by sa pojem významnej zmeny mal chápať tak, že je v podstate rovnocenný s pojmom podstatnej zmeny, ktorý sa používa len v súvislosti s vysokorizikovými systémami umelej inteligencie vymedzenými v tomto nariadení.

[30] 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).

(88) Toto nariadenie by sa malo uplatňovať od ... [*Úrad pre publikácie – vložiť dátum stanovený v článku 85*]. Infraštruktúra súvisiaca so správou a systémom posudzovania zhody by však mala byť funkčná pred uvedeným dátumom, preto by sa ustanovenia o notifikovaných osobách a riadiacej štruktúre mali uplatňovať od ... [*Úrad pre publikácie – vložiť dátum – tri mesiace po nadobudnutí účinnosti tohto nariadenia*]. 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 uplatňovať od [*Úrad pre publikácie – vložiť dátum – dvanásť mesiacov po nadobudnutí účinnosti tohto nariadenia*].

(89) V súlade s článkom 42 ods. 2 nariadenia (EÚ) 2018/1725 sa viedli konzultácie s európskym dozorným úradníkom pre ochranu údajov a Európskym výborom pre ochranu údajov a výsledkom bolo vydanie stanoviska […],

PRIJALI TOTO NARIADENIE:

HLAVA I

VŠEOBECNÉ USTANOVENIA

Článok 1

Predmet úpravy

V tomto nariadení sa stanovujú:

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

a) zákaz určitých praktík v oblasti umelej inteligencie;

b) osobitné požiadavky na vysokorizikové systémy umelej inteligencie a povinnosti prevádzkovateľov takýchto systémov;

c) harmonizované pravidlá transparentnosti pre určité systémy umelej inteligencie;

d) pravidlá monitorovania trhu, dohľadu nad trhom a jeho správy;

e) opatrenia na podporu inovácie.

Článok 2

Rozsah pôsobnosti

1. Toto nariadenie sa vzťahuje na:

a) poskytovateľov uvádzajúcich v Únii na trh alebo do prevádzky systémy umelej inteligencie bez ohľadu na to, či sú títo poskytovatelia fyzicky prítomní alebo usadení v Únii alebo v tretej krajine;

b) používateľov systémov umelej inteligencie, ktorí sú fyzicky prítomní alebo usadení v Únii;

c) poskytovateľov a používateľov systémov umelej inteligencie, ktorí sú fyzicky prítomní alebo usadení v tretej krajine, ak sa výstup vytvorený systémom používa v Únii.

d) dovozcov a distribútorov systémov umelej inteligencie;

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

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

2. Na systémy umelej inteligencie klasifikované v súlade s článkom 6 ods. 1 a 2 ako vysokorizikové systémy umelej inteligencie súvisiace s výrobkami, na ktoré sa vzťahujú harmonizačné právne predpisy Únie uvedené v prílohe II oddiele B, sa vzťahuje len článok 84 tohto nariadenia: Článok 53 sa uplatňuje len vtedy, ak boli požiadavky na vysokorizikové systémy umelej inteligencie podľa tohto nariadenia začlenené do uvedených harmonizačných právnych predpisov Únie.

3. Toto nariadenie sa nevzťahuje na systémy umelej inteligencie, ak sa uvádzajú na trh, uvádzajú do prevádzky alebo sa používajú, či už upravené alebo nie, na účely činností, ktoré nepatria do rozsahu pôsobnosti práva Únie, a v každom prípade na účely vojenských alebo obranných činností alebo činností týkajúcich sa národnej bezpečnosti, a to bez ohľadu na typ subjektu vykonávajúceho tieto činnosti.

   Okrem toho sa toto nariadenie nevzťahuje na systémy umelej inteligencie, ktoré sa neuvádzajú na trh ani do prevádzky v Únii, ak sa výstup používa v Únii na účely činností, ktoré nepatria do rozsahu pôsobnosti práva Únie, a v každom prípade na účely vojenských alebo obranných činností alebo činností týkajúcich sa 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 umelej inteligencie v rámci medzinárodných dohôd o presadzovaní práva a justičnej spolupráci s Úniou alebo s jedným alebo viacerými členskými štátmi.

5. Týmto nariadením nie je dotknuté uplatňovanie ustanovení o zodpovednosti sprostredkovateľov poskytovateľov služieb uvedených v kapitole II oddiele 4 smernice Európskeho parlamentu a Rady 2000/31/ES[31] [*nahradia sa zodpovedajúcimi ustanoveniami aktu o digitálnych službách*].

6. Toto nariadenie sa nevzťahuje na systémy umelej inteligencie vrátane ich výstupov osobitne vyvinutých a uvedených do prevádzky výlučne na účely vedeckého výskumu a vývoja.

7. Toto nariadenie sa nevzťahuje na akúkoľvek výskumnú a vývojovú činnosť týkajúcu sa systémov umelej inteligencie.

8. Toto nariadenie sa nevzťahuje na povinnosti používateľov, ktorí sú fyzickými osobami používajúcimi systémy umelej inteligencie v rámci čisto osobnej neprofesionálnej činnosti, s výnimkou článku 52.

---

[31] Smernica Európskeho parlamentu a Rady 2000/31/ES z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode (smernica o elektronickom obchode) (Ú. v. ES L 178, 17.7.2000, s. 1).

Článok 3

Vymedzenie pojmov

Na účely tohto nariadenia sa uplatňuje toto vymedzenie pojmov:

(1) „systém umelej inteligencie“ je systém, ktorý je navrhnutý tak, aby fungoval s prvkami autonómie, a ktorý na základe údajov a vstupov poskytnutých strojom a/alebo človekom odvodzuje, ako dosiahnuť daný súbor cieľov pomocou strojového učenia a/alebo prístupov založených na logike a znalostiach, a vytvára systémom generované výstupy, ako je obsah (generatívne systémy umelej inteligencie), predpovede, odporúčania alebo rozhodnutia, ktoré ovplyvňujú prostredia, s ktorými systém umelej inteligencie interaguje;

1a. „životný cyklus systému umelej inteligencie“ je trvanie systému umelej inteligencie od návrhu až po vyradenie. Bez toho, aby boli dotknuté právomoci orgánov dohľadu nad trhom, k takémuto vyradeniu môže dôjsť kedykoľvek počas fázy monitorovania po uvedení na trh na základe rozhodnutia poskytovateľa, čo znamená, že systém nemožno ďalej používať. Životný cyklus systému umelej inteligencie sa končí aj podstatnou zmenou systému umelej inteligencie vykonanou poskytovateľom alebo akoukoľvek inou fyzickou alebo právnickou osobou, pričom v takom prípade sa podstatne zmenený systém umelej inteligencie považuje za nový systém umelej inteligencie.

1b. „systém umelej inteligencie na všeobecné účely“ je systém umelej inteligencie, ktorý je, bez ohľadu na to, ako sa uvádza na trh alebo do prevádzky, a to aj ako softvér s otvoreným zdrojovým kódom, určený poskytovateľom na vykonávanie všeobecne uplatniteľných funkcií, ako je rozpoznávanie obrazu alebo reči, generovanie zvuku alebo videa, detekcia vzorov, odpovedanie na otázky, preklad alebo iné; systém umelej inteligencie na všeobecné účely sa môže používať v rôznych kontextoch a môže byť integrovaný do rôznych iných systémov umelej inteligencie;

(2) „poskytovateľ“ je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý vyvíja systém umelej inteligencie alebo ktorý má systém umelej inteligencie vyvinutý a uvádza tento systém na trh alebo do prevádzky pod vlastným menom alebo ochrannou známkou, či už za odplatu alebo bezodplatne;

(3) [vypúšťa sa];

3a. „malé a stredné podniky“ (ďalej len „MSP“) sú podniky v zmysle prílohy k odporúčaniu Komisie 2003/361/ES o vymedzení pojmov mikropodniky, malé a stredné podniky;

(4) „používateľ“ je každá fyzická alebo právnická osoba vrátane orgánu verejnej moci, agentúra alebo iný subjekt, v ktorého právomoci sa systém umelej inteligencie používa;

(5) „splnomocnený zástupca“ je každá fyzická alebo právnická osoba fyzicky prítomná alebo usadená v Únii, ktorá od poskytovateľa systému umelej inteligencie dostala a akceptovala písomné splnomocnenie v jeho mene plniť povinnosti a vykonávať postupy stanovené týmto nariadením;

5a. „výrobca výrobku“ je výrobca v zmysle ktoréhokoľvek z harmonizačných právnych predpisov Únie uvedených v prílohe II;

(6) „dovozca“ je každá fyzická alebo právnická osoba fyzicky prítomná alebo usadená v Únii, ktorá uvádza na trh systém umelej inteligencie, ktorý je označený menom alebo ochrannou známkou fyzickej alebo právnickej osoby usadenej mimo Únie;

(7) „distribútor“ je každá fyzická alebo právnická osoba v dodávateľskom reťazci okrem poskytovateľa alebo dovozcu, ktorá na trhu Únie sprístupňuje systém umelej inteligencie;

(8) „prevádzkovateľ“ je poskytovateľ, výrobca výrobku, používateľ, splnomocnený zástupca, dovozca alebo distribútor;

(9) „uvedenie na trh“ je prvé sprístupnenie systému umelej inteligencie na trhu Únie;

(10) „sprístupnenie na trhu“ je každá dodávka systému umelej inteligencie na účely distribúcie alebo používania na trhu Únie v rámci obchodnej činnosti, či už za odplatu, alebo bezodplatne;

(11) „uvedenie do prevádzky“ je dodanie systému umelej inteligencie na prvé použitie priamo používateľovi alebo na vlastné použitie v Únii na zamýšľaný účel;

(12) „zamýšľaný účel“ je použitie systému umelej inteligencie, ktoré určil poskytovateľ, vrátane osobitného 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) „logicky predvídateľné nesprávne použitie“ je také použitie systému umelej inteligencie, ktoré nie je v súlade so zamýšľaným účelom, ale ktoré môže byť výsledkom logicky predvídateľného ľudského správania alebo interakcie s inými systémami;

(14) „bezpečnostný komponent výrobku alebo systému“ je komponent výrobku alebo systému, ktorý pre daný výrobok alebo systém 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 používateľa najmä o zamýšľanom účele a správnom používaní systému umelej inteligencie;

(16) „stiahnutie systému umelej inteligencie od používateľa“ je každé opatrenie zamerané na to, aby sa systém umelej inteligencie sprístupnený používateľovi vrátil poskytovateľovi, aby sa stiahol z prevádzky alebo aby sa znemožnilo jeho používanie;

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

(18) „výkonnosť systému umelej inteligencie“ je schopnosť systému umelej inteligencie dosiahnuť zamýšľaný účel;

(19) „posudzovanie zhody“ je postup overovania, či boli splnené požiadavky stanovené v hlave III kapitole 2 tohto nariadenia týkajúce sa vysokorizikového systému umelej inteligencie;

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

(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 určený v súlade s týmto nariadením a inými relevantnými harmonizačnými právnymi predpismi Únie;

(23) „podstatná zmena“ je zmena systému umelej inteligencie po jeho uvedení na trh alebo do prevádzky, ktorá ovplyvňuje súlad systému umelej inteligencie s požiadavkami stanovenými v hlave III kapitole 2 tohto nariadenia alebo zmena zamýšľaného účelu, na aký bol systém umelej inteligencie posudzovaný; v prípade vysokorizikových systémov umelej inteligencie, ktoré sa po uvedení na trh alebo do prevádzky ďalej učia, nepredstavujú zmeny vysokorizikového systému umelej inteligencie 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), podstatnú zmenu.

(24) „označenie CE“ je označenie, ktorým poskytovateľ vyjadruje, že systém umelej inteligencie je v zhode s požiadavkami stanovenými v hlave III kapitole 2 alebo v článku 4b tohto nariadenia tohto nariadenia a v iných uplatniteľných právnych aktoch Únie, ktorými sa harmonizujú podmienky uvádzania výrobkov na trh (ďalej len „harmonizačné právne predpisy Únie“) a v ktorých sa stanovuje umiestňovanie tohto označenia;

(25) „systém monitorovania po uvedení na trh“ sú všetky činnosti, ktoré vykonávajú poskytovatelia systémov umelej inteligencie na zhromažďovanie a skúmanie skúseností získaných z používania systémov umelej inteligencie, 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 európska norma podľa vymedzenia v článku 2 ods. 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 ustanovenými v tomto nariadení;

(29) „trénovacie údaje“ sú údaje, ktoré sa používajú na trénovanie systému umelej inteligencie adaptáciou jeho parametrov, ktoré sa dajú naučiť;

(30) „validačné údaje“ sú údaje, ktoré sa používajú na vyhodnotenie natrénovaného systému umelej inteligencie a na doladenie jeho parametrov, ktoré sa nedajú naučiť, a jeho procesu učenia, okrem iného s cieľom zabrániť pretrénovaniu, pričom súbor validačných údajov môže byť samostatný súbor údajov alebo časť súboru trénovacích údajov, a to buď v pevnom alebo variabilnom rozdelení;

(31) „testovacie údaje“ sú údaje, ktoré sa používajú na nezávislé hodnotenie natrénovaného a zvalidovaného systému umelej inteligencie s cieľom potvrdiť očakávanú výkonnosť tohto systému pred jeho uvedením na trh alebo do prevádzky;

(32) „vstupné údaje“ sú údaje poskytnuté systému umelej inteligencie alebo priamo získané týmto systémom, na základe ktorých systém vytvára výstup;

(33) „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;

(34) „systém na rozpoznávanie emócií“ je systém umelej inteligencie na účely identifikácie alebo odvodenia psychologických stavov, emócií alebo úmyslov fyzických osôb na základe ich biometrických údajov;

(35) „systém biometrickej kategorizácie“ je systém umelej inteligencie na účely zaraďovania fyzických osôb do špecifických kategórií na základe ich biometrických údajov;

(36) „systém diaľkovej biometrickej identifikácie“ je systém umelej inteligencie na účely identifikácie fyzických osôb zvyčajne na diaľku, bez ich aktívneho zapojenia, prostredníctvom porovnania biometrických údajov osoby s biometrickými údajmi obsiahnutými v referenčnom registri údajov;

(37) „systém diaľkovej biometrickej identifikácie v reálnom čase“ je systém diaľkovej biometrickej identifikácie, v ktorom zachytávanie biometrických údajov, ich porovnávanie a identifikácia prebiehajú okamžite alebo takmer okamžite;

(38) [vypúšťa sa]

(39) „verejne prístupný priestor“ je akékoľvek verejné fyzické miesto alebo fyzické miesto v súkromnom vlastníctve prístupné neurčenému počtu fyzických osôb bez ohľadu na to, či boli vopred stanovené určité podmienky alebo okolnosti prístupu, a bez ohľadu na možné obmedzenia kapacity;

(40) „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;

(41) „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;

(42) [vypúšťa sa]

(43) „príslušný vnútroštátny orgán“ je notifikujúci orgán a orgán dohľadu nad trhom; Pokiaľ ide o systémy umelej inteligencie uvedené do prevádzky alebo používané inštitúciami, agentúrami, úradmi a orgánmi EÚ, povinnosti, ktoré sú v členských štátoch zverené príslušnému vnútroštátnemu orgánu, plní európsky dozorný úradník pre ochranu údajov a každý odkaz na príslušné vnútroštátne orgány alebo orgány dohľadu nad trhom v tomto nariadení sa podľa potreby chápe ako odkaz na európskeho dozorného úradníka pre ochranu údajov;

(44) „závažný incident“ je každý incident alebo porucha systému umelej inteligencie, ktorá priamo alebo nepriamo vyústi do ktorejkoľvek z týchto situácií:

a) smrť osoby alebo vážne poškodenie zdravia osoby;

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

c) porušenia povinností vyplývajúcich z právnych predpisov Únie, ktorých cieľom je ochrana základných práv;

d) vážne poškodenie majetku alebo životného prostredia;

(45) „kritická infraštruktúra“ je aktívum, systém alebo jeho časť, ktoré sú potrebné na poskytovanie služby, ktorá má zásadný význam z hľadiska zachovania životne dôležitých spoločenských funkcií alebo hospodárskych činností v zmysle článku 2 ods. 4 a 5 smernice o odolnosti kritických subjektov;

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

(47) „iné ako osobné údaje“ sú údaje iné ako osobné údaje vymedzené v článku 4 bode 1 nariadenia (EÚ) 2016/679;

(48) „testovanie v reálnych podmienkach“ je dočasné testovanie systému umelej inteligencie na zamýšľaný účel v reálnych podmienkach mimo laboratória alebo inak simulovaného prostredia s cieľom zhromaždiť spoľahlivé a robustné údaje a posúdiť a overiť súlad systému umelej inteligencie s požiadavkami tohto nariadenia; testovanie v reálnych podmienkach sa nepovažuje za uvedenie systému umelej inteligencie na trh alebo do prevádzky v zmysle tohto nariadenia za predpokladu, že sú splnené všetky podmienky podľa článku 53 alebo 54a;

(49) „plán testovania v reálnych podmienkach“ je dokument, ktorý opisuje ciele, metodiku, geografický, populačný a časový rozsah pôsobnosti, monitorovanie, organizáciu a vykonávanie testovania v reálnych podmienkach;

(50) „účastník“ na účely testovania v reálnom svete je fyzická osoba, ktorá sa zúčastňuje na testovaní v reálnych podmienkach;

(51) „informovaný súhlas“ je slobodné a dobrovoľné vyjadrenie vôle účastníka zúčastniť sa na konkrétnom testovaní v reálnych podmienkach po tom, ako bol informovaný o všetkých aspektoch testovania, ktoré sú relevantné pre jeho rozhodnutie zúčastniť sa; v prípade maloletých osôb a právne nespôsobilých účastníkov poskytuje informovaný súhlas ich zákonom určený zástupca;

(52) „experimentálne regulačné prostredie pre umelú inteligenciu“ je konkrétny rámec zriadený príslušným vnútroštátnym orgánom, ktorý ponúka poskytovateľom alebo potenciálnym poskytovateľom systémov umelej inteligencie možnosť vyvíjať, trénovať, validovať a testovať, ak je to vhodné v reálnych podmienkach, inovačný systém umelej inteligencie podľa konkrétneho plánu na obmedzený čas pod regulačným dohľadom.

Článok 4

Vykonávacie akty

S cieľom zabezpečiť jednotné podmienky vykonávania tohto nariadenia, pokiaľ ide o prístupy strojového učenia a prístupy založených na logike a znalostiach uvedené v článku 3 ods. 1, môže Komisia prijať vykonávacie akty s cieľom spresniť technické prvky týchto prístupov, pričom zohľadní vývoj na trhu a technologický vývoj. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 74 ods. 2.

HLAVA IA

SYSTÉMY UMELEJ INTELIGENCIE NA VŠEOBECNÉ ÚČELY

Článok 4a

Súlad systémov umelej inteligencie na všeobecné účely s týmto nariadením

1. Bez toho, aby boli dotknuté články 5, 52, 53 a 69 tohto nariadenia, systémy umelej inteligencie na všeobecné účely spĺňajú len požiadavky a povinnosti stanovené v článku 4b.

2. Takéto požiadavky a povinnosti sa uplatňujú bez ohľadu na to, či sa systém umelej inteligencie na všeobecné účely uvádza na trh alebo do prevádzky ako vopred trénovaný model a či má ďalšie doladenie modelu vykonať používateľ systému umelej inteligencie na všeobecné účely.

Článok 4b

Požiadavky na systémy umelej inteligencie na všeobecné účely a povinnosti poskytovateľov takýchto systémov

1. Systémy umelej inteligencie na všeobecné účely, ktoré sa môžu používať ako vysokorizikové systémy umelej inteligencie alebo ako komponenty vysokorizikových systémov umelej inteligencie v zmysle článku 6, musia spĺňať požiadavky stanovené v hlave III kapitole 2 tohto nariadenia odo dňa začatia uplatňovania vykonávacích aktov prijatých Komisiou v súlade s postupom preskúmania uvedeným v článku 74 ods. 2 najneskôr 18 mesiacov po nadobudnutí účinnosti tohto nariadenia. v uvedených vykonávacích aktoch sa spresní a prispôsobí uplatňovanie požiadaviek stanovených v hlave III kapitole 2 na systémy umelej inteligencie na všeobecné účely vzhľadom na ich vlastnosti, technickú uskutočniteľnosť, osobitosti hodnotového reťazca umelej inteligencie a trhový a technologický vývoj. Pri plnení týchto požiadaviek sa zohľadňuje všeobecne uznávaný najnovší technologický stav.

2. Poskytovatelia systémov umelej inteligencie na všeobecné účely uvedených v odseku 1 musia od dátumu začatia uplatňovania vykonávacích aktov uvedených v odseku 1 plniť povinnosti stanovené v článkoch 16aa, 16e, 16f, 16g, 16i, 16j, 25, 48 a 61.

3. Na účely splnenia povinností stanovených v článku 16e poskytovatelia dodržiavajú postup posudzovania zhody založený na vnútornej kontrole stanovený v prílohe VI bodoch 3 a 4.

4. Poskytovatelia takýchto systémov tiež uchovávajú technickú dokumentáciu uvedenú v článku 11 pre potreby príslušných vnútroštátnych orgánov počas obdobia, ktoré sa končí desať rokov po uvedení systému umelej inteligencie na všeobecný účel na trh Únie alebo jeho uvedení do prevádzky v Únii.

5. Poskytovatelia systémov umelej inteligencie na všeobecné účely spolupracujú s inými poskytovateľmi, ktorí majú v úmysle uviesť takéto systémy do prevádzky alebo na trh Únie ako vysokorizikové systémy umelej inteligencie alebo ako komponenty vysokorizikových systémov umelej inteligencie, a poskytujú im potrebné informácie, aby im umožnili plniť si povinnosti podľa tohto nariadenia. Pri takejto spolupráci medzi poskytovateľmi sa podľa potreby zachovávajú práva duševného vlastníctva a dôverné obchodné informácie alebo obchodné tajomstvá v súlade s článkom 70. s cieľom zabezpečiť jednotné podmienky vykonávania tohto nariadenia, pokiaľ ide o informácie, ktoré si majú vymieňať poskytovatelia systémov umelej inteligencie na všeobecné účely, môže Komisia prijať vykonávacie akty v súlade s postupom preskúmania uvedeným v článku 74 ods. 2.

6. Pri plnení požiadaviek a povinností uvedených v odsekoch 1, 2 a 3:

– akýkoľvek odkaz na zamýšľaný účel sa chápe ako odkaz na možné použitie systémov umelej inteligencie na všeobecné účely ako vysokorizikových systémov umelej inteligencie alebo ako komponentov vysokorizikových systémov umelej inteligencie v zmysle článku 6,

– akýkoľvek odkaz na požiadavky na vysokorizikové systémy umelej inteligencie v hlave III kapitole II sa chápe ako odkaz len na požiadavky stanovené v tomto článku.

Článok 4c

Výnimky z článku 4b

1. Článok 4b sa neuplatňuje, ak poskytovateľ v návode na použitie alebo v informáciách sprevádzajúcich systém umelej inteligencie na všeobecné účely výslovne vylúčil všetky vysokorizikové použitia.

2. Takéto vylúčenie sa vykoná v dobrej viere a nepovažuje sa za opodstatnené, ak má poskytovateľ dostatočné dôvody domnievať sa, že systém môže byť zneužitý.

3. Ak poskytovateľ zistí zneužitie na trhu alebo o ňom nadobudne vedomosť, prijme všetky potrebné a primerané opatrenia, aby zabránil takémuto ďalšiemu zneužívaniu, najmä s prihliadnutím na rozsah zneužitia a závažnosť súvisiacich rizík.

HLAVA II

ZAKÁZANÉ PRAKTIKY v OBLASTI UMELEJ INTELIGENCIE

Článok 5

1. Zakazujú sa tieto praktiky v oblasti umelej inteligencie:

a) uvádzanie na trh, uvádzanie do prevádzky alebo používanie systému umelej inteligencie, ktorý využíva podprahové techniky mimo vedomia osoby s cieľom alebo účinkom podstatne narušiť správanie osoby tak, že tejto alebo inej osobe spôsobí alebo by s primeranou pravdepodobnosťou mohol spôsobiť fyzickú alebo psychickú ujmu;

b) uvádzanie na trh, uvádzanie do prevádzky alebo používanie systému umelej inteligencie, ktorý využíva ktorúkoľvek zo zraniteľností osobitnej skupiny osôb vyplývajúcich z ich veku, zdravotného postihnutia alebo osobitnej sociálnej alebo ekonomickej situácie s cieľom alebo účinkom podstatne narušiť správanie osoby patriacej do tejto skupiny osôb tak, že tejto alebo inej osobe spôsobí alebo by s primeranou pravdepodobnosťou mohol spôsobiť fyzickú alebo psychickú ujmu;

c) uvádzanie na trh, uvádzanie do prevádzky alebo používanie systémov umelej inteligencie na účely hodnotenia alebo klasifikácie fyzických osôb počas určitého obdobia na základe ich spoločenského správania alebo známych či predpokladaných osobných alebo osobnostných charakteristík, pričom takto získané sociálne skóre vedie k jednému alebo obidvom z týchto výsledkov:

i) škodlivé alebo nepriaznivé zaobchádzanie s určitými fyzickými osobami alebo skupinami fyzických osôb v sociálnych kontextoch, ktoré nesúvisia s kontextmi, v ktorých boli údaje pôvodne generované alebo zhromaždené;

ii) škodlivé alebo nepriaznivé zaobchádzanie s určitými fyzickými osobami alebo skupinami fyzických osôb, ktoré je neodôvodnené alebo neprimerané ich spoločenskému správaniu alebo jeho závažnosti;

d) používanie systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch orgánmi presadzovania práva alebo v ich mene na účely presadzovania práva, pokiaľ takéto použitie nie je nevyhnutne a v nutnej miere potrebné na jeden z týchto cieľov:

i) cielené pátranie po konkrétnych potenciálnych obetiach trestných činov;

ii) predchádzanie konkrétnemu a závažnému ohrozeniu kritickej infraštruktúry, života, zdravia alebo fyzickej bezpečnosti fyzických osôb alebo predchádzanie teroristickým útokom;

iii) lokalizácia alebo identifikácia fyzickej osoby na účely vedenia vyšetrovania, stíhania alebo výkonu trestnej sankcie za trestné činy uvedené v článku 2 ods. 2 rámcového rozhodnutia Rady 2002/584/SVV[32], za ktoré možno v dotknutom členskom štáte uložiť trest odňatia slobody alebo ochranné opatrenie obmedzujúce slobodu s hornou hranicou trestnej sadzby najmenej tri roky, alebo iné osobitné trestné činy, za ktoré možno v dotknutom členskom štáte uložiť trest odňatia slobody alebo ochranné opatrenie obmedzujúce slobodu s hornou hranicou trestnej sadzby najmenej päť rokov, ako sa stanovuje v práve daného členského štátu.

