Rada
Evropské unie

Brusel 25. listopadu 2022
(OR. en)

14954/22

Interinstitucionální spis:
2021/0106(COD)

LIMITE

TELECOM 472
JAI 1494
COPEN 396
CYBER 374
DATAPROTECT 320
EJUSTICE 89
COSI 293
IXIM 267
ENFOPOL 569
RELEX 1556
MI 843
COMPET 918
CODEC 1773

POZNÁMKA

Odesílatel:	Výbor stálých zástupců (část I)
Příjemce:	Rada
Č. předchozího dokumentu:	14336/22
Č. dok. Komise:	8115/21
Předmět:	Návrh nařízení Evropského parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (akt o umělé inteligenci) a mění určité legislativní akty Unie – obecný přístup

I. ÚVOD

1. Dne 21. dubna 2021 přijala Komise návrh nařízení, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (dále jen **„akt o umělé inteligenci“**).

2. Cílem návrhu Komise je zajistit, aby systémy umělé inteligence (systémy UI) uváděné na trh Unie a používané v Unii byly bezpečné a aby byly v souladu se stávajícími právními předpisy v oblasti základních práv a hodnot Unie, zaručit právní jistotu s cílem usnadnit investice a inovace v oblasti umělé inteligence, zlepšit správu a účinné vymáhání stávajících právních předpisů v oblasti základních práv a bezpečnosti a usnadnit rozvoj jednotného trhu pro zákonné, bezpečné a důvěryhodné aplikace umělé inteligence a zároveň zamezit roztříštěnosti trhu.

II. ČINNOST V RÁMCI JINÝCH ORGÁNŮ A INSTITUCÍ

3. V Evropském parlamentu vede jednání Výbor pro vnitřní trh a ochranu spotřebitelů (IMCO; zpravodaj: Brando Benifei, S&D, Itálie) a Výbor pro občanské svobody, spravedlnost a vnitřní věci (LIBE; zpravodaj: Dragos Tudorache, Renew, Rumunsko) v rámci postupu společných schůzí výborů. Výbor pro právní záležitosti (JURI), Výbor pro průmysl, výzkum a energetiku (ITRE) a Výbor pro kulturu a vzdělávání (CULT) jsou zapojeny do legislativní činnosti se sdílenými nebo výlučnými pravomocemi. Oba spoluzpravodajové představili svůj návrh zprávy v dubnu 2022 a hlasování o společné zprávě výborů IMCO a LIBE je naplánováno na první čtvrtletí roku 2023.

4. Evropský hospodářský a sociální výbor vydal stanovisko k návrhu dne 22. září 2021 a Evropský výbor regionů vydal stanovisko následně dne 2. prosince 2021.

5. Dne 18. června 2021 vydaly Evropský sbor pro ochranu osobních údajů (EDPB) a evropský inspektor ochrany údajů (EIOÚ) k návrhu společné stanovisko.

6. Evropská centrální banka (ECB) vydala stanovisko dne 29. prosince 2021 a předložila jej Pracovní skupině pro telekomunikace a informační společnost (dále jen „Pracovní skupina pro telekomunikace“) dne 10. února 2022.

III. AKTUÁLNÍ STAV JEDNÁNÍ V RÁMCI RADY

1. V rámci Rady byl návrh posouzen v Pracovní skupině pro telekomunikace. Pracovní skupina pro telekomunikace zahájila projednávání návrhu během portugalského předsednictví na několika zasedáních a seminářích konaných mezi dubnem a červnem 2021. Práce na návrhu pokračovala za slovinského předsednictví, které vypracovalo první částečný kompromisní návrh zahrnující **články 1–7 a přílohy I–III.** Slovinské předsednictví dále uspořádalo půldenní neformální zasedání Rady ministrů pro telekomunikace, které se zabývalo výhradně návrhem aktu o umělé inteligenci, na němž ministři potvrdili, že podporují horizontální přístup k regulaci umělé inteligence zaměřený na člověka. Francouzské předsednictví pokračovalo v postupu přezkumu a na konci svého funkčního období přepracovalo zbývající části znění **(články 8–85 a přílohy IV–IX)** a dne 17. června 2022 předložilo celý první konsolidovaný kompromisní návrh týkající se aktu o umělé inteligenci.

2. Dne 5. července 2022 uspořádalo české předsednictví v rámci Pracovní skupiny pro telekomunikace politickou rozpravu na základě dokumentu o možnostech politiky, jehož výsledky byly použity k přípravě **druhého kompromisního znění**. Na základě reakcí delegací na tento kompromis připravilo české předsednictví **třetí kompromisní znění**, které bylo předloženo a projednáno na zasedání Pracovní skupiny pro telekomunikace ve dnech 22. a 29. září 2022. Po těchto jednáních byly delegace požádány, aby předložily další písemné připomínky, které české předsednictví použilo k vypracování **čtvrtého kompromisního návrhu**. Na základě jednání o čtvrtém kompromisním návrhu, které se konalo v rámci Pracovní skupiny pro telekomunikace ve dnech 25. října 2022 a 8. listopadu 2022, a s přihlédnutím ke konečným písemným připomínkám členských států vypracovalo české předsednictví **konečnou verzi kompromisního znění**, která je uvedena v příloze. Dne 18. listopadu 2022 Coreper tento kompromisní návrh posoudil a **jednomyslně se dohodl na jeho předložení Radě pro dopravu, telekomunikace a energetiku (telekomunikace) bez jakýchkoli změn za účelem dosažení obecného přístupu** na jejím zasedání dne 6. prosince 2022.

IV. HLAVNÍ PRVKY KOMPROMISNÍHO ZNĚNÍ

1. **Definice systému UI, zakázané postupy v oblasti UI, seznam vysoce rizikových případů použití UI v příloze III a klasifikace systémů UI jako vysoce rizikových**

1.1 Aby se zajistilo, že definice systému UI poskytuje dostatečně jasná kritéria pro odlišení UI od klasičtějších softwarových systémů, zužuje kompromisní znění definici v **čl. 3 odst. 1** na systémy vyvinuté pomocí přístupů strojového učení a přístupů založených na logice a znalostech.

1.2 Pokud jde o přenesení pravomocí na Komisi v souvislosti s aktualizací definice systému UI, **příloha I** a odpovídající zmocnění Komise k její aktualizaci prostřednictvím aktů v přenesené pravomoci byly zrušeny. Namísto toho byly doplněny nové **body odůvodnění 6a a 6b** s cílem objasnit, co by mělo být chápáno jako přístupy strojového učení a přístupy založené na logice a znalostech. Aby se zajistilo, že akt o umělé inteligenci zůstane flexibilní a obstojí i v budoucnu, byla do **článku 4** doplněna možnost přijímat prováděcí akty za účelem dalšího upřesnění a aktualizace technik v rámci přístupů strojového učení a přístupů založených na logice a znalostech.

1.3 Pokud jde o zakázané postupy v oblasti UI, kompromisní znění v **článku 5** obsahuje rozšíření zákazu používání umělé inteligence pro účely sociálního hodnocení i na soukromé subjekty. Kromě toho se ustanovení zakazující používání systémů UI, které využívají zranitelnosti konkrétní skupiny osob, nyní vztahuje i na osoby, které jsou zranitelné v důsledku své sociální nebo ekonomické situace. Pokud jde o zákaz používání systémů biometrické identifikace na dálku „v reálném čase“ na veřejně přístupných místech donucovacími orgány, kompromisní znění vyjasňuje cíle v případech, kdy se takové použití považuje za nezbytně nutné pro účely vymáhání práva, a pro něž by proto donucovací orgány měly mít výjimečně možnost tyto systémy používat.

1.4 Pokud jde o seznam vysoce rizikových případů použití UI v **příloze III**, tři z nich byly vypuštěny (odhalování donucovacími orgány *deep fake*, analýza trestné činnosti, ověřování pravosti cestovních dokladů), dva byly doplněny (kritická digitální infrastruktura a životní a zdravotní pojištění) a další byly doladěny. Zároveň byl změněn **čl. 7 odst. 1** tak, aby umožňoval nejen přidávat vysoce rizikové případy použití na tento seznam prostřednictvím aktů v přenesené pravomoci, ale také je vypustit. Aby byla zajištěna odpovídající ochrana základních práv v případě takového vypuštění, byla do **čl. 7 odst. 3** doplněna dodatečná ustanovení upřesňující podmínky, které by musely být splněny před přijetím aktu v přenesené pravomoci.

1.5 Pokud jde o klasifikaci systémů UI jako vysoce rizikových, kompromisní návrh nyní kromě klasifikace vysoké rizikovosti uvedené v **příloze III** obsahuje další horizontální vrstvu, aby se zajistilo, že systémy UI, u nichž není pravděpodobné, že způsobí závažné porušování základních práv nebo jiná významná rizika, nebudou zahrnuty. Konkrétně **čl. 6 odst. 3** obsahuje nová ustanovení, podle nichž by měl být při klasifikaci systémů UI jako vysoce rizikových rovněž zohledněn význam výstupu systému UI s ohledem na příslušné opatření nebo rozhodnutí, které má být přijato. Význam výstupu systému UI by byl posuzován na základě toho, zda je systém čistě doplňkový, pokud jde o příslušné opatření nebo rozhodnutí, které má být přijato.

2. Požadavky na vysoce rizikové systémy UI a odpovědnost různých subjektů v hodnotovém řetězci UI

2.1 Mnoho požadavků na vysoce rizikové systémy UI, jak je stanoveno v **hlavě III kapitole 2** návrhu, bylo vyjasněno a upraveno tak, aby jejich plnění bylo pro zúčastněné strany technicky proveditelnější a méně zatěžující, například pokud jde o kvalitu údajů nebo v souvislosti s technickou dokumentací, kterou by měly vypracovat malé a střední podniky s cílem prokázat, že jejich vysoce rizikové systémy UI splňují požadavky.

2.2 Vzhledem ke skutečnosti, že systémy UI jsou vyvíjeny a distribuovány prostřednictvím složitých hodnotových řetězců, obsahuje kompromisní znění změny objasňující rozdělení povinností a úloh. Například byla doplněna některá dodatečná ustanovení v **článcích 13 a 14**, která umožňují účinnější spolupráci mezi poskytovateli a uživateli. Cílem kompromisního znění je rovněž vyjasnit vztah mezi povinnostmi podle aktu o umělé inteligenci a povinnostmi, které již existují podle jiných právních předpisů, jako jsou příslušné právní předpisy Unie v oblasti ochrany údajů nebo odvětvové právní předpisy, a to i pokud jde o odvětví finančních služeb. Nový **článek 23a** navíc jasněji uvádí situace, v nichž jsou ostatní subjekty v hodnotovém řetězci povinny převzít odpovědnost poskytovatele.

3. Obecné systémy UI

3.1 Byla přidána **nová hlava IA** s cílem zohlednit situace, kdy lze systémy UI používat pro mnoho různých účelů (UI pro obecné účely) a kdy mohou nastat okolnosti, za nichž je technologie UI pro obecné účely integrována do jiného systému, který se může stát vysoce rizikovým. Kompromisní znění v **čl. 4b odst. 1** upřesňuje, že určité požadavky na vysoce rizikové systémy UI by se vztahovaly i na obecné systémy UI. Namísto přímého uplatňování těchto požadavků by však prováděcí akt specifikoval, jak by měly být uplatňovány ve vztahu k obecným systémům UI, a to na základě konzultací a podrobného posouzení dopadů a s přihlédnutím ke specifickým vlastnostem těchto systémů a souvisejícího hodnotového řetězce, technické proveditelnosti a vývoji trhu a technologií. Použití prováděcího aktu zajistí řádné zapojení členských států a ponechá jim konečné slovo ohledně toho, jak budou požadavky v této souvislosti uplatňovány.

3.2 Kompromisní znění **čl. 4b odst. 5** navíc rovněž zahrnuje možnost přijmout další prováděcí akty, které by stanovily způsoby spolupráce mezi poskytovateli obecných systémů UI a jinými poskytovateli, kteří mají v úmyslu uvést tyto systémy do provozu nebo na trh Unie jako vysoce rizikové systémy UI, zejména pokud jde o poskytování informací.

4. **Vyjasnění oblasti působnosti navrhovaného aktu o umělé inteligenci a ustanovení týkajících se donucovacích orgánů**

4.1 V **článku 2** byl učiněn výslovný odkaz na vyloučení účelů národní bezpečnosti a obranných a vojenských účelů z oblasti působnosti aktu o umělé inteligenci. Podobně bylo vyjasněno, že akt o umělé inteligenci by se neměl vztahovat na systémy UI a jejich výstupy používané výhradně pro účely výzkumu a vývoje a na povinnosti osob využívajících UI pro neprofesionální účely, které by s výjimkou povinností týkajících se transparentnosti nespadaly do oblasti působnosti aktu o umělé inteligenci.

4.2 S cílem zohlednit zvláštní specifika donucovacích orgánů byla provedena řada změn v ustanoveních týkajících se používání systémů umělé inteligence pro účely vymáhání práva. Zejména byly doladěny některé související definice v **článku 3**, jako je „systém biometrické identifikace na dálku“ a „systém biometrické identifikace na dálku, v reálném čase“, s cílem objasnit, které situace by spadaly pod související zákaz a vysoce rizikové případy použití a za jaké situace by tomu tak nebylo. Kompromisní návrh rovněž obsahuje další změny, které mají, s výhradou vhodných záruk, zajistit odpovídající úroveň flexibility při používání vysoce rizikových systémů UI donucovacími orgány nebo zvážit potřebu respektovat důvěrnost citlivých provozních údajů v souvislosti s jejich činnostmi.

5. **Posuzování shody, rámec správy, dozor nad trhem, vymáhání a sankce**

5.1 V zájmu zjednodušení rámce pro dodržování aktu o umělé inteligenci obsahuje kompromisní znění řadu vyjasnění a zjednodušení ustanovení o postupech posuzování shody. Byla rovněž vyjasněna a zjednodušena ustanovení týkající se dozoru nad trhem tak, aby byla účinnější a snadněji proveditelná, s přihlédnutím k potřebě zajmout v tomto ohledu přiměřený přístup. Kromě toho byl důkladně přezkoumán **článek 41** s cílem omezit posuzovací pravomoc Komise, pokud jde o přijímání prováděcích aktů, kterými se stanoví společné technické specifikace pro požadavky na vysoce rizikové systémy UI a obecné systémy UI.

5.2 V kompromisním znění se rovněž podstatně změnila ustanovení týkající se rady pro umělou inteligenci (dále jen „rada“) s cílem zajistit jí větší autonomii a posílit její úlohu v struktuře správy aktu o umělé inteligenci. V této souvislosti byly **články 56 a 58** revidovány s cílem posílit úlohu rady tak, aby mohla lépe poskytovat podporu členským státům při provádění a prosazování aktu o umělé inteligenci. Konkrétně byly rozšířeny úkoly rady a bylo upřesněno její složení. Aby bylo zajištěno zapojení zúčastněných stran v souvislosti se všemi otázkami souvisejícími s prováděním aktu o umělé inteligenci, včetně přípravy prováděcích aktů a aktů v přenesené pravomoci, byl doplněn nový požadavek, aby rada zřídila stálou podskupinu, která by sloužila jako platforma pro širokou škálu zúčastněných stran. Měly by být rovněž zřízeny další dvě stálé podskupiny pro orgány dozoru nad trhem a oznamující orgány s cílem posílit soudržnost správy a prosazování aktu o umělé inteligenci v celé Unii.

5.3 V zájmu dalšího zlepšení rámce správy obsahuje kompromisní znění nové **články 68a a 68b**. **Článek 68a** obsahuje požadavek, aby Komise určila jedno nebo více testovacích zařízení Unie v oblasti umělé inteligence, která by měla na žádost rady nebo orgánů dozoru nad trhem poskytovat nezávislé technické nebo vědecké poradenství, zatímco **článek 68b** ukládá Komisi povinnost vytvořit centrální skupinu nezávislých odborníků na podporu činností v oblasti prosazování práva požadovaných podle aktu o umělé inteligenci. V neposlední řadě je doplněn také nový **článek 58a**, který stanoví povinnost Komise vypracovat pokyny k uplatňování aktu o umělé inteligenci.

5.4 Pokud jde o sankce za porušení ustanovení aktu o umělé inteligenci, kompromisní znění v **článku 71** stanoví přiměřenější mezní hodnoty pro výši správních pokut pro malé a střední podniky a začínající podniky. Kromě toho byla v **čl. 71 odst. 6** doplněna další čtyři kritéria pro rozhodování o výši správních pokut s cílem dále zabezpečit jejich celkovou přiměřenost.

6. **Transparentnost a další ustanovení ve prospěch dotčených osob**

6.1 Kompromisní návrh obsahuje řadu změn, které zvyšují transparentnost, pokud jde o používání vysoce rizikových systémů UI. Zejména byl aktualizován **článek 51** tak, aby uváděl, že někteří uživatelé vysoce rizikových systémů UI, kteří jsou veřejnými orgány, agenturami nebo subjekty, budou rovněž povinni se zaregistrovat do databáze EU pro vysoce rizikové systémy UI uvedené v příloze III. Nově doplněný **čl. 52 odst. 2a** navíc klade důraz na povinnost uživatelů systému rozpoznávání emocí informovat fyzické osoby, pokud jsou takovému systému vystaveny.

6.2 Kompromisní návrh rovněž v nově doplněném **čl. 63 odst. 11** objasňuje, že fyzická nebo právnická osoba, která má důvody se domnívat, že došlo k porušení ustanovení aktu o umělé inteligenci, může podat stížnost příslušnému orgánu dozoru nad trhem a může očekávat, že tato stížnost bude vyřízena v souladu se zvláštními postupy tohoto orgánu.

7. **Opatření na podporu inovací**

7.1 S cílem vytvořit právní rámec, který bude příznivější pro inovace, a s cílem propagovat regulační učení založené na důkazech byla v kompromisním znění v **článku 53** podstatně změněna ustanovení týkající se opatření na podporu inovací. Především bylo objasněno, že tzv. regulační pískoviště UI, jež mají vytvářet kontrolované prostředí pro vývoj, testování a validaci inovativních systémů UI pod přímým dohledem a podle pokynů příslušných vnitrostátních orgánů, by měla umožňovat i testování inovativních systémů UI v reálných podmínkách. Kromě toho byla doplněna nová ustanovení v **článcích 54a a 54b**, která za zvláštních podmínek a záruk umožňují testování systémů UI v reálných podmínkách bez dohledu. V obou případech se v kompromisním znění upřesňuje, jak mají být tato nová pravidla vykládána ve vztahu k jiným stávajícím odvětvovým právním předpisům týkajícím se regulačních pískovišť.