2. Pri používaní systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva na dosiahnutie ktoréhokoľvek z cieľov uvedených v odseku 1 písm. d) sa musia zohľadniť tieto prvky:

a) povaha situácie, ktorá viedla k možnému použitiu, najmä závažnosť, pravdepodobnosť a rozsah poškodenia spôsobeného v prípade nepoužitia systému;

[32] 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).

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 písm. d) musí okrem toho byť v súlade s nevyhnutnými a primeranými zárukami a podmienkami týkajúcimi sa tohto používania, najmä pokiaľ ide o časové, geografické a osobné obmedzenia.

3. Pokiaľ ide o odsek 1 písm. d) a odsek 2, podlieha každé použitie systému diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva predchádzajúcemu povoleniu udelenému súdnym orgánom alebo nezávislým správnym orgánom členského štátu, v ktorom sa má použitie uskutočniť, vydanému na základe odôvodnenej žiadosti a v súlade s podrobnými pravidlami vnútroštátneho práva uvedenými v odseku 4. v riadne odôvodnenej naliehavej situácii sa však používanie systému môže začať bez povolenia za predpokladu, že o takéto povolenie sa požiada bez zbytočného odkladu počas používania systému umelej inteligencie, a ak sa takéto povolenie zamietne, jeho používanie sa s okamžitým účinkom zastaví.

Príslušný súdny alebo správny orgán 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 jedného z cieľov uvedených v odseku 1 písm. d), ako sa uvádza v žiadosti. Pri rozhodovaní o žiadosti príslušný súdny alebo správny orgán zohľadní prvky uvedené v odseku 2.

4. Členský štát sa môže rozhodnúť, že na účely presadzovania práva v rámci obmedzení a za podmienok uvedených v odseku 1 písm. d) a odsekoch 2 a 3 stanoví možnosť úplne alebo čiastočne povoliť používanie systému diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch. Tento členský štát vo svojom vnútroštátnom práve stanoví 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 písm. d) a s ktorým z trestných činov uvedených v jeho bode iii) môžu byť príslušné orgány oprávnené používať tieto systémy na účely presadzovania práva.

HLAVA III

VYSOKORIZIKOVÉ SYSTÉMY UMELEJ INTELIGENCIE

KAPITOLA 1

KLASIFIKÁCIA SYSTÉMOV UMELEJ INTELIGENCIE AKO VYSOKORIZIKOVÝCH SYSTÉMOV

Článok 6

Pravidlá klasifikácie vysokorizikových systémov umelej inteligencie

1. Systém umelej inteligencie, ktorý je sám osebe výrobkom, na ktorý sa vzťahujú harmonizačné právne predpisy Únie uvedené v prílohe II, sa považuje za vysokorizikový, ak sa podľa uvedených právnych predpisov na jeho uvedenie na trh alebo do prevádzky vyžaduje jeho posúdenie zhody treťou stranou.

2. Systém umelej inteligencie určený na používanie ako bezpečnostný komponent výrobku, na ktorý sa vzťahujú právne predpisy uvedené v odseku 1, sa považuje za vysokorizikový, ak sa podľa uvedených právnych predpisov na jeho uvedenie na trh alebo do prevádzky vyžaduje jeho posúdenie zhody treťou stranou. Toto ustanovenie sa uplatňuje bez ohľadu na to, či sa systém umelej inteligencie uvádza na trh alebo do prevádzky nezávisle od výrobku.

3. Systémy umelej inteligencie uvedené v prílohe III sa považujú za vysokorizikové, pokiaľ výstup systému nie je čisto doplnkový vzhľadom na príslušné opatrenie alebo rozhodnutie, ktoré sa má prijať, a preto nie je pravdepodobné, že by viedol k významnému riziku pre zdravie, bezpečnosť alebo základné práva.

S cieľom zabezpečiť jednotné podmienky vykonávania tohto nariadenia Komisia najneskôr do jedného roka od nadobudnutia účinnosti tohto nariadenia prijme vykonávacie akty s cieľom spresniť okolnosti, za ktorých by výstup systémov umelej inteligencie uvedených v prílohe III bol čisto doplnkový vzhľadom na príslušné opatrenie alebo rozhodnutie, ktoré sa má prijať. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 74 ods. 2.

Článok 7

Zmeny prílohy III

1. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 73 s cieľom upravovať zoznam v prílohe III doplnením vysokorizikových systémov umelej inteligencie, ak sú splnené obe tieto podmienky:

   a) systémy umelej inteligencie sú určené na používanie v ktorejkoľvek z oblastí uvedených v prílohe III bodoch 1 až 8;

   b) systémy umelej inteligencie predstavujú riziko poškodenia zdravia a bezpečnosti alebo riziko nepriaznivého vplyvu na základné práva, ktoré je vzhľadom na svoju závažnosť a pravdepodobnosť výskytu prinajmenšom rovnocenné riziku poškodenia alebo nepriaznivého vplyvu, ktoré predstavujú vysokorizikové systémy umelej inteligencie už uvedené v prílohe III.

2. Pri posudzovaní toho, či systém umelej inteligencie predstavuje na účely odseku 1 riziko poškodenia zdravia a bezpečnosti alebo riziko nepriaznivého vplyvu na základné práva, ktoré je prinajmenšom rovnocenné riziku poškodenia, ktoré predstavujú vysokorizikové systémy umelej inteligencie už uvedené v prílohe III, zohľadní Komisia tieto kritériá:

a) zamýšľaný účel systému umelej inteligencie;

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

c) rozsah, v akom používanie systému umelej inteligencie už spôsobilo poškodenie zdravia a bezpečnosti alebo nepriaznivý vplyv na základné práva, alebo vyvolalo vážne obavy v súvislosti s naplnením takéhoto poškodenia alebo nepriaznivého vplyvu, preukázaný správami alebo zdokumentovanými tvrdeniami predloženými príslušným vnútroštátnym orgánom;

d) potenciálny rozsah takéhoto poškodenia alebo nepriaznivého vplyvu, najmä pokiaľ ide o jeho intenzitu a schopnosť zasiahnuť značný počet osôb;

e) rozsah, v akom sú potenciálne poškodené alebo nepriaznivo ovplyvnené osoby závislé od výsledku vytvoreného systémom umelej inteligencie, najmä preto, že z praktických alebo právnych dôvodov nie je odôvodnene možné sa na tomto výsledku nepodieľať;

f) rozsah, v akom sú potenciálne poškodené alebo nepriaznivo ovplyvnené osoby vo vzťahu k používateľovi systému umelej inteligencie v zraniteľnom postavení, najmä v dôsledku nerovnováhy moci, znalostí, hospodárskych alebo sociálnych okolností alebo veku;

g) rozsah, v akom sa výsledok vytvorený systémom umelej inteligencie dá len ťažko zvrátiť, pričom výsledky, ktoré majú vplyv na zdravie alebo bezpečnosť osôb, sa nepovažujú za také, ktoré sa dajú ľahko zvrátiť;

h) rozsah, v akom sa v existujúcich právnych predpisoch Únie stanovujú:

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

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

i) rozsah a pravdepodobnosť prínosu používania umelej inteligencie pre jednotlivcov, skupiny alebo spoločnosť ako celok.

3. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 73 s cieľom upravovať zoznam v prílohe III vypustením vysokorizikových systémov umelej inteligencie, ak sú splnené obe tieto podmienky:

a) dotknutý vysokorizikový systém alebo systémy umelej inteligencie už nepredstavujú 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.

KAPITOLA 2

POŽIADAVKY NA VYSOKORIZIKOVÉ SYSTÉMY UMELEJ INTELIGENCIE

Článok 8

Súlad s požiadavkami

1. Vysokorizikové systémy umelej inteligencie musia spĺňať požiadavky stanovené v tejto kapitole s prihliadnutím na všeobecne uznávaný najnovší technologický stav.

2. Pri zabezpečovaní súladu s týmito požiadavkami sa zohľadňuje zamýšľaný účel vysokorizikového systému umelej inteligencie a systém riadenia rizík uvedený v článku 9.

Článok 9

Systém riadenia rizík

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

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

   a) identifikácia a analýza známych a predvídateľných rizík, ktoré vzhľadom na zamýšľaný účel vysokorizikového systému umelej inteligencie môžu s najväčšou pravdepodobnosťou nastať v oblasti zdravia, bezpečnosti a základných práv;

   b) [vypúšťa sa];

   c) hodnotenie ďalších možných vznikajúcich rizík na základe analýzy údajov získaných zo systému monitorovania po uvedení na trh uvedeného v článku 61;

   d) prijatie vhodných opatrení na riadenie rizík v súlade s ustanoveniami nasledujúcich odsekov.

   Riziká uvedené v tomto odseku sa týkajú len tých, ktoré možno primerane zmierniť alebo odstrániť vývojom alebo návrhom vysokorizikového systému umelej inteligencie alebo poskytnutím primeraných technických informácií.

3. 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 tejto kapitole 2 s cieľom účinnejšie minimalizovať riziká a zároveň dosiahnuť primeranú rovnováhu pri vykonávaní opatrení na splnenie týchto požiadaviek.

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

Pri určovaní najvhodnejších opatrení na riadenie rizík sa zabezpečí:

a) odstránenie alebo zníženie rizík identifikovaných a hodnotených podľa odseku 2, pokiaľ je to možné prostredníctvom primeraného návrhu a vývoja vysokorizikového systému umelej inteligencie;

b) prípadné zavedenie primeraných zmierňujúcich a kontrolných opatrení v súvislosti s rizikami, ktoré nemožno odstrániť;

c) poskytovanie primeraných informácií podľa článku 13, najmä pokiaľ ide o riziká uvedené v odseku 2 písm. b) tohto článku, a prípadne odborná príprava pre používateľov.

V záujme odstraňovania alebo obmedzovania rizík súvisiacich s používaním vysokorizikového systému umelej inteligencie sa náležite zohľadnia technické znalosti, skúsenosti, vzdelanie, odborná príprava, ktoré sa očakávajú od používateľa, ako aj prostredie, v ktorom sa má systém používať.

5. Testovaním vysokorizikových systémov umelej inteligencie sa zabezpečí, aby fungovali v súlade so zamýšľaným účelom a spĺňali požiadavky stanovené v tejto kapitole.

6. Testovacie postupy môžu zahŕňať testovanie v reálnych podmienkach v súlade s článkom 54a.

7. Testovanie vysokorizikových systémov umelej inteligencie sa vykonáva podľa potreby kedykoľvek počas celého procesu vývoja a v každom prípade pred 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 umelej inteligencie.

8. V systéme riadenia rizík opísanom v odsekoch 1 až 7 sa osobitne zohľadní to, či je pravdepodobné, že k vysokorizikovému systému umelej inteligencie budú mať prístup osoby mladšie ako 18 rokov alebo že tieto systémy budú mať na ne vplyv.

9. V prípade poskytovateľov vysokorizikových systémov umelej inteligencie, na ktorých sa vzťahujú požiadavky týkajúce sa vnútorných procesov riadenia rizík podľa príslušného odvetvového práva Únie, môžu byť aspekty opísané v odsekoch 1 až 8 súčasťou postupov riadenia rizík ustanovených podľa uvedeného práva.

Článok 10

Údaje a správa údajov

1. Vysokorizikové systémy umelej inteligencie, ktoré využívajú techniky zahŕňajúce trénovanie modelov s údajmi, sa musia vyvíjať na základe súborov trénovacích, validačných a testovacích údajov, ktoré spĺňajú kritériá kvality uvedené v odsekoch 2 až 5.

2. Pre súbory trénovacích, validačných a testovacích údajov musia platiť primerané postupy správy a riadenia údajov. Tieto postupy sa týkajú najmä:

   a) príslušných rozhodnutí o koncepčných riešeniach;

   b) procesov zberu údajov;

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

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

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

f) preskúmania z hľadiska možných skreslení, ktoré pravdepodobne ovplyvnia zdravie a bezpečnosť fyzických osôb alebo viesť k diskriminácii, ktorú právo Únie zakazuje;

g) identifikácie prípadných medzier alebo nedostatkov v údajoch a spôsobu, akým možno tieto medzery a nedostatky odstrániť.

3. Súbory trénovacích, validačných a testovacích údajov musia byť relevantné, reprezentatívne a v najväčšej možnej miere bezchybné a úplné. Musia mať primerané štatistické vlastnosti, a to prípadne aj pokiaľ ide o osoby alebo skupiny osôb, v prípade ktorých sa má vysokorizikový systém umelej inteligencie používať. Tieto charakteristiky súborov údajov sa môžu splniť na úrovni jednotlivých súborov údajov alebo ich kombinácie.

4. Súbory trénovacích, validačných a testovacích údajov musia, pokiaľ si to vyžaduje zamýšľaný účel, zohľadňovať vlastnosti alebo prvky, ktoré sú špecifické pre konkrétne geografické, behaviorálne alebo funkčné podmienky, v ktorých sa má vysokorizikový systém umelej inteligencie používať.

5. Pokiaľ je to nevyhnutne potrebné na účely zabezpečenia monitorovania, odhaľovania a nápravy skreslenia v súvislosti s vysokorizikovými systémami umelej inteligencie, poskytovatelia takýchto systémov môžu spracúvať osobitné 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, a to pod podmienkou primeraných záruk pre základné práva a slobody fyzických osôb, ku ktorým patria aj technické obmedzenia opätovného použitia a používanie najmodernejších opatrení v oblasti bezpečnosti a ochrany súkromia, ako je pseudonymizácia alebo šifrovanie v prípadoch, v ktorých anonymizácia môže významne ovplyvniť sledovaný účel.

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

Článok 11

Technická dokumentácia

1. Pred uvedením vysokorizikového systému umelej inteligencie 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 umelej inteligencie spĺňa požiadavky stanovené v tejto kapitole, a aby sa príslušným vnútroštátnym orgánom a notifikovaným osobám poskytli v jasnej a komplexnej podobe všetky informácie potrebné na posúdenie súladu systému umelej inteligencie s uvedenými požiadavkami. Musí obsahovať aspoň prvky stanovené v prílohe IV alebo v prípade MSP vrátane startupov akúkoľvek rovnocennú dokumentáciu, ktorá dosahuje rovnaké ciele, za predpokladu, že to príslušný orgán nepovažuje za neprimerané.

2. Ak sa na trh alebo do prevádzky uvádza vysokorizikový systém umelej inteligencie súvisiaci s výrobkom, na ktorý sa vzťahujú právne akty uvedené v prílohe II oddiele A, vypracuje sa jediná technická dokumentácia obsahujúca všetky informácie stanovené v prílohe IV, ako aj informácie požadované podľa uvedených právnych aktov.

3. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 73 s cieľom zmeniť prílohu IV, ak je to potrebné na zabezpečenie toho, aby technická dokumentácia vzhľadom na technický pokrok poskytovala všetky informácie potrebné na posúdenie súladu systému s požiadavkami stanovenými v tejto kapitole.

Článok 12

Vedenie záznamov

1. Vysokorizikové systémy umelej inteligencie musia technicky umožňovať automatické zaznamenávanie udalostí (logy) počas celého životného cyklu systému.

2. S cieľom zabezpečiť úroveň vysledovateľnosti fungovania systému umelej inteligencie, ktorá je primeraná zamýšľanému účelu systému, schopnosti logovania umožňujú zaznamenávanie udalostí relevantných pre:

   i) identifikáciu situácií, ktoré môžu viesť k tomu, že systém umelej inteligencie začne predstavovať riziko v zmysle článku 65 ods. 1, alebo k podstatnej zmene;

   ii) uľahčenie monitorovania po umiestnení na trh, ako sa uvádza v článku 61, a

   iii) monitorovanie prevádzky vysokorizikových systémov umelej inteligencie uvedené v článku 29 ods. 4.

4. V prípade vysokorizikových systémov umelej inteligencie uvedených v prílohe III odseku 1 písm. a) sa v rámci logovania musí dať zabezpečiť aspoň:

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

   b) referenčná databáza, na základe 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 používateľom

1. Vysokorizikové systémy umelej inteligencie musia byť koncipované a vyvinuté tak, aby sa zabezpečilo, že ich prevádzka je dostatočne transparentná s cieľom dosiahnuť súlad s príslušnými povinnosťami používateľa a poskytovateľa stanovenými v kapitole 3 tejto hlavy a umožniť používateľom systém pochopiť a primerane používať.

2. K vysokorizikovým systémom umelej inteligencie musí byť vo vhodnom digitálnom formáte alebo inak priložený návod na použitie obsahujúci stručné, úplné, správne a jasné informácie, ktoré sú pre používateľov relevantné, prístupné a zrozumiteľné.

3. V informáciách podľa odseku 2 sa uvádzajú:

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

   b) charakteristiky, schopnosti a obmedzenia výkonnosti vysokorizikového systému umelej inteligencie vrátane:

      i) jeho zamýšľaného účelu vrátane konkrétnych geografických, behaviorálnych alebo funkčných podmienok, v ktorých sa má vysokorizikový systém umelej inteligencie používať;

      ii) úrovne presnosti vrátane jej metriky, spoľahlivosti a kybernetickej bezpečnosti podľa článku 15, na základe ktorej bol vysokorizikový systém umelej inteligencie 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 umelej inteligencie v súlade s jeho zamýšľaným účelom, ktoré môžu viesť k rizikám pre zdravie a bezpečnosť alebo pre základné práva, ako sa uvádza v článku 9 ods. 2;

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

v) 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 systému umelej inteligencie;

vi) v príslušných prípadoch, opisu očakávaného výstupu systému.

c) prípadné zmeny vysokorizikového systému umelej inteligencie a jeho výkonnosti, ktoré v čase počiatočného posudzovania zhody vopred určil poskytovateľ;

d) opatrenia na zabezpečenie ľudského dohľadu uvedené v článku 14 vrátane technických opatrení zavedených na uľahčenie výkladu výstupov systémov umelej inteligencie používateľmi;

e) potrebné výpočtové a hardvérové zdroje, očakávaná životnosť vysokorizikového systému umelej inteligencie a všetky opatrenia potrebné na údržbu a starostlivosť vrátane frekvencie ich využívania, ktorými sa má zabezpečiť riadne fungovanie tohto systému umelej inteligencie, a to aj pokiaľ ide o aktualizácie softvéru;

f) opis mechanizmu zahrnutého do systému umelej inteligencie, ktorý v príslušných prípadoch umožňuje používateľom riadne zhromažďovať, uchovávať a interpretovať logy.

Článok 14

Ľudský dohľad

1. Vysokorizikové systémy umelej inteligencie musia byť koncipované a vyvinuté tak, aby nad nimi počas obdobia používania systému umelej inteligencie 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 umelej inteligencie v súlade so zamýšľaným účelom alebo za podmienok logicky predvídateľného nesprávneho použitia, najmä ak takéto riziká bez ohľadu na uplatňovanie iných požiadaviek stanovených v tejto kapitole pretrvávajú.

3. Ľudský dohľad sa zabezpečuje jedným alebo všetkými nasledujúcimi druhmi opatrení:

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

b) opatrenia, ktoré identifikuje poskytovateľ pred uvedením vysokorizikového systému umelej inteligencie na trh alebo do prevádzky a ktoré môže zaviesť používateľ.

4. Na účely vykonávania odsekov 1 až 3 sa vysokorizikový systém umelej inteligencie poskytuje používateľovi takým spôsobom, aby fyzickým osobám, ktorým je zverený ľudský dohľad, umožňoval podľa potreby a primerane okolnostiam:

a) pochopiť kapacity a obmedzenia vysokorizikového systému umelej inteligencie a riadne monitorovať jeho prevádzku;

b) neustále si uvedomovať možnú tendenciu automatického spoliehania sa alebo nadmerného spoliehania sa na výstup produkovaný vysokorizikovým systémom umelej inteligencie („automatizačné skreslenie“);

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

d) v akejkoľvek konkrétnej situácii rozhodnúť, že sa vysokorizikový systém umelej inteligencie nebude používať alebo sa výstup vysokorizikového systému umelej inteligencie inak nezohľadní, potlačí alebo zvráti;

e) zasiahnuť do prevádzky vysokorizikového systému umelej inteligencie alebo ho prerušiť tlačidlom zastavenia alebo podobným postupom.

5. V prípade vysokorizikových systémov umelej inteligencie uvedených v prílohe III bode 1 písm. a) musia byť opatrenia podľa odseku 3 také, aby sa navyše zabezpečilo, že používateľ na základe identifikácie vyplývajúcej zo systému neprijme žiadne kroky ani rozhodnutie, pokiaľ tento výsledok nebol zvlášť overený a potvrdený aspoň dvoma fyzickými osobami. Požiadavka na samostatné overenie aspoň dvoma fyzickými osobami sa nevzťahuje na vysokorizikové systémy umelej inteligencie používané na účely presadzovania práva, migrácie, kontroly hraníc alebo azylu v prípadoch, keď sa podľa práva Únie alebo vnútroštátneho práva uplatňovanie tejto požiadavky považuje za neprimerané.

Článok 15

Presnosť, spoľahlivosť a kybernetická bezpečnosť

1. Vysokorizikové systémy umelej inteligencie musia byť koncipované a vyvinuté tak, aby vzhľadom na svoj zamýšľaný účel dosahovali primeranú úroveň presnosti, spoľahlivosti a kybernetickej bezpečnosti a aby v týchto ohľadoch konzistentne fungovali počas celého svojho životného cyklu.

2. Úrovne presnosti a príslušné metriky na meranie presnosti vysokorizikových systémov umelej inteligencie sa musia uvádzať v priloženom návode na použitie.

3. Vysokorizikové systémy umelej inteligencie musia byť odolné voči chybám, poruchám alebo nezrovnalostiam, 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.

Spoľahlivosť vysokorizikových systémov umelej inteligencie možno dosiahnuť technickými riešeniami na vytvorenie redundancie, ktoré môžu zahŕňať plány zálohovania alebo zaistenia v prípade zlyhania.

Vysokorizikové systémy umelej inteligencie, ktoré sa po uvedení na trh alebo do prevádzky ďalej učia, sa musia vyvíjať tak, aby sa odstránilo alebo v čo najväčšej miere znížilo riziko, že prípadné skreslené výstupy s vplyvom na vstup pre budúce operácie („slučky spätnej väzby“) budú náležite riešené vhodnými zmierňujúcimi opatreniami.

4. Vysokorizikové systémy umelej inteligencie musia byť odolné voči pokusom neoprávnených tretích strán o zmenu ich používania alebo výkonnosti využívaním zraniteľností systému.

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

Technické riešenia na riešenie zraniteľností špecifických pre umelú inteligenciu musia v prípade potreby zahŕňať opatrenia na prevenciu a kontrolu útokov, ktoré sa pokúšajú manipulovať súbor trénovacích údajov („otrávenie údajov“), vstupov upravených tak, aby model urobil chybu („odporujúce si príklady“), alebo nedostatkov modelu.

KAPITOLA 3

POVINNOSTI POSKYTOVATEĽOV A POUŽÍVATEĽOV VYSOKORIZIKOVÝCH SYSTÉMOV UMELEJ INTELIGENCIE A INÝCH STRÁN

Článok 16

Povinnosti poskytovateľov vysokorizikových systémov umelej inteligencie

Poskytovatelia vysokorizikových systémov umelej inteligencie musia:

a) zabezpečiť, aby ich vysokorizikové systémy umelej inteligencie boli v súlade s požiadavkami stanovenými v kapitole 2 tejto hlavy;

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

b) mať zavedený systém riadenia kvality, ktorý je v súlade s článkom 17;

c) uchovávať dokumentáciu podľa článku 18;

d) uchovávať logy automaticky generované ich vysokorizikovými systémami umelej inteligencie, ak ich majú pod kontrolou, ako sa uvádza v článku 20;

e) zabezpečiť, aby sa vysokorizikový systém umelej inteligencie pred uvedením na trh alebo do prevádzky podrobil príslušnému postupu posudzovania zhody, ako sa uvádza v článku 43;

f) plniť povinnosti týkajúce sa registrácie uvedené v článku 51 ods. 1;

g) prijať potrebné nápravné opatrenia uvedené v článku 21, ak vysokorizikový systém umelej inteligencie nie je v súlade s požiadavkami stanovenými v kapitole 2 tejto hlavy;

h) informovať o nesúlade a o všetkých prijatých nápravných opatreniach príslušný vnútroštátny orgán členských štátov, v ktorých systém umelej inteligencie sprístupnili alebo uviedli do prevádzky, a v relevantných prípadoch aj notifikovanú osobu;

i) umiestniť označenie CE na svoje vysokorizikové systémy umelej inteligencie, a tak v súlade s článkom 49 vyjadriť zhodu s týmto nariadením;

j) na žiadosť príslušného vnútroštátneho orgánu preukázať zhodu vysokorizikového systému umelej inteligencie s požiadavkami stanovenými v kapitole 2 tejto hlavy.

Článok 17

Systém riadenia kvality

1. Poskytovatelia vysokorizikových systémov umelej inteligencie 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 musí zahŕňať aspoň tieto aspekty:

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

b) techniky, postupy a systematické opatrenia, ktoré sa majú použiť pri koncipovaní vysokorizikového systému umelej inteligencie, kontrole jeho koncepcie a jej overovaní;

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

d) postupy preskúmania, testovania a validácie, ktoré sa majú vykonávať pred vývojom vysokorizikového systému umelej inteligencie, počas neho a po ňom, a častosť, 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, prostriedky, ktoré sa majú použiť na zabezpečenie toho, aby vysokorizikový systém umelej inteligencie spĺňal požiadavky stanovené v kapitole 2 tejto hlavy;

f) systémy a postupy správy údajov vrátane 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 umelej inteligencie 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 61;

i) postupy týkajúce sa podávania správ o závažnom incidente v súlade s článkom 62;

j) vybavovanie komunikácie s príslušnými vnútroštátnymi orgánmi, príslušnými orgánmi vrátane odvetvových orgánov, 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. Vykonávanie aspektov uvedených v odseku 1 musí byť primerané veľkosti organizácie poskytovateľa.

2a. V prípade poskytovateľov vysokorizikových systémov umelej inteligencie, na ktorých sa vzťahujú povinnosti týkajúce sa systémov riadenia kvality podľa príslušného odvetvového práva Únie, môžu byť aspekty opísané v odseku 1 súčasťou systémov riadenia kvality ustanovených podľa uvedeného práva.

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

Článok 18

Uchovávanie dokumentácie

1. Počas obdobia končiaceho sa desať rokov po uvedení systému umelej inteligencie na trh alebo do prevádzky uchováva poskytovateľ pre potreby príslušných vnútroštátnych 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 48.

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

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

Článok 19

Posudzovanie zhody

1. Poskytovatelia vysokorizikových systémov umelej inteligencie musia zabezpečiť, aby sa ich systémy pred uvedením na trh alebo do prevádzky podrobili príslušnému postupu posudzovania zhody v súlade s článkom 43. Ak sa po tomto posúdení zhody preukáže súlad systémov umelej inteligencie s požiadavkami stanovenými v kapitole 2 tejto hlavy, poskytovatelia vypracujú EÚ vyhlásenie o zhode v súlade s článkom 48 a umiestnia označenie zhody CE v súlade s článkom 49.

2. [vypúšťa sa]

Článok 20

Automaticky generované logy

1. Poskytovatelia vysokorizikových systémov umelej inteligencie uchovávajú logy uvedené v článku 12 ods. 1 automaticky generované svojimi vysokorizikovými systémami umelej inteligencie, pokiaľ sú tieto logy na základe zmluvnej dohody s používateľom alebo zo zákona pod ich kontrolou. Uchovávajú ich najmenej počas šiestich mesiacov, pokiaľ sa v platnom práve Únie, najmä o ochrane osobných údajov, alebo vo vnútroštátnom práve nestanovuje inak.

2. Poskytovatelia, ktorí sú finančnými inštitúciami, na ktorých sa vzťahujú požiadavky týkajúce sa ich vnútornej správy a riadenia, dojednaní alebo postupov podľa právnych predpisov Únie o finančných službách, uchovávajú logy automaticky generované ich vysokorizikovými systémami umelej inteligencie ako súčasť dokumentácie uchovávanej podľa príslušných právnych predpisov o finančných službách.

Článok 21

Nápravné opatrenia

Poskytovatelia vysokorizikových systémov umelej inteligencie, ktorí sa domnievajú alebo majú dôvod domnievať sa, že vysokorizikový systém umelej inteligencie, ktorý uviedli na trh alebo do prevádzky, nie je v zhode s týmto nariadením, v príslušných prípadoch bezodkladne vyšetria príčiny tohto stavu v spolupráci s nahlasujúcim používateľom a prijmú potrebné nápravné opatrenia s cieľom dosiahnuť podľa potreby zhodu tohto systému alebo ho stiahnuť z trhu či od používateľa. Informujú o tom distribútorov daného vysokorizikového systému umelej inteligencie a v relevantných prípadoch splnomocneného zástupcu a dovozcov.

Článok 22

Povinnosť informovať

Ak vysokorizikový systém umelej inteligencie predstavuje riziko v zmysle článku 65 ods. 1 a poskytovateľ systému o tomto riziku vie, tento poskytovateľ bezodkladne informuje príslušné vnútroštátne orgány členských štátov, v ktorých systém sprístupnil, a prípadne notifikovanú osobu, ktorá vydala pre vysokorizikový systém umelej inteligencie certifikát, a to najmä o nesúlade systému a o všetkých prijatých nápravných opatreniach.

Článok 23

Spolupráca s príslušnými orgánmi

Poskytovatelia vysokorizikových systémov umelej inteligencie na žiadosť príslušného vnútroštátneho orgánu poskytnú tomuto orgánu všetky informácie a dokumentáciu potrebnú na preukázanie zhody vysokorizikového systému umelej inteligencie s požiadavkami stanovenými v kapitole 2 tejto hlavy, a to v jazyku, ktorému orgán dotknutého členského štátu bez problémov rozumie. Na základe odôvodnenej žiadosti príslušného vnútroštátneho orgánu sprístupnia poskytovatelia tomuto orgánu aj logy uvedené v článku 12 ods. 1 automaticky generované vysokorizikovým systémom umelej inteligencie, pokiaľ sú tieto logy na základe zmluvnej dohody s používateľom alebo zo zákona pod ich kontrolou.

Článok 23a

Podmienky pre iné osoby, na ktoré sa majú vzťahovať povinnosti poskytovateľa

1. Každá fyzická osoba alebo právnická osoba sa na účely tohto nariadenia považuje za poskytovateľa nového vysokorizikového systému umelej inteligencie a vzťahujú sa na ňu povinnosti poskytovateľa podľa článku 16 za ktorejkoľvek z týchto okolností:

   a) umiestni svoje meno alebo ochrannú známku na vysokorizikový systém umelej inteligencie, 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) [vypúšťa sa]

c) významne modifikuje vysokorizikový systém umelej inteligencie, ktorý už bol uvedený na trh alebo do prevádzky;

d) mení plánovaný účel systému umelej inteligencie, ktorý nie je vysokorizikový a už bol uvedený na trh alebo do prevádzky, a to tak, že sa zmenený systém stáva vysokorizikovým systémom umelej inteligencie;

e) uvádza na trh alebo do prevádzky systém umelej inteligencie na všeobecné účely ako vysokorizikový systém umelej inteligencie alebo ako komponent vysokorizikového systému umelej inteligencie.

2. Ak nastanú okolnosti uvedené v odseku 1 písm. b) alebo c), poskytovateľ, ktorý pôvodne uviedol vysokorizikový systém umelej inteligencie na trh alebo do prevádzky, sa už na účely tohto nariadenia za poskytovateľa nepovažuje.

3. V prípade vysokorizikových systémov umelej inteligencie, ktoré sú bezpečnostnými komponentmi výrobkov, na ktoré sa vzťahujú právne akty uvedené v prílohe II oddiele A, sa výrobca týchto výrobkov považuje za poskytovateľa vysokorizikového systému umelej inteligencie a podlieha povinnostiam podľa článku 16 v ktoromkoľvek z týchto scenárov:

i) vysokorizikový systém umelej inteligencie sa uvádza na trh spolu s výrobkom pod menom alebo ochrannou známkou výrobcu výrobku;

ii) vysokorizikový systém umelej inteligencie sa po uvedení výrobku na trh uvedie do prevádzky pod menom alebo ochrannou známkou výrobcu výrobku.

Článok 24

[vypúšťa sa]

Článok 25

Splnomocnení zástupcovia

1. Poskytovatelia usadení mimo Únie pred sprístupnením svojich systémov na trhu Únie písomným splnomocnením vymenujú splnomocneného zástupcu usadeného v Únii.

2. Splnomocnený zástupca vykonáva úlohy uvedené v splnomocnení, ktoré mu udelil poskytovateľ. Na účely tohto nariadenia splnomocnenie poveruje splnomocneného zástupcu vykonávaním výlučne týchto úloh:

-a) overiť, či sa vypracovalo EÚ vyhlásenie o zhode a technická dokumentácia a či poskytovateľ vykonal príslušný postup posudzovania zhody;

a) uchovávať pre príslušné vnútroštátne orgány a vnútroštátne orgány uvedené v článku 63 ods. 7 počas obdobia, ktoré sa končí 10 rokov po uvedení vysokorizikového systému umelej inteligencie na trh alebo do prevádzky, kontaktné údaje poskytovateľa, ktorý splnomocneného zástupcu vymenoval, kópiu EÚ vyhlásenia o zhode, technickú dokumentáciu a prípadne certifikát vydaný notifikovanou osobou;

b) poskytnúť príslušnému vnútroštátnemu orgánu na základe odôvodnenej žiadosti všetky informácie a dokumentáciu vrátane dokumentácie uchovávanej podľa písmena b) potrebné na preukázanie súladu vysokorizikového systému umelej inteligencie s požiadavkami stanovenými v kapitole 2 tejto hlavy vrátane prístupu k logom uvedeným v článku 12 ods. 1 automaticky generovaným vysokorizikovým systémom umelej inteligencie, pokiaľ sú tieto logy na základe zmluvnej dohody s používateľom alebo zo zákona pod kontrolou poskytovateľa;

c) na základe odôvodnenej žiadosti spolupracovať s príslušnými vnútroštátnymi orgánmi pri každom opatrení, ktoré tieto orgány v súvislosti s vysokorizikovým systémom umelej inteligencie prijmú;

d) plniť registračné povinnosti uvedené v článku 51 ods. 1 a v prípade, že registráciu systému vykonáva samotný poskytovateľ, overiť, či sú informácie uvedené v prílohe VIII časti II bodoch 1 až 11 správne.

Splnomocnený zástupca vypovie splnomocnenie, ak má dostatočné dôvody domnievať sa, že poskytovateľ koná v rozpore so svojimi povinnosťami podľa tohto nariadenia. v takom prípade tiež bezodkladne informuje orgán dohľadu nad trhom členského štátu, v ktorom je usadený, ako aj prípadne príslušnú notifikovanú osobu o výpovedi splnomocnenia a jej dôvodoch.

Splnomocnený zástupca je, pokiaľ ide o jeho potenciálnu zodpovednosť podľa smernice Rady 85/374/EHS, právne zodpovedný za chybné systémy umelej inteligencie na rovnakom základe ako poskytovateľ a spoločne a nerozdielne s ním.

Článok 26

Povinnosti dovozcov

1. Pred uvedením vysokorizikového systému umelej inteligencie na trh jeho dovozcovia zabezpečia, aby tento systém bol v súlade s týmto nariadením, a to tým, že overia, že:

a) poskytovateľ uvedeného systému umelej inteligencie vykonal príslušný postup posudzovania zhody uvedený v článku 43;

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

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

d) poskytovateľ ustanovil splnomocneného zástupcu uvedeného v článku 25.

2. Ak má dovozca dostatočné dôvody domnievať sa, že vysokorizikový systém umelej inteligencie nie je v súlade s týmto nariadením, je sfalšovaný, alebo že ho sprevádza sfalšovaná dokumentácia, nesmie tento systém uviesť na trh, kým sa tento systém umelej inteligencie neuvedie do súladu. Ak vysokorizikový systém umelej inteligencie predstavuje riziko v zmysle článku 65 ods. 1, dovozca o tom informuje poskytovateľa systému umelej inteligencie, splnomocnených zástupcov a orgány dohľadu nad trhom.

3. Dovozcovia na vysokorizikovom systéme umelej inteligencie, alebo ak to nie je možné, na jeho obale, prípadne v jeho sprievodnej dokumentácii uvedú svoje meno, registrované obchodné meno alebo registrovanú ochrannú známku a adresu, na ktorej ich možno kontaktovať.

4. Dovozcovia zabezpečia, aby v čase, keď nesú za vysokorizikový systém umelej inteligencie zodpovednosť, podmienky jeho uskladnenia alebo prepravy v relevantných prípadoch neohrozovali jeho súlad s požiadavkami stanovenými v kapitole 2 tejto hlavy.

4a. Dovozcovia uchovávajú kópiu prípadného certifikátu vydaného notifikovanou osobou, návodu na použitie a EÚ vyhlásenia o zhode počas obdobia, ktoré sa končí 10 rokov po uvedení systému umelej inteligencie na trh alebo do prevádzky.

5. Dovozcovia poskytnú príslušným vnútroštátnym orgánom na základe odôvodnenej žiadosti všetky informácie a dokumentáciu vrátane dokumentácie uchovávanej v súlade s odsekom 5 potrebné na preukázanie zhody vysokorizikového systému umelej inteligencie s požiadavkami stanovenými v kapitole 2 tejto hlavy v jazyku, ktorému príslušný vnútroštátny orgán bez problémov rozumie. Na tento účel takisto zabezpečia, aby sa týmto orgánom mohla sprístupniť technická dokumentácia.

5a. Dovozcovia spolupracujú s príslušnými vnútroštátnymi orgánmi pri každom opatrení, ktoré tieto orgány prijmú v súvislosti so systémom umelej inteligencie, ktorý dovážajú.

Článok 27

Povinnosti distribútorov

1. Pred sprístupnením vysokorizikového systému umelej inteligencie na trhu distribútori overia, či je tento vysokorizikový systém umelej inteligencie označený požadovaným označením zhody CE, či je k nemu pripojená kópia EÚ vyhlásenia o zhode a návod na použitie a či si poskytovateľ, prípadne dovozca systému splnil povinnosti stanovené v článku 16 písm. b), respektíve v článku 26 ods. 3.

2. Ak sa distribútor domnieva alebo má dôvod domnievať sa, že vysokorizikový systém umelej inteligencie nie je v súlade s požiadavkami stanovenými v kapitole 2 tejto hlavy, nesmie tento systém sprístupniť na trhu, kým sa tento systém neuvedie do súladu s uvedenými požiadavkami. Ak systém navyše predstavuje riziko v zmysle článku 65 ods. 1, distribútor o tom informuje poskytovateľa, prípadne dovozcu systému.

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

4. Distribútor, ktorý sa domnieva alebo má dôvod domnievať sa, že vysokorizikový systém umelej inteligencie, ktorý sprístupnil na trhu, nie je v súlade s požiadavkami stanovenými v kapitole 2 tejto hlavy, prijme nápravné opatrenia potrebné na dosiahnutie súladu tohto systému s uvedenými požiadavkami, na jeho stiahnutie z trhu alebo od používateľa, alebo zabezpečí, aby uvedené nápravné opatrenia prijal poskytovateľ, dovozca alebo prípadne akýkoľvek relevantný prevádzkovateľ. Ak vysokorizikový systém umelej inteligencie predstavuje riziko v zmysle článku 65 ods. 1, distribútor o tom bezodkladne informuje príslušné vnútroštátne orgány členských štátov, v ktorých výrobok sprístupnil, pričom uvedie podrobnosti najmä o nedodržaní požiadaviek a o všetkých prijatých nápravných opatreniach.

5. Na základe odôvodnenej žiadosti príslušného vnútroštátneho orgánu distribútori vysokorizikových systémov umelej inteligencie poskytnú tomuto orgánu všetky informácie a dokumentáciu o svojej činnosti podľa odsekov 1 až 4.

5a. Distribútori spolupracujú s príslušnými vnútroštátnymi orgánmi pri každom opatrení, ktoré tieto orgány prijmú v súvislosti so systémom umelej inteligencie, ktorý distribuujú.

Článok 28

[vypúšťa sa]

Článok 29

Povinnosti používateľov vysokorizikových systémov umelej inteligencie

1. Používatelia vysokorizikových systémov umelej inteligencie musia tieto systémy používať v súlade s návodom na použitie k nim priloženým, a to podľa odsekov 2 a 5 tohto článku.

1a. Používatelia pridelia ľudský dohľad fyzickým osobám, ktoré majú potrebnú spôsobilosť, odbornú prípravu a právomoci.

2. Povinnosťami uvedenými v odseku 1 a 1a nie sú dotknuté iné povinnosti používateľov vyplývajúce z právnych predpisov Únie alebo vnútroštátneho práva ani rozhodovanie používateľov pri organizovaní vlastných zdrojov a činností na účely vykonávania opatrení na zabezpečenie ľudského dohľadu uvedených poskytovateľom.

3. Bez toho, aby bol dotknutý odsek 1 a pokiaľ má používateľ kontrolu nad vstupnými údajmi, tento používateľ zabezpečí, aby vstupné údaje boli relevantné z hľadiska zamýšľaného účelu vysokorizikového systému umelej inteligencie.

4. Používatelia zavedú ľudský dohľad a monitorujú prevádzku vysokorizikového systému umelej inteligencie na základe návodu na použitie. Ak majú dôvody domnievať sa, že používanie v súlade s návodom na použitie môže viesť k tomu, že systém umelej inteligencie bude predstavovať riziko v zmysle článku 65 ods. 1, informujú poskytovateľa alebo distribútora a pozastavia používanie systému. Poskytovateľa alebo distribútora informujú aj vtedy, keď zistia akýkoľvek závažný incident, a používanie systému umelej inteligencie prerušia. v prípade, že používateľ sa s poskytovateľom nedokáže spojiť, uplatňuje sa mutatis mutandis článok 62. Táto povinnosť sa nevzťahuje na citlivé prevádzkové údaje používateľov systémov umelej inteligencie, ktorí sú orgánmi presadzovania práva.

V prípade používateľov, ktorí sú finančnými inštitúciami, na ktoré sa vzťahujú požiadavky týkajúce sa ich vnútornej správy a riadenia, dojednaní alebo postupov podľa právnych predpisov Únie v oblasti finančných služieb, sa monitorovacia povinnosť ustanovená v prvom pododseku považuje za splnenú dodržiavaním pravidiel týkajúcich sa dojednaní, postupov a mechanizmov vnútornej správy a riadenia podľa príslušných právnych predpisov v oblasti finančných služieb.

5. Používatelia vysokorizikových systémov umelej inteligencie uchovávajú logy uvedené v článku 12 ods. 1 automaticky generované týmito systémami, pokiaľ sú tieto logy pod ich kontrolou. Uchovávajú ich najmenej počas šiestich mesiacov, pokiaľ sa v platnom práve Únie, najmä o ochrane osobných údajov, alebo vo vnútroštátnom práve nestanovuje inak.

Používatelia, ktorí sú finančnými inštitúciami, na ktoré sa vzťahujú požiadavky týkajúce sa ich vnútornej správy a riadenia, dojednaní alebo postupov podľa právnych predpisov Únie v oblasti finančných služieb, uchovávajú logy ako súčasť dokumentácie uchovávanej v súlade s príslušnými právnymi predpismi Únie v oblasti finančných služieb.

5a. Používatelia vysokorizikových systémov umelej inteligencie, ktorí sú orgánmi verejnej moci, verejnými agentúrami alebo verejnými subjektmi, s výnimkou orgánov presadzovania práva, kontroly hraníc, imigračných alebo azylových orgánov, musia dodržiavať registračné povinnosti uvedené v článku 51. Ak zistia, že systém, ktorý plánujú používať, nebol zaregistrovaný v databáze EÚ uvedenej v článku 60, nepoužívajú tento systém a informujú o tom poskytovateľa alebo distribútora.

6. Na splnenie svojej povinnosti vykonať posúdenie vplyvu na ochranu údajov podľa článku 35 nariadenia (EÚ) 2016/679 alebo prípadne článku 27 smernice (EÚ) 2016/680 využijú používatelia vysokorizikových systémov umelej inteligencie informácie poskytnuté podľa článku 13.

6a. Používatelia spolupracujú s príslušnými vnútroštátnymi orgánmi pri každom opatrení, ktoré tieto orgány prijmú v súvislosti so systémom umelej inteligencie, ktorý používajú.

KAPITOLA 4

NOTIFIKUJÚCE ORGÁNY A NOTIFIKOVANÉ OSOBY

Článok 30

Notifikujúce orgány

1. Každý členský štát určí alebo zriadi aspoň jeden notifikujúci orgán zodpovedný za stanovenie a vykonávanie nevyhnutných postupov na posudzovanie, určovanie a notifikáciu orgánov posudzovania zhody a za ich monitorovanie.

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

3. Notifikujúce orgány sa zriaďujú, organizujú a prevádzkujú tak, aby nedochádzalo ku konfliktu záujmov s orgánmi posudzovania zhody a aby bola zabezpečená objektivita a nestrannosť ich činností.

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

5. Notifikujúce orgány nesmú ponúkať ani poskytovať žiadne činnosti, ktoré vykonávajú orgány posudzovania zhody, ani žiadne poradenské služby na komerčnom či konkurenčnom základe.

6. Notifikujúce orgány musia zabezpečiť dôvernosť informácií, ktoré získajú, v súlade s článkom 70.

7. Notifikujúce orgány majú na riadne vykonávanie svojich úloh k dispozícii primeraný počet odborne spôsobilých zamestnancov.

8. [vypúšťa sa]

Článok 31

Žiadosť orgánov posudzovania zhody o notifikáciu

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

2. Súčasťou žiadosti o notifikáciu je opis činností posudzovania zhody, modulu alebo modulov posudzovania zhody a systémov umelej inteligencie, v súvislosti s ktorými orgán posudzovania zhody tvrdí, že je odborne spôsobilý, a ak existuje, aj osvedčenie o akreditácii vydané vnútroštátnym akreditačným orgánom, ktorým sa potvrdzuje, že orgán posudzovania zhody spĺňa požiadavky stanovené v článku 33. 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 toho, či plní požiadavky stanovené v článku 33. 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 odseku 2 a 3 vždy, keď dôjde k relevantným zmenám, čím sa orgánu zodpovednému za notifikované osoby umožní monitorovať a overovať nepretržité plnenie všetkých požiadaviek stanovených v článku 33.

Článok 32

Notifikačný postup

1. Notifikujúce orgány môžu notifikovať iba orgány posudzovania zhody, ktoré splnili požiadavky ustanovené v článku 33.

2. Komisii a ostatným členským štátom podávajú notifikujúce orgány notifikácie uvedených orgánov prostredníctvom elektronického notifikačného nástroja vyvinutého a spravovaného Komisiou.

3. V notifikácii uvedenej v odseku 2 sú zahrnuté všetky podrobnosti o činnostiach posudzovania zhody, modul alebo moduly posudzovania zhody a príslušné systémy umelej inteligencie a príslušné potvrdenie odbornej spôsobilosti. Ak sa notifikácia nezakladá na osvedčení o akreditácii uvedenom v článku 31 ods. 2, notifikujúci orgán poskytne Komisii a ostatným členským štátom dokumentáciu potvrdzujúcu odbornú spôsobilosť orgánu posudzovania zhody a zavedené opatrenia, ktorými sa zabezpečí, že tento orgán sa bude pravidelne monitorovať a bude naďalej plniť požiadavky stanovené v článku 33.

4. Predmetný orgán posudzovania zhody môže vykonávať činnosti notifikovaného orgánu iba v prípade, že Komisia ani členské štáty nevznesú námietky do dvoch týždňov po notifikácii notifikujúcim orgánom s uplatnením osvedčenia o akreditácii uvedeného v článku 31 ods. 2 alebo do dvoch mesiacov po notifikácii notifikujúcim orgánom s uplatnením listinných dôkazov uvedených v článku 31 ods. 3.

5. [vypúšťa sa]

Článok 33

Požiadavky týkajúce sa notifikovaných osôb

1. Notifikovaná osoba sa zriaďuje podľa vnútroštátneho práva a má právnu subjektivitu.

2. Notifikované osoby musia spĺňať požiadavky týkajúce sa organizácie, riadenia kvality, zdrojov a postupov potrebné na plnenie svojich úloh.

3. Organizačná štruktúra, rozdelenie zodpovedností, hierarchické vzťahy a fungovanie notifikovaných osôb musia byť také, aby sa zabezpečila dôvera v ich konanie a vo výsledky činností posudzovania zhody, ktoré notifikované osoby vykonávajú.

4. Notifikované osoby musia byť nezávislé od poskytovateľa vysokorizikového systému umelej inteligencie, v súvislosti s ktorým vykonávajú činnosti posudzovania zhody. Takisto musia byť nezávislé od akéhokoľvek iného prevádzkovateľa, ktorý má na posudzovanom vysokorizikovom systéme umelej inteligencie hospodársky záujem, ako aj od akýchkoľvek konkurentov poskytovateľa.

5. Notifikované osoby musia mať takú organizačnú štruktúru a fungovať tak, aby sa zaručila nezávislosť, objektivita a nestrannosť ich činností. Notifikované osoby musia zdokumentovať a zaviesť štruktúru a postupy, ktorými sa zaručí nestrannosť a ktorými sa budú presadzovať a uplatňovať zásady nestrannosti v celej ich organizačnej štruktúre, u všetkých zamestnancov a pri všetkých činnostiach posudzovania.

6. Notifikované osoby musia mať zavedené zdokumentované postupy, ktorými sa zabezpečí, aby ich zamestnanci, výbory, dcérske spoločnosti, subdodávatelia a akýkoľvek pridružený subjekt alebo zamestnanci externých subjektov zachovávali dôvernosť informácií, ktoré získajú počas vykonávania činností posudzovania zhody, podľa článku 70 s výnimkou prípadov, keď sa zverejnenie týchto informácií vyžaduje podľa zákona. Zamestnanci notifikovaných osôb sú povinní zachovávať služobné tajomstvo, pokiaľ ide o všetky informácie, 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.

7. Na vykonávanie činností musia mať notifikované osoby postupy, pri ktorých sa náležite zohľadňuje veľkosť podniku, odvetvie, v ktorom podnik pôsobí, jeho štruktúra a stupeň zložitosti príslušného systému umelej inteligencie.

8. Notifikované osoby musia v súvislosti so svojimi činnosťami posudzovania zhody uzavrieť 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.

9. Všetky úlohy, ktoré im prináležia podľa tohto nariadenia, musia byť notifikované osoby schopné 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.

10. Notifikované osoby musia byť na internej úrovni dostatočne spôsobilé, aby mohli účinne hodnotiť úlohy, ktoré v ich mene vykonávajú externé subjekty. Notifikovaná osoba má neustále k dispozícii dostatočný počet administratívnych, technických, právnych a vedeckých pracovníkov, ktorí majú skúsenosti a znalosti týkajúce sa príslušných technológií umelej inteligencie, údajov a výpočtov a požiadaviek stanovených v kapitole 2 tejto hlavy.

11. 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 neustále informované o aktuálnom stave príslušných noriem.

12. [vypúšťa sa]

Článok 33a

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 33 v rozsahu, v akom sa na uvedené požiadavky uplatňujú harmonizované normy.

Článok 34

Dcérske spoločnosti a subdodávatelia notifikovaných osôb

1. Ak notifikovaná osoba zadáva osobitné úlohy spojené s posudzovaním zhody subdodávateľovi alebo ich prenesie na dcérsku spoločnosť, musí zabezpečiť, aby tento subdodávateľ alebo táto dcérska spoločnosť spĺňali požiadavky stanovené v článku 33, a náležite o tom informuje notifikujúci orgán.

2. Notifikované osoby nesú plnú zodpovednosť za úlohy vykonávané subdodávateľmi alebo dcérskymi spoločnosťami bez ohľadu na to, kde sú usadené.

3. Vykonávanie činností sa môže zadať subdodávateľovi alebo preniesť na dcérsku spoločnosť iba so súhlasom poskytovateľa.

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 subdodávateľskej činnosti.

Článok 34a

Povinnosti notifikovaných osôb týkajúce sa výkonu ich činností

1. Notifikované osoby overujú zhodu vysokorizikového systému umelej inteligencie v súlade s postupmi posudzovania zhody uvedenými v článku 43.