7.2 Za účelem zmírnění administrativní zátěže pro menší společnosti obsahuje kompromisní znění v **článku 55** seznam opatření, která má Komise přijmout na podporu těchto hospodářských subjektů, a v **článku 55a** stanoví některé omezené a jasně stanovené výjimky.

V. ZÁVĚR

1. S ohledem na výše uvedené skutečnosti se Rada vyzývá, aby:
   - projednala kompromisní znění uvedené v příloze tohoto dokumentu
   - potvrdila obecný přístup k návrhu nařízení, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (akt o umělé inteligenci), na zasedání Rady pro dopravu, telekomunikace a energetiku (telekomunikace) dne 6. prosince 2022.

_____

PŘÍLOHA

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY,

KTERÝM SE STANOVÍ HARMONIZOVANÁ PRAVIDLA PRO UMĚLOU INTELIGENCI (AKT O UMĚLÉ INTELIGENCI) A MĚNÍ URČITÉ LEGISLATIVNÍ AKTY UNIE

(Text s významem pro EHP)

EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na články 16 a 114 této smlouvy,

s ohledem na návrh Evropské komise,

po postoupení návrhu legislativního aktu vnitrostátním parlamentům,

s ohledem na stanovisko Evropského hospodářského a sociálního výboru[1],

s ohledem na stanovisko Výboru regionů[2],

s ohledem na stanovisko Evropské centrální banky[3],

v souladu s řádným legislativním postupem,

vzhledem k těmto důvodům:

[1] Úř. věst. C […], […], s. […].
[2] Úř. věst. C […], […], s. […].
[3] Odkaz na stanovisko ECB

(1) Účelem tohoto nařízení je zlepšit fungování vnitřního trhu stanovením jednotného právního rámce zejména pro vývoj umělé inteligence, její uvádění na trh a využívání v souladu s hodnotami Unie. Toto nařízení sleduje řadu naléhavých důvodů veřejného zájmu, jako je například vysoká úroveň ochrany zdraví, bezpečnosti a základních práv, a zajišťuje volný pohyb zboží a služeb založených na UI přes hranice, čímž brání členským státům ukládat omezení vývoje, uvádění na trh a používání systémů UI, pokud to není tímto nařízením výslovně povoleno.

(2) Systémy umělé inteligence (systémy UI) lze snadno uplatnit v řadě hospodářských a společenských odvětví, včetně přeshraničních, a mohou obíhat v celé Unii. Některé členské státy již zkoumají možnost přijetí vnitrostátních pravidel, která by zajišťovala, že umělá inteligence bude bezpečná a že bude vyvíjena a používána v souladu s povinnostmi v oblasti základních práv. Rozdílné vnitrostátní předpisy mohou vést k roztříštěnosti vnitřního trhu a ke snížení právní jistoty pro provozovatele, kteří systémy UI vyvíjejí, dovážejí nebo používají. Proto je třeba zajistit jednotnou a vysokou úroveň ochrany v celé Unii a zároveň zabránit rozdílům, které jsou překážkou volného oběhu systémů UI a souvisejících produktů a služeb na vnitřním trhu, tím, že budou stanoveny jednotné povinnosti provozovatelů a bude zaručena jednotná ochrana naléhavých důvodů obecného zájmu a práv osob na celém vnitřním trhu na základě článku 114 Smlouvy o fungování Evropské unie (SFEU). V rozsahu, v němž toto nařízení obsahuje zvláštní pravidla ochrany fyzických osob v souvislosti se zpracováním osobních údajů, která se týkají omezení používání systémů UI pro biometrickou identifikaci na dálku v „reálném čase“ na veřejně přístupných místech pro účely prosazování práva, je vhodné, aby se ve vztahu k těmto zvláštním pravidlům zakládalo na článku 16 SFEU. S ohledem na tato zvláštní pravidla a na použití článku 16 SFEU je vhodné provést konzultace s Evropským sborem pro ochranu osobních údajů.

(3) Umělá inteligence je rychle se vyvíjející skupina technologií, které mohou přispět k široké škále hospodářských a společenských přínosů v celém spektru průmyslových odvětví a sociálních aktivit. Díky zlepšení predikcí, optimalizaci provozu a přidělování zdrojů a personalizaci digitálních řešení dostupných pro jednotlivce a organizace může využívání umělé inteligence poskytnout společnostem klíčové konkurenční výhody a podpořit sociálně a environmentálně prospěšné výsledky, například v oblasti zdravotnictví, zemědělství, vzdělávání a odborné přípravy, správy infrastruktury, energetiky, dopravy a logistiky, veřejných služeb, bezpečnosti, spravedlnosti, účinného využívání zdrojů a energetické účinnosti a zmírňování změny klimatu a přizpůsobování se této změně.

(4) Umělá inteligence může zároveň v závislosti na okolnostech týkajících se jejího konkrétního uplatňování a využívání vytvářet rizika a působit újmu veřejným zájmům a právům, které jsou chráněny právem Unie. Tato újma může být hmotná nebo nehmotná.

(5) Je proto nezbytné zavést právní rámec Unie, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci, s cílem podpořit vývoj, využívání a zavádění umělé inteligence na vnitřním trhu, který by zároveň splňoval vysokou úroveň ochrany veřejných zájmů, jako je například zdraví, bezpečnost a ochrana základních práv, která jsou uznávána a chráněna právem Unie. K dosažení tohoto cíle by měla být stanovena pravidla, která budou regulovat uvádění určitých systémů UI na trh a do provozu a tím zajišťovat bezproblémové fungování vnitřního trhu a umožňovat, aby tyto systémy měly prospěch ze zásady volného pohybu zboží a služeb. Stanovením těchto pravidel a v návaznosti na práci odborné skupiny na vysoké úrovni pro umělou inteligenci, jak je zohledněno v pokynech pro důvěryhodnou umělou inteligenci v EU, toto nařízení podporuje cíl Unie zastávat v celosvětovém kontextu čelnou pozici, pokud jde o rozvoj bezpečné, důvěryhodné a etické umělé inteligence, který vytyčila Evropská rada[4], a zajišťuje ochranu etických zásad, kterou výslovně požadoval Evropský parlament[5].

---

[4] Evropská rada, mimořádné zasedání Evropské rady (1. a 2. října 2020) – závěry, EUCO 13/20, 2020, s. 6.

[5] Usnesení Evropského parlamentu ze dne 20. října 2020 obsahující doporučení Komisi k rámci pro etické aspekty umělé inteligence, robotiky a souvisejících technologií, 2020/2012(INL).

(5a) Harmonizovaná pravidla pro uvádění systémů UI na trh a do provozu a pro jejich použití stanovená v tomto nařízení by se měla vztahovat na všechna odvětví a v souladu s přístupem nového legislativního rámce by jimi neměly být dotčeny stávající právní předpisy Unie, zejména v oblasti ochrany údajů, ochrany spotřebitele, základních práv, zaměstnanosti a bezpečnosti výrobků, které toto nařízení doplňuje. V důsledku toho zůstávají všechna práva a opravné prostředky, které toto právo Unie poskytuje spotřebitelům a dalším osobám, jež mohou být systémy UI negativně ovlivněny, a to i pokud jde o náhradu možné škody podle směrnice Rady 85/374/EHS ze dne 25. července 1985 o sbližování právních a správních předpisů členských států týkajících se odpovědnosti za vadné výrobky, nadále nedotčeny a plně použitelné. Kromě toho je cílem tohoto nařízení posílit účinnost těchto stávajících práv a opravných prostředků stanovením zvláštních požadavků a povinností, mimo jiné pokud jde o transparentnost, technickou dokumentaci a vedení záznamů o systémech UI. Povinnosti uložené různým provozovatelům zapojeným do hodnotového řetězce UI podle tohoto nařízení by se navíc měly uplatňovat, aniž by byly dotčeny vnitrostátní právní předpisy v souladu s právem Unie, jejichž účinkem je omezení používání určitých systémů UI, pokud tyto právní předpisy nespadají do oblasti působnosti tohoto nařízení nebo sledují jiné legitimní cíle veřejného zájmu než ty, které sleduje toto nařízení. Tímto nařízením by například nemělo být dotčeno vnitrostátní pracovní právo a právní předpisy na ochranu nezletilých osob (tj. osob mladších 18 let) s ohledem na obecnou připomínku OSN č. 25 (2021) o právech dětí, pokud nejsou omezené na systémy UI a sledují jiné legitimní cíle veřejného zájmu.

(6) Je třeba jednoznačně definovat pojem „systém UI“ s cílem zajistit právní jistotu a zároveň poskytnout flexibilitu umožňující přizpůsobit se budoucímu technologickému vývoji. Tato definice by měla být založena na klíčových funkčních vlastnostech umělé inteligence, jako je její schopnost učení, uvažování nebo modelování, a měla by ji odlišit od jednodušších softwarových systémů a programovacích přístupů. Pro účely tohoto nařízení by systémy UI měly být zejména schopny na základě strojových nebo lidských údajů a vstupních dat odvodit způsob, jak dosáhnout souboru konečných cílů, které jim dává člověk, s využitím strojového učení nebo přístupů založených na logice a znalostech a vytvářet výstupy, jako je například obsah pro generativní systémy UI (např. text, video nebo obrázky), predikce, doporučení nebo rozhodnutí, které ovlivňují prostředí, s nímž systém komunikuje, ať už ve fyzické, nebo digitální dimenzi. Systém, který používá pravidla vymezená výhradně fyzickými osobami k automatickému provádění operací, by neměl být považován za systém UI. Systémy UI mohou být navrženy tak, aby fungovaly s různou úrovní samostatnosti a aby mohly být použity buď samostatně, nebo jako součást určitého produktu bez ohledu na to, zda je systém do tohoto produktu fyzicky zabudován (vestavěný systém), nebo zda napomáhá funkčnosti tohoto produktu, aniž by do něho byl zabudován (nevestavěný systém). Koncepce autonomie systému UI se vztahuje k tomu, do jaké míry tento systém funguje bez zapojení člověka.

(6a) Přístupy strojového učení se zaměřují na vývoj systémů, které jsou schopny učit se a odvozovat z údajů, za účelem vyřešení problému aplikace, aniž by byly výslovně plánovány pomocí souboru postupných pokynů od vstupu po výstup. Učením se rozumí výpočetní proces optimalizace parametrů modelu z dat, což je matematická konstrukce vytvářející výstup na základě vstupních údajů. Škála problémů řešených strojovým učením obvykle zahrnuje úkoly, u nichž jiné přístupy selhávají, a to buď proto, že neexistuje vhodná formalizace problému, nebo proto, že řešení problému je složité prostřednictvím přístupů bez učení. Přístupy strojového učení zahrnují například učení s učitelem, bez učitele a posilované učení používající celou řadu metod, včetně hlubokého učení s neuronovými sítěmi, statistické techniky učení a inference (včetně například logistické regrese či bayesovského odhadování) a metod vyhledávání a optimalizace.

(6b) Přístupy založené na logice a znalostech se zaměřují na vývoj systémů se schopnostmi logického uvažování o znalostech za účelem vyřešení problému aplikace. Tyto systémy obvykle zahrnují znalostní základnu a inferenční mechanismus, který generuje výstupy na základě uvažování o znalostní základně. Znalostní základna, která je obvykle zadána lidskými odborníky, představuje subjekty a logické vztahy relevantní pro problém aplikace prostřednictvím formalismů založených na pravidlech, ontologii nebo znalostních grafech. Inferenční mechanismus pracuje se znalostní základnou a extrahuje nové informace prostřednictvím operací, jako je třídění, vyhledávání, párování nebo řetězení. Přístupy založené na logice a znalostech zahrnují například reprezentaci znalostí, induktivní (logické) programování, znalostní základny, inferenční a deduktivní mechanismy, (symbolické) uvažování, expertní systémy a metody vyhledávání a optimalizace.

(6c) Aby byly zajištěny jednotné podmínky pro provádění tohoto nařízení, pokud jde o přístupy strojového učení a přístupy založené na logice a znalostech, a aby byl zohledněn vývoj trhu a technologií, měly by být Komisi svěřeny prováděcí pravomoci.

(6d) Pojem „uživatel“ uvedený v tomto nařízení by měl být vykládán jako jakákoli fyzická nebo právnická osoba, včetně veřejného orgánu, agentury nebo jiného subjektu, používající systém UI, v rámci jejíž pravomoci je systém používán. V závislosti na typu systému UI může používání systému ovlivňovat jiné osoby než uživatele.

(7) Pojem „biometrické údaje“ používaný v tomto nařízení by měl být vykládán konzistentně s pojmem „biometrické údaje“ definovaným v čl. 4 bodě 14 nařízení Evropského parlamentu a Rady (EU) 2016/679[6], v čl. 3 bodě 18 nařízení Evropského parlamentu a Rady (EU) 2018/1725[7] a v čl. 3 bodě 13 směrnice Evropského parlamentu a Rady (EU) 2016/680[8].

[6] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1).

[7] Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES (Úř. věst. L 295, 21.11.2018, s. 39).

[8] Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV (směrnice o prosazování práva) (Úř. věst. L 119, 4.5.2016, s. 89).

(8) Pojem „systém biometrické identifikace na dálku“ používaný v tomto nařízení by měl být definován funkčně jako systém UI určený k identifikaci fyzických osob obvykle na dálku bez jejich aktivního zapojení prostřednictvím porovnání biometrických údajů dané osoby s biometrickými údaji obsaženými v úložišti referenčních údajů, bez ohledu na konkrétní technologii, procesy nebo typy použitých biometrických údajů. Tyto systémy biometrické identifikace na dálku se obvykle používají ke snímání(skenování) vícero osob nebo jejich chování současně, s cílem významně usnadnit identifikaci řady osob bez jejich aktivního zapojení. Z této definice jsou vyloučeny ověřovací/autentizační systémy, jejichž jediným účelem by bylo potvrdit, že konkrétní fyzická osoba je osobou, kterou tvrdí být, a systémy, které se používají k potvrzení totožnosti fyzické osoby pouze za účelem přístupu ke službě, zařízení nebo prostorám. Toto vyloučení je odůvodněno skutečností, že tyto systémy budou mít ve srovnání se systémy biometrické identifikace na dálku, které mohou být použity ke zpracování biometrických údajů velkého počtu osob, pravděpodobně menší dopad na základní práva fyzických osob. V případě systémů provádějících identifikaci „v reálném čase“ probíhá jak zaznamenání biometrických údajů, tak porovnání a identifikace okamžitě, téměř okamžitě nebo v každém případě bez významného zpoždění. V tomto ohledu by neměl existovat žádný prostor pro obcházení pravidel tohoto nařízení o používání dotčených systémů UI „v reálném čase“ stanovením menších zpoždění. Systémy fungující „v reálném čase“ zahrnují použití materiálu „živě“ nebo jen „s malým časovým posunem“ jako jsou například videozáznamy generované kamerou nebo jiným zařízením s podobnými funkcemi. Naproti tomu v případě systémů, ve kterých identifikace probíhá „zpětně,“ dochází k porovnání a identifikaci zachycených údajů až se značným zpožděním. Jedná se o materiály, jako jsou například fotografie nebo videozáznamy generované kamerami s uzavřeným televizním okruhem nebo soukromými zařízeními, které byly vytvořeny před použitím tohoto systému ve vztahu k dotčeným fyzickým osobám.

(9) Pro účely tohoto nařízení by se pod pojmem „veřejně přístupné místo“ mělo rozumět jakékoli fyzické místo, které je přístupné neurčenému počtu fyzických osob, bez ohledu na to, zda je dané místo v soukromém nebo veřejném vlastnictví, a bez ohledu na činnost, pro kterou může být místo využíváno, jako je obchod (například obchody, restaurace, kavárny), služby (například banky, profesní činnosti, pohostinství), sport (například plavecké bazény, tělocvičny, stadiony), doprava (například autobusy, metro a železniční nádraží, letiště, dopravní prostředky), zábava (například kina, divadla, muzea, koncertní a konferenční haly), volný čas nebo jiné (například veřejné komunikace a náměstí, parky, lesy, hřiště). Místo by mělo být klasifikováno jako veřejně přístupné i tehdy, podléhá-li přístup bez ohledu na potenciální kapacitu nebo bezpečnostní omezení určitým předem stanoveným podmínkám, které mohou být splněny neurčeným počtem osob, jako je nákup jízdenky nebo přepravního dokladu, předchozí registrace nebo dosažení určitého věku. Místo by naopak nemělo být považováno za veřejně přístupné, pokud je přístup omezen na konkrétní a vymezené fyzické osoby buď prostřednictvím právních předpisů Unie nebo vnitrostátních právních předpisů přímo souvisejících s veřejnou bezpečností nebo ochranou, nebo prostřednictvím jasného projevu vůle osobou, která má na daném místě příslušnou pravomoc. Samotná faktická možnost přístupu (např. odemčené dveře, otevřená brána v plotu) neznamená, že místo je veřejně přístupné, existují-li indikace nebo okolnosti naznačující opak (např. značky/cedule? zakazující nebo omezující přístup). Prostory společností a továren, jakož i kanceláře a pracoviště, do nichž mají mít přístup pouze příslušní zaměstnanci a poskytovatelé služeb, jsou místa, která nejsou veřejně přístupná. Veřejně přístupná místa by neměla zahrnovat věznice ani místa hraniční kontroly. Některé další prostory mohou být tvořeny jak veřejně nepřístupnými, tak veřejně přístupnými prostory, jako je hala soukromé obytné budovy, která je nezbytná pro přístup do lékařské ordinace, anebo letiště. Tento pojem nezahrnuje ani on-line prostory, protože se nejedná o prostory fyzické. To, zda je daný prostor přístupný veřejnosti, by však mělo být určováno případ od případu s ohledem na zvláštnosti dané konkrétní situace.

(10) V zájmu zajištění rovných podmínek a účinné ochrany práv a svobod jednotlivců v celé Unii by se pravidla stanovená tímto nařízením měla vztahovat na poskytovatele systémů UI nediskriminačním způsobem bez ohledu na to, zda jsou usazeni v Unii nebo ve třetí zemi, a na uživatele systémů UI usazené v Unii.