2. Notifikované osoby pri výkone svojej činnosti predchádzajú zbytočnej záťaži pre poskytovateľov a náležite zohľadňujú veľkosť podniku, odvetvie, v ktorom podnik pôsobí, jeho štruktúru a stupeň zložitosti príslušného vysokorizikového systému umelej inteligencie. Notifikovaná osoba však pri tom dodržiavajú mieru prísnosti a úroveň ochrany, ktoré sú potrebné na zabezpečenie súladu vysokorizikového systému umelej inteligencie s požiadavkami stanovenými v tomto nariadení.

3. Notifikujúcemu orgánu uvedenému v článku 30 notifikované osoby sprístupnia a na požiadanie predložia všetky príslušné dokumenty vrátane dokumentácie poskytovateľa, aby tento orgán mohol vykonávať svoje činnosti posudzovania, určovania, notifikácie a monitorovania a aby sa uľahčilo posudzovanie podľa tejto kapitoly.

Článok 35

Identifikačné čísla a zoznamy notifikovaných osôb určených podľa tohto nariadenia

1. Každej notifikovanej osobe pridelí Komisia identifikačné číslo. Notifikovanej osobe pridelí len jedno číslo, a to aj keď je notifikovaná na základe viacerých aktov Únie.

2. Komisia zverejní zoznam osôb notifikovaných podľa tohto nariadenia vrátane identifikačných čísiel, ktoré im boli pridelené, a činností, v súvislosti s ktorými boli notifikované. Komisia zabezpečuje aktuálnosť tohto zoznamu.

Článok 36

Zmeny notifikácií

1. Notifikujúci orgán oznamuje Komisii a ostatným členským štátom všetky relevantné zmeny týkajúce sa notifikácie notifikovanej osoby prostredníctvom elektronického notifikačného nástroja uvedeného v článku 32 ods. 2.

2. Postupy opísané v článku 31 a 32 sa uplatňujú na rozširovanie rozsahu notifikácie. v prípade iných zmien notifikácie, ako je rozšírenie jej rozsahu, sa uplatňujú postupy ustanovené v nasledujúcich odsekoch.

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

3. Ak má notifikujúci orgán dostatočné dôvody domnievať sa, že notifikovaná osoba už nespĺňa požiadavky stanovené v článku 33 alebo si neplní svoje povinnosti, notifikujúci orgán za predpokladu, že notifikovaná osoba mala príležitosť vyjadriť svoje stanovisko, podľa potreby obmedzí, pozastaví alebo stiahne notifikáciu v závislosti od vážnosti neplnenia uvedených požiadaviek alebo neplnenia uvedených povinností. Okamžite o tom informuje Komisiu a ostatné členské štáty.

4. Ak je určenie notifikovanej osoby pozastavené, obmedzené alebo úplne či čiastočne stiahnuté, notifikovaná osoba o tom informuje príslušných výrobcov najneskôr do 10 dní.

5. V prípade obmedzenia, pozastavenia alebo stiahnutia notifikácie notifikujúci orgán prijme vhodné opatrenia, ktorými zabezpečí, aby bola dokumentácia príslušného notifikovanej osoby uchovaná a na požiadanie ju sprístupní notifikujúcim orgánom v iných členských štátoch a orgánom dohľadu nad trhom.

6. V prípade obmedzenia, pozastavenia alebo stiahnutia 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 notifikácie;

   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 zhodu systémov umelej inteligencie na trhu;

   d) informuje Komisiu a členské štáty o certifikátoch, v prípade ktorých požiadal o pozastavenie alebo stiahnutie;

e) poskytne príslušným vnútroštátnym 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, príslušný orgán prijme primerané opatrenia.

7. S výnimkou certifikátov, ktoré boli vydané neoprávnene, a prípadov, keď bola notifikácia pozastavená alebo obmedzená, zostávajú certifikáty platné za 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 a činnosti, ktoré by mali viesť k zrušeniu uvedeného pozastavenia alebo obmedzenia, alebo

b) notifikujúci orgán potvrdil, že sa počas daného 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 orgán zodpovedný za notifikované osoby zistí, že notifikovaná osoba nie je spôsobilá podporovať existujúce vydané certifikáty, poskytovateľ poskytne príslušným vnútroštátnym orgánom členského štátu, v ktorom má poskytovateľ systému, na ktorý sa vzťahuje certifikát, zaregistrované miesto podnikania, do troch mesiacov od pozastavenia alebo obmedzenia písomné potvrdenie, že iná kvalifikovaná notifikovaná osoba dočasne preberá funkcie notifikovanej osoby monitorovať certifikáty a zostáva za ne zodpovedná počas obdobia pozastavenia alebo obmedzenia.

8. S výnimkou certifikátov, ktoré boli vydané neoprávnene, a prípadov, keď bolo určenie stiahnuté, zostávajú certifikáty platné na obdobie deviatich mesiacov za týchto okolností:

a) ak príslušný vnútroštátny orgán členského štátu, v ktorom má poskytovateľ systému umelej inteligencie, na ktorý sa vzťahuje certifikát, zaregistrované miesto podnikania, potvrdil, že v súvislosti s dotknutými systémami neexistuje žiadne riziko pre zdravie, bezpečnosť a základné práva, a

b) ďalšia notifikovaná osoba písomne potvrdila, že okamžite prevezme zodpovednosť za tieto systémy a dokončí ich posúdenie do dvanástich mesiacov od stiahnutia určenia.

Za okolností uvedených v prvom pododseku môže príslušný vnútroštátny orgán členského štátu, v ktorom má poskytovateľ systému, na ktorý sa certifikát vzťahuje, zaregistrované miesto podnikania, predĺžiť obdobie prechodnej platnosti certifikátov na ďalšie obdobia troch mesiacov, ktoré spolu nesmú prekročiť dvanásť mesiacov.

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

Článok 37

Napadnutie spôsobilosti notifikovaných osôb

1. Komisia v prípade potreby vyšetrí všetky prípady, v ktorých sú odôvodnené pochybnosti o tom, či notifikovaná osoba spĺňa požiadavky stanovené v článku 33.

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

3. Komisia zabezpečí dôverné zaobchádzanie v súlade s článkom 70 so všetkými dôvernými informáciami získanými počas jej vyšetrovaní podľa tohto článku.

4. Keď Komisia zistí, že notifikovaná osoba nespĺňa alebo prestala spĺňať požiadavky stanovené v článku 33, oznámi notifikujúcemu orgánu dôvody takéhoto zistenia a požiada ho, aby prijal potrebné nápravné opatrenia vrátane prípadného pozastavenia, obmedzenia alebo stiahnutia určenia. Ak notifikujúci orgán neprijme potrebné nápravné opatrenia, Komisia môže prostredníctvom vykonávacích aktov pozastaviť, obmedziť alebo stiahnuť notifikáciu. Uvedený vykonávací akt sa prijme v súlade s postupom preskúmania uvedeným v článku 74 ods. 2.

Článok 38

Koordinácia notifikovaných osôb

1. Komisia zabezpečí, aby sa so zreteľom na vysokorizikové systémy umelej inteligencie, 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. Notifikujúci orgán zabezpečí, aby sa osoby, ktoré notifikovali, priamo alebo prostredníctvom určených zástupcov zúčastňovali na práci tejto skupiny.

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 článku 33.

KAPITOLA 5

NORMY, POSUDZOVANIE ZHODY, CERTIFIKÁTY, REGISTRÁCIA

Článok 40

Harmonizované normy

1. Vysokorizikové systémy umelej inteligencie alebo systémy umelej inteligencie na všeobecné účely, ktoré sú v zhode s harmonizovanými normami alebo ich časťami, na ktoré boli uverejnené odkazy v Úradnom vestníku Európskej únie, sa považujú za systémy, ktoré sú v zhode s požiadavkami stanovenými v kapitole 2 tejto hlavy, prípadne požiadavkami stanovenými v článku 4a a článku 4b, a to v rozsahu, v akom sa tieto normy vzťahujú na uvedené požiadavky.

2. Pri vydávaní žiadosti o normalizáciu adresovanej európskym normalizačným organizáciám v súlade s článkom 10 nariadenia č. 1025/2012 Komisia uvedie, že normy sú jednotné, jasné a navrhnuté tak, aby sa zameriavali najmä na splnenie týchto cieľov:

   a) zabezpečiť, aby systémy umelej inteligencie uvedené na trh alebo do prevádzky v Únii boli bezpečné a aby rešpektovali hodnoty Únie a posilňovali otvorenú strategickú autonómiu Únie;

   b) podporovať investície a inovácie v oblasti umelej inteligencie, a to aj zvyšovaním právnej istoty, a podporovať konkurencieschopnosť a rast trhu Únie;

   c) posilniť viacstrannú správu a riadenie so zastúpením všetkých relevantných európskych zainteresovaných strán (napr. priemysel, MSP, občiansku spoločnosť a výskumných pracovníkov);

   d) prispievať k posilneniu globálnej spolupráce v oblasti normalizácie umelej inteligencie, ktorá je v zhode s hodnotami a záujmami Únie.

   Komisia požiada európske normalizačné organizácie, aby poskytli dôkazy o svojom maximálnom úsilí o plnenie uvedených cieľov.

Článok 41

Spoločné špecifikácie

1. Komisia je splnomocnená prijímať po konzultácii s radou pre umelú inteligenciu uvedenou v článku 56 vykonávacie akty v súlade s postupom preskúmania uvedeným v článku 74 ods. 2, ktorými sa stanovujú spoločné technické špecifikácie pre požiadavky stanovené v kapitole 2 tejto hlavy alebo prípadne s požiadavkami stanovenými v článku 4a a článku 4b, ak sú splnené tieto podmienky:

   a) v Úradnom vestníku Európskej únie nie sú v súlade s nariadením (EÚ) č. 1025/2012 uverejnené žiadne odkazy na harmonizované normy týkajúce sa príslušných základných obáv súvisiacich s bezpečnosťou alebo základnými právami;

   b) Komisia podľa článku 10 ods. 1 nariadenia č. 1025/2012 požiadala jednu alebo viacero európskych normalizačných organizácií, aby vypracovali harmonizovanú normu pre požiadavky stanovené v kapitole 2 tejto hlavy;

   c) žiadna z európskych normalizačných organizácií neprijala žiadosť uvedenú v písmene b), harmonizované normy na riešenie tejto žiadosti neboli doručené v lehote stanovenej v súlade s článkom 10 ods. 1 nariadenia č. 1025/2012 alebo tieto normy nie sú v súlade so žiadosťou.

1a. 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 sú splnené.

2. V skorej fáze prípravy návrhu vykonávacieho aktu, ktorým sa stanovuje spoločná špecifikácia, Komisia plní ciele uvedené v článku 40 ods. 2 a zhromažďuje názory príslušných orgánov alebo expertných skupín zriadených podľa príslušného odvetvového práva Únie. Na základe týchto konzultácií Komisia vypracuje návrh vykonávacieho aktu.

3. Vysokorizikové systémy umelej inteligencie alebo systémy umelej inteligencie na všeobecné účely, ktoré sú v zhode so spoločnými špecifikáciami podľa odseku 1, sa považujú za systémy, ktoré sú v zhode s požiadavkami stanovenými v kapitole 2 tejto hlavy, prípadne požiadavkami stanovenými v článku 4a a článku 4b, a to v rozsahu, v akom sa tieto špecifikácie vzťahujú na uvedené požiadavky.

4. Keď sa odkazy na harmonizovanú normu uverejnia v Úradnom vestníku Európskej únie, vykonávacie akty uvedené v odseku 1, ktoré sa vzťahujú na požiadavky stanovené v kapitole 2 tejto hlavy alebo požiadavky stanovené v článku 4a a článku 4b, sa podľa potreby zrušia.

5. Ak sa členský štát domnieva, že spoločná špecifikácia úplne nespĺňa požiadavky stanovené v kapitole 2 tejto hlavy alebo prípadne požiadavky stanovené v článku 4a a článku 4b, informuje o tom Komisiu s podrobným vysvetlením a Komisia tieto informácie posúdi a v prípade potreby zmení vykonávací akt, ktorým sa daná spoločná špecifikácia ustanovuje.

Článok 42

Predpoklad zhody s určitými požiadavkami

1. Pri vysokorizikových systémoch umelej inteligencie, ktoré boli trénované a testované na údajoch, ktoré odzrkadľujú konkrétne geografické, behaviorálne a funkčné podmienky, v ktorých sa majú používať, sa predpokladá, že t sú v súlade s príslušnými požiadavkami stanovenými v článku 10 ods. 4.

2. Vysokorizikové systémy umelej inteligencie alebo systémy umelej inteligencie na všeobecné účely, pre ktoré bol v rámci systému kybernetickej bezpečnosti podľa nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881[33] vydaný certifikát alebo vyhlásenie o zhode 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 umelej inteligencie uvedeného v prílohe III bode 1 s požiadavkami stanovenými v kapitole 2 tejto hlavy uplatnil harmonizované normy uvedené v článku 40 alebo prípadne spoločné špecifikácie uvedené v článku 41, musí sa rozhodnúť pre jeden z týchto postupov:

   a) postup posudzovania zhody na základe vnútornej kontroly uvedený v prílohe VI alebo

   b) postup posudzovania zhody na základe posúdenia systému riadenia kvality a posúdenia technickej dokumentácie za účasti notifikovanej osoby uvedený v prílohe VII.

   Ak poskytovateľ pri preukazovaní súladu vysokorizikového systému umelej inteligencie s požiadavkami stanovenými v kapitole 2 tejto hlavy neuplatnil harmonizované normy uvedené v článku 40 alebo ich uplatnil len čiastočne, alebo ak takéto harmonizované normy neexistujú a spoločné špecifikácie uvedené v článku 41 nie sú k dispozícii, poskytovateľ musí dodržať postup posudzovania zhody stanovený v prílohe VII.

[33] 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. 1).

Na účely postupu posudzovania zhody uvedeného v prílohe VII si poskytovateľ môže vybrať ktorúkoľvek z notifikovaných osôb. Ak však majú systém uviesť do prevádzky orgány presadzovania práva, imigračné alebo azylové orgány, ako aj inštitúcie, orgány alebo agentúry EÚ, ako notifikovaná osoba koná orgán dohľadu nad trhom uvedený v článku 63 ods. 5 alebo 6.

2. V prípade vysokorizikových systémov umelej inteligencie uvedených v prílohe III bodoch 2 až 8 a systémov umelej inteligencie na všeobecné účely uvedených v hlave 1a musia poskytovatelia dodržať postup posudzovania zhody na základe vnútornej kontroly uvedený v prílohe VI, v ktorom sa nestanovuje účasť notifikovanej osoby.

3. V prípade vysokorizikových systémov umelej inteligencie, na ktoré sa vzťahujú právne akty uvedené v prílohe II oddiele A, sa poskytovateľ riadi príslušným posúdením zhody vyžadovaným podľa uvedených právnych aktov. Na uvedené vysokorizikové systémy umelej inteligencie sa vzťahujú požiadavky stanovené v kapitole 2 tejto hlavy a musia byť zahrnuté do tohto posúdenia. Uplatňujú sa aj body 4.3, 4.4, 4.5 a piaty odsek bodu 4.6 prílohy VII.

Na účely uvedeného posúdenia sú notifikované osoby, ktoré boli notifikované podľa uvedených právnych aktov, oprávnené kontrolovať zhodu vysokorizikových systémov umelej inteligencie s požiadavkami stanovenými v kapitole 2 tejto hlavy za predpokladu, že v rámci postupu notifikácie podľa uvedených právnych aktov sa posúdil súlad týchto notifikovaných osôb s požiadavkami stanovenými v článku 33 ods. 4, 9 a 10.

Ak právne akty uvedené v prílohe II oddiele a umožňujú výrobcovi výrobku za predpokladu, že uplatnil všetky harmonizované normy vzťahujúce sa na všetky príslušné požiadavky, neuplatňovať posudzovanie zhody treťou stranou, môže tento výrobca využiť túto možnosť len vtedy, ak uplatnil aj harmonizované normy alebo prípadne spoločné špecifikácie uvedené v článku 41, ktoré sa vzťahujú na požiadavky stanovené v kapitole 2 tejto hlavy.

4. [vypúšťa sa]

5. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 73 na účely aktualizácie príloh VI a VII vzhľadom na technický pokrok.

6. Komisia je splnomocnená prijímať delegované akty na zmenu odsekov 1 a 2 s cieľom podrobiť vysokorizikové systémy umelej inteligencie 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 nesmie presiahnuť päť rokov. Na žiadosť poskytovateľa možno platnosť certifikátu predĺžiť na ďalšie obdobia, z ktorých žiadne nesmie presiahnuť päť rokov, 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 umelej inteligencie už nespĺňa požiadavky stanovené v kapitole 2 tejto hlavy, 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 zdôvodní.

Článok 45

Odvolanie proti rozhodnutiam notifikovaných osôb

Proti rozhodnutiam notifikovaného orgánu je možné odvolať sa.

Článok 46

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 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 kvality, ktoré vydala;

b) certifikátoch EÚ o posúdení technickej dokumentácie alebo 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 systémy umelej inteligencie, relevantné informácie o otázkach týkajúcich sa negatívnych a na požiadanie aj pozitívnych výsledkov posudzovania zhody.

4. Povinnosti uvedené v odsekoch 1 až 3 sa plnia v súlade s článkom 70.

Článok 47

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 špecifických vysokorizikových systémov umelej inteligencie 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 ukončia bez zbytočného odkladu.

1a. 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 umelej inteligencie bez povolenia uvedeného v odseku 1 za predpokladu, že o takéto povolenie sa bez zbytočného odkladu požiada počas jeho používania alebo po ňom, a ak sa takéto povolenie zamietne, jeho používanie sa s okamžitým účinkom zastaví a všetky výsledky a výstupy tohto použitia sa okamžite zničia.

2. Povolenie uvedené v odseku 1 sa vydá len vtedy, ak orgán dohľadu nad trhom dospeje k záveru, že vysokorizikový systém umelej inteligencie spĺňa požiadavky kapitoly 2 tejto hlavy. o každom povolení vydanom podľa odseku 1 informuje orgán dohľadu nad trhom Komisiu a ostatné členské štáty. Táto povinnosť sa nevzťahuje na citlivé prevádzkové údaje vo vzťahu k orgánom presadzovania práva.

3. [vypúšťa sa]

4. [vypúšťa sa]

5. [vypúšťa sa]

6. V prípade vysokorizikových systémov umelej inteligencie súvisiacich s výrobkami, na ktoré sa vzťahujú harmonizačné právne predpisy Únie uvedené v prílohe II oddiele A, sa uplatňujú len výnimky z postupu posudzovania zhody, ktoré sú uvedené v daných právnych predpisoch.

Článok 48
EÚ vyhlásenie o zhode

1. Pre každý systém umelej inteligencie poskytovateľ vyhotoví EÚ vyhlásenie o zhode v písomnej podobe alebo sprevádzané elektronickým podpisom, ktoré desať rokov po uvedení systému umelej inteligencie na trh alebo do prevádzky uchováva k dispozícii pre potreby príslušných vnútroštátnych orgánov. v EÚ vyhlásení o zhode musí byť uvedený systém umelej inteligencie, pre ktorý bolo vyhotovené. Na požiadanie sa kópia EÚ vyhlásenia o zhode predloží príslušným vnútroštátnym orgánom.

2. V EÚ vyhlásení o zhode sa uvedie, že príslušný vysokorizikový systém umelej inteligencie spĺňa požiadavky stanovené v kapitole 2 tejto hlavy. EÚ vyhlásenie o zhode musí obsahovať informácie uvedené v prílohe v a musí byť preložené do jazyka, ktorému príslušné vnútroštátne orgány členského štátu alebo štátov, kde sa vysokorizikový systém umelej inteligencie sprístupňuje, bez problémov rozumejú.

3. Ak sa na vysokorizikové systémy umelej inteligencie 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 umelej inteligencie jedno EÚ vyhlásenie o zhode. Toto vyhlásenie musí obsahovať všetky informácie potrebné na to, aby bolo možné identifikovať harmonizačné právne predpisy Únie, na ktoré sa vyhlásenie vzťahuje.

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

5. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 73 na účely aktualizácie obsahu EÚ vyhlásenia o zhode stanoveného v prílohe v s cieľom zaviesť prvky, ktorých potreba vznikne vzhľadom na technický pokrok.

Článok 49

Označenie CE

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

2. Označenie CE sa na vysokorizikové systémy umelej inteligencie umiestni tak, aby bolo viditeľné, čitateľné a neodstrániteľné. Ak to nie je možné alebo odôvodnené z hľadiska povahy vysokorizikového systému umelej inteligencie, označenie sa umiestni na obale alebo prípadne v sprievodnej dokumentácii.

3. V relevantných prípadoch za označením CE nasleduje identifikačné číslo notifikovanej osoby zodpovednej za postupy posudzovania zhody stanovené v článku 43. Identifikačné číslo sa uvedie aj v akomkoľvek reklamnom materiáli, v ktorom sa nachádza informácia, že vysokorizikový systém umelej inteligencie spĺňa požiadavky na označenie CE.

Článok 50

[vypúšťa sa]

Článok 51

Registrácia príslušných prevádzkovateľov a vysokorizikových systémov umelej inteligencie uvedených v prílohe III

1. Pred uvedením vysokorizikového systému umelej inteligencie uvedeného v prílohe III na trh alebo do prevádzky s výnimkou vysokorizikových systémov umelej inteligencie uvedených v prílohe III bodoch 1, 6 a 7 v oblastiach presadzovania práva, migrácie, azylu a riadenia kontroly hraníc a vysokorizikových systémov umelej inteligencie uvedených v prílohe III bode 2 sa poskytovateľ a prípadne splnomocnený zástupca zaregistrujú v databáze EÚ uvedenej v článku 60. Poskytovateľ prípadne splnomocnený zástupca zaregistruje v uvedenej databáze aj svoje systémy.

2. Pred použitím vysokorizikového systému umelej inteligencie uvedeného v prílohe III sa používatelia vysokorizikových systémov umelej inteligencie, ktorí sú orgánmi verejnej moci, verejnými agentúrami alebo verejnými subjektmi alebo subjektmi konajúcimi v ich mene, zaregistrujú v databáze EÚ uvedenej v článku 60 a vyberú systém, ktorý plánujú používať.

   Povinnosti stanovené v predchádzajúcom pododseku sa nevzťahujú na orgány, agentúry ani subjekty v oblasti presadzovania práva, kontroly hraníc, imigrácie a azylu, orgány, agentúry ani subjekty, ktoré používajú vysokorizikové systémy umelej inteligencie uvedené v prílohe III bode 2, ani na subjekty konajúce v ich mene.

HLAVA IV

POVINNOSTI V OBLASTI TRANSPARENTNOSTI PRE POSKYTOVATEĽOV A POUŽÍVATEĽOV URČITÝCH SYSTÉMOV UMELEJ INTELIGENCIE

Článok 52

Povinnosti v oblasti transparentnosti pre poskytovateľov a používateľov určitých systémov umelej inteligencie

1. Poskytovatelia zabezpečia, aby systémy umelej inteligencie určené na interakciu s fyzickými osobami boli koncipované a vyvinuté tak, aby boli fyzické osoby informované o tom, že komunikujú so systémom umelej inteligencie, 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 umelej inteligencie, ktoré sa podľa zákona môžu používať na odhaľovanie, prevenciu, vyšetrovanie a 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. Používatelia systému biometrickej kategorizácie musia o prevádzke takéhoto systému informovať fyzické osoby, ktoré sú mu vystavené. Táto povinnosť sa nevzťahuje na systémy umelej inteligencie používané na biometrickú kategorizáciu, ktoré zákon povoľuje na odhaľovanie, prevenciu a vyšetrovanie trestných činov, s výhradou primeraných záruk ochrany práv a slobôd tretích strán.

2a. Používatelia systému na rozpoznávanie emócií musia o prevádzke takéhoto systému informovať fyzické osoby, ktoré sú mu vystavené. Táto povinnosť sa nevzťahuje na systémy umelej inteligencie používané na rozpoznávanie emócií, ktoré zákon povoľuje na odhaľovanie, prevenciu a vyšetrovanie trestných činov, s výhradou primeraných záruk ochrany práv a slobôd tretích strán.

3. Používatelia systému umelej inteligencie, ktorý vytvára obrazový obsah, zvukový obsah alebo videoobsah, alebo s takýmto obsahom manipuluje, pričom tento obsah sa zjavne podobá existujúcim osobám, predmetom, miestam alebo iným subjektom či udalostiam a niektorým osobám by sa mohol mylne javiť ako pravý alebo pravdivý („deepfake“), musia informovať, že tento obsah bol umelo vytvorený alebo zmanipulovaný.

Prvý pododsek sa však neuplatňuje, ak je použitie povolené zákonom na odhaľovanie, prevenciu, vyšetrovanie a stíhanie trestných činov alebo ak je obsah súčasťou zjavne tvorivého, satirického, umeleckého alebo fiktívneho diela alebo programu, ktorý podlieha primeraným zárukám ochrany práv a slobôd tretích strán.

3a. Informácie uvedené v odsekoch 1 až 3 sa fyzickým osobám poskytnú jasným a rozlíšiteľným spôsobom najneskôr v čase prvej interakcie alebo vystavenia.

4. Odsekmi 1, 2, 2a, 3 a 3a nie sú dotknuté požiadavky a povinnosti stanovené v hlave III tohto nariadenia ani iné povinnosti v oblasti transparentnosti pre používateľov systémov umelej inteligencie stanovené v práve Únie alebo vo vnútroštátnom práve.

HLAVA V

OPATRENIA NA PODPORU INOVÁCIÍ

Článok 53

Experimentálne regulačné prostredia pre umelú inteligenciu

-1a. Príslušné vnútroštátne orgány môžu zriadiť experimentálne regulačné prostredia pre umelú inteligenciu na vývoj, trénovanie, testovanie a validáciu inovačných systémov umelej inteligencie pod priamym dohľadom príslušného vnútroštátneho orgánu, za jeho usmerňovania a s jeho podporou pred uvedením týchto systémov na trh alebo do prevádzky. Takéto experimentálne regulačné prostredia môžu zahŕňať testovanie v reálnych podmienkach pod dohľadom príslušných vnútroštátnych orgánov.

-1b. [vypúšťa sa]

-1c. Príslušné vnútroštátne orgány v prípade potreby spolupracujú s inými relevantnými orgánmi a môžu umožniť zapojenie ďalších aktérov v rámci ekosystému umelej inteligencie.

-1d. Tento článok nemá vplyv na iné experimentálne regulačné prostredia zriadené podľa vnútroštátneho práva alebo práva Únie, a to ani v prípadoch, keď výrobky alebo služby, ktoré sa v nich testujú, sú spojené s používaním inovačných systémov umelej inteligencie. Členské štáty zabezpečia primeranú úroveň spolupráce medzi orgánmi vykonávajúcimi dohľad nad týmito inými experimentálnymi prostrediami a príslušnými vnútroštátnymi orgánmi.

1. [vypúšťa sa]

1a. [vypúšťa sa]

1b. Účelom zriadenia experimentálnych regulačných prostredí pre umelú inteligenciu podľa tohto nariadenia je prispieť k jednému alebo viacerým z týchto cieľov:

a) podporovať inováciu a konkurencieschopnosť a uľahčovať rozvoj ekosystému umelej inteligencie;
b) uľahčovať a urýchliť prístup systémov umelej inteligencie na trh Únie, najmä ak ich poskytujú malé a stredné podniky (MSP) vrátane startupov;
c) zlepšiť právnu istotu a prispieť k výmene najlepších postupov prostredníctvom spolupráce s orgánmi zapojenými do experimentálneho regulačného prostredia pre umelú inteligenciu s cieľom zabezpečiť budúci súlad s týmto nariadením a prípadne s inými právnymi predpismi Únie a členských štátov;
d) prispievať k regulačnému vzdelávaniu založenému na dôkazoch.

2. [vypúšťa sa]

2a. Prístup k experimentálnym regulačným prostrediam pre umelú inteligenciu je otvorený pre každého poskytovateľa alebo potenciálneho poskytovateľa systému umelej inteligencie, ktorý spĺňa kritériá oprávnenosti a podmienky účasti uvedené v odseku 6 písm. a) a ktorého vybrali príslušné vnútroštátne orgány na základe výberového konania uvedeného v odseku 6 písm. b). Poskytovatelia alebo potenciálni poskytovatelia môžu takisto predkladať žiadosti v partnerstve s používateľmi alebo akýmikoľvek inými relevantnými tretími stranami.

Účasť na experimentálnom regulačnom prostredí pre umelú inteligenciu je obmedzená na obdobie, ktoré je primerané zložitosti a rozsahu projektu. Príslušný vnútroštátny orgán môže túto lehotu predĺžiť.

Účasť na experimentálnom regulačnom prostredí pre umelú inteligenciu vychádza z osobitného plánu uvedeného v odseku 6 tohto článku, na ktorom sa podľa potreby dohodne účastník alebo účastníci a príslušný vnútroštátny orgán alebo orgány.

3. Právomoci orgánov dohliadajúcich na experimentálne regulačné prostredie týkajúce sa dohľadu a nápravy nie sú ich účasťou na takomto prostredí dotknuté. Uvedené orgány vykonávajú svoje právomoci v oblasti dohľadu flexibilným spôsobom v medziach príslušných právnych predpisov, pričom pri vykonávaní právnych ustanovení v prípade konkrétneho projektu experimentálneho prostredia pre umelú inteligenciu využívajú svoje diskrečné právomoci s cieľom podporovať inovácie v oblasti umelej inteligencie v Únii.

Za predpokladu, že účastník alebo účastníci dodržiavajú plán experimentálneho prostredia a podmienky svojej účasti uvedené v odseku 6 písm. c) a v dobrej viere dodržiavajú usmernenia orgánov, neuložia orgány žiadne správne pokuty za porušenie uplatniteľných právnych predpisov Únie alebo členských štátov týkajúcich sa systému umelej inteligencie, nad ktorým sa vykonáva dohľad v experimentálnom prostredí, vrátane ustanovení tohto nariadenia.

4. Účastníci ostávajú zodpovední za všetky škody spôsobené počas ich účasti na experimentálnom regulačnom prostredí pre umelú inteligenciu podľa uplatniteľných právnych predpisov Únie a členských štátov o zodpovednosti.

4a. Na žiadosť poskytovateľa alebo potenciálneho poskytovateľa systému umelej inteligencie poskytne príslušný vnútroštátny orgán v prípade potreby písomný dôkaz o činnostiach úspešne vykonávaných v experimentálnom prostredí. Príslušný vnútroštátny orgán poskytne aj výstupnú správu, v ktorej podrobne opíše činnosti vykonávané v experimentálnom prostredí a súvisiace výsledky a vzdelávacie výstupy. Takéto písomné dôkazy a výstupné správy by mohli orgány dohľadu nad trhom alebo notifikované osoby prípadne zohľadniť v kontexte postupov posudzovania zhody alebo kontrol v rámci dohľadu nad trhom.

S výhradou ustanovení o dôvernosti v článku 70 a so súhlasom účastníkov experimentálneho prostredia sú Európska komisia a rada pre umelú inteligenciu oprávnené na prístup k výstupným správam a podľa potreby ich zohľadňujú pri vykonávaní svojich úloh podľa tohto nariadenia. Ak s tým účastník aj príslušný vnútroštátny orgán výslovne súhlasia, výstupná správa sa môže zverejniť prostredníctvom jednotnej informačnej platformy uvedenej v článku 55 ods. 3 písm. b).

4b. Experimentálne regulačné prostredia pre umelú inteligenciu musia byť navrhnuté a realizované tak, aby v relevantných prípadoch uľahčovali cezhraničnú spoluprácu medzi príslušnými vnútroštátnymi orgánmi.

5. Príslušné vnútroštátne orgány zverejňujú výročné správy o realizácii experimentálnych regulačných prostredí pre umelú inteligenciu vrátane osvedčených postupov, získaných poznatkov a odporúčaní týkajúcich sa ich organizácie a prípadne aj uplatňovania tohto nariadenia a iných právnych predpisov Únie, nad ktorým sa v rámci regulačného prostredia vykonáva dohľad. Tieto výročné správy sa predkladajú rade pre umelú inteligenciu, ktorá zverejní súhrn všetkých osvedčených postupov, získaných poznatkov a odporúčaní. Táto povinnosť zverejňovať výročné správy sa nevzťahuje na citlivé prevádzkové údaje týkajúce sa činností orgánov presadzovania práva, kontroly hraníc a imigračných alebo azylových orgánov. Komisia a rada pre umelú inteligenciu v prípade potreby zohľadnia výročné správy pri vykonávaní svojich úloh podľa tohto nariadenia.

5b. Komisia zabezpečí, aby informácie o experimentálnych regulačných prostrediach pre umelú inteligenciu vrátane tých, ktoré sa zriadia podľa tohto článku, boli dostupné prostredníctvom jednotnej informačnej platformy uvedenej v článku 55 ods. 3 písm. b).

6. Spôsoby a podmienky zriadenia a prevádzky experimentálnych regulačných prostredí pre umelú inteligenciu podľa tohto nariadenia sa prijmú prostredníctvom vykonávacích aktov v súlade s postupom preskúmania uvedeným v článku 74 ods. 2.

Spôsoby a podmienky v najväčšej možnej miere podporujú flexibilitu príslušných vnútroštátnych orgánov pri zriaďovaní a prevádzkovaní ich experimentálnych regulačných prostredí pre umelú inteligenciu, podporujú inováciu a regulačné vzdelávanie a zohľadňujú najmä osobitné okolnosti a kapacity zúčastnených MSP vrátane startupov.

Uvedené vykonávacie akty obsahujú spoločné hlavné zásady týkajúce sa týchto otázok:

a) oprávnenosť a výber účastníkov experimentálneho regulačného prostredia pre umelú inteligenciu;
b) postup podávania žiadostí, účasti, monitorovania, odchodu z experimentálneho regulačného prostredia pre umelú inteligenciu a jeho ukončenia vrátane plánu experimentálneho prostredia a výstupnej správy;
c) podmienky vzťahujúce sa na účastníkov.

7. Ak príslušné vnútroštátne orgány zvažujú povolenie testovania v reálnych podmienkach, nad ktorými sa vykonáva dohľad v rámci experimentálneho regulačného prostredia pre umelú inteligenciu 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. v prípade potreby spolupracujú s inými príslušnými vnútroštátnymi orgánmi s cieľom zabezpečiť jednotné postupy v celej Únii.

Článok 54

Ďalšie spracovanie osobných údajov na účely vývoja určitých systémov umelej inteligencie vo verejnom záujme v experimentálnom regulačnom prostredí pre umelú inteligenciu

1. Osobné údaje zákonne zozbierané na iné účely sa v experimentálnom regulačnom prostredí pre umelú inteligenciu môžu spracúvať na účely vývoja, testovania a trénovania inovačných systémov umelej inteligencie v regulačnom prostredí za týchto kumulatívnych podmienok:

   a) inovačné systémy umelej inteligencie sa vyvíjajú na ochranu závažného verejného záujmu orgánom verejnej moci alebo inou fyzickou alebo právnickou osobou, ktorá sa spravuje verejným právom alebo súkromným právom, a to v jednej alebo viacerých z týchto oblastí:

      i) [vypúšťa sa]

      ii) verejná bezpečnosť a zdravie vrátane prevencie, kontroly a liečby chorôb a zlepšovania systémov zdravotnej starostlivosti;

      iii) ochrana a zlepšovanie kvality životného prostredia vrátane zelenej transformácie, zmierňovania zmeny klímy a adaptácie na ňu;

      iv) energetická udržateľnosť, doprava a mobilita;

      v) efektívnosť a kvalita verejnej správy a verejných služieb;

      vi) kybernetické bezpečnosť a odolnosť kritickej infraštruktúry.

   b) spracúvané údaje sú potrebné na splnenie jednej alebo viacerých požiadaviek uvedených v hlave III kapitole 2, ak tieto požiadavky nie je možné účinne splniť spracovaním anonymizovaných, syntetických alebo iných ako osobných údajov;

c) existujú účinné mechanizmy monitorovania umožňujúce zistiť, či počas experimentovania v regulačných 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 mechanizmus reakcie na rýchle zmiernenie týchto rizík a v prípade potreby na zastavenie spracúvania;

d) všetky osobné údaje, ktoré sa majú spracúvať v rámci experimentálneho prostredia, sú vo funkčne oddelenom, izolovanom a chránenom prostredí spracovania údajov pod kontrolou účastníkov a prístup k týmto údajom majú len oprávnené osoby;

e) žiadne spracúvané osobné údaje sa nesmú posielať, prenášať ani inak sprístupňovať iným stranám, ktoré nie sú účastníkmi experimentálneho prostredia, pokiaľ k takémuto zverejneniu nedôjde v súlade s nariadením (EÚ) 2016/679 prípadne nariadením 2018/725 a pokiaľ s tým všetci účastníci nesúhlasia;

f) akékoľvek spracovanie osobných údajov v rámci experimentálneho prostredia nemá vplyv na uplatňovanie práv dotknutých osôb, ktoré sú ustanovené v právnych predpisoch Únie o ochrane osobných údajov, najmä v článku 22 nariadenia (EÚ) 2016/679 a článku 24 nariadenia (EÚ) 2018/1725;

g) všetky osobné údaje spracúvané v rámci 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 na 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 umelej inteligencie;

j) na webovom sídle príslušných orgánov sa zverejní krátke zhrnutie projektu umelej inteligencie vyvinutého v regulačnom prostredí, jeho cieľov a očakávaných výsledkov. Táto povinnosť sa nevzťahuje na citlivé prevádzkové údaje týkajúce sa činností orgánov presadzovania práva, kontroly hraníc, imigračných alebo azylových orgánov.

1a. 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 pod kontrolou a v zodpovednosti orgánov presadzovania práva sa spracúvanie osobných údajov v experimentálnych regulačných prostrediach pre umelú inteligenciu zakladá na osobitnom právnom predpise členského štátu alebo Únie a podlieha rovnakým kumulatívnym podmienkam, ktoré sa uvádzajú v odseku 1.

2. Odsekom 1 nie sú dotknuté právne predpisy Únie ani členských štátov, ktorými sa stanovuje základ pre spracúvanie osobných údajov, ktoré je potrebné na účely vývoja, testovania a trénovania inovačných systémov umelej inteligencie, alebo akýkoľvek iný právny základ v súlade s právom Únie o ochrane osobných údajov.

Článok 54a

Testovanie vysokorizikových systémov umelej inteligencie v reálnych podmienkach mimo experimentálnych regulačných prostredí pre umelú inteligenciu

1. Poskytovatelia alebo potenciálni poskytovatelia vysokorizikových systémov umelej inteligencie uvedených v prílohe III môžu vykonávať testovanie systémov umelej inteligencie v reálnych podmienkach mimo experimentálnych regulačných prostredí pre umelú inteligenciu v súlade s ustanoveniami tohto článku a plánom testovania v reálnych podmienkach uvedeným v tomto článku.

Podrobné prvky plánu testovania v reálnych podmienkach sa spresnia vo vykonávacích aktoch prijatých Komisiou v súlade s postupom preskúmania uvedeným v článku 74 ods. 2.

Týmto ustanovením nie sú dotknuté právne predpisy Únie ani členských štátov týkajúce sa testovania v reálnych podmienkach, pokiaľ ide o vysokorizikové systémy umelej inteligencie súvisiace s výrobkami, na ktoré sa vzťahujú právne predpisy uvedené v prílohe II.

2. Poskytovatelia alebo potenciálni poskytovatelia môžu vykonávať testovanie vysokorizikových systémov umelej inteligencie uvedených v prílohe III v reálnych podmienkach kedykoľvek pred uvedením systému umelej inteligencie na trh alebo do prevádzky samostatne alebo v partnerstve s jedným alebo viacerými potenciálnymi používateľmi.

3. Testovaním vysokorizikových systémov umelej inteligencie v reálnych podmienkach podľa tohto článku nie je dotknuté etické preskúmanie, ktoré sa môže vyžadovať podľa vnútroštátneho práva alebo práva Únie.

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 alebo štátoch, v ktorých sa má testovanie v reálnych podmienkach vykonať;

b) orgán dohľadu nad trhom v členskom štáte alebo štátoch, v ktorých sa má testovanie v reálnych podmienkach vykonať, nevzniesol námietku voči testovaniu do 30 dní od predloženia plánu;

c) poskytovateľ alebo potenciálny poskytovateľ s výnimkou vysokorizikových systémov umelej inteligencie uvedených v prílohe III bodoch 1, 6 a 7 v oblastiach presadzovania práva, migrácie, azylu a riadenia kontroly hraníc a vysokorizikových systémov umelej inteligencie uvedených v prílohe III bode 2 zaregistroval testovanie v reálnych podmienkach v databáze EÚ uvedenej v článku 60 ods. 5a s jedinečným jednotným identifikačným číslom pre celú Úniu a predložil informácie uvedené v prílohe VIIIa;

d) poskytovateľ alebo potenciálny poskytovateľ vykonávajúci testovanie v reálnych podmienkach je usadený v Únii alebo vymenoval právneho zástupcu na účely testovania v reálnych podmienkach, ktorý je usadený v Únii;

e) údaje zhromaždené a spracované na účely testovania v reálnych podmienkach sa neprenášajú do krajín mimo Únie, pokiaľ prenos a spracovanie neposkytujú záruky rovnocenné zárukám stanoveným v práve Únie;

f) testovanie v reálnych podmienkach netrvá dlhšie, ako je potrebné na dosiahnutie jeho cieľov, a v žiadnom prípade nie dlhšie ako 12 mesiacov;

g) osoby patriace do zraniteľných skupín vzhľadom na svoj vek, telesné alebo duševné postihnutie sú primerane chránené;

h) [vypúšťa sa]

i) ak poskytovateľ alebo potenciálny poskytovateľ organizuje testovanie v reálnych podmienkach v spolupráci s jedným alebo viacerými potenciálnymi používateľmi, títo boli informovaní o všetkých aspektoch testovania, ktoré sú relevantné pre ich rozhodnutie zúčastniť sa, a dostali príslušný návod na použitie systému umelej inteligencie uvedený v článku 13; poskytovateľ alebo potenciálny poskytovateľ a používateľ alebo používatelia 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 iných uplatniteľných právnych predpisov Únie a členských štátov;

j) účastníci testovania v reálnych podmienkach poskytli informovaný súhlas v súlade s článkom 54b alebo v prípade presadzovania práva, ak by získanie informovaného súhlasu bránilo testovaniu systému umelej inteligencie, samotné testovanie a výsledok testovania v reálnych podmienkach nesmú mať negatívny vplyv na subjekt;

k) na testovanie v reálnych podmienkach účinne dohliada poskytovateľ alebo potenciálny poskytovateľ a používateľ alebo používatelia s osobami, ktoré sú primerane kvalifikované v príslušnej oblasti a majú potrebnú kapacitu, odbornú prípravu a právomoc na vykonávanie svojich úloh;

l) predpovede, odporúčania alebo rozhodnutia systému umelej inteligencie možno účinne zvrátiť alebo nezohľadniť.

5. Ktorýkoľvek subjekt testovania v reálnych podmienkach, prípadne jeho zákonom určený zástupca, môže kedykoľvek odstúpiť od testovania odvolaním svojho informovaného súhlasu bez akejkoľvek následnej ujmy a bez toho, aby musel poskytnúť akékoľvek odôvodnenie. Odvolanie informovaného súhlasu nemá vplyv na už vykonané činnosti a použitie údajov získaných na základe informovaného súhlasu pred jeho odvolaním.

6. Každý závažný incident zistený počas testovania v reálnych podmienkach sa oznamuje vnútroštátnemu orgánu dohľadu nad trhom v súlade s článkom 62 tohto nariadenia. 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 umelej inteligencie od používateľa pri takomto ukončení testovania v reálnych podmienkach.

7. Poskytovateľ alebo potenciálni poskytovatelia informujú vnútroštátny orgán dohľadu nad trhom v členskom štáte alebo štátoch, v ktorých sa má vykonať testovanie v reálnych podmienkach, o pozastavení alebo ukončení testovania v reálnych podmienkach a o konečných výsledkoch.

8. Poskytovateľ alebo potenciálni poskytovatelia ostávajú zodpovední za všetky škody spôsobené počas ich účasti na testovaní v reálnych podmienkach podľa uplatniteľných právnych predpisov Únie a členských štátov o zodpovednosti.

Článok 54b

Informovaný súhlas s účasťou na testovaní v reálnych podmienkach mimo experimentálnych regulačných prostredí pre umelú inteligenciu

1. Na účely testovania v reálnych podmienkach podľa článku 54a subjekt testovania slobodne udelí informovaný súhlas pred svojou účasťou na takomto testovaní a po tom, ako bol riadne informovaný stručnými, jasnými, relevantnými a zrozumiteľnými informáciami, ktoré sa týkajú:

i) povahy a cieľov testovania v reálnych podmienkach a možných nepríjemností, ktoré môžu byť spojené s jeho účasťou;

ii) podmienok, za ktorých sa má vykonávať testovanie v reálnych podmienkach, vrátane očakávaného trvania účasti subjektu;

iii) práv a záruk subjektu týkajúcich sa účasti, najmä jeho práva odmietnuť účasť a práva kedykoľvek odstúpiť od testovania v reálnych podmienkach bez akejkoľvek následnej ujmy a bez toho, aby musel poskytnúť akékoľvek odôvodnenie;

iv) spôsobov žiadosti o zvrátenie alebo nezohľadnenie predpovedí, odporúčaní alebo rozhodnutí systému umelej inteligencie;

v) jedinečného jednotného identifikačného čísla testovania v reálnych podmienkach pre celú Úniu v súlade s článkom 54a ods. 4c a kontaktných údajov poskytovateľa alebo jeho právneho zástupcu, od ktorého možno získať ďalšie informácie.

2. Informovaný súhlas musí byť datovaný a zdokumentovaný a kópia sa poskytne subjektu alebo jeho právnemu zástupcovi.

Článok 55

Podporné opatrenia pre prevádzkovateľov, najmä MSP vrátane startupov

1. Členské štáty prijmú tieto opatrenia:

a) MSP vrátane startupom poskytnú prednostný prístup k experimentálnym regulačným prostrediam pre umelú inteligenciu, pokiaľ spĺňajú kritériá oprávnenosti a podmienky účasti;

b) organizujú osobitné činnosti na zvyšovanie informovanosti a činnosti odbornej prípravy o uplatňovaní tohto nariadenia prispôsobené potrebám MSP vrátane startupov a prípadne miestnych orgánov verejnej správy;

c) v prípade potreby zriadia osobitný kanál na komunikáciu s MSP vrátane startupov a prípadne 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 na experimentálnych regulačných prostrediach pre umelú inteligenciu.

2. Pri stanovovaní poplatkov za posudzovanie zhody podľa článku 43 sa zohľadnia osobitné záujmy a potreby MSP vrátane startupov tak, že sa tieto poplatky znížia úmerne k ich veľkosti, veľkosti trhu a iným relevantným ukazovateľom.

3. Komisia prijme tieto opatrenia:

a) na žiadosť rady pre umelú inteligenciu poskytne štandardizované vzory pre oblasti, na ktoré sa vzťahuje toto nariadenie;

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 informovanosti o povinnostiach vyplývajúcich z tohto nariadenia;

d) hodnotí a podporuje zbližovanie najlepších postupov v postupoch verejného obstarávania v súvislosti so systémami umelej inteligencie.

Článok 55a

Výnimky pre špecifických prevádzkovateľov

1. Povinnosti stanovené v článku 17 tohto nariadenia sa nevzťahujú na mikropodniky vymedzené v článku 2 ods. 3 prílohy k odporúčaniu Komisie 2003/361/ES o vymedzení mikropodnikov, malých a stredných podnikov za predpokladu, že tieto podniky nemajú partnerské podniky ani prepojené podniky vymedzené v článku 3 tej istej prílohy.

2. Odsek 1 sa nesmie vykladať tak, že týchto prevádzkovateľov oslobodzuje od plnenia akýchkoľvek iných požiadaviek a povinností stanovených v tomto nariadení vrátane tých, ktoré sú stanovené v článkoch 9, 61 a 62.

3. Požiadavky a povinnosti týkajúce sa systémov umelej inteligencie na všeobecné účely stanovené v článku 4b sa nevzťahujú na mikropodniky, malé a stredné podniky za predpokladu, že tieto podniky nemajú partnerské ani prepojené podniky vymedzené v článku 3 prílohy k odporúčaniu Komisie 2003/361/ES o vymedzení mikropodnikov, malých a stredných podnikov.

HLAVA VI

SPRÁVA A RIADENIE

KAPITOLA 1

EURÓPSKA RADA PRE UMELÚ INTELIGENCIU

Článok56

Zriadenie a štruktúra Európskej rady pre umelú inteligenciu

1. Zriaďuje sa Európska rada pre umelú inteligenciu (ďalej len „rada“).

2. Rada sa skladá z jedného zástupcu každého členského štátu. Európsky dozorný úradník pre ochranu údajov sa zúčastňuje ako pozorovateľ. Komisia sa tiež zúčastňuje na zasadnutiach rady bez toho, aby sa zúčastňovala na hlasovaní.

   Rada môže v jednotlivých prípadoch prizvať na zasadnutia iné orgány, subjekty alebo expertov členských štátov a Únie, ak sú prerokúvané otázky pre nich relevantné.

2a. Každého zástupcu určí členský štát na obdobie troch rokov, ktoré možno raz obnoviť.

2aa. Členské štáty zabezpečia, aby ich zástupcovia v rade:

   i) mali vo svojom členskom štáte príslušné kompetencie a právomoci na to, aby aktívne prispievali k plneniu úloh rady uvedených v článku 58;

   i). boli určení ako jednotné kontaktné miesto vo vzťahu k rade a v prípade potreby s prihliadnutím na potreby členských štátov ako jednotné kontaktné miesto pre zainteresované strany;

iii) boli splnomocnení uľahčovať konzistentnosť a koordináciu medzi príslušnými vnútroštátnymi 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.

3. Určení zástupcovia členských štátov prijmú rokovací poriadok rady dvojtretinovou väčšinou.

V rokovacom poriadku sa stanovujú najmä postupy výberového konania, trvanie mandátu a špecifikácie úloh predsedu, postupy hlasovania a organizácia činností rady a jej podskupín.

Rada zriadi stálu podskupinu slúžiacu ako platforma pre zainteresované strany na poskytovanie poradenstva rade vo všetkých otázkach týkajúcich sa vykonávania tohto nariadenia vrátane prípravy vykonávacích a delegovaných aktov. Na tento účel sa na účasť v tejto podskupine prizvú organizácie zastupujúce záujmy poskytovateľov a používateľov systémov umelej inteligencie vrátane MSP a startupov, ako aj organizácie občianskej spoločnosti, zástupcovia dotknutých osôb, výskumní pracovníci, normalizačné organizácie, notifikované osoby, laboratóriá a skúšobné a experimentačné zariadenia. Výbor 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, respektíve notifikovaných osôb.

Na účely preskúmania konkrétnych otázok môže rada podľa potreby zriaďovať ďalšie stále alebo dočasné podskupiny. Zainteresované strany uvedené v predchádzajúcom pododseku môžu byť v prípade potreby prizvané do takýchto podskupín alebo na osobitné zasadnutia týchto podskupín ako pozorovatelia.

3a. Rada je organizovaná a funguje tak, aby sa zabezpečila objektivita a nestrannosť jej činností.

4. Rade predsedá jeden zo zástupcov členských štátov. Komisia na žiadosť predsedu zvoláva zasadnutia a pripravuje program v súlade s úlohami rady podľa tohto nariadenia a s rokovacím poriadkom rady. Činnostiam rady podľa tohto nariadenia poskytuje Komisia administratívnu a analytickú podporu.