(11) Do oblasti působnosti tohoto nařízení by měly spadat i určité systémy UI s ohledem na svou digitální povahu, i když nejsou uvedeny ani na trh, ani do provozu, ani nejsou používány v Unii. Jedná se například o provozovatele usazeného v Unii, který smluvně zadává určité služby provozovateli usazenému mimo Unii v souvislosti s činností, kterou má provádět systém UI, jejž by bylo možno označit jako vysoce rizikový. Za těchto okolností by systém UI používaný provozovatelem mimo Unii mohl zpracovávat údaje zákonně shromážděné v Unii a převáděné z Unie a poskytovat zadávajícímu provozovateli v Unii výstup z tohoto systému UI vyplývající z tohoto zpracování, aniž by byl tento systém UI uveden na trh nebo do provozu v Unii nebo v ní byl používán. Aby se předešlo obcházení tohoto nařízení a aby byla zajištěna účinná ochrana fyzických osob nacházejících se v Unii, mělo by se toto nařízení vztahovat také na poskytovatele a uživatele systémů UI, kteří jsou usazeni ve třetí zemi, v rozsahu, v jakém jsou výstupy vytvořené těmito systémy používány v Unii.
S ohledem na již existující ujednání a na zvláštní potřeby budoucí spolupráce se zahraničními partnery, s nimiž probíhá výměna informací a důkazů, by se však toto nařízení nemělo vztahovat na veřejné orgány třetí země a na mezinárodní organizace, pokud jednají v rámci mezinárodních dohod týkajících se prosazování práva a justiční spolupráce s Unií nebo s jejími členskými státy, uzavřených na vnitrostátní nebo evropské úrovni. Tyto dohody byly uzavřeny dvoustranně mezi členskými státy a třetími zeměmi nebo mezi Evropskou unií, Europolem a dalšími agenturami EU a třetími zeměmi a mezinárodními organizacemi. Orgány přijímajících členských států a orgány, instituce a jiné subjekty Unie, které tyto výstupy v Unii využívají, jsou i nadále odpovědné za zajištění toho, aby jejich používání bylo v souladu s právem Unie. Při revizi těchto mezinárodních dohod nebo při uzavírání nových dohod v budoucnu by smluvní strany měly vyvinout maximální úsilí, aby tyto dohody uvedly do souladu s požadavky tohoto nařízení.

(12) Toto nařízení by se mělo vztahovat také na instituce, úřady, orgány a agentury Unie, pokud jednají jako poskytovatel nebo uživatel systému UI.

(-12a) Pokud jsou systémy UI uvedeny na trh nebo do provozu nebo jsou používány se změnami těchto systémů nebo bez nich pro vojenské účely, obranné účely nebo pro účely národní bezpečnosti, měly by být z oblasti působnosti tohoto nařízení vyloučeny bez ohledu na to, jaký typ subjektu tyto činnosti provádí, například zda se jedná o veřejný nebo soukromý subjekt. Pokud jde o vojenské a obranné účely, je toto vyloučení odůvodněno jak čl. 4 odst. 2 SEU, tak specifiky členských států a společné obranné politiky Unie, na něž se vztahuje hlava V kapitola 2 Smlouvy o Evropské unii (SEU), jež podléhají mezinárodnímu právu veřejnému, což je proto vhodnější právní rámec pro regulaci systémů UI v souvislosti s použitím smrtící síly a jiných systémů UI v souvislosti s vojenskými a obrannými činnostmi. Pokud jde o účely národní bezpečnosti, je vyloučení odůvodněno jak skutečností, že národní bezpečnost zůstává v souladu s čl. 4 odst. 2 SEU výhradní odpovědností členských států, tak zvláštní povahou a operativními potřebami činností v oblasti národní bezpečnosti a zvláštními vnitrostátními pravidly použitelnými na tyto činnosti. Pokud je však systém UI vyvinutý, uvedený na trh nebo do provozu nebo používaný pro vojenské nebo obranné účely nebo pro účely národní bezpečnosti používán dočasně nebo trvale pro jiné účely (například pro civilní nebo humanitární účely, pro účely prosazování práva nebo pro účely veřejné bezpečnosti), spadal by do oblasti působnosti tohoto nařízení. V takovém případě by subjekt, který systém používá pro jiné než vojenské nebo obranné účely nebo účely národní bezpečnosti, měl zajistit soulad systému s tímto nařízením, pokud systém již není v souladu s tímto nařízením. Systémy UI uváděné na trh nebo do provozu pro vyloučené účely (tj. vojenské nebo obranné účely nebo účely národní bezpečnost) a jeden nebo více účelů, které vyloučeny nejsou (např. civilní účely, prosazování práva atd.), spadají do oblasti působnosti tohoto nařízení a poskytovatelé těchto systémů by měli zajistit soulad s tímto nařízením. V těchto případech by skutečností, že systém UI může spadat do oblasti působnosti tohoto nařízení, neměla být dotčena možnost subjektů provádějících činnosti v oblasti národní bezpečnosti nebo obranné a vojenské činnosti, bez ohledu na typ subjektu, který tyto činnosti provádí, používat systémy UI pro účely národní bezpečnosti nebo vojenské a obranné účely, jejichž použití je z oblasti působnosti tohoto nařízení vyloučeno. Systém UI uváděný na trh pro civilní účely nebo pro účely prosazování práva, který se používá se změnami nebo bez nich pro vojenské nebo obranné účely nebo pro účely národní bezpečnosti, by neměl spadat do oblasti působnosti tohoto nařízení, a to bez ohledu na typ subjektu, který tyto činnosti provádí.

(12a) Tímto nařízením by neměla být dotčena ustanovení týkající se odpovědnosti poskytovatelů zprostředkovatelských služeb stanovená ve směrnici Evropského parlamentu a Rady 2000/31/ES [ve znění aktu o digitálních službách].

(12b) Toto nařízení by nemělo narušovat výzkum a vývoj a mělo by respektovat svobodu vědy. Je proto nezbytné vyloučit z oblasti jeho působnosti systémy UI speciálně vyvinuté a uvedené do provozu výhradně za účelem vědeckého výzkumu a vývoje a zajistit, aby nařízení žádným jiným způsobem neovlivňovalo činnost v oblasti vědeckého výzkumu a vývoje systémů UI. Pokud jde o výzkumnou činnost poskytovatelů zaměřenou na produkty, ustanovení tohoto nařízení by se rovněž neměla použít. Tím není dotčena povinnost dodržovat toto nařízení, pokud je systém UI spadající do oblasti působnosti tohoto nařízení uveden na trh nebo do provozu v důsledku této výzkumné a vývojové činnosti, ani uplatňování ustanovení o regulačních pískovištích a testování v reálných podmínkách. Kromě toho, aniž je dotčeno výše uvedené, pokud jde o systémy UI speciálně vyvinuté a uvedené do provozu výhradně za účelem vědeckého výzkumu a vývoje, na jakýkoli jiný systém UI, který může být použit k provádění jakékoli výzkumné a vývojové činnosti, by se měla i nadále vztahovat ustanovení tohoto nařízení. Za všech okolností by měla být veškerá výzkumná a vývojová činnost prováděna v souladu s uznávanými etickými a profesními normami vědeckého výzkumu.

(12c) Vzhledem k povaze a složitosti hodnotového řetězce systémů UI je nezbytné vyjasnit úlohu aktérů, kteří mohou přispívat k vývoji systémů UI, zejména vysoce rizikových systémů UI. Zejména je nezbytné vyjasnit, že obecné systémy UI jsou systémy UI, které jsou určeny poskytovatelem k vykonávání obecně použitelných funkcí, jako je rozpoznávání obrazu nebo řeči, a to v různých kontextech. Mohou být samy o sobě používány jako vysoce rizikové systémy UI nebo mohou být součástí jiných vysoce rizikových systémů UI. Vzhledem ke své zvláštní povaze a s cílem zajistit spravedlivé sdílení odpovědnosti v celém hodnotovém řetězci UI by se na tyto systémy proto měly vztahovat přiměřené a konkrétnější požadavky a povinnosti podle tohoto nařízení a zároveň by měla být zajištěna vysoká úroveň ochrany základních práv, zdraví a bezpečnosti. Kromě toho by poskytovatelé obecných systémů UI bez ohledu na to, zda mohou být používány jako vysoce rizikové systémy UI jako takové jinými poskytovateli, nebo jako součásti vysoce rizikových systémů UI, měli případně spolupracovat s poskytovateli příslušných vysoce rizikových systémů UI, aby mohli plnit příslušné povinnosti podle tohoto nařízení, a s příslušnými orgány zřízenými podle tohoto nařízení. Aby se zohlednily zvláštní vlastnosti obecných systémů UI a rychle se vyvíjející trh a technologický vývoj v této oblasti, měly by být Komisi svěřeny prováděcí pravomoci k upřesnění a přizpůsobení uplatňování požadavků stanovených tímto nařízením na obecné systémy UI a k upřesnění informací, které mají poskytovatelé obecných systémů UI sdílet, aby poskytovatelé příslušného vysoce rizikového systému UI mohli plnit své povinnosti podle tohoto nařízení.

(13) V zájmu zajištění jednotné a vysoké úrovně ochrany veřejných zájmů, pokud jde o zdraví, bezpečnost a základní práva, by měly být pro všechny vysoce rizikové systémy UI stanoveny společné normativní standardy. Tyto standardy by měly být v souladu s Listinou základních práv Evropské unie (dále jen „Listina“) a se závazky Unie v oblasti mezinárodního obchodu a měly by být nediskriminační.

(14) Aby bylo možné zavést přiměřený a účinný soubor závazných pravidel pro systémy UI, měl by být dodržován jasně definovaný přístup založený na posouzení rizik. Tento přístup by měl přizpůsobit typ a obsah těchto pravidel intenzitě a rozsahu rizik, která mohou systémy UI vytvářet. Je proto nezbytné zakázat některé postupy v oblasti UI a stanovit požadavky na vysoce rizikové systémy UI a povinnosti příslušných provozovatelů, jakož i povinnosti transparentnosti pro určité systémy UI.

(15) Na jedné straně přináší využívání umělé inteligence celou řadu výhod, avšak tuto technologii lze používat i nesprávně a může se stát zdrojem nových a výkonných nástrojů umožňujících manipulativní a vykořisťovatelské praktiky a praktiky v oblasti sociální kontroly. Tyto praktiky jsou mimořádně škodlivé a měly by být zakázány, protože jsou v rozporu s hodnotami Unie v oblasti úcty k lidské důstojnosti, svobody, rovnosti, demokracie a právního státu a se základními právy Unie, včetně práva na zákaz diskriminace, na ochranu údajů a soukromí a práva dítěte.

(16) Manipulativní techniky založené na umělé inteligenci lze použít k přesvědčování osob k nežádoucímu chování nebo k jejich klamání tím, že je povzbuzují k rozhodování způsobem, který podkopává a narušuje jejich autonomii, rozhodování a svobodnou volbu. Uvádění na trh, uvádění do provozu nebo využívání určitých systémů UI, které podstatně ovlivňují lidské chování tak, že by mohly způsobit fyzickou nebo psychickou újmu, je obzvláště nebezpečné a mělo by proto být zakázáno. Tyto systémy UI využívají složky uplatňující podprahové techniky, jako jsou zvukové, obrazové a video stimuly, které osoby nemohou vnímat, neboť jsou mimo rámec lidského vnímání, nebo jiných podprahových technik, které podkopávají nebo narušují autonomii, rozhodování nebo svobodnou volbu osoby způsobem, který lidé vědomě nerozpoznají, nebo dokonce, pokud si tuto skutečnost uvědomí, nejsou schopni ji ovládat nebo jí odolávat, například v případě rozhraní stroj–mozek nebo virtuální reality. Kromě toho mohou systémy UI rovněž jinak zneužívat zranitelnost určité skupiny osob z důvodu jejich věku, zdravotního postižení ve smyslu směrnice (EU) 2019/882 nebo zvláštní sociální nebo ekonomické situace, která pravděpodobně zvýší zranitelnost těchto osob vůči zneužívání, jako jsou osoby žijící v extrémní chudobě nebo etnické nebo náboženské menšiny. Tyto systémy mohou být uváděny na trh nebo do provozu nebo používány s cílem nebo za účelem podstatného narušení chování určité osoby, a to takovým způsobem, který této nebo jiné osobě nebo skupinám osob způsobuje nebo může důvodně způsobit fyzickou nebo psychickou újmu, včetně škod, které se mohou v průběhu času nahromadit. Záměr narušit chování nelze předpokládat, pokud k narušení dochází v důsledku faktorů nesouvisejících se systémem UI, které jsou mimo kontrolu poskytovatele nebo uživatele, tedy faktorů, které poskytovatel ani uživatel systému UI nemůže rozumně předvídat a zmírnit. V každém případě není nutné, aby poskytovatel nebo uživatel měli v úmyslu způsobit fyzickou nebo psychickou újmu, pokud tato újma vyplývá z manipulativních nebo vykořisťujících praktik založených na umělé inteligenci. Zákazy těchto praktik UI doplňují ustanovení obsažená ve směrnici 2005/29/ES, zejména pokud jde o to, že nekalé obchodní praktiky vedoucí k hospodářské nebo finanční újmě pro spotřebitele jsou zakázány za všech okolností bez ohledu na to, zda jsou zavedeny prostřednictvím systémů UI, nebo jinak. Zákazy manipulativních a vykořisťujících praktik v tomto nařízení by neměly mít vliv na zákonné postupy v souvislosti s lékařskou péčí, jako je psychologická léčba duševní nemoci nebo tělesná rehabilitace, jsou-li tyto praktiky prováděny v souladu s platnými lékařskými normami a právními předpisy. Kromě toho by běžné a legitimní obchodní praktiky, které jsou v souladu s platnými právními předpisy, neměly být samy o sobě považovány za škodlivé manipulativní praktiky umělé inteligence.

(17) Systémy UI provádějící hodnocení sociálního kreditu fyzických osob ze strany veřejných orgánů nebo ze strany soukromých aktérů mohou vést k diskriminačním výsledkům a k vyloučení určitých skupin. Mohou porušovat právo na důstojnost a zákaz diskriminace a hodnoty rovnosti a spravedlnosti. Tyto systémy UI hodnotí nebo klasifikují fyzické osoby na základě jejich sociálního chování v různých kontextech nebo známých či předvídaných osobních či osobnostních vlastností. Sociální kredit získaný na základě těchto systémů UI může vést ke znevýhodňujícímu nebo nepříznivému zacházení s fyzickými osobami nebo s celými skupinami těchto osob v sociálních kontextech nesouvisejících s kontextem, ve kterém byly dané údaje původně vytvořeny nebo shromážděny, případně ke znevýhodňujícímu zacházení, které je nepřiměřené nebo neodůvodněné s ohledem na závažnost jejich sociálního chování. Systémy UI, které zahrnují takové nepřijatelné postupy bodování, by proto měly být zakázány. Tímto zákazem by neměly být dotčeny zákonné postupy posuzování fyzických osob prováděné pro jeden nebo více konkrétních účelů v souladu s právními předpisy.

(18) Využívání systémů UI pro biometrickou identifikaci fyzických osob na dálku „v reálném čase“ na veřejně přístupných místech pro účely prosazování práva je považováno za zvláště rušivý zásah do práv a svobod dotčených osob, neboť může ovlivnit soukromý život velké části populace, vyvolávat pocit neustálého sledování a nepřímo odrazovat od využívání svobody shromažďování a dalších základních práv. Bezprostřednost dopadu a omezené možnosti dalších kontrol nebo oprav v souvislosti s používáním těchto systémů fungujících „v reálném čase“ s sebou navíc nesou zvýšené riziko z hlediska práv a svobod osob, kterých se týkají činnosti v oblasti prosazování práva.

(19) Používání těchto systémů pro účely prosazování práva by proto mělo být zakázáno s výjimkou taxativně vyjmenovaných a úzce definovaných situací, kdy je toto použití nezbytně nutné k dosažení významného veřejného zájmu, jehož význam převažuje nad uvedenými riziky. Tyto situace zahrnují hledání potenciálních obětí trestných činů, včetně pohřešovaných dětí; některé případy ohrožení života nebo fyzické bezpečnosti fyzických osob nebo hrozby teroristického útoku a odhalování, lokalizaci, identifikaci nebo stíhání pachatelů nebo osob podezřelých z trestných činů uvedených v rámcovém rozhodnutí Rady 2002/584/SVV[9], pokud lze tyto trestné činy v dotčeném členském státě potrestat trestem odnětí svobody nebo ochranným opatřením spojeným s odnětím osobní svobody s horní hranicí sazby v délce nejméně tři roky a jsou-li vymezeny právem tohoto členského státu. Tato hranice pro trest odnětí svobody nebo ochranné opatření spojené s odnětím osobní svobody v souladu s vnitrostátními právními předpisy přispívá k zajištění toho, že použití systémů biometrické identifikace na dálku „v reálném čase“ bude možno potenciálně odůvodnit jen dostatečnou závažností daného trestného činu. Je navíc pravděpodobné, že některé z 32 trestných činů uvedených v rámcovém rozhodnutí Rady 2002/584/SVV budou v praxi relevantnější než jiné v tom smyslu, že nezbytnost a přiměřenost využívání biometrické identifikace na dálku „v reálném čase“ bude pravděpodobně velmi různorodá jak z hlediska praktické snahy o odhalování, lokalizaci, identifikaci nebo stíhání pachatelů jednotlivých uvedených trestných činů nebo osob podezřelých z jejich spáchání, tak s ohledem na pravděpodobné rozdíly v závažnosti, pravděpodobnosti a rozsahu způsobené újmy nebo možných negativních důsledků. Kromě toho by toto nařízení mělo zachovat schopnost donucovacích orgánů, orgánů odpovědných za ochranu hranic, imigračních nebo azylových orgánů provádět kontroly totožnosti za přítomnosti dotčené osoby v souladu s podmínkami stanovenými pro tyto kontroly v právu Unie a vnitrostátním právu. Donucovací orgány, orgány odpovědné za ochranu hranic, imigrační nebo azylové orgány by zejména měly mít možnost používat informační systémy v souladu s právem Unie nebo vnitrostátním právem k identifikaci osoby, která během kontroly totožnosti buď odmítne být identifikována, nebo není schopna uvést či prokázat svou totožnost, aniž by byly podle tohoto nařízení povinny získat předchozí povolení. Může se jednat například o osobu zapojenou do trestného činu, která není ochotna nebo kvůli nehodě nebo zdravotnímu stavu schopna sdělit svou totožnost donucovacím orgánům.

[9] Rámcové rozhodnutí Rady 2002/584/SVV ze dne 13. června 2002 o evropském zatýkacím rozkazu a postupech předávání mezi členskými státy (Úř. věst. L 190, 18.7.2002, s. 1).