Článok 57
[vypúšťa sa]

Článok 58
Úlohy rady

Rada poskytuje poradenstvo a pomoc Komisii a členským štátom s cieľom uľahčiť konzistentné a účinné uplatňovanie tohto nariadenia. Na tento účel môže rada najmä:

a) zhromažďovať technické a regulačné znalosti a najlepšie postupy a zdieľať ich s členskými štátmi;

b) prispievať k harmonizácii administratívnych postupov v členských štátoch, a to aj pokiaľ ide o výnimku z postupov posudzovania zhody uvedenú v článku 47, fungovanie experimentálnych regulačných prostredí a testovanie v reálnych podmienkach uvedené v článkoch 53, 54 a 54a;

c) 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 k:

   i) technickým špecifikáciám alebo existujúcim normám v súvislosti s požiadavkami stanovenými v hlave III kapitole 2;

   ii) používaniu harmonizovaných noriem alebo spoločných špecifikácií uvedených v článkoch 40 a 41;

iii) vypracovaniu usmerňujúcich dokumentov vrátane usmernení týkajúcich sa stanovovania správnych pokút uvedených v článku 71;

d) poskytovať Komisii poradenstvo o prípadnej potrebe zmeny prílohy III v súlade s článkami 4 a 7, pričom zohľadňuje relevantné dostupné dôkazy a najnovší technologický vývoj;

e) poskytovať Komisii poradenstvo počas vypracúvania delegovaného alebo vykonávacieho aktu podľa tohto nariadenia;

f) podľa potreby spolupracovať s príslušnými orgánmi EÚ, expertnými skupinami a sieťami, najmä v oblasti bezpečnosti výrobkov, kybernetickej bezpečnosti, hospodárskej súťaže, digitálnych a mediálnych služieb, finančných služieb, kryptomien, ochrany spotrebiteľa, ochrany údajov a ochrany základných práv;

g) prispievať a poskytovať Komisii príslušné poradenstvo pri vypracúvaní usmernení uvedených v článku 58a alebo požiadať o vypracovanie takýchto usmernení;

h) pomáhať orgánom dohľadu nad trhom pri práci a v spolupráci a po dohode s dotknutými orgánmi dohľadu nad trhom presadzovať a podporovať cezhraničné vyšetrovania v rámci dohľadu nad trhom, a to aj pokiaľ ide o vznik rizík systémovej povahy, ktoré môžu vyplývať zo systémov umelej inteligencie;

i) prispievať k posudzovaniu potrieb odbornej prípravy zamestnancov členských štátov zapojených do vykonávania tohto nariadenia;

j) poskytovať Komisii poradenstvo v súvislosti s medzinárodnými záležitosťami týkajúcimi sa umelej inteligencie.

KAPITOLA 1A

USMERNENIA KOMISIE

Článok 58a

Usmernenia Komisie k vykonávaniu tohto nariadenia

1. Komisia na žiadosť členských štátov alebo rady alebo z vlastnej iniciatívy vydá usmernenia o praktickom vykonávaní tohto nariadenia, a najmä o

   i) uplatňovaní požiadaviek uvedených v článkoch 8 až 15;

   ii) zakázaných praktikách uvedených v článku 5;

   iii) praktickom vykonávaní ustanovení týkajúcich sa podstatnej zmeny;

   iv) praktickom vykonávaní jednotných podmienok uvedených v článku 6 ods. 3 vrátane príkladov týkajúcich sa vysokorizikových systémov umelej inteligencie uvedených v prílohe III;

   v) praktickom plnení povinností v oblasti transparentnosti stanovených v článku 52;

   vi) vzťahu tohto nariadenia s inými príslušnými právnymi predpismi Únie, a to aj pokiaľ ide o konzistentnosť ich presadzovania.

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.

KAPITOLA 2

PRÍSLUŠNÉ VNÚTROŠTÁTNE ORGÁNY

Článok 59

Určenie príslušných vnútroštátnych orgánov

1. [vypúšťa sa]

2. Každý členský štát zriadi alebo určí aspoň jeden notifikujúci orgán a aspoň jeden orgán dohľadu nad trhom na účely tohto nariadenia ako príslušné vnútroštátne orgány. Tieto príslušné vnútroštátne orgány majú takú organizačnú štruktúru, aby zabezpečili zásady objektivity a nestrannosti vykonávania svojich činností a úloh. 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.

3. Členské štáty informujú Komisiu o orgáne alebo orgánoch, ktoré určili.

4. Členské štáty zabezpečia, aby príslušné vnútroštátne orgány mali na účinné plnenie svojich úloh podľa tohto nariadenia k dispozícii primerané finančné zdroje, technické vybavenie a riadne kvalifikované ľudské zdroje.

5. Členské štáty do [*jeden rok od nadobudnutia účinnosti tohto nariadenia*] a potom šesť mesiacov pred uplynutím lehoty uvedenej v článku 84 ods. 2 informujú Komisiu o stave finančných zdrojov, technického vybavenia a ľudských zdrojov príslušných vnútroštátnych orgánov spolu s posúdením ich primeranosti. Komisia tieto informácie postúpi rade na prerokovanie a prípadné odporúčania.

6. Komisia podporuje výmenu skúseností medzi príslušnými vnútroštátnymi orgánmi.

7. Príslušné vnútroštátne orgány môžu poskytovať poradenstvo týkajúce sa vykonávania tohto nariadenia, a to aj poradenstvo na mieru prispôsobené poskytovateľom z radov MSP vrátane startupov. Vždy, keď príslušné vnútroštátne orgány zamýšľajú poskytnúť usmernenia a poradenstvo v súvislosti so systémom umelej inteligencie v oblastiach, na ktoré sa vzťahujú iné právne predpisy Únie, podľa potreby uskutočnia konzultácie s vnútroštátnymi orgánmi, ktoré sú príslušné podľa uvedených právnych predpisov Únie. Členské štáty môžu takisto zriadiť jedno centrálne kontaktné miesto na komunikáciu s prevádzkovateľmi.

8. Pokiaľ do rozsahu pôsobnosti tohto nariadenia spadajú inštitúcie, agentúry a orgány Únie, koná ako príslušný orgán pre dohľad nad nimi európsky dozorný úradník pre ochranu údajov.

HLAVA VII

DATABÁZA EÚ PRE VYSOKORIZIKOVÉ SYSTÉMY UMELEJ INTELIGENCIE UVEDENÉ V PRÍLOHE III

Článok 60

Databáza EÚ pre vysokorizikové systémy umelej inteligencie uvedené v prílohe III

1. Komisia v spolupráci s členskými štátmi zriadi a spravuje databázu EÚ obsahujúcu informácie uvedené v odseku 2 týkajúce sa príslušných prevádzkovateľov a vysokorizikových systémov umelej inteligencie uvedených v prílohe III, ktoré sú registrované v súlade s článkami 51 a 54a. Pri stanovovaní funkčných špecifikácií takejto databázy Komisia konzultuje s radou pre umelú inteligenciu.

2. Údaje uvedené v prílohe VIII časti I vkladajú do databázy EÚ poskytovatelia, splnomocnení zástupcovia a prípadne príslušní používatelia pri svojej registrácii. Údaje uvedené v prílohe VIII časti II bodoch 1 až 11 vkladajú do databázy EÚ poskytovatelia prípadne splnomocnený zástupca v súlade s článkom 51. Údaje uvedené v prílohe VIII časti II bode 12 sa automaticky generujú v databáze na základe informácií poskytnutých príslušnými používateľmi podľa článku 51 ods. 2. Údaje uvedené v prílohe VIIIa vkladajú do databázy potenciálni poskytovatelia alebo poskytovatelia v súlade s článkom 54a.

3. [vypúšťa sa]

4. Databáza EÚ neobsahuje žiadne osobné údaje okrem informácií uvedených v prílohe VIII a nie je ňou dotknutý článok 70.

5. Prevádzkovateľom databázy EÚ je Komisia. Poskytovateľom, potenciálnym poskytovateľom a používateľom poskytuje primeranú technickú a administratívnu podporu.

5a. Informácie obsiahnuté v databáze EÚ zaregistrované v súlade s článkom 51 sú prístupné verejnosti. Informácie zaregistrované v súlade s článkom 54a sú prístupné len orgánom dohľadu nad trhom a Komisii, pokiaľ potenciálny poskytovateľ alebo poskytovateľ neudelil súhlas aj so sprístupnením týchto informácií verejnosti.

HLAVA VIII

MONITOROVANIE PO UVEDENÍ NA TRH, VÝMENA INFORMÁCIÍ, DOHĽAD NAD TRHOM

KAPITOLA 1

MONITOROVANIE PO UVEDENÍ NA TRH

Článok 61

Monitorovanie po uvedení na trh vykonávané poskytovateľmi a plán monitorovania vysokorizikových systémov umelej inteligencie po uvedení na trh

1. Poskytovatelia zavedú a zdokumentujú systém monitorovania po uvedení na trh spôsobom, ktorý je primeraný rizikám vysokorizikového systému umelej inteligencie.

2. S cieľom umožniť poskytovateľovi hodnotiť súlad systémov umelej inteligencie s požiadavkami stanovenými v hlave III kapitole 2 počas ich životného cyklu systém monitorovania po uvedení na trh zhromažďuje, dokumentuje a analyzuje relevantné údaje o výkonnosti vysokorizikových systémov umelej inteligencie, ktoré môžu poskytnúť používatelia alebo ktoré sa môžu zbierať z iných zdrojov. Táto povinnosť sa nevzťahuje na citlivé prevádzkové údaje používateľov systémov umelej inteligencie, ktorí sú orgánmi presadzovania práva.

3. Systém monitorovania po uvedení na trh sa musí zakladať na pláne monitorovania po uvedení na trh. Plán monitorovania po uvedení na trh tvorí súčasť technickej dokumentácie uvedenej v prílohe IV. Komisia prijme vykonávací akt, v ktorom stanoví podrobné ustanovenia, ktorými sa vytvorí vzor plánu monitorovania po uvedení na trh a zoznam prvkov, ktoré sa majú do plánu zahrnúť.

4. V prípade vysokorizikových systémov umelej inteligencie, na ktoré sa vzťahujú právne akty uvedené v prílohe II oddiele a a pre ktoré už sú systém a plán monitorovania po uvedení na trh zavedené podľa uvedených právnych predpisov, sa dokumentácia súvisiaca s monitorovaním po uvedení na trh vypracovaná podľa uvedených predpisov považuje za dostatočnú za predpokladu, že sa používa vzor uvedený v odseku 3.

Prvý pododsek sa uplatňuje aj na vysokorizikové systémy umelej inteligencie 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 právnych predpisov Únie v oblasti finančných služieb.

KAPITOLA 2

ZDIEĽANIE INFORMÁCIÍ O ZÁVAŽNÝCH INCIDENTOCH

Článok 62

Podávanie správ o závažných incidentoch

1. Poskytovatelia vysokorizikových systémov umelej inteligencie uvedených na trh Únie podávajú o akomkoľvek závažnom incidente správu orgánom dohľadu nad trhom členských štátov, v ktorých k tomuto závažnému incidentu došlo.

Takéto oznámenie sa musí vykonať ihneď po tom, ako poskytovateľ zistí príčinnú súvislosť medzi systémom umelej inteligencie a závažným incidentom alebo logickú pravdepodobnosť takejto súvislosti, a v každom prípade najneskôr do 15 dní po tom, ako sa poskytovateľ nadobudne vedomosť o závažnom incidente.

2. Po doručení oznámenia týkajúceho sa závažného incidentu uvedeného v článku 3 ods. 44 písm. c) príslušný orgán dohľadu nad trhom informuje vnútroštátne orgány verejnej moci alebo subjekty uvedené v článku 64 ods. 3. Na uľahčenie plnenia povinností stanovených v odseku 1 vypracuje Komisia osobitné usmernenia. Tieto usmernenia sa vydajú najneskôr 12 mesiacov po nadobudnutí účinnosti tohto nariadenia.

3. V prípade vysokorizikových systémov umelej inteligencie uvedených v prílohe III bode 5, ktoré uvádzajú na trh alebo do prevádzky poskytovatelia, ktorí sú finančnými inštitúciami, na ktorých sa vzťahujú požiadavky týkajúce sa ich vnútornej správy a riadenia, dojednaní alebo postupov podľa právnych predpisov Únie v oblasti finančných služieb, sa oznamovanie závažných incidentov obmedzuje na tie, ktoré sú uvedené v článku 3 ods. 44 písm. c).

4. V prípade vysokorizikových systémov umelej inteligencie, ktoré sú bezpečnostnými komponentmi zariadení alebo sú samy zariadeniami, na ktoré sa vzťahuje nariadenie (EÚ) 2017/745 a nariadenie (EÚ) 2017/746, sa oznamovanie závažných incidentov obmedzuje na tie, ktoré sú uvedené v článku 3 ods. 44 písm. c), a podáva sa príslušnému vnútroštátnemu orgánu, ktorý na tento účel vybrali členské štáty, v ktorých k tomuto incidentu došlo.

KAPITOLA 3

PRESADZOVANIE PRÁVA

Článok 63

Dohľad nad trhom a kontrola systémov umelej inteligencie na trhu Únie

1. Na systémy umelej inteligencie v rozsahu pôsobnosti tohto nariadenia sa vzťahuje nariadenie (EÚ) 2019/1020. Na účely účinného presadzovania tohto nariadenia sa však:

   a) každý odkaz na hospodársky subjekt podľa nariadenia (EÚ) 2019/1020 chápe tak, že zahŕňa všetkých prevádzkovateľov uvedených v článku 2 tohto nariadenia;

   b) každý odkaz na výrobok podľa nariadenia (EÚ) 2019/1020 chápe tak, že zahŕňa všetky systémy umelej inteligencie, ktoré patria do rozsahu pôsobnosti tohto nariadenia.

2. Orgány dohľadu nad trhom v rámci svojich oznamovacích povinností podľa článku 34 ods. 4 nariadenia (EÚ) 2019/1020 podávajú Komisii správy o výsledkoch príslušných činností dohľadu nad trhom podľa tohto nariadenia.

3. V prípade vysokorizikových systémov umelej inteligencie súvisiacich s výrobkami, na ktoré sa vzťahujú právne akty uvedené v prílohe II oddiele A, je orgánom dohľadu nad trhom na účely tohto nariadenia orgán zodpovedný za činnosti dohľadu nad trhom určený podľa uvedených právnych aktov alebo, za opodstatnených okolností a za predpokladu, že sa zabezpečí koordinácia, iný príslušný orgán, ktorý určí členský štát.

Postupy uvedené v článkoch 65, 66, 67 a 68 tohto nariadenia sa neuplatňujú na systémy umelej inteligencie súvisiace s výrobkami, na ktoré sa vzťahujú právne akty uvedené v oddiele a prílohy II, ak sa v takýchto právnych aktoch už ustanovujú postupy s rovnakým cieľom. v takom prípade sa namiesto toho uplatnia tieto odvetvové postupy.

4. V prípade vysokorizikových systémov umelej inteligencie, ktoré uvádzajú na trh, do prevádzky alebo používajú finančné inštitúcie regulované právnymi predpismi Únie o finančných službách, je orgánom dohľadu nad trhom na účely tohto nariadenia príslušný vnútroštátny orgán zodpovedný za finančný dohľad nad týmito inštitúciami podľa uvedených právnych predpisov, pokiaľ uvádzanie na trh, uvádzanie do prevádzky alebo používanie systému umelej inteligencie priamo súvisí s poskytovaním týchto finančných služieb.

Odchylne od predchádzajúceho pododseku môže členský štát za odôvodnených okolností a za predpokladu, že je zabezpečená koordinácia, určiť za orgán dohľadu nad trhom na účely tohto nariadenia iný príslušný orgán.

Vnútroštátne orgány dohľadu nad trhom, ktoré vykonávajú dohľad nad regulovanými úverovými inštitúciami regulovanými podľa smernice 2013/36/EÚ, ktoré sa zúčastňujú na jednotnom mechanizme dohľadu („SSM“) zriadenom nariadením Rady č. 1204/2013, by mali 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 danom nariadení.

5. Členské štáty v prípade vysokorizikových systémov umelej inteligencie uvedených v bode 1 písm. a), pokiaľ sa tieto systémy používajú na účely presadzovania práva, a v prílohe III bodoch 6, 7 a 8 určia za orgány dohľadu nad trhom na účely tohto nariadenia buď vnútroštátne orgány vykonávajúce dohľad nad činnosťami orgánov presadzovania práva, kontroly hraníc, imigračných, azylových alebo justičných orgánov, alebo príslušné dozorné orgány pre ochranu údajov podľa smernice (EÚ) 2016/680 alebo nariadenia 2016/679. Činnosti dohľadu nad trhom nesmú žiadnym spôsobom ovplyvňovať nezávislosť justičných orgánov ani inak zasahovať do ich činnosti pri výkone ich súdnej právomoci.

6. Pokiaľ do rozsahu pôsobnosti tohto nariadenia spadajú inštitúcie, agentúry a orgány Únie, koná ako ich orgán pre dohľad nad trhom európsky dozorný úradník pre ochranu údajov.

7. Členské štáty podporujú koordináciu medzi orgánmi dohľadu nad trhom určenými podľa tohto nariadenia a inými príslušnými vnútroštátnymi orgánmi alebo subjektmi, ktoré vykonávajú dohľad nad uplatňovaním harmonizačných právnych predpisov Únie uvedených v prílohe II alebo iných právnych predpisov Únie, ktoré by mohli byť relevantné pre vysokorizikové systémy umelej inteligencie uvedené v prílohe III.

8. Poskytovateľ poskytne orgánom dohľadu nad trhom v relevantných prípadoch a s obmedzením na to, čo je potrebné na plnenie ich úloh, úplný prístup k dokumentácii, ako aj súborom trénovacích, validačných a testovacích údajov používaných na vývoj vysokorizikového systému umelej inteligencie, v prípade potreby a s výhradou bezpečnostných záruk aj prostredníctvom aplikačných programovacích rozhraní („API“) alebo iných relevantných technických prostriedkov a nástrojov umožňujúcich diaľkový prístup, a to bez toho, aby boli dotknuté právomoci stanovené v nariadení (EÚ) 2019/1020.

9. Orgánom dohľadu nad trhom sa udelí prístup k zdrojovému kódu vysokorizikového systému umelej inteligencie na základe odôvodnenej žiadosti a len vtedy, ak sú splnené tieto kumulatívne podmienky:

a) prístup k zdrojovému kódu je potrebný na posúdenie súladu vysokorizikového systému umelej inteligencie s požiadavkami stanovenými v hlave III kapitole 2 a

b) postupy testovania/auditu a overovania založené na údajoch a dokumentácii, ktoré poskytol poskytovateľ, boli vyčerpané alebo sa ukázali ako nedostatočné.

10. Orgány dohľadu nad trhom zaobchádzajú so všetkými získanými informáciami a dokumentáciou v súlade s povinnosťami zachovávať ich dôvernosť podľa článku 70.

11. Akákoľvek 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 článkom 11 ods. 3 písm. e) a článkom 11 ods. 7 písm. a) nariadenia (EÚ) 2019/1020 sa sťažnosti zohľadňujú na účely vykonávania činností dohľadu nad trhom a vybavujú sa v súlade so špecializovanými postupmi, ktoré na to stanovili orgány dohľadu nad trhom.

Článok 63a

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 umelej inteligencie, nad ktorými sa vykonáva dohľad v rámci experimentálneho regulačného prostredia pre umelú inteligenciu podľa článku 54, orgány dohľadu nad trhom overia súlad s ustanoveniami článku 54a ako súčasť svojej úlohy dohľadu nad experimentálnym regulačným prostredím pre umelú inteligenciu. Uvedené orgány môžu v prípade potreby povoliť, aby poskytovateľ alebo potenciálny poskytovateľ vykonal testovanie v reálnych podmienkach odchylne od podmienok stanovených v článku 54a 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 54a a 54b 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 používateľa alebo používateľov, 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 54a ods. 4 písm. b), v rozhodnutí alebo námietke sa uvedú dôvody tohto rozhodnutia alebo námietky, ako aj spôsoby a podmienky, za ktorých poskytovateľ alebo potenciálny poskytovateľ môže toto rozhodnutie alebo námietku napadnúť.

5. Ak orgán dohľadu nad trhom prijal rozhodnutie uvedené v odseku 3 tohto článku, v náležitých prípadoch oznámi dôvody tohto rozhodnutia orgánom dohľadu nad trhom ostatných členských štátov, v ktorých bol systém umelej inteligencie testovaný v súlade s plánom testovania.

Článok 64

Právomoci orgánov chrániacich základné práva

1. [vypúšťa sa]

2. [vypúšťa sa]

3. 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 umelej inteligencie uvedených v prílohe III alebo dodržiavanie týchto povinností presadzujú, majú právomoc požadovať akúkoľvek dokumentáciu vytvorenú alebo udržiavanú podľa tohto nariadenia a mať k nej prístup, ak je prístup k tejto dokumentácii potrebný na plnenie právomocí v rámci ich mandátu a jurisdikcie. o každej takejto žiadosti príslušný orgán verejnej moci alebo subjekt informuje orgán dohľadu nad trhom dotknutého členského štátu.

4. Do 3 mesiacov od nadobudnutia účinnosti tohto nariadenia každý členský štát určí orgány verejnej moci alebo subjekty uvedené v odseku 3 a ich zoznam zverejní. Tento zoznam členské štáty oznámia Komisii a všetkým ostatným členským štátom a udržujú ho v aktuálnom stave.

5. Ak dokumentácia uvedená v odseku 3 nepostačuje na zistenie toho, či došlo k porušeniu povinností podľa právnych predpisov Únie určených na ochranu základných práv, orgán verejnej moci alebo subjekt uvedený v odseku 3 môže orgánu dohľadu nad trhom predložiť odôvodnenú žiadosť, aby zorganizoval testovanie vysokorizikového systému umelej inteligencie technickými prostriedkami. Orgán dohľadu nad trhom zorganizuje testovanie v primeranom čase od podania žiadosti v úzkej spolupráci so žiadajúcim orgánom verejnej moci alebo subjektom.

6. So všetkými informáciami a s dokumentáciou, ktoré vnútroštátne orgány verejnej moci alebo subjekty uvedené v odseku 3 získali podľa ustanovení tohto článku, sa zaobchádza v súlade s povinnosťami zachovávania dôvernosti stanovenými v článku 70.

Článok 65

Postup zaobchádzania so systémami umelej inteligencie, ktoré predstavujú riziko na vnútroštátnej úrovni

1. Systémy umelej inteligencie predstavujúce riziko sa chápu ako výrobky predstavujúce riziko vymedzené v článku 3 bode 19 nariadenia (EÚ) 2019/1020, pokiaľ ide o riziká pre zdravie, bezpečnosť alebo základné práva osôb.

2. Ak má orgán dohľadu nad trhom členského štátu dostatočné dôvody domnievať sa, že systém umelej inteligencie predstavuje riziko uvedené v odseku 1, vykoná hodnotenie dotknutého systému umelej inteligencie, pokiaľ ide o jeho súlad so všetkými požiadavkami a povinnosťami stanovenými v tomto nariadení. Ak sa identifikujú riziká pre základné práva, orgán dohľadu nad trhom informuje aj príslušné vnútroštátne orgány verejnej moci alebo subjekty uvedené v článku 64 ods. 3. s orgánmi dohľadu nad trhom a ostatnými vnútroštátnymi orgánmi verejnej moci alebo subjektmi uvedenými v článku 64 ods. 3 podľa potreby spolupracujú príslušní prevádzkovatelia.

   Ak v priebehu uvedeného hodnotenia orgán dohľadu nad trhom zistí, že systém umelej inteligencie nespĺňa požiadavky a povinnosti stanovené v tomto nariadení, bez zbytočného odkladu požiada príslušného prevádzkovateľa, aby prijal všetky primerané nápravné opatrenia, ktoré vedú k zosúladeniu systému umelej inteligencie s uvedenými požiadavkami a povinnosťami, jeho stiahnutiu z trhu alebo od používateľa, v lehote, ktorú môže orgán stanoviť.

   Orgán dohľadu nad trhom o tom informuje príslušnú notifikovanú osobu. Na opatrenia uvedené v druhom pododseku sa uplatňuje článok 18 nariadenia (EÚ) 2019/1020.

3. Ak sa orgán dohľadu nad trhom domnieva, že nesúlad s požiadavkami a povinnosťami sa neobmedzuje na územie jeho štátu, bez zbytočného odkladu informuje Komisiu a ostatné členské štáty o výsledkoch hodnotenia a opatreniach, o ktorých prijatie požiadal prevádzkovateľa.

4. Prevádzkovateľ zabezpečí prijatie všetkých primeraných nápravných opatrení v súvislosti so všetkými dotknutými systémami umelej inteligencie, ktoré sprístupnil na trhu v celej Únii.

5. Ak prevádzkovateľ systému umelej inteligencie 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 umelej inteligencie na svojom vnútroštátnom trhu, výrobok z uvedeného trhu stiahnuť alebo ho stiahnuť od používateľa. Uvedený orgán tieto opatrenia bez zbytočného odkladu oznámi Komisii a ostatným členským štátom.

6. Oznámenie uvedené v odseku 5 musí obsahovať všetky podrobné údaje, ktoré sú k dispozícii, najmä informácie potrebné na identifikáciu nevyhovujúceho systému umelej inteligencie, jeho pôvod, povahu údajného nesúladu a z neho vyplývajúce riziko, povahu a trvanie prijatých vnútroštátnych opatrení a stanoviská, ktoré predložil príslušný prevádzkovateľ. Orgány dohľadu nad trhom musia predovšetkým uviesť, či k nesúladu došlo v dôsledku jedného alebo viacerých z týchto dôvodov:

-a) nedodržiavanie zákazu praktík v oblasti umelej inteligencie uvedených v článku 5;

a) vysokorizikový systém umelej inteligencie nespĺňa požiadavky stanovené v hlave III kapitole 2;

b) existujú nedostatky v harmonizovaných normách alebo spoločných špecifikáciách uvedených v článkoch 40 a 41, ktoré sú základom pre predpoklad zhody.

c) nedodržiavanie ustanovení uvedených v článku 52;

d) nesúlad systémov umelej inteligencie na všeobecné účely s požiadavkami a povinnosťami uvedenými v článku 4a.

7. Orgány dohľadu nad trhom členských štátov iné než orgán dohľadu nad trhom členského štátu, ktorý postup začal, bez zbytočného odkladu oboznámia Komisiu a ostatné členské štáty so všetkými prijatými opatreniami a s akýmikoľvek dodatočnými informáciami týkajúcimi sa nesúladu dotknutého systému umelej inteligencie, ktoré majú k dispozícii, a v prípade, že nesúhlasia s oznámeným vnútroštátnym opatrením, aj so svojimi námietkami.

8. Ak do troch mesiacov od doručenia oznámenia uvedeného v odseku 5 žiaden členský štát ani Komisia nevznesú námietku proti predbežnému opatreniu prijatému členským štátom, opatrenie sa považuje za opodstatnené. Týmto nie sú dotknuté procesné práva dotknutého prevádzkovateľa v súlade s článkom 18 nariadenia (EÚ) 2019/1020. Lehota uvedená v prvej vete tohto odseku sa skracuje na 30 dní v prípade nedodržania zákazu praktík v oblasti umelej inteligencie podľa článku 5.

9. Orgány dohľadu nad trhom všetkých členských štátov následne zabezpečia, aby sa vo vzťahu k dotknutému systému umelej inteligencie bez zbytočného odkladu prijali primerané reštriktívne opatrenia, ako je napríklad stiahnutie výrobku z ich trhu.

Článok 66

Ochranný postup Únie

1. Ak do troch mesiacov od doručenia oznámenia uvedeného v článku 65 ods. 5 alebo do 30 dní v prípade nedodržania zákazu praktík v oblasti umelej inteligencie uvedených v článku 5 členský štát vznesie námietky proti opatreniu prijatému iným členským štátom alebo ak Komisia pokladá toto opatrenie za také, ktoré je v rozpore s právnymi predpismi Únie, Komisia bez zbytočného odkladu začne konzultácie s orgánom dohľadu nad trhom príslušného členského štátu a prevádzkovateľom alebo prevádzkovateľmi a vnútroštátne opatrenie vyhodnotí. Na základe výsledkov tohto hodnotenia Komisia rozhodne, či je vnútroštátne opatrenie opodstatnené alebo nie, a to do 9 mesiacov od doručenia oznámenia uvedeného v článku 65 ods. 5 alebo v prípade nedodržania zákazu praktík v oblasti umelej inteligencie uvedených v článku 5 do 60 dní. Toto rozhodnutie oznámi dotknutému členskému štátu. Komisia o takomto rozhodnutí informuje aj všetky ostatné členské štáty.

2. Ak Komisia považuje opatrenie prijaté orgánom dohľadu nad trhom príslušného členského štátu za opodstatnené, orgány dohľadu nad trhom všetkých členských štátov zabezpečia prijatie primeraných reštriktívnych opatrení v súvislosti s dotknutým systémom umelej inteligencie, ako je napríklad stiahnutie systému umelej inteligencie z ich trhu bez zbytočného odkladu, a informujú o tom Komisiu. Ak Komisia považuje vnútroštátne opatrenie za neodôvodnené, orgán dohľadu nad trhom dotknutého členského štátu toto opatrenie stiahne a informuje o tom Komisiu.

3. Ak sa vnútroštátne opatrenie považuje za opodstatnené a nesúlad systému umelej inteligencie 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 67

Vyhovujúce vysokorizikové systémy umelej inteligencie alebo systémy umelej inteligencie na všeobecné účely, ktoré predstavujú riziko

1. Ak po vykonaní hodnotenia podľa článku 65 orgán dohľadu nad trhom členského štátu zistí, že vysokorizikový systém umelej inteligencie alebo systém umelej inteligencie na všeobecné účely, ktorý je v súlade s týmto nariadením, napriek tomu predstavuje riziko pre zdravie alebo bezpečnosť osôb alebo pre základné práva, požiada príslušného prevádzkovateľa, aby prijal všetky primerané opatrenia, ktorými sa zabezpečí, aby dotknutý systém umelej inteligencie pri uvedení na trh alebo do prevádzky už takéto riziko nepredstavoval alebo aby bez zbytočného odkladu došlo k jeho stiahnutiu z trhu alebo od používateľa v lehote, ktorú môže orgán stanoviť.

2. Poskytovateľ alebo iní relevantní prevádzkovatelia v lehote predpísanej orgánom dohľadu nad trhom členského štátu v zmysle odseku 1 zabezpečia prijatie nápravných opatrení v súvislosti so všetkými dotknutými systémami umelej inteligencie, ktoré sprístupnili na trhu v celej Únii.

3. Členský štát o tom okamžite informuje Komisiu a ostatné členské štáty. Tieto informácie musia obsahovať všetky podrobnosti, ktoré sú k dispozícii, najmä údaje potrebné na identifikáciu dotknutého systému umelej inteligencie, 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 príslušným prevádzkovateľom a prijaté vnútroštátne opatrenia vyhodnotí. Na základe výsledkov tohto hodnotenia Komisia rozhodne, či je opatrenie opodstatnené, a podľa potreby navrhne primerané opatrenia.

5. Svoje rozhodnutie Komisia adresuje dotknutému členskému štátu a informuje všetky ostatné členské štáty.

Článok 68

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 zhody bolo umiestnené v rozpore s článkom 49;

   b) označenie zhody nebolo umiestnené;

   c) nebolo vyhotovené EÚ vyhlásenie o zhode;

   d) EÚ vyhlásenie o zhode nebolo vyhotovené správne;

   e) nebolo umiestnené identifikačné číslo notifikovanej osoby zapojenej v relevantných prípadoch do postupu posudzovania zhody.

2. Ak nesúlad uvedený v odseku 1 pretrváva, dotknutý členský štát prijme všetky náležité opatrenia na obmedzenie alebo zákaz sprístupňovania vysokorizikového systému umelej inteligencie na trhu alebo zabezpečí jeho stiahnutie od používateľa alebo z trhu.

Článok 68a

Skúšobné zariadenia Únie v oblasti umelej inteligencie

1. Komisia určí jedno alebo viacero skúšobných zariadení Únie podľa článku 21 nariadenia (EÚ) 1020/2019 v oblasti umelej inteligencie.

2. Bez toho, aby boli dotknuté činnosti skúšobných zariadení Únie uvedené v článku 21 ods. 6 nariadenia (EÚ) 1020/2019, skúšobné zariadenia Únie uvedené v odseku 1 poskytujú aj nezávislé technické alebo vedecké poradenstvo na žiadosť rady alebo orgánov dohľadu nad trhom.

Článok 68b

Centrálna rezerva nezávislých expertov

1. Na žiadosť rady pre umelú inteligenciu Komisia prostredníctvom vykonávacieho aktu prijme ustanovenia o zriadení, udržiavaní a financovaní centrálnej rezervy nezávislých expertov na podporu činností presadzovania podľa tohto nariadenia.

2. Expertov vyberá Komisia a zaraďuje ich do centrálnej rezervy na základe aktuálnych vedeckých alebo technických odborných znalostí v oblasti umelej inteligencie, pričom sa náležite zohľadňujú technické oblasti, na ktoré sa vzťahujú požiadavky a povinnosti stanovené v tomto nariadení, a činnosti orgánov dohľadu nad trhom podľa článku 11 nariadenia (EÚ) 1020/2019. Komisia určí počet členov v rezerve v súlade s potrebami.

3. Experti môžu mať tieto úlohy:

a) poskytujú poradenstvo a na žiadosť orgánov dohľadu nad trhom podporujú ich prácu;

b) podporujú cezhraničné vyšetrovania v rámci dohľadu nad trhom uvedené v článku 58 písm. h) bez toho, aby boli dotknuté právomoci orgánov dohľadu nad trhom;

c) poskytujú poradenstvo a podporu Komisii pri plnení jej povinností v súvislosti s ochrannou doložkou podľa článku 66.

4. Experti vykonávajú svoje úlohy nestranne, objektívne a zabezpečujú dôvernosť informácií a údajov získaných pri vykonávaní svojich úloh a činností. Každý expert vypracuje vyhlásenie o záujmoch, ktoré sa sprístupní verejnosti. Komisia zavedie systémy a postupy na aktívne riadenie možných konfliktov záujmov a na predchádzanie týmto konfliktom.

5. Od členských štátov sa môže vyžadovať, aby za poradenstvo a podporu expertov platili poplatky. Komisia prijme štruktúru a výšku poplatkov, ako aj rozsah a štruktúru nahraditeľných nákladov prostredníctvom vykonávacieho aktu uvedeného v odseku 1, pričom zohľadní ciele primeraného vykonávania tohto nariadenia, nákladovú efektívnosť a potrebu zabezpečiť účinný prístup všetkých členských štátov k expertom.

6. Komisia podľa potreby uľahčuje členským štátom včasný prístup k expertom a zabezpečí, aby sa kombinácia podporných činností vykonávaných skúšobnými zariadeniami Únie podľa článku 68a a expertmi podľa tohto článku účinne organizovala a poskytovala najlepšiu možnú pridanú hodnotu.

HLAVA IX

KÓDEXY SPRÁVANIA

Článok 69

Kódex správania pre dobrovoľné uplatňovanie osobitných požiadaviek

1. Komisia a členské štáty uľahčujú vypracúvanie kódexov správania určených na podporu dobrovoľného uplatňovania jednej alebo viacerých požiadaviek stanovených v hlave III kapitole 2 tohto nariadenia v čo najväčšej miere na systémy umelej inteligencie iné ako vysokorizikové, pričom zohľadnia dostupné technické riešenia umožňujúce uplatňovanie takýchto požiadaviek.

2. Komisia a členské štáty uľahčujú vypracúvanie kódexov správania určených na to, aby sa pri všetkých systémoch umelej inteligencie nabádalo na dobrovoľné uplatňovanie osobitných požiadaviek týkajúcich sa napríklad environmentálnej udržateľnosti, a to aj pokiaľ ide o energeticky efektívne programovanie, prístupnosti pre osoby so zdravotným postihnutím, účasti zainteresovaných strán na koncipovaní a vývoji systémov umelej inteligencie a rozmanitosti vývojových tímov na základe jasných cieľov a kľúčových ukazovateľov výkonnosti na meranie dosahovania týchto cieľov, a podporujú vypracúvanie takýchto kódexov. Komisia a členské štáty takisto v prípade potreby uľahčujú vypracúvanie kódexov správania uplatniteľných na dobrovoľnom základe, pokiaľ ide o povinnosti používateľov vo vzťahu k systémom umelej inteligencie.

3. Kódexy správania uplatniteľné na dobrovoľnom základe môžu vypracovať jednotliví poskytovatelia systémov umelej inteligencie alebo organizácie, ktoré ich zastupujú, alebo obaja, a to aj v spolupráci s používateľmi a akýmikoľvek zainteresovanými stranami a organizáciami, ktoré ich zastupujú, prípadne používateľmi vo vzťahu k ich povinnostiam. Kódexy správania sa môžu vzťahovať na jeden alebo viacero systémov umelej inteligencie, pričom sa zohľadní podobnosť zamýšľaného účelu príslušných systémov.

4. Komisia a členské štáty pri nabádaní k vypracúvaniu kódexov správania a jeho uľahčovaní zohľadňujú osobitné záujmy a potreby MSP vrátane startupov.

HLAVA X

DÔVERNOSŤ A SANKCIE

Článok 70

Dôvernosť

1. Príslušné vnútroštátne orgány, notifikované osoby, Komisia, rada a akékoľvek iné fyzické alebo právnické osoby podieľajúce sa na uplatňovaní tohto nariadenia zavedú v súlade s právom Únie alebo vnútroštátnym právom vhodné technické a organizačné opatrenia s cieľom zabezpečiť 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 2016/943 o ochrane nesprístupneného know-how a obchodných informácií (obchodného tajomstva) pred ich neoprávneným získaním, využitím a sprístupnením;

b) účinné vykonávanie tohto nariadenia, najmä na účely inšpekcií, vyšetrovaní alebo auditov;

c) verejné záujmy a záujmy národnej bezpečnosti;

d) integritu trestného alebo správneho konania;

e) integritu utajovaných skutočností v súlade s právom Únie alebo vnútroštátnym právom.

2. Bez toho, aby bol dotknutý odsek 1, sa informácie, ktoré sa vymieňajú na dôvernom základe medzi príslušnými vnútroštátnymi orgánmi navzájom a medzi príslušnými vnútroštátnymi orgánmi a Komisiou, nezverejňujú bez predchádzajúcej konzultácie s príslušným vnútroštátnym orgánom, od ktorého pochádzajú, a používateľom, ak vysokorizikové systémy umelej inteligencie uvedené v prílohe III bodoch 1, 6 a 7 používajú orgány presadzovania práva, kontroly hraníc, imigračné alebo azylové orgány a ak by takéto zverejnenie ohrozilo verejné záujmy a záujmy národnej bezpečnosti. Táto povinnosť vymieňať si informácie sa nevzťahuje na citlivé prevádzkové údaje týkajúce sa činností orgánov presadzovania práva, kontroly hraníc, imigračných alebo azylových orgánov.

Ak sú poskytovateľmi vysokorizikových systémov umelej inteligencie uvedených v prílohe III bodoch 1, 6 a 7 orgány presadzovania práva, imigračné alebo azylové orgány, technická dokumentácia uvedená v prílohe IV musí zostať v priestoroch týchto orgánov. Tieto orgány zabezpečia, aby orgány dohľadu nad trhom uvedené v článku 63 ods. 5 a 6 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.

3. Odsekmi 1 a 2 nie sú dotknuté práva a povinnosti Komisie, členských štátov a ich príslušných orgánov, ani 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.

Článok 71

Sankcie

1. Členské štáty v súlade s podmienkami stanovenými v tomto nariadení stanovia pravidlá týkajúce sa sankcií vrátane správnych pokút, ktoré sa uplatňujú pri porušeniach tohto nariadenia, a prijmú všetky opatrenia potrebné na zabezpečenie ich riadneho a účinného vykonávania. Stanovené sankcie musia byť účinné, primerané a odrádzajúce. Musia zohľadňovať najmä veľkosť a záujmy poskytovateľov z radov MSP vrátane startupov a ich ekonomickú životaschopnosť. Zohľadňujú aj to, či sa systém umelej inteligencie používa v kontexte osobnej, neprofesionálnej činnosti.

2. Členské štáty bezodkladne informujú Komisiu o týchto pravidlách a opatreniach, ako aj o všetkých následných zmenách, ktoré sa ich týkajú.

3. Za nedodržanie akýchkoľvek zákazov praktík v oblasti umelej inteligencie uvedených v článku 5 sa ukladajú správne pokuty až do výšky 30 000 000 EUR, alebo ak je porušiteľom spoločnosť, až do výšky 6 % jej celkového celosvetového ročného obratu za predchádzajúci finančný rok, podľa toho, ktorá suma je vyššia. v prípade MSP vrátane startupov sú tieto pokuty až do výšky 3 % ich celosvetového ročného obratu za predchádzajúci finančný rok.

4. Správne pokuty až do výšky 20 000 000 EUR, alebo ak je porušiteľom spoločnosť, až do výšky 4 % jej celkového celosvetového ročného obratu za predchádzajúci finančný rok podľa toho, ktorá suma je vyššia, sa ukladajú za porušenia týchto ustanovení týkajúcich sa prevádzkovateľov alebo notifikovaných osôb:

-a) povinnosti poskytovateľov podľa článkov 4b a 4c;

a) povinnosti poskytovateľov podľa článku 16;

b) povinnosti určitých ďalších osôb podľa článku 23a;

c) povinnosti splnomocnených zástupcov podľa článku 25;

d) povinnosti dovozcov podľa článku 26;

e) povinnosti distribútorov podľa článku 27;

f) povinnosti používateľov podľa článku 29 ods. 1 až 6a;

g) požiadavky a povinnosti notifikovaných osôb podľa článku 33, článku 34 ods. 1, článku 34 ods. 3, článku 34 ods. 4 a článku 34a;

h) povinnosti v oblasti transparentnosti pre poskytovateľov a používateľov podľa článku 52.

V prípade MSP vrátane startupov sú tieto pokuty až do výšky 2 % ich celosvetového ročného obratu za predchádzajúci finančný rok.

5. Za poskytnutie nesprávnych, neúplných alebo zavádzajúcich informácií v odpovedi na žiadosť notifikovaných osôb a príslušných vnútroštátnych orgánov sa ukladajú správne pokuty až do výšky 10 000 000 EUR, alebo ak je porušiteľom spoločnosť, až do výšky 2 % jej celkového svetového ročného obratu za predchádzajúci účtovný rok, podľa toho, ktorá suma je vyššia. v prípade MSP vrátane startupov sú tieto pokuty až do výšky 1 % ich celosvetového ročného obratu za predchádzajúci finančný rok.

6. Pri rozhodovaní o výške správnej pokuty 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 dôsledkov;

aa) úmyselný alebo nedbanlivostný charakter porušenia;

ab) všetky opatrenia, ktoré prevádzkovateľ prijal pri náprave porušenia a zmiernení možných nepriaznivých dôsledkov porušenia;

b) či už tomu istému prevádzkovateľovi uložili za to isté porušenie správne pokuty iné orgány dohľadu nad trhom v iných členských štátoch;

ba) 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 zákona;

c) veľkosť, ročný obrat a trhový podiel prevádzkovateľa, ktorý sa dopustil porušenia;

d) akékoľvek iné priťažujúce alebo poľahčujúce okolnosti prípadu, ako napríklad akékoľvek získané finančné výhody alebo straty, ktorým sa zabránilo, priamo alebo nepriamo v súvislosti s porušením.

7. Každý členský štát stanoví pravidlá, či a v akom rozsahu sa môžu správne pokuty uložiť orgánom verejnej moci a subjektom zriadeným v danom členskom štáte.

8. 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.

9. Výkon právomocí orgánu dohľadu nad trhom podľa tohto článku podlieha primeraným procesným zárukám v súlade s právom Únie a právom členského štátu vrátane účinného súdneho prostriedku nápravy a riadneho procesu.

Článok 72

Správne pokuty uložené inštitúciám, agentúram a orgánom Únie

1. Európsky dozorný úradník pre ochranu údajov môže uložiť správne pokuty inštitúciám, agentúram a orgánom 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 dôsledkov;

   b) spolupráca 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, agentúre alebo dotknutému orgánu Únie v rovnakej veci;

   c) všetky podobné predchádzajúce porušenia, ku ktorým došlo zo strany inštitúcie, agentúry alebo orgánu Únie.

2. Za nedodržanie akýchkoľvek zákazov praktík v oblasti umelej inteligencie uvedených v článku 5 sa ukladajú správne pokuty až do výšky 500 000 EUR.

3. Za nesúlad systému umelej inteligencie s požiadavkami alebo povinnosťami podľa tohto nariadenia, ktoré nie sú stanovené v článkoch 5 a 10, sa ukladajú správne pokuty až do výšky 250 000 EUR.

4. Pred prijatím rozhodnutí podľa tohto článku európsky dozorný úradník pre ochranu údajov poskytne inštitúcii, agentúre alebo orgánu Únie, voči ktorým vedie konanie, príležitosť na vyjadrenie v záležitostiach týkajúcich sa možného porušenia. Európsky dozorný úradník pre ochranu údajov pri svojich rozhodnutiach vychádza len z prvkov 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 svojich osobných údajov alebo obchodného tajomstva majú strany právo na prístup k spisu európskeho dozorného úradníka pre ochranu údajov.

6. Prostriedky získané z pokút uložených podľa tohto článku sú príjmom všeobecného rozpočtu Únie.

HLAVA XI

DELEGOVANIE PRÁVOMOCI A POSTUP VÝBORU

Článok 73

Vykonávanie delegovania právomoci

1. Komisii sa udeľuje právomoc prijímať delegované akty za podmienok stanovených v tomto článku.

2. Delegovanie právomoci uvedené v článku 7 ods. 1, článku 7 ods. 3, článku 11 ods. 3, článku 43 ods. 5 a 6 a článku 48 ods. 5 sa Komisii udeľuje na obdobie piatich rokov od [*nadobudnutia účinnosti nariadenia*].

Komisia vypracuje správu týkajúcu sa delegovania právomoci najneskôr deväť mesiacov pred uplynutím tohto 5- ročného 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 7 ods. 1, článku 7 ods. 3, článku 11 ods. 3, článku 43 ods. 5 a 6 a článku 48 ods. 5 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 oznamuje delegovaný akt hneď po jeho prijatí súčasne Európskemu parlamentu a Rade.

5. Delegovaný akt prijatý podľa článku 7 ods. 1, článku 7 ods. 3, článku 11 ods. 3, článku 43 ods. 5 a 6 a článku 48 ods. 5 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 74

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.

HLAVA XII

ZÁVEREČNÉ USTANOVENIA

Článok 75

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 umelej inteligencie v zmysle nariadenia Európskeho parlamentu a Rady (EÚ) RRR/XX [o umelej inteligencii]* sa zohľadňujú požiadavky stanovené v hlave III kapitole 2 uvedeného nariadenia.

_____

* Nariadenie (EÚ) RRR/XX [o umelej inteligencii] (Ú. v. EÚ...).“;

Článok 76

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 umelej inteligencie, ktoré sú bezpečnostnými komponentmi v zmysle nariadenia Európskeho parlamentu a Rady (EÚ) RRR/XX [o umelej inteligencii]*, sa zohľadňujú požiadavky stanovené v hlave III kapitole 2 uvedeného nariadenia.

_____

* Nariadenie (EÚ) RRR/XX [o umelej inteligencii] (Ú. v. EÚ...).“;

Článok 77

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 umelej inteligencie, ktoré sú bezpečnostnými komponentmi v zmysle nariadenia Európskeho parlamentu a Rady (EÚ) RRR/XX [o umelej inteligencii]*, sa zohľadňujú požiadavky stanovené v hlave III kapitole 2 uvedeného nariadenia.

_____

* Nariadenie (EÚ) RRR/XX [o umelej inteligencii] (Ú. v. EÚ...).“;

Článok 78

Zmena smernice 2014/90/EÚ

V článku 8 smernice 2014/90/EÚ sa dopĺňa tento odsek:

„4. v prípade systémov umelej inteligencie, ktoré sú bezpečnostnými komponentmi v zmysle nariadenia Európskeho parlamentu a Rady (EÚ) RRR/XX [o umelej inteligencii]*, 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 hlave III kapitole 2 uvedeného nariadenia.

_____

* Nariadenie (EÚ) RRR/XX [o umelej inteligencii] (Ú. v. EÚ...).“;

Článok 79

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 umelej inteligencie, ktoré sú bezpečnostnými komponentmi v zmysle nariadenia Európskeho parlamentu a Rady (EÚ) RRR/XX [o umelej inteligencii]*, sa zohľadňujú požiadavky stanovené v hlave III kapitole 2 uvedeného nariadenia.

_____

* Nariadenie (EÚ) RRR/XX [o umelej inteligencii] (Ú. v. EÚ...).“;

Článok 80

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 umelej inteligencie, ktoré sú bezpečnostnými komponentmi v zmysle nariadenia Európskeho parlamentu a Rady (EÚ) RRR/XX [o umelej inteligencii]*, sa zohľadňujú požiadavky stanovené v hlave III kapitole 2 uvedeného nariadenia.

_____

* Nariadenie (EÚ) RRR/XX [o umelej inteligencii] (Ú. v. EÚ...).“;

Článok 81

Zmena 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, sa pri prijímaní vykonávacích aktov podľa odseku 1 týkajúcich sa systémov umelej inteligencie, ktoré sú bezpečnostnými komponentmi v zmysle nariadenia Európskeho parlamentu a Rady (EÚ) RRR/XX [o umelej inteligencii]*, zohľadňujú požiadavky stanovené v hlave III kapitole 2 uvedeného nariadenia.

_____

* Nariadenie (EÚ) RRR/XX [o umelej inteligencii] (Ú. v. EÚ...).“;

2. v článku 19 sa dopĺňa tento odsek:

„4. Pri prijímaní delegovaných aktov podľa odsekov 1 a 2 týkajúcich sa systémov umelej inteligencie, ktoré sú bezpečnostnými komponentmi v zmysle nariadenia (EÚ) RRR/XX [o umelej inteligencii], sa zohľadňujú požiadavky stanovené v hlave III kapitole 2 uvedeného nariadenia.“;

3. v článku 43 sa dopĺňa tento odsek:

„4. Pri prijímaní vykonávacích aktov podľa odseku 1 týkajúcich sa systémov umelej inteligencie, ktoré sú bezpečnostnými komponentmi v zmysle nariadenia (EÚ) RRR/XX [o umelej inteligencii], sa zohľadňujú požiadavky stanovené v hlave III kapitole 2 uvedeného nariadenia.“;

4. v článku 47 sa dopĺňa tento odsek:

„3. Pri prijímaní delegovaných aktov podľa odsekov 1 a 2 týkajúcich sa systémov umelej inteligencie, ktoré sú bezpečnostnými komponentmi v zmysle nariadenia (EÚ) RRR/XX [o umelej inteligencii], sa zohľadňujú požiadavky stanovené v hlave III kapitole 2 uvedeného nariadenia.“;

5. v článku 57 sa dopĺňa tento odsek:

„Pri prijímaní uvedených vykonávacích aktov týkajúcich sa systémov umelej inteligencie, ktoré sú bezpečnostnými komponentmi v zmysle nariadenia (EÚ) RRR/XX [o umelej inteligencii], sa zohľadňujú požiadavky stanovené v hlave III kapitole 2 uvedeného nariadenia.“;

6. v článku 58 sa dopĺňa tento odsek:

„3. Pri prijímaní delegovaných aktov podľa odsekov 1 a 2 týkajúcich sa systémov umelej inteligencie, ktoré sú bezpečnostnými komponentmi v zmysle nariadenia (EÚ) RRR/XX [o umelej inteligencii], sa zohľadňujú požiadavky stanovené v hlave III kapitole 2 uvedeného nariadenia.“

Článok 82

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 umelej inteligencie, ktoré sú bezpečnostnými komponentmi v zmysle nariadenia Európskeho parlamentu a Rady (EÚ) RRR/XX [o umelej inteligencii]*, sa zohľadňujú požiadavky stanovené v hlave III kapitole 2 uvedeného nariadenia.

_____

* Nariadenie (EÚ) RRR/XX [o umelej inteligencii] (Ú. v. EÚ...).“;

Článok 83

Systémy umelej inteligencie, ktoré už boli uvedené na trh alebo do prevádzky

1. Toto nariadenie sa neuplatňuje na systémy umelej inteligencie, ktoré sú komponentmi rozsiahlych IT systémov zriadených právnymi aktmi uvedenými v prílohe IX, ktoré boli uvedené na trh alebo do prevádzky pred [12 mesiacov po dátume začatia uplatňovania tohto nariadenia uvedenom v článku 85 ods. 2], pokiaľ nahradenie alebo zmena uvedených právnych aktov nespôsobí významnú zmenu koncepcie alebo zamýšľaného účelu dotknutého systému umelej inteligencie, príp. systémov umelej inteligencie.

   Pri hodnotení každého rozsiahleho IT systému zriadeného právnymi aktmi uvedenými v prílohe IX, ktoré sa má vykonať podľa uvedených príslušných aktov, sa v prípade potreby zohľadnia požiadavky stanovené v tomto nariadení.

2. Na vysokorizikové systémy umelej inteligencie iné ako tie, ktoré sú uvedené v odseku 1, ktoré boli uvedené na trh alebo do prevádzky pred [dátum začatia uplatňovania tohto nariadenia uvedený v článku 85 ods. 2], sa toto nariadenie uplatňuje len vtedy, ak v týchto systémoch došlo od uvedeného dátumu k významným zmenám koncepcie alebo zamýšľaného účelu.