(20) Aby bylo zajištěno odpovědné a přiměřené používání těchto systémů, je rovněž důležité stanovit, že v každé z těchto taxativně vyjmenovaných a úzce definovaných situací je třeba zohlednit určité prvky, zejména pokud jde o povahu situace, která vedla k předložení žádosti, o důsledky užití těchto systémů pro práva a svobody všech dotčených osob a o záruky a podmínky zajištěné při tomto použití. Na využívání systémů biometrické identifikace na dálku „v reálném čase“ na veřejně přístupných místech pro účely prosazování práva by se navíc měla vztahovat vhodná časová a prostorová omezení, zejména s ohledem na důkazy nebo náznaky týkající se daných hrozeb, obětí nebo pachatele. Pro každý případ použití v každé z výše uvedených situací by mělo být vhodné využití referenční databáze osob.

(21) Každé použití systému biometrické identifikace na dálku „v reálném čase“ na veřejně přístupných místech pro účely prosazování práva by mělo podléhat výslovnému a konkrétnímu povolení justičního orgánu nebo nezávislého správního orgánu členského státu. Toto povolení by mělo být v zásadě získáno před použitím systému za účelem identifikace osoby nebo osob. Výjimky z tohoto pravidla by měly být povoleny v řádně odůvodněných naléhavých situacích, tj. situacích, kdy je potřeba použít dotyčné systémy tak naléhavá, že je účinně a objektivně nemožné získat povolení před zahájením tohoto použití. V těchto naléhavých situacích by použití mělo být omezeno na absolutně nezbytné minimum a mělo by podléhat příslušným zárukám a podmínkám, které stanoví vnitrostátní právo a specifikuje samotný donucovací orgán v kontextu každého jednotlivého případu naléhavého použití. Donucovací orgán by měl v těchto situacích rovněž usilovat o co nejvčasnější získání povolení a měl by uvést důvody, proč o něj nemohl požádat již dříve.

(22) Dále je vhodné v rámci taxativně vymezeném tímto nařízením stanovit, že toto použití na území členského státu v souladu s tímto nařízením by mělo být možné pouze tehdy a do té míry, do níž se dotčený členský stát rozhodl výslovně stanovit možnost povolit toto použití ve své podrobné vnitrostátní úpravě. V důsledku toho se členské státy mohou podle tohoto nařízení i nadále dle vlastního uvážení rozhodnout, že tuto možnost vůbec nestanoví, případně že ji stanoví pouze ve vztahu k některým cílům, které mohou povolené použití určené v tomto nařízení odůvodnit.

(23) Využívání systémů UI pro biometrickou identifikaci fyzických osob na dálku „v reálném“ čase na veřejně přístupných místech pro účely prosazování práva nutně zahrnuje i zpracování biometrických údajů. Pravidla tohoto nařízení, která toto použití až na určité výjimky zakazují a která jsou založena na článku 16 SFEU, by se měla použít jako *lex specialis*, pokud jde o pravidla zpracování biometrických údajů uvedená v článku 10 směrnice (EU) 2016/680, což by toto použití a zpracování biometrických údajů vyčerpávajícím způsobem regulovalo. Toto použití a zpracování by proto mělo být možné jen v případě, že bude slučitelné s rámcem stanoveným tímto nařízením, a mimo tento rámec by neměl existovat prostor pro to, aby příslušné orgány jednající za účelem prosazování práva používaly tyto systémy a zpracovávaly tyto údaje v souvislosti s nimi z důvodů uvedených v článku 10 směrnice (EU) 2016/680. V této souvislosti není cílem tohoto nařízení poskytnout právní základ zpracování osobních údajů podle článku 8 směrnice 2016/680. Na používání systémů biometrické identifikace na dálku „v reálném čase“ na veřejně přístupných místech pro jiné účely než prosazování práva, a to i příslušnými orgány, by se však neměl vztahovat zvláštní rámec týkající se tohoto použití pro účely prosazování práva, stanovený tímto nařízením. Toto použití pro jiné účely než pro účely prosazování práva by proto nemělo podléhat požadavku na povolení podle tohoto nařízení a použitelným podrobným pravidlům vnitrostátního práva, která ho případně mohou uvést v účinnost.

(24) Jakékoli zpracování biometrických údajů a dalších osobních údajů související s používáním systémů UI pro účely biometrické identifikace jinak než v souvislosti s používáním systémů biometrické identifikace na dálku „v reálném čase“ na veřejně přístupných místech pro účely prosazování práva podle tohoto nařízení by mělo i nadále splňovat všechny požadavky vyplývající z článku 10 směrnice (EU) 2016/680. Pro jiné účely, než je vymáhání práva, čl. 9 odst. 1 nařízení (EU) 2016/679 a čl. 10 odst. 1 nařízení (EU) 2018/1725 zakazují zpracování biometrických údajů pro účely jedinečné identifikace fyzické osoby, pokud nenastane jedna ze situací uvedených v příslušných druhých pododstavcích těchto dvou článků.

(25) V souladu s článkem 6a Protokolu č. 21 o postavení Spojeného království a Irska s ohledem na prostor svobody, bezpečnosti a práva, připojeného ke Smlouvě o EU a Smlouvě o fungování EU, není Irsko vázáno pravidly stanovenými v čl. 5 odst. 1 písm. d) a čl. 5 odst. 2, 3 a 4 tohoto nařízení přijatého na základě článku 16 Smlouvy o fungování EU, která se týkají zpracování osobních údajů členskými státy, vykonávají-li činnosti spadající do oblasti působnosti části třetí hlavy V kapitoly 4 nebo 5 Smlouvy o fungování EU, pokud není Irsko vázáno pravidly Unie upravujícími formy justiční spolupráce v trestních věcech nebo policejní spolupráce, v jejichž rámci musí být dodržována pravidla přijatá na základě článku 16 Smlouvy o fungování EU.

(26) V souladu s články 2 a 2a Protokolu č. 22 o postavení Dánska, připojeného ke Smlouvě o EU a Smlouvě o fungování EU, nejsou pro Dánsko závazná ani použitelná pravidla stanovená v čl. 5 odst. 1 písm. d) a v čl. 5 odst. 2, 3 a 4 tohoto nařízení přijatého na základě článku 16 Smlouvy o fungování EU, která se týkají zpracování osobních údajů členskými státy, vykonávají-li činnosti spadající do oblasti působnosti části třetí hlavy V kapitoly 4 nebo 5 Smlouvy o fungování EU.

(27) Vysoce rizikové systémy UI by měly být uváděny na trh Unie nebo do provozu pouze tehdy, splňují-li určité závazné požadavky. Tyto požadavky by měly zajistit, aby vysoce rizikové systémy UI, které jsou dostupné v Unii nebo jejichž výstupy jsou v Unii jinak využívány, nepředstavovaly nepřijatelné riziko pro důležité veřejné zájmy Unie uznané a chráněné právem Unie. Systémy UI označené jako vysoce rizikové by měly být omezeny na systémy, které mají významný škodlivý dopad na zdraví, bezpečnost a základní práva osob v Unii, a toto omezení minimalizuje jakékoli případné omezení mezinárodního obchodu.

(28) Systémy UI by mohly mít nepříznivé účinky na zdraví a bezpečnost osob, zejména pokud tyto systémy fungují jako součásti produktů. V souladu s cíli harmonizačních právních předpisů Unie, které mají usnadnit volný pohyb produktů na vnitřním trhu a zajistit, aby se na trh dostávaly pouze bezpečné a jinak vyhovující produkty, je důležitá náležitá prevence a zmírňování bezpečnostních rizik, která mohou případně vyplývat z produktu jako celku v důsledku jeho digitálních prvků, včetně systémů UI. Například stále autonomnější roboti, ať už v kontextu výroby, nebo osobní asistence a péče, by měli být schopni bezpečně fungovat a vykonávat své funkce ve složitých prostředích. Obdobně ve zdravotnictví, kde existuje obzvláště vysoké riziko v oblasti života a zdraví, by měly být stále sofistikovanější diagnostické systémy a systémy podporující lidská rozhodnutí spolehlivé a přesné. Míra nepříznivého dopadu systému UI na základní práva chráněná Listinou je obzvláště důležitá v případě, že je systém UI klasifikován jako vysoce rizikový. Tato práva zahrnují právo na lidskou důstojnost, respektování soukromého a rodinného života, ochranu osobních údajů, svobodu projevu a informací, svobodu shromažďování a sdružování a zákaz diskriminace, ochranu spotřebitele, práva pracovníků, práva osob s postižením, právo na účinnou právní ochranu a spravedlivý proces, právo na obhajobu a presumpci neviny a právo na řádnou správu. Kromě těchto práv je třeba zdůraznit zvláštní práva dětí zakotvená v článku 24 Listiny základních práv EU a v Úmluvě OSN o právech dítěte (ve vztahu k digitálním prostředí dále rozpracovaná v obecné připomínce č. 25 k Úmluvě o právech dítěte), které v obou případech vyžadují zohlednění zranitelnosti dětí a poskytnutí této ochrany a péče, která je nezbytná pro jejich blaho. Při posuzování závažnosti újmy, kterou může systém UI způsobit, a to i ve vztahu ke zdraví a bezpečnosti osob, by mělo být zohledněno také základní právo na vysokou úroveň ochrany životního prostředí zakotvené v Listině a provedené do politik Unie.

(29) Pokud jde o vysoce rizikové systémy UI, které jsou bezpečnostními součástmi produktů nebo systémů, případně které jsou samy produkty nebo systémy spadajícími do působnosti nařízení Evropského parlamentu a Rady (ES) č. 300/2008[10], nařízení Evropského parlamentu a Rady (EU) č. 167/2013[11], nařízení Evropského parlamentu a Rady (EU) č. 168/2013[12], směrnice Evropského parlamentu a Rady 2014/90/EU[13], směrnice Evropského parlamentu a Rady (EU) 2016/797[14], nařízení Evropského parlamentu a Rady (EU) 2018/858[15], nařízení Evropského parlamentu a Rady (EU) 2018/1139[16] a nařízení Evropského parlamentu a Rady (EU) 2019/2144[17], je vhodné tyto akty pozměnit s cílem zajistit, aby Komise při přijímání jakýchkoli budoucích relevantních aktů v přenesené pravomoci nebo prováděcích aktů na základě výše uvedených aktů zohledňovala povinné požadavky na vysoce rizikové systémy UI stanovené v tomto nařízení na základě technických a regulačních specifik jednotlivých odvětví, aniž by zasahovala do stávajících mechanismů správy, posuzování shody a prosazování ani do orgánů zřízených v rámci uvedených aktů.

---

10 Nařízení Evropského parlamentu a Rady (ES) č. 300/2008 ze dne 11. března 2008 o společných pravidlech v oblasti ochrany civilního letectví před protiprávními činy a o zrušení nařízení (ES) č. 2320/2002 (Úř. věst. L 97, 9.4.2008, s. 72).

11 Nařízení Evropského parlamentu a Rady (EU) č. 167/2013 ze dne 5. února 2013 o schvalování zemědělských a lesnických vozidel a dozoru nad trhem s těmito vozidly (Úř. věst. L 60, 2.3.2013, s. 1).

12 Nařízení Evropského parlamentu a Rady (EU) č. 168/2013 ze dne 15. ledna 2013 o schvalování dvoukolových nebo tříkolových vozidel a čtyřkolek a dozoru nad trhem s těmito vozidly (Úř. věst. L 60, 2.3.2013, s. 52).

13 Směrnice Evropského parlamentu a Rady 2014/90/EU ze dne 23. července 2014 o lodní výstroji a o zrušení směrnice Rady 96/98/ES (Úř. věst. L 257, 28.8.2014, s. 146).

14 Směrnice Evropského parlamentu a Rady (EU) 2016/797 ze dne 11. května 2016 o interoperabilitě železničního systému v Evropské unii (Úř. věst. L 138, 26.5.2016, s. 44).

15 Nařízení Evropského parlamentu a Rady (EU) 2018/858 ze dne 30. května 2018 o schvalování motorových vozidel a jejich přípojných vozidel, jakož i systémů, konstrukčních částí a samostatných technických celků určených pro tato vozidla a o dozoru nad trhem s nimi, o změně nařízení (ES) č. 715/2007 a č. 595/2009 a o zrušení směrnice 2007/46/ES (Úř. věst. L 151, 14.6.2018, s. 1).

16 Nařízení Evropského parlamentu a Rady (EU) 2018/1139 ze dne 4. července 2018 o společných pravidlech v oblasti civilního letectví a o zřízení Agentury Evropské unie pro bezpečnost letectví, kterým se mění nařízení (ES) č. 2111/2005, (ES) č. 1008/2008, (EU) č. 996/2010, (EU) č. 376/2014 a směrnice Evropského parlamentu a Rady 2014/30/EU a 2014/53/EU a kterým se zrušuje nařízení Evropského parlamentu a Rady (ES) č. 552/2004 a (ES) č. 216/2008 a nařízení Rady (EHS) č. 3922/91 (Úř. věst. L 212, 22.8.2018, s. 1).

17 Nařízení Evropského parlamentu a Rady (EU) 2019/2144 ze dne 27. listopadu 2019 o požadavcích pro schvalování typu motorových vozidel a jejich přípojných vozidel a systémů, konstrukčních částí a samostatných technických celků určených pro tato vozidla z hlediska obecné bezpečnosti a ochrany cestujících ve vozidle a zranitelných účastníků silničního provozu, o změně nařízení Evropského parlamentu a Rady (EU) 2018/858 a o zrušení nařízení Evropského parlamentu a Rady (ES) č. 78/2009, (ES) č. 79/2009 a (ES) č. 661/2009 a nařízení Komise (ES) č. 631/2009, (EU) č. 406/2010, (EU) č. 672/2010, (EU) č. 1003/2010, (EU) č. 1005/2010, (EU) č. 1008/2010, (EU) č. 1009/2010, (EU) č. 19/2011, (EU) č. 109/2011, (EU) č. 458/2011, (EU) č. 65/2012, (EU) č. 130/2012, (EU) č. 347/2012, (EU) č. 351/2012, (EU) č. 1230/2012 a (EU) 2015/166 (Úř. věst. L 325, 16.12.2019, s. 1).

(30) Pokud jde o systémy UI, které jsou bezpečnostními součástmi produktů nebo jsou produkty samy o sobě, a které spadají do oblasti působnosti některých harmonizačních právních předpisů Unie, je vhodné je podle tohoto nařízení klasifikovat jako vysoce rizikové, pokud u daného produktu provádí postup posuzování shody subjekt, který vykonává činnosti posuzování shody jakožto třetí strana podle příslušných harmonizačních právních předpisů Unie. Těmito produkty jsou zejména strojní zařízení, hračky, výtahy, zařízení a ochranné systémy určené k použití v prostředí s nebezpečím výbuchu, rádiová zařízení, tlaková zařízení, zařízení pro rekreační plavidla, lanové dráhy, spotřebiče plynných paliv, zdravotnické prostředky a diagnostické zdravotnické prostředky in vitro.

(31) Klasifikace systému UI jako vysoce rizikového podle tohoto nařízení by neměla nutně znamenat, že produkt, jehož je daný systém UI bezpečnostní součástí, případně tento samotný systém UI jako produkt, je považován za „vysoce rizikový“ podle kritérií stanovených v příslušných harmonizačních právních předpisech Unie, které se na tento produkt vztahují. To platí zejména pro nařízení Evropského parlamentu a Rady (EU) 2017/745[18] a nařízení Evropského parlamentu a Rady (EU) 2017/746[19], kde je pro produkty se středním a vysokým rizikem vyžadováno posuzování shody subjektem, který vykonává činnosti posuzování shody jakožto třetí strana.

[18] Nařízení Evropského parlamentu a Rady (EU) 2017/745 ze dne 5. dubna 2017 o zdravotnických prostředcích, změně směrnice 2001/83/ES, nařízení (ES) č. 178/2002 a nařízení (ES) č. 1223/2009 a o zrušení směrnic Rady 90/385/EHS a 93/42/EHS (Úř. věst. L 117, 5.5.2017, s. 1).

[19] Nařízení Evropského parlamentu a Rady (EU) 2017/746 ze dne 5. dubna 2017 o diagnostických zdravotnických prostředcích in vitro a o zrušení směrnice 98/79/ES a rozhodnutí Komise 2010/227/EU (Úř. věst. L 117, 5.5.2017, s. 176).

(32) Pokud jde o vysoce rizikové systémy UI s výjimkou těch, které představují bezpečnostní součásti produktů nebo které jsou samy produkty, je vhodné je klasifikovat jako vysoce rizikové, pokud s ohledem na určený účel představují vysoké riziko újmy na zdraví a bezpečnosti nebo na základních právech osob s přihlédnutím jak k závažnosti možné újmy, tak k pravděpodobnosti, že nastane, a pokud jsou využívány v celé řadě oblastí uvedených v tomto nařízení, které jsou výslovně definovány předem. Identifikace těchto systémů je založena na stejné metodice a kritériích, jaké se předpokládají i u jakýchkoli budoucích změn seznamu vysoce rizikových systémů UI. Je rovněž důležité vyjasnit, že v rámci scénářů s vysokým rizikem uvedených v příloze III mohou existovat systémy, které nevedou k významnému riziku pro právní zájmy chráněné v rámci těchto scénářů, s přihlédnutím k výstupům vytvořeným systémem UI. Systém UI by proto měl být považován za vysoce rizikový pouze v případě, že vytváří výstup, který má ve vztahu k příslušnému opatření nebo rozhodnutí vysokou důležitost (tj. není čistě doplňkový), aby tvořil významné riziko pro chráněné právní zájmy. Například pokud informace poskytované systémy UI člověku spočívají v profilování fyzických osob ve smyslu čl. 4 odst. 4 nařízení (EU) 2016/679 a čl. 3 odst. 4 směrnice (EU) 2016/680 a čl. 3 odst. 5 nařízení (EU) 2018/1725, neměly by být tyto informace obvykle považovány za informace doplňkové povahy v souvislosti s vysoce rizikovými systémy UI, jak je uvedeno v příloze III. Pokud má však výstup systému UI pouze zanedbatelný nebo malý význam pro lidskou činnost nebo rozhodnutí, lze jej považovat za čistě doplňkový, včetně například systémů UI používaných pro překlad pro informativní účely nebo pro správu dokumentů.