Článok 84

Hodnotenie a preskúmanie

1. [vypúšťa sa]

1b. Komisia každých 24 mesiacov po nadobudnutí účinnosti tohto nariadenia a až do konca obdobia delegovania právomoci posúdi potrebu zmeny zoznamu v prílohe III. Zistenia tohto posúdenia sa predložia Európskemu parlamentu a Rade.

2. Komisia do [tri roky od dátumu začatia uplatňovania tohto nariadenia uvedeného v článku 85 ods. 2] a potom každé štyri roky predloží Európskemu parlamentu a Rade správu o hodnotení a preskúmaní tohto nariadenia. Správy sa zverejnia.

3. Správy uvedené v odseku 2 venujú osobitnú pozornosť:

   a) stavu finančných zdrojov, technického vybavenia a ľudských zdrojov príslušných vnútroštátnych orgánov na účinné vykonávanie úloh, ktoré im boli pridelené podľa tohto nariadenia;

   b) stavu sankcií, a najmä správnych pokút uvedených v článku 71 ods. 1, ktoré členské štáty uplatňujú za porušenie ustanovení tohto nariadenia.

4. Komisia do *[tri roky od dátumu začatia uplatňovania tohto nariadenia uvedeného v článku 85 ods. 2*] a potom podľa potreby každé štyri roky vyhodnotí vplyv a účinnosť dobrovoľných kódexov správania na podporu uplatňovania požiadaviek stanovených v hlave III kapitole 2 na iné ako vysokorizikové systémy umelej inteligencie a prípadne ďalších dodatočných požiadaviek na systémy umelej inteligencie, a to aj pokiaľ ide o environmentálnu udržateľnosť.

5. Rada pre umelú inteligenciu, členské štáty a príslušné vnútroštátne orgány poskytnú Komisii na jej žiadosť informácie na účely odsekov 1a až 4.

6. Pri hodnoteniach a preskúmaniach uvedených v odsekoch 1a až 4 Komisia zohľadní stanoviská a zistenia rady pre umelú inteligenciu, Európskeho parlamentu, Rady a iných relevantných subjektov alebo zdrojov.

7. V prípade potreby Komisia predloží vhodné návrhy na zmenu tohto nariadenia, pričom zohľadní najmä vývoj v oblasti technológií a vezme do úvahy aktuálny stav pokroku v informačnej spoločnosti.

Článok 85

Nadobudnutie účinnosti a uplatňovanie

1. Toto nariadenie nadobúda účinnosť dvadsiatym dňom po jeho uverejnení v *Úradnom vestníku Európskej únie*.

2. Toto nariadenie sa uplatňuje od [36 mesiacov po nadobudnutí účinnosti nariadenia].

3. Odchylne od odseku 2:

   a) hlava III kapitola 4 a hlava VI sa uplatňujú od [dvanásť mesiacov po nadobudnutí účinnosti tohto nariadenia];

   b) článok 71 sa uplatňuje od [dvanásť mesiacov po nadobudnutí účinnosti tohto nariadenia].

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli

Za Európsky parlament	*Za Radu*
predseda/predsedníčka	*predseda/predsedníčka*

PRÍLOHA I

[vypúšťa sa]

PRÍLOHA II

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

1. 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)

2. 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)

3. 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)

4. 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)

5. 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)

6. 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)

7. 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)

8. 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 vzdušných prostriedkov a ide o ich motory, vrtule, súčasti a vybavenie na ich diaľkové ovládanie

PRÍLOHA III

VYSOKORIZIKOVÉ SYSTÉMY UMELEJ INTELIGENCIE UVEDENÉ v ČLÁNKU 6 ODS. 3

V každej z oblastí uvedených v bodoch 1 až 8 sa systémy umelej inteligencie osobitne uvedené v každom písmene považujú za vysokorizikové systémy umelej inteligencie podľa článku 6 ods. 3:

1. Biometria:

   a) systémy diaľkovej biometrickej identifikácie.

2. Kritická infraštruktúra:

   a) systémy umelej inteligencie, ktoré sa majú používať ako bezpečnostné komponenty pri riadení a prevádzke kritickej digitálnej infraštruktúry, cestnej premávky a pri dodávkach vody, plynu, tepla a elektriny.

3. Vzdelávanie a odborná príprava:

   a) systémy umelej inteligencie, ktoré sa majú používať na určenie prístupu, prijatia alebo pridelenia fyzických osôb do inštitúcií alebo programov vzdelávania a odbornej prípravy na všetkých úrovniach;

   b) systémy umelej inteligencie, ktoré sa majú používať na hodnotenie vzdelávacích výstupov, a to aj vtedy, keď sa tieto výsledky používajú na riadenie procesu učenia sa fyzických osôb v inštitúciách alebo programoch vzdelávania a odbornej prípravy na všetkých úrovniach.

4. Zamestnanosť, riadenie pracovníkov a prístup k samostatnej zárobkovej činnosti:

   a) systémy umelej inteligencie určené 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 umelej inteligencie, ktoré sa majú používať pri rozhodovaní o kariérnom postupe v zamestnaní a ukončení zmluvných pracovných vzťahov, pri prideľovaní úloh na základe individuálneho správania sa alebo osobných čŕt, alebo vlastností a pri monitorovaní a hodnotení výkonnosti a správania sa osôb v rámci takýchto vzťahov.

5. Prístup k základným súkromným službám a základným verejným službám a dávkam a ich využívanie:

a) systémy umelej inteligencie, ktoré sa majú používať orgánmi verejnej moci alebo v ich mene na hodnotenie oprávnenosti fyzických osôb na základné dávky a služby verejnej pomoci, ako aj na poskytovanie, zníženie či zrušenie takýchto dávok a služieb alebo na žiadosti o ich vrátenie;

b) systémy umelej inteligencie, ktoré sa majú používať na hodnotenie úverovej bonity fyzických osôb alebo stanovenie ich bodového hodnotenia kreditného rizika, s výnimkou systémov umelej inteligencie, ktoré na vlastné použitie uviedli do prevádzky poskytovatelia, ktorí sú mikropodnikmi a malými podnikmi v zmysle prílohy k odporúčaniu Komisie 2003/361/ES;

c) systémy umelej inteligencie určené na vysielanie záchranných služieb prvej reakcie vrátane hasičov a zdravotníckej pomoci alebo na stanovovanie priority ich vysielania;

d) systémy umelej inteligencie, ktoré sa majú používať na posúdenie rizika a cenotvorbu vo vzťahu k fyzickým osobám v prípade životného a zdravotného poistenia, s výnimkou systémov umelej inteligencie, ktoré na vlastné použitie uviedli do prevádzky poskytovatelia, ktorí sú mikropodnikmi a malými podnikmi v zmysle prílohy k odporúčaniu Komisie 2003/361/ES.

6. Presadzovanie práva:

a) systémy umelej inteligencie, ktoré majú používať orgány presadzovania práva alebo ktoré sa majú používať v ich mene na posúdenie rizika, že fyzická osoba spácha alebo opakovane spácha trestný čin, alebo rizika, že fyzická osoba sa stane potenciálnou obeťou trestných činov;

b) systémy umelej inteligencie, ktoré majú používať orgány presadzovania práva alebo ktoré sa majú používať v ich mene, ako napríklad detektory lži a podobné nástroje, alebo na zisťovanie emocionálneho stavu fyzickej osoby;

c) [vypúšťa sa]

d) systémy umelej inteligencie, ktoré majú používať orgány presadzovania práva alebo ktoré sa majú používať v ich mene na hodnotenie spoľahlivosti dôkazov v priebehu vyšetrovania alebo stíhania trestných činov;

e) systémy umelej inteligencie, ktoré majú používať orgány presadzovania práva alebo ktoré sa majú používať v ich mene na predvídanie výskytu alebo opakovaného výskytu skutočného alebo potenciálneho trestného činu na základe profilovania fyzických osôb uvedeného v článku 3 bode 4 smernice (EÚ) 2016/680 alebo na posúdenie osobnostných a povahových rysov alebo trestnej činnosti fyzických osôb alebo skupín v minulosti;

f) systémy umelej inteligencie, ktoré majú používať orgány presadzovania práva alebo ktoré sa majú používať v ich mene na profilovanie fyzických osôb uvedené v článku 3 bode 4 smernice (EÚ) 2016/680 v priebehu odhaľovania, vyšetrovania alebo stíhania trestných činov.

g) [vypúšťa sa]

7. Migrácia, azyl a riadenie kontroly hraníc:

a) systémy umelej inteligencie, ktoré majú používať príslušné orgány verejnej moci alebo ktoré sa majú používať v ich mene, ako napríklad detektory lži a podobné nástroje, alebo na zisťovanie emocionálneho stavu fyzickej osoby;

b) systémy umelej inteligencie, ktoré majú používať príslušné orgány verejnej moci alebo ktoré sa majú používať v ich mene na posúdenie rizika vrátane bezpečnostného rizika, rizika nelegálnej migrácie alebo zdravotného rizika, ktoré predstavuje fyzická osoba, ktorá má v úmysle vstúpiť na územie členského štátu alebo naň už vstúpila;

c) [vypúšťa sa]

d) systémy umelej inteligencie, ktoré majú používať príslušné orgány verejnej moci alebo ktoré sa majú používať v ich mene pri skúmaní žiadostí o azyl, víza a povolení na pobyt a súvisiacich sťažností týkajúcich sa oprávnenosti fyzických osôb žiadajúcich o určitý status.

8. Výkon spravodlivosti a demokratické procesy:

a) systémy umelej inteligencie, ktoré majú používať justičné orgány alebo ktoré sa majú používať v ich mene pri interpretácii skutočností alebo práva a pri uplatňovaní práva na konkrétny súbor skutočností.

PRÍLOHA IV

TECHNICKÁ DOKUMENTÁCIA uvedená v článku 11 ods. 1

Technická dokumentácia uvedená v článku 11 ods. 1 obsahuje v závislosti od príslušného systému umelej inteligencie aspoň tieto informácie:

1. všeobecný opis systému umelej inteligencie vrátane týchto prvkov:

   a) jeho zamýšľaný účel, osoba/osoby, ktoré systém vyvíjajú, dátum a verzia systému;

   b) spôsob interakcie systému umelej inteligencie s hardvérom alebo softvérom, ktorý nie je súčasťou samotného systému umelej inteligencie, alebo ako ho prípadne možno na takúto interakciu použiť;

   c) verzie príslušného softvéru alebo firmvéru a všetky požiadavky súvisiace s aktualizáciou verzií;

   d) opis všetkých foriem, v ktorých sa systém umelej inteligencie uvádza na trh alebo do prevádzky (napr. softvérový balík zabudovaný do hardvéru, stiahnuteľný, API atď.);

   e) opis hardvéru, na ktorom má systém umelej inteligencie fungovať;

   f) ak je systém umelej inteligencie komponentom výrobkov, fotografií alebo ilustrácií zobrazujúcich vonkajšie vlastnosti, tak označenie a vnútorné usporiadanie týchto výrobkov;

   g) návod na použitie pre používateľa a v náležitom prípade návod na montáž;

2. podrobný opis prvkov systému umelej inteligencie a procesu jeho vývoja, a to:

   a) metódy a kroky vykonané pri vývoji systému umelej inteligencie vrátane prípadného využívania vopred natrénovaných systémov alebo nástrojov poskytnutých tretími stranami a spôsobu, akým ich poskytovateľ používal, integroval alebo upravil;

b) špecifikácie koncepcie systému, konkrétne všeobecná logika systému umelej inteligencie a algoritmov; kľúčové rozhodnutia o koncepčných riešeniach vrátane odôvodnenia a predpokladov, a to aj so zreteľom na osoby alebo skupiny osôb, v prípade ktorých sa má systém používať; hlavné možnosti klasifikácie; čo má systém optimalizovať a relevantnosť jednotlivých parametrov; opis očakávaného výstupu systému; rozhodnutia o akomkoľvek možnom kompromise vykonanom v súvislosti s technickými riešeniami prijatými na dosiahnutie súladu s požiadavkami stanovenými v hlave III kapitole 2;

c) opis architektúry systému, v ktorom sa vysvetľuje, ako softvérové komponenty na seba nadväzujú alebo ako sa navzájom dopĺňajú a integrujú do celkového spracovania; výpočtové zdroje používané na vývoj, trénovanie, testovanie a validáciu systému umelej inteligencie;

d) v príslušnom prípade požiadavky 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 vlastnostiach; spôsob získavania a výberu údajov; postupy označovania (napr. pre učenie s učiteľom), metodiky čistenia údajov (napr. zisťovanie odľahlých hodnôt);

e) posúdenie potrebných opatrení na zabezpečenie ľudského dohľadu v súlade s článkom 14 vrátane posúdenia technických opatrení potrebných na uľahčenie interpretácie výstupov systémov umelej inteligencie používateľmi v súlade s článkom 13 ods. 3 písm. d);

f) v náležitom prípade podrobný opis vopred určených zmien systému umelej inteligencie a jeho výkonnosti spolu so všetkými relevantnými informáciami týkajúcimi sa technických riešení prijatých na zabezpečenie trvalého súladu systému umelej inteligencie s príslušnými požiadavkami stanovenými v hlave III kapitole 2;

g) použité postupy validácie a testovania vrátane informácií o použitých validačných a testovacích údajoch a ich hlavných vlastnostiach; metriky používané na meranie presnosti, spoľahlivosti, kybernetickej bezpečnosti a dosiahnutie súladu s inými relevantnými požiadavkami stanovenými v hlave III kapitole 2, ako aj potenciálne diskriminačné vplyvy; testovacie logy a všetky správy o testoch s dátumom a podpisom zodpovedných osôb, a to aj pokiaľ ide o vopred určené zmeny uvedené v písmene f);

3. podrobné informácie o monitorovaní, fungovaní a kontrole systému umelej inteligencie, najmä pokiaľ ide o: jeho schopnosti a obmedzenia výkonnosti vrátane miery presnosti v prípade konkrétnych osôb alebo skupín osôb, u 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 umelej inteligencie; opatrenia ľudského dohľadu potrebné v súlade s článkom 14 vrátane technických opatrení zavedených na uľahčenie interpretácie výstupov systémov umelej inteligencie používateľmi; prípadné špecifikácie vstupných údajov;

4. podrobný opis systému riadenia rizík v súlade s článkom 9;

5. opis relevantných zmien systému, ktoré vykonal poskytovateľ počas jeho životného cyklu;

6. 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 hlave III kapitole 2 vrátane zoznamu iných príslušných noriem a technických špecifikácií, ktoré sa uplatnili;

7. kópiu EÚ vyhlásenia o zhode;

8. podrobný opis systému zavedeného na hodnotenie výkonnosti systému umelej inteligencie vo fáze po uvedení na trh v súlade s článkom 61 vrátane plánu monitorovania po uvedení na trh v zmysle článku 61 ods. 3.

PRÍLOHA V
EÚ VYHLÁSENIE o ZHODE

EÚ vyhlásenie o zhode uvedené v článku 48 musí obsahovať všetky tieto informácie:

1. názov a typ systému umelej inteligencie a akýkoľvek ďalší jednoznačný odkaz umožňujúci identifikáciu a vysledovateľnosť daného systému umelej inteligencie;

2. meno a adresa poskytovateľa alebo v náležitom prípade jeho splnomocneného zástupcu;

3. vyhlásenie o tom, že EÚ vyhlásenie o zhode sa vydáva na výhradnú zodpovednosť poskytovateľa;

4. vyhlásenie, že daný systém umelej inteligencie je v súlade s týmto nariadením a prípadne aj s akýmikoľvek inými príslušnými právnymi predpismi Únie, ktorými sa stanovuje vydávanie EÚ vyhlásenia o zhode;

5. odkazy na všetky príslušné použité harmonizované normy alebo akékoľvek iné spoločné špecifikácie, v súvislosti s ktorými sa vyhlasuje zhoda;

6. v náležitom prípade meno a identifikačné číslo notifikovanej osoby, opis použitého postupu posudzovania zhody a identifikácia vydaného certifikátu;

7. miesto a dátum vydania vyhlásenia, meno a funkcia osoby, ktorá ho podpísala, ako aj informácia o tom, pre koho a v mene koho daná osoba vyhlásenie podpísala, a podpis.

PRÍLOHA VI

POSTUP POSUDZOVANIA ZHODY NA ZÁKLADE VNÚTORNEJ KONTROLY

1. Postup posudzovania zhody založený na vnútornej kontrole je postup posudzovania zhody založený na bodoch 2 až 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 umelej inteligencie s príslušnými základnými požiadavkami stanovenými v hlave III kapitole 2.

4. Poskytovateľ takisto overí, či je proces koncipovania a vývoja systému umelej inteligencie a jeho monitorovanie po uvedení na trh v zmysle článku 61 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 koncipovanie, vývoj a testovanie systémov umelej inteligencie podľa článku 17 sa preskúma v súlade s bodom 3 a podlieha dohľadu v zmysle bodu 5. Technická dokumentácia systému umelej inteligencie 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 jeho splnomocnený zástupca, aj jeho meno a adresu;

b) zoznam systémov umelej inteligencie, na ktoré sa vzťahuje ten istý systém riadenia kvality;

c) technickú dokumentáciu pre každý systém umelej inteligencie, 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 musí obsahovať závery posúdenia systému riadenia kvality a odôvodnené rozhodnutie o posúdení.

3.3. Schválený systém riadenia kvality musí poskytovateľ naďalej uplatňovať a udržiavať 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 umelej inteligencie, 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 musí obsahovať závery preskúmania zmien a odôvodnené rozhodnutie o posúdení.

4. Kontrola technickej dokumentácie

4.1. Okrem žiadosti uvedenej v bode 3 poskytovateľ predkladá notifikovanej osobe podľa svojho výberu žiadosť o posúdenie technickej dokumentácie vzťahujúcej sa na systém umelej inteligencie, ktorý plánuje uviesť na trh alebo do prevádzky a na ktorý sa vzťahuje systém riadenia kvality uvedený v bode 3.

4.2. Žiadosť musí obsahovať:

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 aplikačných programovacích rozhraní („API“) 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 umelej inteligencie s požiadavkami stanovenými v hlave III kapitole 2. Ak notifikovaná osoba nie je s testmi, ktoré vykonal poskytovateľ, spokojná, zodpovedajúce testy vykoná v prípade potreby priamo notifikovaná osoba.

4.5. Notifikovaným osobám sa udelí prístup k zdrojovému kódu systému umelej inteligencie na základe odôvodnenej žiadosti a len vtedy, ak sú splnené tieto kumulatívne podmienky:

a) prístup k zdrojovému kódu je potrebný na posúdenie súladu vysokorizikového systému umelej inteligencie s požiadavkami stanovenými v hlave III kapitole 2 a

b) postupy testovania/auditu a overovania založené na údajoch a dokumentácii, ktoré poskytol poskytovateľ, boli vyčerpané alebo sa ukázali ako nedostatočné.

4.6. Rozhodnutie sa oznámi poskytovateľovi alebo jeho splnomocnenému zástupcovi. Oznámenie musí obsahovať závery posúdenia technickej dokumentácie a odôvodnené rozhodnutie o posúdení.

Ak je systém umelej inteligencie v súlade s požiadavkami stanovenými v hlave III kapitole 2, notifikovaná osoba vydá certifikát EÚ 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 umelej inteligencie.

Certifikát a jeho prílohy obsahujú všetky relevantné informácie, ktoré umožňujú vyhodnotiť zhodu systému umelej inteligencie a v prípade potreby kontrolu systému umelej inteligencie počas používania.

Ak systém umelej inteligencie nie je v zhode s požiadavkami stanovenými v hlave III kapitole 2, notifikovaná osoba odmietne vydať certifikát EÚ o posúdení technickej dokumentácie a následne o tom informuje žiadateľa, pričom uvedie podrobné dôvody svojho odmietnutia.

Ak systém umelej inteligencie nespĺňa požiadavku týkajúcu sa údajov použitých na jeho trénovanie, pred podaním žiadosti o nové posúdenie zhody bude potrebné opätovné trénovanie systému umelej inteligencie. v tomto prípade musí odôvodnené rozhodnutie notifikovanej osoby o posúdení, ktorým sa zamieta vydanie certifikátu EÚ o posúdení technickej dokumentácie, obsahovať konkrétne vyjadrenia o kvalite údajov použitých na trénovanie systému umelej inteligencie, najmä o dôvodoch nesúladu.

4.7. Každú zmenu systému umelej inteligencie, ktorá by mohla ovplyvniť súlad systému umelej inteligencie s požiadavkami alebo jeho zamýšľaným účelom, schvaľuje notifikovaná osoba, ktorá vydala certifikát EÚ o posúdení technickej dokumentácie. Poskytovateľ musí takúto notifikovanú osobu informovať 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 EÚ o posúdení technickej dokumentácie. v druhom prípade notifikovaná osoba tieto zmeny preskúma, svoje rozhodnutie oznámi poskytovateľovi a v prípade schválenia zmien mu vydá dodatok k certifikátu EÚ 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 spĺňal podmienky schváleného systému riadenia kvality.

5.2. Na účely posúdenia musí poskytovateľ umožniť notifikovanej osobe prístup do priestorov, v ktorých sa uskutočňuje koncipovanie, vývoj a testovanie systémov umelej inteligencie. Poskytovateľ ďalej musí notifikovanej osobe poskytovať 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 umelej inteligencie, pre ktoré bol vydaný certifikát EÚ o posúdení technickej dokumentácie.

PRÍLOHA VIII

INFORMÁCIE, KTORÉ SA MAJÚ PREDLOŽIŤ PRI REGISTRÁCII PREVÁDZKOVATEĽOV a VYSOKORIZIKOVÝCH SYSTÉMOV UMELEJ INTELIGENCIE v SÚLADE s ČLÁNKOM 51

Poskytovatelia, splnomocnení zástupcovia a používatelia, ktorí sú orgánmi verejnej moci, verejnými agentúrami alebo verejnými subjektmi, predkladajú informácie uvedené v časti I. Poskytovatelia alebo prípadne splnomocnení zástupcovia zabezpečia, aby informácie o ich vysokorizikových systémoch umelej inteligencie uvedené v časti II bodoch 1 až 11 boli úplné, správne a aktualizované. Informácie stanovené v bode II.12 sa automaticky generujú v databáze.

Časť I. Informácie týkajúce sa prevádzkovateľov (pri registrácii prevádzkovateľov)

-1. Typ prevádzkovateľa (poskytovateľ, splnomocnený zástupca alebo používateľ)

1. Meno, adresa a ďalšie kontaktné údaje poskytovateľa

2. V prípade, že informácie za prevádzkovateľa predkladá iná osoba, meno, adresa a kontaktné údaje danej osoby

Časť II. Informácie týkajúce sa vysokorizikového systému umelej inteligencie

1. Meno, adresa a ďalšie kontaktné údaje poskytovateľa

2. V náležitom prípade meno, adresa a kontaktné údaje splnomocneného zástupcu

3. Obchodné meno systému umelej inteligencie a akýkoľvek ďalší jednoznačný odkaz umožňujúci identifikáciu a vysledovateľnosť daného systému umelej inteligencie

4. Opis zamýšľaného účelu systému umelej inteligencie

5. Status systému umelej inteligencie (na trhu alebo v prevádzke; už nie je na trhu/v prevádzke, stiahnutý z používania)

6. Typ, číslo a dátum skončenia platnosti certifikátu vydaného notifikovanou osobou a prípadne meno alebo identifikačné číslo tejto notifikovanej osoby

7. V náležitom prípade naskenovaná kópia certifikátu uvedeného v bode 6

8. Členské štáty, v ktorých je alebo bol systém umelej inteligencie uvedený na trh, uvedený do prevádzky alebo sprístupnený v Únii

9. Kópia EÚ vyhlásenia o zhode uvedeného v článku 48

10. Elektronické pokyny na použitie

11. URL pre doplňujúce informácie (nepovinné)

12. Meno, adresa a ďalšie kontaktné údaje používateľov

PRÍLOHA VIIIa

INFORMÁCIE, KTORÉ SA PREDKLADAJÚ PRI REGISTRÁCII RIZIKOVÝCH SYSTÉMOV UMELEJ INTELIGENCIE UVEDENÝCH v PRÍLOHE III VO VZŤAHU K TESTOVANIU v REÁLNYCH PODMIENKACH v SÚLADE s ČLÁNKOM 54A

V súvislosti s testovaním v reálnych podmienkach, ktoré sa má zaregistrovať v súlade s článkom 54a, sa musia poskytnúť a následne aktualizovať tieto informácie:

1. jedinečné jednotné identifikačné číslo testovania v reálnych podmienkach pre celú Úniu;

2. meno a kontaktné údaje poskytovateľa alebo potenciálneho poskytovateľa a používateľov zapojených do testovania v reálnych podmienkach;

3. stručný opis systému umelej inteligencie, jeho zamýšľaný účel a ďalšie informácie potrebné na identifikáciu systému;

4. súhrn hlavných čŕt plánu testovania v reálnych podmienkach;

5. informácie o pozastavení alebo ukončení testovania v reálnych podmienkach.

PRÍLOHA IX

Právne predpisy 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) Návrh NARIADENIA EURÓPSKEHO PARLAMENTU a RADY, ktorým sa mení nariadenie (ES) č. 767/2008, nariadenie (ES) č. 810/2009, nariadenie (EÚ) 2017/2226, nariadenie (EÚ) 2016/399, nariadenie XX/2018 [nariadenie o interoperabilite] a rozhodnutie 2004/512/ES a zrušuje rozhodnutie Rady 2008/633/SVV – COM(2018) 302 final Aktualizovať po prijatí nariadenia spoluzákonodarcami (apríl/máj 2021).

3. Eurodac

a) Zmenený návrh NARIADENIA EURÓPSKEHO PARLAMENTU a RADY o zriadení systému Eurodac na porovnávanie biometrických údajov pre účinné uplatňovanie nariadenia (EÚ) XXX/XXX [nariadenie o riadení azylu a migrácie] a nariadenia (EÚ) XXX/XXX [nariadenie o presídlení], na zistenie totožnosti neoprávnene sa zdržiavajúcich štátnych príslušníkov tretích krajín alebo osôb bez štátnej príslušnosti a o žiadostiach orgánov členských štátov na presadzovanie práva a Europolu o porovnanie s údajmi v systéme Eurodac na účely presadzovania práva a o zmene nariadení (EÚ) 2018/1240 a (EÚ) 2019/818 – COM(2020) 614 final

4. Systém vstup/výstup

a) 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)

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

a) 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 (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 (Ú. v. EÚ L 135, 22.5.2019, s. 85)

_____ma