(33) Technické nepřesnosti systémů UI určených pro biometrickou identifikaci fyzických osob na dálku mohou vést ke zkresleným výsledkům a mít diskriminační účinky. To je relevantní zejména v případě věku, etnického původu, rasy, pohlaví nebo zdravotních postižení. Proto by měly být systémy biometrické identifikace na dálku „v reálném čase“ i „zpětně“ klasifikovány jako vysoce rizikové. S ohledem na rizika, která oba typy systémů biometrické identifikace na dálku představují, by se na ně měly vztahovat zvláštní požadavky v oblasti schopnosti zaznamenávání dat a lidského dohledu.

(34) Pokud jde o správu a provoz kritické infrastruktury, je vhodné klasifikovat jako vysoce rizikové takové systémy UI, které jsou určeny k použití jako bezpečnostní součásti při řízení a provozu kritické digitální infrastruktury, jak je uvedeno v příloze I bodu 8 směrnice o odolnosti kritických subjektů, silniční dopravy a při zásobování vodou, plynem, teplem a elektřinou, protože jejich porucha nebo chybné fungování může ohrozit život a zdraví osob ve velkém rozsahu a vést ke značnému narušení běžného provozování sociálních a hospodářských činností. Bezpečnostní součásti kritické infrastruktury, včetně kritické digitální infrastruktury, jsou systémy používané k přímé ochraně fyzické integrity kritické infrastruktury nebo zdraví a bezpečnosti osob a majetku, které však nemusí být nutně v zájmu zajištění funkčnosti systému. Selhání nebo špatné fungování těchto součástí může přímo vést k ohrožení fyzické integrity kritické infrastruktury, a tím i k ohrožení zdraví a bezpečnosti osob a majetku. Součásti určené k použití výhradně pro účely kybernetické bezpečnosti by neměly být považovány za bezpečnostní součásti. Mezi příklady bezpečnostních součástí takové kritické infrastruktury mohou patřit systémy pro monitorování tlaku vody nebo systémy řízení požárního poplachu ve střediscích cloud computingu.

(35) Za vysoce rizikové by měly být považovány systémy UI používané ve vzdělávání nebo v odborné přípravě, zejména při určování přístupu osob do školských institucí nebo programů a institucí nebo programů odborného vzdělávání, jejich přijímání nebo přidělování do těchto institucí nebo programů na všech úrovních nebo pro hodnocení výsledků učení osob, protože mohou určovat vzdělávací a profesní průběh života lidí a tak ovlivňovat jejich schopnost zajišťovat si živobytí. Pokud budou tyto systémy navrženy a používány nesprávně, mohou porušovat právo na vzdělávání a odbornou přípravu i právo nebýt diskriminován a fixovat historické vzorce diskriminace.

(36) Jako vysoce rizikové mohou být klasifikovány systémy UI používané při zaměstnávání, řízení pracovníků a při přístupu k samostatné výdělečné činnosti, zejména při náboru a výběru osob, při rozhodování o povýšení nebo propuštění a při přidělování úkolů na základě individuálního chování nebo osobnostních rysů či vlastností, monitorování nebo hodnocení osob ve smluvních pracovněprávních vztazích, protože mohou významně ovlivnit budoucí kariérní vyhlídky a živobytí těchto osob. Příslušné smluvní pracovněprávní vztahy by měly zahrnovat zaměstnance a osoby poskytující služby prostřednictvím platforem, jak je uvedeno v pracovním programu Komise na rok 2021. Tyto osoby by v zásadě neměly být považovány za uživatele ve smyslu tohoto nařízení. Tyto systémy mohou v průběhu celého procesu náboru a při hodnocení, povyšování nebo udržování osob ve smluvních pracovněprávních vztazích fixovat historické vzorce diskriminace, například vůči ženám, určitým věkovým skupinám, osobám se zdravotním postižením nebo osobám určitého rasového nebo etnického původu nebo sexuální orientace. Systémy UI používané k monitorování výkonnosti a chování těchto osob mohou ovlivnit rovněž jejich práva na ochranu údajů a soukromí.

(37) Další oblastí, ve které si používání systémů UI zaslouží zvláštní pozornost, je přístup k určitým základním soukromým a veřejným službám a výhodám nezbytným pro plné zapojení osob do společnosti nebo pro zlepšení jejich životní úrovně. Jako vysoce rizikové systémy UI by měly být klasifikovány zejména systémy UI používané k hodnocení rizika úvěrů nebo úvěruschopnosti fyzických osob, protože určují přístup těchto osob k finančním zdrojům nebo k základním službám, jako je bydlení, elektřina a telekomunikační služby. Systémy UI používané k tomuto účelu mohou vést k diskriminaci osob nebo skupin a fixovat historické vzorce diskriminace, například na základě rasového nebo etnického původu, zdravotního postižení, věku a sexuální orientace, nebo vytvářet nové formy diskriminačních dopadů. Vzhledem k velmi omezenému rozsahu tohoto dopadu a dostupným alternativám na trhu je vhodné stanovit výjimku pro systémy UI užívané pro účely posouzení úvěruschopnosti a hodnocení rizika úvěrů, pokud je uvedou do provozu mikropodniky nebo malé podniky, jak je vymezeno v příloze doporučení Komise 2003/36/ES, pro svou vlastní potřebu. Fyzické osoby, které žádají o základní dávky sociálního zabezpečení a veřejné asistenční služby u veřejných orgánů, případně kterým jsou tyto dávky a služby poskytovány, jsou zpravidla na těchto dávkách a službách závislé a nacházejí se ve vztahu k odpovědným orgánům ve zranitelném postavení. Jsou-li systémy UI využívány k určování toho, zda by tyto orgány měly tyto dávky a služby zamítnout, omezit, zrušit nebo žádat jejich navrácení, včetně toho, zda mají příjemci na tyto dávky nebo služby legitimní nárok, mohou tyto systémy mít významný dopad na živobytí daných osob a mohou porušovat jejich základní práva, jako je právo na sociální ochranu, na zákaz diskriminace, na lidskou důstojnost nebo na účinnou právní ochranu. Tyto systémy by proto měly být klasifikovány jako vysoce rizikové. Toto nařízení by však nemělo bránit rozvoji a využívání inovativních přístupů ve veřejné správě, pro kterou by mohlo být širší využívání vyhovujících a bezpečných systémů UI prospěšné, pokud tyto systémy nepředstavují vysoké riziko pro právnické a fyzické osoby. A konečně by měly být jako vysoce rizikové klasifikovány rovněž systémy UI používané při dispečinku pohotovostních služeb nebo stanovení priorit při tomto dispečinku, protože rozhodují v situacích, které jsou velmi kritické pro život a zdraví osob a jejich majetek. Systémy UI se rovněž stále častěji používají k posouzení rizik ve vztahu k fyzickým osobám a stanovování cen v případě životního a zdravotního pojištění, což, pokud nejsou řádně navrženy, vyvinuty a používány, může mít závažné důsledky pro život a zdraví lidí, včetně finančního vyloučení a diskriminace. Aby byl zajištěn jednotný přístup v odvětví finančních služeb, měla by se výše uvedená výjimka pro mikropodniky nebo malé podniky pro jejich vlastní potřebu uplatnit, pokud samy poskytují a uvádějí do provozu systém UI za účelem prodeje svých vlastních pojistných produktů.

(38) Opatření donucovacích orgánů zahrnující určitá použití systémů UI se vyznačují značným stupněm nerovnováhy sil a mohou vést ke sledování fyzické osoby, jejímu zatčení nebo zbavení svobody, jakož i k dalším nepříznivým dopadům na základní práva zaručená Listinou. Zejména v případě, že systém UI nebyl trénován na vysoce kvalitních datech, nesplňuje odpovídající požadavky na přesnost nebo spolehlivost nebo není před uvedením na trh nebo jiným uvedením do provozu řádně navržen a otestován, může dojít k vyčleňování osob diskriminačním nebo jinak nesprávným nebo nespravedlivým způsobem. Kromě toho by mohl být omezen výkon důležitých základních procesních práv, jako je právo na účinnou právní ochranu a na spravedlivý proces, jakož i právo na obhajobu a presumpce neviny, zejména pokud tyto systémy UI nejsou dostatečně transparentní, vysvětlitelné a zdokumentované. Je proto vhodné označit za vysoce rizikové celou řadu systémů UI určených k použití v kontextu prosazování práva, kde je přesnost, spolehlivost a transparentnost obzvláště důležitá, s cílem zabránit nepříznivým dopadům, zachovat důvěru veřejnosti a zajistit odpovědnost a účinné opravné prostředky. S ohledem na povahu dotčených činností a na rizika s nimi spojená by tyto vysoce rizikové systémy UI měly zahrnovat zejména systémy UI určené k využívání donucovacími orgány k individuálnímu hodnocení rizik, polygrafy a podobné nástroje, případně systémy užívané k detekci emočního stavu fyzických osob, k vyhodnocování spolehlivosti důkazů v trestním řízení, k predikci výskytu nebo opakování skutečné nebo potenciální trestné činnosti na základě profilování fyzických osob nebo k posuzování osobnostních a povahových rysů nebo předchozí trestné činnosti fyzických osob nebo skupin, k profilování v průběhu odhalování, vyšetřování nebo stíhání trestných činů. Systémy UI výslovně určené k použití daňovými a celními orgány při správním řízení, jakož i finančními zpravodajskými jednotkami provádějícími administrativní úkoly při analýze informací podle právních předpisů EU proti praní peněz, by neměly být považovány za vysoce rizikové systémy UI používané donucovacími orgány za účelem prevence, odhalování, vyšetřování a stíhání trestných činů.

(39) Systémy UI využívané pro účely migrace, azylu a řízení ochrany hranic ovlivňují osoby, které jsou často v obzvláště zranitelném postavení a jsou závislé na výsledku činnosti příslušných veřejných orgánů. Přesnost, nediskriminační povaha a transparentnost systémů UI používaných v těchto kontextech jsou proto obzvláště důležité pro zajištění dodržování základních práv dotčených osob, zejména jejich práva na volný pohyb, na zákaz diskriminace, na ochranu soukromého života a osobních údajů, na mezinárodní ochranu a na řádnou správu. Je proto vhodné označit jako vysoce rizikové ty systémy UI, které jsou určeny k použití příslušnými veřejnými orgány pověřenými úkoly v oblasti migrace, azylu a řízení ochrany hranic, jako jsou například polygrafy a podobné nástroje, případně nástroje určené k detekci emočního stavu fyzické osoby; k posuzování určitých rizik, která představují fyzické osoby vstupující na území členského státu nebo žádající o vízum nebo azyl; jako pomoc příslušným veřejným orgánům při posuzování žádostí o azyl, vízum a povolení k pobytu a souvisejících stížností, pokud jde o cíl, jímž je zjištění způsobilosti fyzických osob žádajících o určitý status. Systémy UI v oblasti migrace, azylu a řízení ochrany hranic, na které se vztahuje toto nařízení, by měly splňovat příslušné procesní požadavky stanovené směrnicí Evropského parlamentu a Rady 2013/32/EU[20], nařízením Evropského parlamentu a Rady (ES) č. 810/2009[21] a dalšími příslušnými právními předpisy.

[20] Směrnice Evropského parlamentu a Rady 2013/32/EU ze dne 26. června 2013 o společných řízeních pro přiznávání a odnímání statusu mezinárodní ochrany (Úř. věst. L 180, 29.6.2013, s. 60).

[21] Nařízení Evropského parlamentu a Rady (ES) č. 810/2009 ze dne 13. července 2009 o kodexu Společenství o vízech (vízový kodex) (Úř. věst. L 243, 15.9.2009, s. 1).

(40) Určité systémy UI určené k výkonu spravedlnosti a demokratických procesů by měly být klasifikovány jako vysoce rizikové s ohledem na jejich potenciálně významný dopad na demokracii, právní stát a individuální svobody, jakož i na právo na účinnou právní ochranu a na spravedlivý proces. Jako vysoce rizikové je vhodné kvalifikovat systémy UI, jejichž cílem je poskytovat pomoc justičním orgánům při výkladu skutečností a práva a při uplatňování práva na konkrétní soubor skutečností, zejména z důvodu řešení rizik možného zkreslení, chyb a neprůhlednosti. Tato kvalifikace by se však neměla vztahovat na systémy UI určené pro čistě pomocné správní činnosti, které neovlivňují faktický výkon spravedlnosti v jednotlivých případech, jako je například anonymizace nebo pseudonymizace soudních rozhodnutí, dokumentů nebo údajů, komunikace mezi zaměstnanci, administrativní úkoly.

(41) Skutečnost, že daný systém UI je podle tohoto nařízení klasifikován jako vysoce rizikový, by neměla být vykládána v tom smyslu, že používání tohoto systému musí být zákonné podle jiných aktů práva Unie nebo podle vnitrostátních právních předpisů slučitelných s právem Unie, které se týkají například ochrany osobních údajů, používání polygrafů a podobných nástrojů nebo jiných systémů ke zjišťování emočního stavu fyzických osob. K jakémukoli takovému využívání by mělo i nadále docházet pouze v souladu s příslušnými požadavky vyplývajícími z Listiny a z příslušných aktů sekundárního práva Unie a vnitrostátního práva. Toto nařízení by nemělo být chápáno tak, že poskytuje právní základ pro zpracování osobních údajů, případně včetně zvláštních kategorií osobních údajů, není-li v konkrétních případech v tomto nařízení stanoveno jinak.

(42) Ke zmírnění rizik, která vyplývají z vysoce rizikových systémů UI uváděných na trh Unie nebo jinak uváděných do provozu na tomto trhu, by měly být uplatňovány určité povinné požadavky s přihlédnutím k určenému účelu používání tohoto systému a v souladu se systémem řízení rizik, který stanoví poskytovatel. Systém řízení rizik by měl především spočívat v nepřetržitém opakujícím se procesu plánovaném a prováděném v rámci celého životního cyklu vysoce rizikového systému UI. Tento proces by měl zajistit, aby poskytovatel určil a analyzoval rizika pro zdraví, bezpečnost a základní práva osob, které mohou být systémem dotčeny s ohledem na jeho zamýšlený účel, včetně možných rizik vyplývajících z interakce mezi systémem UI a prostředím, v němž systém působí, a aby v souladu s tím přijal vhodná opatření k řízení rizik s ohledem na nejnovější vývoj.

(43) Na vysoce rizikové systémy UI by se měly vztahovat požadavky týkající se kvality použitých souborů dat, technické dokumentace a uchovávání záznamů, transparentnosti a poskytování informací uživatelům, lidského dohledu a spolehlivosti, přesnosti a kybernetické bezpečnosti. Tyto požadavky jsou nezbytným předpokladem účinného zmírňování rizik pro zdraví, bezpečnost a základní práva v závislosti na určeném účelu tohoto systému; žádná další opatření méně omezující obchod nejsou rozumně dostupná, a tudíž nedochází k bezdůvodným omezením obchodu.

(44) Pro výkonnost celé řady systémů UI má zásadní význam vysoká kvalita dat, zejména pokud jsou používány techniky zahrnující trénování modelů s cílem zajistit, aby vysoce rizikový systém UI fungoval dle předpokladu a bezpečně a aby se nestal zdrojem diskriminace, kterou právo Unie zakazuje. Soubory vysoce kvalitních tréninkových dat, dat pro ověřování platnosti a testovacích dat vyžadují zavedení vhodných postupů správy a řízení dat. Měly by být dostatečně relevantní, reprezentativní a měly by vykazovat příslušné statistické vlastnosti, včetně údajů o osobách nebo skupinách osob, pro které má být daný vysoce rizikový systém UI používán. Tyto soubory dat by rovněž měly být v nejvyšší možné míře bez chyb a co nejúplnější s ohledem na zamýšlený účel systému UI, přičemž by měly přiměřeným způsobem zohledňovat technickou proveditelnost a nejnovější vývoj, dostupnost dat a provádění vhodných opatření k řízení rizik, aby byly řádně řešeny případné nedostatky souborů dat. Požadavek, aby soubory dat byly úplné a bez chyb, by neměl mít vliv na používání technik ochrany soukromí v souvislosti s vývojem a testováním systémů UI. Soubory tréninkových dat, dat pro ověřování platnosti a testovacích dat by měly s ohledem na svůj určený účel zohledňovat rysy, vlastnosti nebo prvky, které jsou specifické pro konkrétní zeměpisné, behaviorální nebo funkční prostředí nebo kontext, ve kterém má být systém UI používán. V zájmu ochrany práva jiných osob na zabránění diskriminaci, která by mohla vyplynout ze zkreslení v rámci systémů UI, by poskytovatelé měli mít možnost zpracovávat také zvláštní kategorie osobních údajů jako záležitost významného veřejného zájmu ve smyslu čl. 9 odst. 2 písm. g) nařízení (EU) 2016/679 a čl. 10 odst. 2 písm. g) nařízení (EU) 2018/1725 s cílem zajistit sledování, detekci a opravu tohoto zkreslení ve vztahu k vysoce rizikovým systémům UI.

(44a) Při uplatňování zásad uvedených v čl. 5 odst. 1 písm. c) nařízení 2016/679 a čl. 4 odst. 1 písm. c) nařízení 2018/1725, zejména zásady minimalizace údajů, pokud jde o soubory tréninkových dat, dat pro ověřování platnosti a testovacích dat podle tohoto nařízení, by měl být náležitě zohledněn celý životní cyklus systému UI.

(45) Při vývoji vysoce rizikových systémů UI by měli mít některé subjekty, jako jsou poskytovatelé, oznámené subjekty a další příslušné subjekty, například centra pro digitální inovace, pokusná zkušební zařízení a výzkumní pracovníci, přístup k vysoce kvalitním datovým souborům ve svých příslušných oborech činnosti, které souvisejí s tímto nařízením. Zásadní význam pro zajištění důvěryhodného, odpovědného a nediskriminačního přístupu k vysoce kvalitním datům pro účely trénování, ověřování a testování systémů UI budou mít společné evropské datové prostory vytvořené Komisí, jakož i usnadnění sdílení údajů ve veřejném zájmu mezi podniky a s vládou. Například v oblasti zdraví umožní společný evropský prostor pro data z oblasti veřejného zdraví nediskriminační přístup k údajům o zdraví a trénování algoritmů umělé inteligence na těchto souborech dat, a to způsobem, který bude chránit soukromí, bude bezpečný, včasný, transparentní a důvěryhodný a bude u něj zajištěna vhodná institucionální správa. Poskytování vysoce kvalitních dat pro účely trénování, ověřování a testování systémů UI mohou podporovat rovněž odpovídající příslušné orgány, včetně odvětvových, které poskytují nebo podporují přístup k datům.

(46) Pro ověření souladu s požadavky tohoto nařízení má zásadní význam, aby byly k dispozici informace, jak byly vysoce rizikové systémy UI vytvořeny a jak fungují po celou dobu své životnosti. To vyžaduje vedení záznamů a dostupnost technické dokumentace obsahující informace nezbytné k posouzení souladu daného systému UI s příslušnými požadavky. Tyto informace by měly zahrnovat obecné vlastnosti, schopnosti a omezení tohoto systému, použité algoritmy, data, postupy při trénování, testování a ověřování, jakož i dokumentaci příslušného systému řízení rizik. Technická dokumentace by měla být průběžně aktualizována. Kromě toho by poskytovatelé nebo uživatelé měli vést a uchovávat protokoly automaticky generované vysoce rizikovým systémem UI, včetně například výstupních údajů, data a času zahájení atd., a to v rozsahu, v jakém jsou takový systém a související protokoly pod jejich kontrolou, po dobu, která je přiměřená k tomu, aby mohli plnit své povinnosti.

(47) Aby se vyřešila neprůhlednost, kvůli níž mohou být určité systémy UI pro fyzické osoby nepochopitelné nebo příliš složité, je u vysoce rizikových systémů UI zapotřebí určitá míra transparentnosti. Uživatelé by měli být schopni interpretovat výstup systému a používat jej vhodným způsobem. K vysoce rizikovým systémům UI by proto měla být připojena příslušná dokumentace a návod k použití a měly by obsahovat stručné a jasné informace, včetně informací týkajících se potenciálního rizika pro základní práva a rizika diskriminace osob, které mohou být systémem dotčeny s ohledem na určený účel. Aby uživatelé lépe porozuměli návodům k použití, měly by případně obsahovat ilustrativní příklady.

(48) Vysoce rizikové systémy UI by měly být navrženy a vyvinuty tak, aby na jejich fungování mohly dohlížet fyzické osoby. Za tímto účelem by měl poskytovatel systému před uvedením systému na trh nebo do provozu stanovit vhodná opatření lidského dohledu. Tato opatření by případně měla zajistit zejména to, aby byla do systému zabudována provozní omezení, která samotný systém není schopen překonat a která reagují na lidskou obsluhu, a aby fyzické osoby, které byly pověřeny lidským dohledem, měly odbornou způsobilost, odbornou přípravu a pravomoc nezbytné k výkonu této funkce. Vzhledem k závažným důsledkům pro osoby v případě nesprávných shod některých systémů biometrické identifikace je vhodné stanovit požadavek na posílený lidský dohled nad těmito systémy, aby uživatel nemohl přijmout žádné opatření nebo rozhodnutí na základě identifikace vyplývající ze systému, pokud ji samostatně neověřily a nepotvrdily alespoň dvě fyzické osoby. Tyto osoby by mohly pocházet z jednoho nebo více subjektů a zahrnovat osobu, která systém provozuje nebo používá. Tento požadavek by neměl představovat zbytečnou zátěž nebo zdržení a mohlo by postačovat, aby byla samostatná ověření různými osobami automaticky zaznamenávána v protokolech generovaných systémem.

(49) Vysoce rizikové systémy UI by měly po celou dobu svého životního cyklu fungovat konzistentně a splňovat příslušnou úroveň přesnosti, spolehlivosti a kybernetické bezpečnosti v souladu s obecně uznávaným nejnovějším vývojem. Uživatelé by měli být informováni o úrovni a měřítkách přesnosti.

(50) U vysoce rizikových systémů UI je klíčovým požadavkem technická spolehlivost. Měly by být odolné vůči škodlivému nebo jinak nežádoucímu chování, které může být důsledkem omezení uvnitř systémů nebo prostředí, v němž systémy fungují (např. chyby, závady, nesrovnalosti, neočekávané situace). Vysoce rizikové systémy UI by proto měly být navrhovány a vyvíjeny s vhodnými technickými řešeními pro prevenci nebo minimalizaci tohoto škodlivého nebo jiného nežádoucího chování, jako jsou například mechanismy umožňující systému bezpečně přerušit provoz (plány zajištění proti selhání) v přítomnosti určitých anomálií nebo v případě, že provoz probíhá mimo určité předem stanovené hranice. Neschopnost ochrany před těmito riziky by mohla vést k dopadům na bezpečnost nebo negativně ovlivnit základní práva, například v důsledku chybných rozhodnutí nebo nesprávných či zkreslených výstupů systému UI.

(51) Zásadní úlohu při zajišťování odolnosti systémů UI proti pokusům o změnu jejich použití, chování nebo výkonnosti nebo o ohrožení jejich bezpečnostních vlastností třetími stranami, které se škodlivým záměrem zneužívají zranitelných míst tohoto systému, hraje kybernetická bezpečnost. Kybernetické útoky na systémy UI mohou využívat aktiva specifická pro UI, jako jsou například soubory tréninkových dat (například tzv. data poisoning) nebo trénované modely (například nepřátelské útoky), nebo zneužívat slabých míst digitálních aktiv daného systému UI nebo příslušné infrastruktury IKT. Pro zajištění úrovně kybernetické bezpečnosti odpovídající těmto rizikům by proto poskytovatelé vysoce rizikových systémů UI měli přijmout vhodná opatření, případně současně zohlednit i příslušnou infrastrukturu IKT.

(52) V rámci harmonizačních právních předpisů Unie by měla být pravidla použitelná pro uvádění na trh, uvádění do provozu a používání vysoce rizikových systémů UI stanovena v souladu s nařízením Evropského parlamentu a Rady (ES) č. 765/2008[22], kterým se stanoví požadavky na akreditaci a dozor nad trhem s výrobky, s rozhodnutím Evropského parlamentu a Rady č. 768/2008/ES[23] o společném rámci pro uvádění výrobků na trh a s nařízením Evropského parlamentu a Rady (EU) 2019/1020[24] o dozoru nad trhem a souladu výrobků s předpisy („nový legislativní rámec pro uvádění výrobků na trh“).

(52a) V souladu se zásadami nového legislativního rámce by měly být stanoveny konkrétní povinnosti příslušných subjektů v rámci hodnotového řetězce UI s cílem zajistit právní jistotu a usnadnit soulad s tímto nařízením. V určitých situacích by tito provozovatelé mohli jednat ve více než jedné roli současně, a měli by proto kumulativně plnit všechny příslušné povinnosti spojené s těmito úlohami. Provozovatel by například mohl jednat současně jako distributor a dovozce.

(53) Je vhodné, aby za uvedení vysoce rizikového systému UI na trh nebo do provozu převzala odpovědnost konkrétní fyzická nebo právnická osoba definovaná jako poskytovatel bez ohledu na to, zda je tato fyzická nebo právnická osoba totožná s osobou, která tento systém navrhla nebo vyvinula.

---

22 Nařízení Evropského parlamentu a Rady (ES) č. 765/2008 ze dne 9. července 2008, kterým se stanoví požadavky na akreditaci a dozor nad trhem týkající se uvádění výrobků na trh a kterým se zrušuje nařízení (EHS) č. 339/93 (Úř. věst. L 218, 13.8.2008, s. 30).

23 Rozhodnutí Evropského parlamentu a Rady č. 768/2008/ES ze dne 9. července 2008 o společném rámci pro uvádění výrobků na trh a o zrušení rozhodnutí Rady 93/465/EHS (Úř. věst. L 218, 13.8.2008, s. 82).

24 Nařízení Evropského parlamentu a Rady (EU) 2019/1020 ze dne 20. června 2019 o dozoru nad trhem a souladu výrobků s předpisy a o změně směrnice 2004/42/ES a nařízení (ES) č. 765/2008 a (EU) č. 305/2011 (Text s významem pro EHP) (Úř. věst. L 169, 25.6.2019, s. 1).

(54) Poskytovatel by měl zavést spolehlivý systém řízení jakosti, zajistit provedení požadovaného postupu posuzování shody, vypracovat příslušnou dokumentaci a zavést spolehlivý systém monitorování po uvedení na trh. Veřejné orgány, které uvádějí do provozu vysoce rizikové systémy UI pro vlastní potřebu, mohou přijímat a provádět pravidla pro systém řízení jakosti jako součást systému řízení jakosti přijatého na vnitrostátní nebo regionální úrovni, případně s přihlédnutím ke zvláštnostem daného odvětví a k pravomocím a organizaci příslušného veřejného orgánu.

(54a) V zájmu zajištění právní jistoty je nezbytné vyjasnit, že za určitých zvláštních podmínek by každá fyzická nebo právnická osoba měla být považována za poskytovatele nového vysoce rizikového systému UI, a proto by měla převzít všechny příslušné povinnosti. Tak by tomu bylo například v případě, že tato osoba uvede své jméno nebo ochrannou známku na vysoce rizikový systém UI, který již byl uveden na trh nebo do provozu, nebo pokud tato osoba změní určený účel systému UI, který není vysoce rizikový a je již uveden na trh nebo do provozu způsobem, který činí z upraveného systému vysoce rizikový systém UI. Tato ustanovení by se měla použít, aniž by byla dotčena konkrétnější ustanovení zavedená v některých odvětvových právních předpisech nového legislativního rámce, s nimiž by se toto nařízení mělo uplatňovat společně. Například čl. 16 odst. 2 nařízení č. 745/2017, kterým se stanoví, že některé změny by neměly být považovány za úpravy prostředku, které by mohly ovlivnit jeho soulad s platnými požadavky, by se měl i nadále vztahovat na vysoce rizikové systémy UI, které jsou zdravotnickými prostředky ve smyslu uvedeného nařízení.

(55) Pokud není vysoce rizikový systém UI, který je bezpečnostní součástí produktu, na nějž se vztahují příslušné odvětvové právní předpisy nového legislativního rámce, uveden na trh nebo do provozu nezávisle na tomto produktu, měl by výrobce produktu definovaného v příslušných právních předpisech nového legislativního rámce splňovat povinnosti poskytovatele stanovené v tomto nařízení a zejména zajistit, aby systém UI zabudovaný do konečného produktu splňoval požadavky tohoto nařízení.

(56) Aby bylo umožněno prosazování tohoto nařízení a byly vytvořeny rovné podmínky pro provozovatele, a rovněž s přihlédnutím k různým formám zpřístupňování digitálních produktů, je důležité zajistit, aby osoby usazené v Unii mohly za všech okolností poskytnout orgánům veškeré nezbytné informace o souladu systému UI. Poskytovatelé usazení mimo Unii proto v případě, že dodávají do Unie systémy UI, u nichž nelze identifikovat dovozce, předem jmenují formou písemného pověření svého zplnomocněného zástupce usazeného v Unii.

(56a) V případě poskytovatelů, kteří nejsou usazeni v Unii, hraje klíčovou roli při zajišťování shody vysoce rizikových systémů UI uváděných na trh nebo do provozu v Unii uvedenými poskytovateli zplnomocněný zástupce, který vystupuje jako jejich kontaktní osoba usazená v Unii. Vzhledem k této klíčové úloze a s cílem zajistit převzetí odpovědnosti pro účely prosazování tohoto nařízení je vhodné, aby zplnomocněný zástupce odpovídal za vadné vysoce rizikové systémy UI společně a nerozdílně s poskytovatelem. Odpovědností zplnomocněného zástupce stanovenou v tomto nařízení nejsou dotčena ustanovení směrnice 85/374/EHS o odpovědnosti za vadné výrobky.

(57) [vypouští se]

(58) Vzhledem k povaze systémů UI a rizikům z hlediska bezpečnosti a základních práv, která mohou souviset s jejich používáním, a to i pokud jde o potřebu zajistit řádné monitorování výkonnosti daného systému UI v reálných podmínkách, je vhodné stanovit konkrétní odpovědnost uživatelů. Uživatelé by zejména měli vysoce rizikové systémy UI využívat v souladu s návodem k použití a měly by být stanoveny některé další povinnosti týkající se monitorování fungování systémů UI a případně uchovávání záznamů. Těmito povinnostmi by neměly být dotčeny jiné povinnosti uživatelů ve vztahu k vysoce rizikovým systémům UI podle práva Unie nebo vnitrostátního práva a neměly by se vztahovat na případy, kdy k použití dochází při osobní neprofesionální činnosti.

(58a) Je vhodné vyjasnit, že tímto nařízením nejsou dotčeny povinnosti poskytovatelů a uživatelů systémů UI v jejich úloze správců nebo zpracovatelů údajů vyplývající z právních předpisů Unie o ochraně osobních údajů, pokud návrh, vývoj nebo používání systémů UI zahrnuje zpracování osobních údajů. Je rovněž vhodné vyjasnit, že subjekty údajů nadále požívají všech práv a záruk, které jim takové právní předpisy Unie přiznávají, včetně práv souvisejících s výhradně automatizovaným individuálním rozhodováním, včetně profilování. Harmonizovaná pravidla pro uvádění na trh, uvádění do provozu a používání systémů UI zřízených podle tohoto nařízení by měla usnadnit účinné provádění a umožnit výkon práv subjektů údajů a dalších opravných prostředků zaručených právními předpisy Unie v oblasti ochrany osobních údajů a dalších základních práv.

(59) [vypouští se]

(60) [vypouští se]

(61) Klíčovou úlohu při poskytování technických řešení zajišťujících dodržování tohoto nařízení poskytovatelům by měla hrát normalizace, v souladu s aktuálním stavem vývoje. Jeden z prostředků, které poskytovatelům umožní prokázat soulad s požadavky tohoto nařízení, by mělo představovat dodržování harmonizovaných norem, jež by měly obvykle odrážet aktuální stav vývoje, definovaných v nařízení Evropského parlamentu a Rady (EU) č. 1025/2012[25]. Pokud však nejsou k dispozici příslušné odkazy na harmonizované normy, měla by mít Komise možnost stanovit prostřednictvím prováděcích aktů společné specifikace pro určité požadavky podle tohoto nařízení jako výjimečné záložní řešení, které by usnadnilo povinnost poskytovatele dodržovat požadavky tohoto nařízení, je-li proces normalizace zablokován nebo dochází-li ke zpožděním při vytváření vhodné harmonizované normy. Je-li toto zpoždění způsobeno technickou složitostí dané normy, měla by to Komise zvážit před tím, než bude uvažovat o stanovení společných specifikací. Náležité zapojení malých a středních podniků do vypracovávání norem podporujících provádění tohoto nařízení má zásadní význam pro podporu inovací a konkurenceschopnosti v oblasti umělé inteligence v Unii. Toto zapojení by mělo být odpovídajícím způsobem zajištěno v souladu s články 5 a 6 nařízení č. 1025/2012.

[25] Nařízení Evropského parlamentu a Rady (EU) č. 1025/2012 ze dne 25. října 2012 o evropské normalizaci, změně směrnic Rady 89/686/EHS a 93/15/EHS a směrnic Evropského 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 kterým se ruší rozhodnutí Rady 87/95/EHS a rozhodnutí Evropského parlamentu a Rady č. 1673/2006/ES (Úř. věst. L 316, 14.11.2012, s. 12).

(61a) Aniž je dotčeno používání harmonizovaných norem a společných specifikací, je vhodné, aby u poskytovatelů platil předpoklad shody s příslušným požadavkem na údaje, pokud byl jejich vysoce rizikový systém UI trénován a testován na údajích odrážejících konkrétní zeměpisné, behaviorální nebo funkční prostředí, v němž má být systém UI používán. Podobně by se v souladu s čl. 54 odst. 3 nařízení Evropského parlamentu a Rady (EU) 2019/881 mělo předpokládat, že vysoce rizikové systémy UI, které byly certifikovány nebo pro něž bylo vydáno prohlášení o shodě v rámci systému kybernetické bezpečnosti podle uvedeného nařízení a na něž byly zveřejněny odkazy v Úředním věstníku Evropské unie, jsou v souladu s požadavkem na kybernetickou bezpečnost stanoveným v tomto nařízení. Tím není dotčena dobrovolná povaha tohoto systému kybernetické bezpečnosti.

(62) Aby byla zajištěna vysoká úroveň důvěryhodnosti vysoce rizikových systémů UI, mělo by být u těchto systémů před jejich uvedením na trh nebo do provozu provedeno posouzení shody.

(63) V případě vysoce rizikových systémů UI vztahujících se k produktům upraveným stávajícími harmonizačními právními předpisy Unie v souladu s přístupem nového legislativního rámce je v zájmu minimalizace zátěže provozovatelů a předcházení případnému zdvojování vhodné, aby byl soulad těchto systémů UI s požadavky tohoto nařízení posuzován v rámci posuzování shody, které uvedené právní předpisy již upravují. Použitelnost požadavků tohoto nařízení by tedy neměla mít vliv na konkrétní logiku, metodiku nebo obecnou strukturu posuzování shody podle příslušných zvláštních právních předpisů nového legislativního rámce. Tento přístup se plně odráží ve vzájemném vztahu mezi tímto nařízením a [nařízením o strojních zařízeních]. Bezpečnostní rizika systémů UI zajišťujících bezpečnostní funkce u strojních zařízení jsou sice řešena v rámci požadavků tohoto nařízení, avšak [nařízení o strojních zařízeních] obsahuje některé konkrétní požadavky zajišťující bezpečné začlenění daného systému UI do strojního zařízení obecně, aby nedocházelo k ohrožení bezpečnosti daného strojního zařízení jako celku. [Nařízení o strojních zařízeních] používá stejnou definici systému UI jako toto nařízení. Pokud jde o vysoce rizikové systémy UI související s produkty, na něž se vztahují nařízení 2017/745 a 2017/746 o zdravotnických prostředcích, použitelnost požadavků tohoto nařízení by se neměla dotýkat logiky řízení rizik a posouzení přínosů a rizik prováděných podle rámce pro zdravotnické prostředky a měla by je zohledňovat.

(64) Vzhledem k rozsáhlejším zkušenostem profesionálních ověřovatelů před uvedením na trh v oblasti bezpečnosti produktů a k odlišné povaze souvisejících rizik je vhodné alespoň v počáteční fázi uplatňování tohoto nařízení omezit oblast působnosti posuzování shody vysoce rizikových systémů UI třetími stranami v případech, které se netýkají produktů. Posuzování shody těchto systémů by proto měl provádět zpravidla poskytovatel na vlastní odpovědnost s jedinou výjimkou, kterou tvoří systémy UI určené pro biometrickou identifikaci osob na dálku, u nichž by mělo být předpokládáno zapojení oznámeného subjektu do posuzování shody, pokud nejsou tyto systémy zakázány.

(65) Příslušné vnitrostátní orgány by v souladu s tímto nařízením měly určit oznámené subjekty pro účely posouzení shody systémů UI oznámených pro biometrickou identifikaci osob na dálku třetími stranami pod podmínkou, že splňují určitý soubor požadavků, zejména požadavku na nezávislost, způsobilost a neexistenci střetu zájmů. Oznámení těchto subjektů by měly příslušné vnitrostátní orgány zasílat Komisi a ostatním členským státům prostřednictvím elektronického nástroje pro oznamování vyvinutého a spravovaného Komisí podle článku R23 rozhodnutí 768/2008.

(66) V souladu s obecně zavedeným pojmem „podstatná změna“ u produktů regulovaných harmonizačními právními předpisy Unie je vhodné pokaždé, když dojde ke změně, která může ovlivnit soulad vysoce rizikového systému UI s tímto nařízením (např. změna operačního systému nebo softwarové architektury), nebo pokud se změní určený účel tohoto systému, aby byl tento systém UI považován za nový systém UI, který by měl být podroben novému posouzení shody. Změny, k nimž dochází v algoritmu a výkonnosti systémů UI, které se i po uvedení na trh nebo do provozu dále „učí“ (tj. automaticky přizpůsobují způsob výkonu funkcí), by však neměly představovat podstatnou změnu, pokud byly tyto změny předem stanoveny poskytovatelem a posouzeny v okamžiku posuzování shody.

(67) Vysoce rizikové systémy UI by měly být opatřeny označením CE prokazujícím jejich shodu s tímto nařízením, aby jim byl umožněn volný pohyb v rámci vnitřního trhu. Členské státy by neměly vytvářet neodůvodněné překážky uvádění na trh nebo do provozu u vysoce rizikových systémů UI, které jsou v souladu s požadavky stanovenými v tomto nařízení a jsou opatřeny označením CE.

(68) Rychlá dostupnost inovativních technologií může mít za určitých podmínek zásadní význam pro zdraví a bezpečnost osob i pro společnost jako celek. Je proto vhodné, aby členské státy mohly z výjimečných důvodů veřejné bezpečnosti nebo ochrany života a zdraví fyzických osob a ochrany průmyslového a obchodního vlastnictví povolit uvedení na trh nebo do provozu v případě systémů UI, u nichž nebylo provedeno posouzení shody.

(69) Z důvodu usnadnění práce Komise a členských států v oblasti umělé inteligence a zvýšení transparentnosti vůči veřejnosti by poskytovatelé vysoce rizikových systémů UI s výjimkou těch, které se vztahují k produktům spadajícím do oblasti působnosti příslušných stávajících harmonizačních právních předpisů Unie, měli mít povinnost se zaregistrovat, jakož i zaregistrovat informace o svém vysoce rizikovém systému UI do databáze EU, kterou zřídí a bude spravovat Komise. Před použitím vysoce rizikového systému UI uvedeného v příloze III se uživatelé vysoce rizikových systémů UI, které jsou veřejnými orgány, agenturami nebo subjekty, s výjimkou donucovacích orgánů, orgánů hraniční kontroly, imigračních nebo azylových orgánů, a orgány, které jsou uživateli vysoce rizikových systémů UI v oblasti kritické infrastruktury, rovněž zaregistrují do této databáze a zvolí si systém, který hodlají používat. Komise by měla být správcem této databáze v souladu s nařízením Evropského parlamentu a Rady (EU) 2018/1725[26]. Aby byla zajištěna plná funkčnost této databáze při jejím zavedení, měl by postup při vytváření databáze zahrnovat vypracování funkčních specifikací ze strany Komise a nezávislou zprávu o auditu.

[26] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1).

(70) Určité systémy UI určené k interakci s fyzickými osobami nebo ke generování obsahu mohou představovat specifická rizika vydávání se za jinou osobu nebo podvodu bez ohledu na to, zda je lze či nelze označit za vysoce rizikové. Na používání těchto systémů by se proto měly za určitých okolností vztahovat zvláštní povinnosti transparentnosti, aniž by tím byly dotčeny požadavky a povinnosti kladené na vysoce rizikové systémy UI. Zejména fyzické osoby by měly být upozorněny, že komunikují se systémem UI, není-li to zřejmé z pohledu fyzické osoby, která je přiměřeně informovaná, pozorná a obezřetná, při zohlednění okolností a kontextu použití. Při provádění této povinnosti by měly být zohledněny vlastnosti jednotlivců náležejících ke zranitelným skupinám vzhledem k jejich věku nebo zdravotnímu postižení, a to v rozsahu, v jakém je systém UI určen i pro komunikaci s těmito skupinami. Fyzické osoby by navíc měly být informovány v případě, že jsou vystaveny systémům, které zpracováním svých biometrických údajů mohou identifikovat nebo odvodit emoce nebo záměry těchto osob nebo je zařadit do konkrétních kategorií. Tyto zvláštní kategorie se mohou týkat takových aspektů, jako je pohlaví, věk, barva vlasů, barva očí, tetování, osobnostní rysy, etnický původ, osobní preference a zájmy, nebo jiné aspekty, jako je sexuální nebo politická orientace. Tyto informace a oznámení by měly být poskytovány ve formátech přístupných pro osoby se zdravotním postižením. Uživatelé, kteří používají systém UI k vytváření obrazového, zvukového nebo video obsahu, který se znatelně podobá existujícím osobám, místům nebo událostem a určité osobě by se mohl nepravdivě jevit jako autentický, případně s tímto obsahem manipulují, by měli zveřejnit, že tento obsah byl uměle vytvořen nebo s ním bylo manipulováno, tím, že daný výstup umělé inteligence odpovídajícím způsobem označí a odhalí jeho umělý původ. Dodržování výše uvedených informačních povinností by nemělo být vykládáno tak, že naznačuje, že používání systému nebo jeho výstupu je zákonné podle tohoto nařízení nebo jiného práva Unie a členských států, a neměly by jím být dotčeny jiné povinnosti týkající se transparentnosti pro uživatele systémů UI stanovené v unijním nebo vnitrostátním právu. Dále by nemělo být vykládáno tak, že naznačuje, že používání systému nebo jeho výstupu znemožňuje uplatňování práva na svobodu projevu a práva na svobodu umění a věd zaručených Listinou základních práv EU, zejména pokud je obsah součástí zjevně tvůrčího, satirického, uměleckého nebo fiktivního díla nebo programu, s výhradou vhodných záruk práv a svobod třetích stran.

(71) Umělá inteligence je rychle se vyvíjející skupina technologií, která vyžaduje nové formy regulačního dohledu a bezpečný prostor pro experimentování při současném zajištění odpovědné inovace a integrace vhodných záruk a opatření ke zmírnění rizika. K zajištění právního rámce příznivého pro vznik inovací, použitelného i v budoucnosti a odolného vůči narušení je třeba podporovat příslušné vnitrostátní orgány jednoho nebo více členských států ve vytváření regulačních pískovišť umělé inteligence s cílem usnadnit vývoj a testování inovativních systémů UI pod přísným regulačním dohledem dříve, než budou tyto systémy uvedeny na trh nebo jinak uvedeny do provozu.

(72) Cílem těchto regulačních pískovišť UI by měla být podpora inovací UI na základě vytvoření kontrolovaného experimentálního a testovacího prostředí ve fázi vývoje a před uvedením na trh s cílem zajistit soulad inovativních systémů UI s tímto nařízením a s dalšími příslušnými právními předpisy Unie a členských států; dále posílení právní jistoty inovátorů, dohledu příslušných orgánů a jejich porozumění příležitostem, vznikajícím rizikům a dopadům používání UI, jakož i urychlení přístupu na trhy, mimo jiné odstraněním překážek pro malé a střední podniky včetně začínajících podniků. Účast v regulačním pískovišti UI by se měla zaměřit na otázky, které zvyšují právní nejistotu pro poskytovatele a potenciální poskytovatele, pokud jde o inovace, experimentování s UI v Unii a přispívání k fakticky podloženému regulačnímu učení. Dohled nad systémy UI v regulačním pískovišti UI by proto měl zahrnovat jejich vývoj, odbornou přípravu, testování a validaci před uvedením systémů na trh nebo do provozu, jakož i pojem a výskyt podstatných změn, které mohou vyžadovat nový postup posuzování shody. Příslušné vnitrostátní orgány, které zřizují regulační pískoviště UI, by případně měly spolupracovat s dalšími příslušnými orgány, včetně těch, které dohlížejí na ochranu základních práv, a mohly by umožnit zapojení dalších subjektů v rámci ekosystému UI, jako jsou vnitrostátní nebo evropské normalizační organizace, oznámené subjekty, zkušební a experimentální zařízení, výzkumné a experimentální laboratoře, inovační centra a příslušné zúčastněné strany a organizace občanské společnosti. Aby bylo zajištěno jednotné provádění v celé Unii a úspory z rozsahu, je vhodné stanovit společná pravidla pro zavádění regulačních pískovišť a rámec spolupráce mezi příslušnými orgány, které se podílejí na dohledu nad těmito pískovišti. Regulačními pískovišti UI zřízenými podle tohoto nařízení by neměly být dotčeny jiné právní předpisy umožňující zřízení jiných pískovišť, jejichž cílem je zajistit soulad s jinými právními předpisy, než je toto nařízení. Příslušné orgány odpovědné za tato jiná regulační pískoviště by případně měly zvážit přínosy používání těchto pískovišť rovněž pro účely zajištění souladu systémů UI s tímto nařízením. Na základě dohody mezi příslušnými vnitrostátními orgány a účastníky regulačního pískoviště UI může být testování v reálných podmínkách rovněž prováděno a kontrolováno v rámci regulačního pískoviště UI.

(–72a) Toto nařízení by mělo poskytnout právní základ pro účastníky regulačního pískoviště UI pro použití osobních údajů shromážděných pro jiné účely k vývoji určitých systémů UI ve veřejném zájmu v rámci regulačního pískoviště UI v souladu s čl. 6 odst. 4 a čl. 9 odst. 2 písm. g) nařízení (EU) 2016/679 a s článkem 5 a 10 nařízení (EU) 2018/1725, aniž je dotčen čl. 4 odst. 2 a článek 10 směrnice (EU) 2016/680. Nadále platí všechny ostatní povinnosti správců údajů a práva subjektů údajů podle nařízení (EU) 2016/679, nařízení (EU) 2018/1725 a směrnice (EU) 2016/680. Toto nařízení by zejména nemělo poskytovat právní základ ve smyslu čl. 22 odst. 2 písm. b) nařízení (EU) 2016/679 a čl. 24 odst. 2 písm. b) nařízení (EU) 2018/1725. Účastníci pískoviště by měli zajistit vhodné záruky a spolupracovat s příslušnými orgány, mimo jiné tím, že budou postupovat podle jejich pokynů a budou jednat rychle a v dobré víře s cílem zmírnit veškerá vysoká rizika pro bezpečnost a základní práva, která případně vzniknou v průběhu vývoje a experimentování v rámci pískoviště. Chování účastníků pískoviště by mělo být zohledněno při rozhodování příslušných orgánů o tom, zda uloží správní pokutu podle čl. 83 odst. 2 nařízení 2016/679 a podle článku 57 směrnice 2016/680.

(72a) V zájmu urychlení procesu vývoje vysoce rizikových systémů UI uvedených v příloze III a jejich uvádění na trh je důležité, aby poskytovatelé nebo potenciální poskytovatelé těchto systémů mohli rovněž využívat zvláštního režimu pro testování těchto systémů v reálných podmínkách, aniž by se účastnili regulačního pískoviště UI. V takových případech a s ohledem na možné důsledky takového testování pro jednotlivce by však mělo být zajištěno, aby nařízení zavedlo vhodné a dostatečné záruky a podmínky pro poskytovatele nebo potenciální poskytovatele. Tyto záruky by měly mimo jiné zahrnovat požadavek na informovaný souhlas fyzických osob s účastí na testování v reálných podmínkách, s výjimkou prosazování práva v případech, kdy by získání informovaného souhlasu bránilo testování systému UI. Souhlas subjektů údajů s účastí na takovém testování podle tohoto nařízení je odlišný od souhlasu subjektů údajů se zpracováním jejich osobních údajů podle příslušných právních předpisů o ochraně údajů a není jím dotčen.

(73) V zájmu podpory a ochrany inovací je důležité, aby byly obzvláště zohledněny zájmy poskytovatelů z řad malých a středních podniků a uživatelů systémů UI. Za tímto účelem by členské státy měly vyvíjet iniciativy zaměřené na tyto provozovatele, a to včetně zvyšování povědomí a informační komunikace. Oznámené subjekty by navíc měly zohledňovat zvláštní zájmy a potřeby poskytovatelů z řad malých a středních podniků při stanovování poplatků za posuzování shody. Značné náklady pro poskytovatele a další provozovatele, zejména jedná-li se o poskytovatele a provozovatele menšího rozsahu, mohou představovat náklady na překlady související s povinnou dokumentací a s komunikací s úřady. Členské státy by případně měly zajistit, aby jedním z jazyků, který určí a přijmou pro účely dokumentace příslušných poskytovatelů a komunikace s provozovateli, byl jazyk, kterému obecně rozumí co nejvyšší počet přeshraničních uživatelů.

(73a) Za účelem podpory a ochrany inovací by k dosažení cílů tohoto nařízení měly přispívat platforma UI na vyžádání, všechny příslušné programy a projekty financování EU, jako je program Digitální Evropa a program Horizont Evropa, prováděné Komisí a členskými státy na vnitrostátní úrovni nebo na úrovni EU.

(74) K provádění tohoto nařízení, především s cílem minimalizovat rizika v oblasti provádění vyplývající z nedostatku věcných a odborných znalostí na trhu, jakož i usnadnit dodržování povinností poskytovatelů, zejména malých a středních podniků, a oznámených subjektů podle tohoto nařízení, by mohly potenciálně přispět platformy pro UI na vyžádání, evropská centra pro digitální inovace a zkušební a experimentální zařízení zřízená Komisí a členskými státy na vnitrostátní úrovni nebo na úrovni EU. Tyto organizace mohou poskytovatelům a oznámeným subjektům poskytovat zejména technickou a vědeckou podporu v rámci svých úkolů a oblastí působnosti.

(74a) Kromě toho je v zájmu zajištění proporcionality s ohledem na velmi malou velikost některých provozovatelů, pokud jde o náklady na inovace, vhodné osvobodit mikropodniky od nejnákladnějších povinností, jako je například zavedení systému řízení kvality, což by snížilo administrativní zátěž a náklady pro tyto podniky, aniž by to ovlivnilo úroveň ochrany a potřebu souladu s požadavky na vysoce rizikové systémy UI.

(75) Je vhodné, aby Komise v maximální možné míře usnadnila přístup ke zkušebním a experimentálním zařízením orgánům, skupinám nebo laboratořím, které jsou zřízeny nebo akreditovány podle příslušných harmonizačních právních předpisů Unie a které plní úkoly v souvislosti s posuzováním shody produktů nebo zařízení, na něž se uvedené harmonizační právní předpisy Unie vztahují. To platí zejména pro odborné skupiny, odborné laboratoře a referenční laboratoře v oblasti zdravotnických prostředků podle nařízení (EU) 2017/745 a nařízení (EU) 2017/746.

(76) V zájmu usnadnění hladkého, účinného a harmonizovaného provádění tohoto nařízení by měla být zřízena Evropská rada pro umělou inteligenci. Tato rada by měla odrážet různé zájmy ekosystému UI a měla by se skládat ze zástupců členských států. V zájmu zajištění zapojení příslušných zúčastněných stran by měla být vytvořena stálá podskupina rady. Tato rada by měla odpovídat za řadu poradenských úkolů, včetně vydávání stanovisek, doporučení, rad nebo příspěvků k pokynům v záležitostech souvisejících s prováděním tohoto nařízení, včetně otázek prosazování, technických specifikací nebo stávajících norem týkajících se požadavků stanovených v tomto nařízení a poskytování poradenství Komisi a členským státům a jejich vnitrostátních orgánům v konkrétních otázkách týkajících se umělé inteligence. S cílem poskytnout členským státům určitou flexibilitu při jmenování jejich zástupců do Evropské rady pro umělou inteligenci mohou být těmito zástupci jakékoli osoby patřící k veřejným subjektům, které by měly mít příslušné kompetence a pravomoci, aby usnadnily koordinaci na vnitrostátní úrovni a přispívaly k plnění úkolů rady. Rada by měla zřídit dvě stálé podskupiny, které by poskytovaly platformu pro spolupráci a výměnu mezi orgány dozoru nad trhem a oznamujícími orgány v otázkách týkajících se dozoru nad trhem a oznámených subjektů. Stálá podskupina pro dozor nad trhem by měla působit jako skupina pro správní spolupráci (ADCO) pro toto nařízení ve smyslu článku 30 nařízení (EU) 2019/1020. V souladu s úlohou a úkoly Komise podle článku 33 nařízení (EU) 2019/1020 by Komise měla podporovat činnosti stálé podskupiny pro dozor nad trhem prováděním hodnocení trhu nebo studií, zejména s cílem určit aspekty tohoto nařízení, které vyžadují zvláštní a naléhavou koordinaci mezi orgány dozoru nad trhem. Rada může podle potřeby zřizovat další stálé nebo dočasné podskupiny pro účely zkoumání konkrétních otázek. Rada by měla rovněž případně spolupracovat s příslušnými subjekty EU, skupinami odborníků a sítěmi působícími v souvislosti s příslušnými právními předpisy EU, zejména včetně těch, které působí podle příslušného nařízení EU o datech, digitálních produktech a službách.

(76a) Komise by měla aktivně podporovat členské státy a provozovatele při provádění a prosazování tohoto nařízení. V tomto ohledu by měla vypracovat pokyny ke konkrétním tématům s cílem usnadnit uplatňování tohoto nařízení, přičemž by měla věnovat zvláštní pozornost potřebám malých a středních podniků a začínajících podniků v odvětvích, která budou s největší pravděpodobností postižena. Na podporu náležitého prosazování práva a kapacit členských států by měla být zřízena a členským státům zpřístupněna zkušební zařízení Unie pro UI a skupina příslušných odborníků.

(77) Při uplatňování a prosazování tohoto nařízení hrají klíčovou roli členské státy. V tomto ohledu by měl každý členský stát určit jeden nebo více příslušných vnitrostátních orgánů pro účely dohledu nad uplatňováním a prováděním tohoto nařízení. Členské státy mohou rozhodnout, že určí jakýkoli druh veřejného subjektu, který bude plnit úkoly příslušných vnitrostátních orgánů ve smyslu tohoto nařízení, v souladu s jejich specifickými vnitrostátními organizačními charakteristikami a potřebami.

(78) Všichni poskytovatelé vysoce rizikových systémů UI by měli mít zaveden systém monitorování po uvedení na trh s cílem zajistit, že budou schopni zohlednit zkušenosti s používáním vysoce rizikových systémů UI při zlepšování svých systémů a procesu návrhu a vývoje, případně že budou schopni včas přijmout veškerá případná nápravná opatření. Tento systém je rovněž klíčovým předpokladem zajištění účinnějšího a včasnějšího řešení potenciálních rizik vyplývajících ze systémů UI, které se po uvedení na trh nebo do provozu dále „učí“. Poskytovatelé by měli mít v této souvislosti rovněž povinnost zavést systém hlášení veškerých závažných incidentů, k nimž dojde v důsledku používání jejich systémů UI, příslušným orgánům.

(79) V zájmu zajištění náležitého a účinného vymáhání požadavků a povinností stanovených tímto nařízením, které představuje harmonizační právní předpis Unie, by se měl v plném rozsahu uplatňovat systém dozoru nad trhem a souladu výrobků s předpisy stanovený nařízením (EU) 2019/1020. Orgány dozoru nad trhem určené podle tohoto nařízení by měly mít veškeré donucovací pravomoci podle tohoto nařízení a nařízení (EU) 2019/1020 a měly by vykonávat své pravomoci a plnit své povinnosti nezávisle, nestranně a nezaujatě. Ačkoli většina systémů UI nepodléhá zvláštním požadavkům a povinnostem podle tohoto nařízení, mohou orgány dozoru nad trhem přijmout opatření ve vztahu ke všem systémům UI, pokud představují riziko v souladu s tímto nařízením. Vzhledem ke zvláštní povaze orgánů, institucí a jiných subjektů Unie spadajících do oblasti působnosti tohoto nařízení je vhodné pro ně jmenovat jako příslušný orgán dozoru nad trhem evropského inspektora ochrany údajů. Tím by nemělo být dotčeno určení příslušných vnitrostátních orgánů členskými státy. Činnostmi v oblasti dozoru nad trhem by neměla být dotčena schopnost subjektů, nad nimiž je vykonáván dohled, plnit své úkoly nezávisle, pokud tuto nezávislost vyžaduje právo Unie.

(79a) Tímto nařízením nejsou dotčeny kompetence, úkoly, pravomoci a nezávislost příslušných vnitrostátních veřejných orgánů nebo subjektů veřejného sektoru, které dohlížejí na uplatňování práva Unie na ochranu základních práv, včetně orgánů pro rovné zacházení a orgánů pro ochranu údajů. Pokud je to nutné pro výkon jejich pověření, tyto vnitrostátní veřejné orgány nebo subjekty veřejného sektoru by rovněž měly mít přístup k veškeré dokumentaci vytvořené podle tohoto nařízení. Měl by být stanoven zvláštní ochranný postup pro zajištění přiměřeného a včasného prosazování předpisů proti systémům UI, které představují riziko pro zdraví, bezpečnost a základní práva. Postup pro tyto systémy UI představující riziko by se měl vztahovat na vysoce rizikové systémy UI představující riziko, zakázané systémy, které byly uvedeny na trh nebo do provozu nebo používány v rozporu se zakázanými praktikami stanovenými v tomto nařízení, a na systémy UI, které byly dodány na trh v rozporu s požadavky na transparentnost stanovenými v tomto nařízení a představují riziko.

(80) Právní předpisy Unie týkající se finančních služeb zahrnují pravidla a požadavky vnitřní správy a řízení rizik, které se vztahují na regulované finanční instituce v průběhu poskytování těchto služeb, včetně případů, kdy využívají systémy UI. V zájmu zajištění jednotného uplatňování a vymáhání povinností vyplývajících z tohoto nařízení a příslušných pravidel a požadavků právních předpisů Unie o finančních službách by měly být jako příslušné orgány pro účely dohledu nad prováděním tohoto nařízení, včetně činností dozoru nad trhem ve vztahu k systémům UI poskytovaným nebo používaným finančními institucemi, které jsou předmětem regulace nebo dozoru, určeny orgány odpovědné za dohled nad právními předpisy o finančních službách a jejich vymáhání, ledaže se členské státy rozhodnou určit jiný orgán ke splnění těchto úkolů dozoru nad trhem. Tyto příslušné orgány by měly mít veškeré pravomoci podle tohoto nařízení a nařízení (EU) 2019/1020 o dozoru nad trhem, aby mohly prosazovat požadavky a povinnosti podle tohoto nařízení, včetně pravomocí provádět následné činnosti dozoru nad trhem, které mohou být případně začleněny do jejich stávajících mechanismů a postupů dohledu podle příslušných právních předpisů Unie v oblasti finančních služeb. Je vhodné stanovit, že při jednání jakožto orgány dozoru nad trhem podle tohoto nařízení by vnitrostátní orgány odpovědné za dohled nad úvěrovými institucemi, na něž se vztahuje směrnice 2013/36/EU a které se účastní jednotného mechanismu dohledu zřízeného nařízením Rady č. 1024/2013, měly neprodleně podat Evropské centrální bance zprávu o veškerých informacích zjištěných v průběhu jejich činností v oblasti dozoru nad trhem, které by mohly mít potenciální význam pro úkoly Evropské centrální banky v oblasti obezřetnostního dohledu podle uvedeného nařízení. V zájmu dalšího posílení souladu mezi tímto nařízením a pravidly platnými pro úvěrové instituce podléhající směrnici Evropského parlamentu a Rady 2013/36/EU[27] je rovněž vhodné začlenit některé procesní povinnosti poskytovatelů v souvislosti s řízením rizik, monitorováním po uvedení na trh a dokumentací do stávajících povinností a postupů podle směrnice 2013/36/EU. Aby nedocházelo k překrývání, je třeba počítat rovněž s omezenými výjimkami ve vztahu k systému řízení kvality poskytovatelů a k povinnosti monitorování uložené uživatelům vysoce rizikových systémů UI v rozsahu, v jakém se vztahují na úvěrové instituce podléhající směrnici 2013/36/EU. Stejný režim by se měl vztahovat na pojišťovny, zajišťovny a pojišťovací holdingové společnosti podle směrnice 2009/138/EU (Solventnost II) a na zprostředkovatele pojištění podle směrnice 2016/97/EU

[27] Směrnice Evropského parlamentu a Rady 2013/36/EU ze dne 26. června 2013 o přístupu k činnosti úvěrových institucí a o obezřetnostním dohledu nad úvěrovými institucemi a investičními podniky, o změně směrnice 2002/87/ES a zrušení směrnic 2006/48/ES a 2006/49/ES (Úř. věst. L 176, 27.6.2013, s. 338).

a na další typy finančních institucí, na něž se vztahují požadavky týkající se vnitřní správy, opatření nebo postupů zavedených podle příslušných právních předpisů Unie v oblasti finančních služeb, aby byla zajištěna soudržnost a rovné zacházení ve finančním sektoru.

(81) Vývoj systémů UI s výjimkou vysoce rizikových systémů UI v souladu s požadavky tohoto nařízení může vést k rozsáhlejšímu zavádění důvěryhodné umělé inteligence v Unii. Poskytovatelé systémů UI, které nejsou vysoce rizikové, by měli být vybízeni k vytváření kodexů chování určených k podpoře dobrovolného uplatňování požadavků platných pro vysoce rizikové systémy UI, přizpůsobených zamýšlenému účelu těchto systémů a souvisejícímu nižšímu riziku. Poskytovatelé by také měli být povzbuzováni k tomu, aby dobrovolně uplatňovali další požadavky týkající se například udržitelnosti životního prostředí, přístupnosti pro osoby se zdravotním postižením, zapojení zúčastněných stran do návrhu a vývoje systémů UI a rozmanitosti vývojových týmů. Komise může vyvíjet iniciativy, včetně iniciativ odvětvové povahy, s cílem usnadnit snižování technických překážek bránících přeshraniční výměně dat pro účely rozvoje UI, a to i ohledně infrastruktury pro přístup k datům a sémantické a technické interoperability různých druhů dat.

(82) Je důležité, aby systémy UI související s produkty, které podle tohoto nařízení nejsou vysoce rizikové, a proto nemusí splňovat požadavky, které jsou v něm stanoveny, byly při uvedení na trh nebo do provozu přesto bezpečné. Jako záchranná síť pro přispění k tomuto cíli by se uplatnila směrnice Evropského parlamentu a Rady 2001/95/ES[28].

(83) V zájmu zajištění důvěryhodné a konstruktivní spolupráce příslušných orgánů na úrovni Unie a na vnitrostátní úrovni by měly všechny strany zapojené do uplatňování tohoto nařízení respektovat důvěrnost informací a údajů získaných při plnění svých úkolů, v souladu s unijními a vnitrostátními právními předpisy.

[28] Směrnice Evropského parlamentu a Rady 2001/95/ES ze dne 3. prosince 2001 o obecné bezpečnosti výrobků (Úř. věst. L 11, 15.1.2002, s. 4).

(84) Členské státy by měly přijmout veškerá nezbytná opatření k zajištění toho, aby byla ustanovení tohoto nařízení prováděna, a to i stanovením účinných, přiměřených a odrazujících sankcí za jejich porušení a s ohledem na zásadu *ne bis in idem*. U určitých konkrétních porušení by členské státy měly zohlednit rozpětí a kritéria stanovená v tomto nařízení. Evropský inspektor ochrany údajů by měl být oprávněn ukládat pokuty orgánům, institucím a subjektům Unie spadajícím do oblasti působnosti tohoto nařízení.

(85) Za účelem zajištění toho, že v případě potřeby bude možné regulační rámec upravit, by měla být na Komisi přenesena pravomoc přijímat akty v souladu s článkem 290 Smlouvy o fungování EU, pokud jde o změnu harmonizačních právních předpisů Unie uvedených v příloze II, vysoce rizikových systémů UI uvedených v příloze III, ustanovení týkajících se technické dokumentace uvedených v příloze IV, obsahu EU prohlášení o shodě uvedeného v příloze V, ustanovení týkajících se postupů posuzování shody v přílohách VI a VII a ustanovení zavádějících vysoce rizikové systémy UI, na které by se měl vztahovat postup posuzování shody založený na posouzení systému řízení kvality a posouzení technické dokumentace. Je obzvláště důležité, aby Komise vedla v rámci přípravné činnosti odpovídající konzultace, a to i na odborné úrovni, a aby tyto konzultace probíhaly v souladu se zásadami stanovenými v interinstitucionální dohodě ze dne 13. dubna 2016 o zdokonalení tvorby právních předpisů[29]. Pro zajištění rovné účasti na vypracovávání aktů v přenesené pravomoci obdrží Evropský parlament a Rada veškeré dokumenty současně s odborníky z členských států a jejich odborníci mají automaticky přístup na setkání skupin odborníků Komise, jež se věnují přípravě aktů v přenesené pravomoci. Tyto konzultace a poradenská podpora by měly být rovněž prováděny v rámci činností rady pro umělou inteligenci a jejích podskupin.

[29] Úř. věst. L 123, 12.5.2016, s. 1.

(86) Za účelem zajištění jednotných podmínek k provedení tohoto nařízení by měly být Komisi svěřeny prováděcí pravomoci. Tyto pravomoci by měly být vykonávány v souladu s nařízením Evropského parlamentu a Rady (EU) č. 182/2011[30]. Je obzvláště důležité, aby Komise v souladu se zásadami stanovenými v interinstitucionální dohodě ze dne 13. dubna 2016 o zdokonalení tvorby právních předpisů v případech, kdy jsou v rané fázi přípravy návrhů prováděcích aktů zapotřebí širší odborné znalosti, využívala odborné skupiny, konzultovala cílové zúčastněné strany nebo případně vedla veřejné konzultace. Tyto konzultace a poradenská podpora by měly být rovněž prováděny v rámci činností rady pro umělou inteligenci a jejích podskupin, včetně přípravy prováděcích aktů ve vztahu k článkům 4, 4b a 6.

(87) Jelikož cíle tohoto nařízení nemůže být uspokojivě dosaženo na úrovni členských států a spíše jich z důvodu rozsahu nebo účinků může být lépe dosaženo na úrovni Unie, může Unie přijmout opatření v souladu se zásadou subsidiarity stanovenou v článku 5 Smlouvy o EU. V souladu se zásadou proporcionality stanovenou v uvedeném článku nepřekračuje toto nařízení rámec toho, co je nezbytné pro dosažení tohoto cíle.

(87a) V zájmu zabezpečení právní jistoty, zajištění vhodného adaptačního období pro provozovatele a zabránění narušení trhu, mimo jiné zajištěním kontinuity používání systémů UI, je vhodné, aby se toto nařízení vztahovalo na vysoce rizikové systémy UI, které byly uvedeny na trh nebo do provozu před obecným datem jeho použitelnosti, pouze pokud od uvedeného data dojde k významným změnám jejich návrhu nebo určeného účelu. Je vhodné vyjasnit, že v tomto ohledu by pojem „významná změna“ měl být v podstatě chápán jako rovnocenný pojmu „podstatná změna“, který se používá pouze ve vztahu k vysoce rizikovým systémům UI, jak jsou definovány v tomto nařízení.

[30] Nařízení Evropského parlamentu a Rady (EU) č. 182/2011 ze dne 16. února 2011, kterým se stanoví pravidla a obecné zásady způsobu, jakým členské státy kontrolují Komisi při výkonu prováděcích pravomocí (Úř. věst. L 55, 28.2.2011, s. 13).

(88) Toto nařízení by se mělo použít ode dne … [*Úřad pro publikace – vložte datum uvedené v článku 85*]. Infrastruktura související se správou a se systémem posuzování shody by však měla být funkční již před tímto datem, a proto by se ustanovení o oznámených subjektech a o struktuře řízení měla použít ode dne … [*Úřad pro publikace – vložte datum – tři měsíce od vstupu tohoto nařízení v platnost*]. Kromě toho by členské státy měly stanovit pravidla ukládání sankcí, včetně správních pokut, a oznámit je Komisi a zajistit, aby byla řádně a účinně provedena do data použitelnosti tohoto nařízení. Ustanovení o sankcích by proto měla platit ode dne [*Úřad pro publikace – vložte datum – dvanáct měsíců od vstupu tohoto nařízení v platnost*].

(89) V souladu s čl. 42 odst. 2 nařízení (EU) 2018/1725 byl konzultován evropský inspektor ochrany údajů a Evropský sbor pro ochranu osobních údajů, a jejich stanovisko bylo vydáno dne […].

PŘIJALY TOTO NAŘÍZENÍ:

HLAVA I

OBECNÁ USTANOVENÍ

Článek 1

Předmět

Toto nařízení stanoví:

a) harmonizovaná pravidla pro uvádění systémů umělé inteligence (dále jen „systémy UI“) na trh a do provozu a pro jejich používání v Unii;

a) zákaz určitých postupů v oblasti umělé inteligence;

b) zvláštní požadavky na vysoce rizikové systémy UI a povinnosti provozovatelů těchto systémů;

c) harmonizovaná pravidla transparentnosti pro některé systémy UI;

d) pravidla monitorování trhu, dozoru nad trhem a jeho správy;

e) opatření na podporu inovací.

Článek 2

Oblast působnosti

1. Toto nařízení se vztahuje na:

a) poskytovatele, kteří uvádějí na trh nebo do provozu systémy UI v Unii bez ohledu na to, zda jsou tito poskytovatelé fyzicky přítomni nebo usazeni v Unii nebo ve třetí zemi;

b) uživatele systémů UI, kteří jsou fyzicky přítomni nebo jsou usazeni v Unii;

c) poskytovatele a uživatele systémů UI, kteří jsou fyzicky přítomni nebo jsou usazeni ve třetí zemi, pokud se výstup systému používá v Unii;

d) dovozce a distributory systémů UI;

e) výrobce produktů, kteří uvádějí na trh nebo do provozu systém UI společně se svým produktem a pod svým jménem nebo ochrannou známkou;

f) zplnomocněné zástupce poskytovatelů, kteří jsou usazeni v Unii.

2. Pro systémy UI klasifikované jako vysoce rizikové systémy v souladu s čl. 6 odst. 1 a 2, které se pojí s produkty, na něž se vztahují harmonizační právní předpisy Unie uvedené v příloze II oddíle B, se použije pouze článek 84 tohoto nařízení. Článek 53 se použije pouze v případě, že požadavky na vysoce rizikové systémy UI podle tohoto nařízení byly začleněny do uvedených harmonizačních právních předpisů Unie.

3. Toto nařízení se nevztahuje na systémy UI, pouze tehdy a do té míry, v jakém jsou uváděny na trh nebo do provozu nebo jsou používány se změnami těchto systémů nebo bez nich pro účely činností, které nespadají do oblasti působnosti práva Unie, a v každém případě činností týkajících se vojenské či obranné oblasti nebo národní bezpečnosti, bez ohledu na typ subjektu, který tyto činnosti provádí.

   Kromě toho se toto nařízení nevztahuje na systémy UI, které nejsou uváděny na trh nebo do provozu v Unii, pokud se výstup používá v Unii pro účely činností, které nespadají do oblasti působnosti práva Unie, a v každém případě na činnosti týkající se vojenské či obranné oblasti nebo národní bezpečnosti, bez ohledu na typ subjektu, který tyto činnosti provádí.

4. Toto nařízení se nevztahuje na veřejné orgány ve třetí zemi ani na mezinárodní organizace spadající do oblasti působnosti tohoto nařízení podle odstavce 1, pokud tyto orgány nebo organizace používají systémy UI v rámci mezinárodních dohod o prosazování práva a o justiční spolupráci s Unií nebo s jedním či více členskými státy.

5. Tímto nařízením není dotčeno uplatňování ustanovení o odpovědnosti poskytovatelů zprostředkovatelských služeb uvedených v kapitole II oddíle 4 směrnice Evropského parlamentu a Rady 2000/31/ES[31] [*bude nahrazeno odpovídajícími ustanoveními aktu o digitálních službách*].

6. Toto nařízení se nevztahuje na systémy UI, včetně jejich výstupů, které byly speciálně vyvinuty a uvedeny do provozu výhradně za účelem vědeckého výzkumu a vývoje.

7. Toto nařízení se nevztahuje na žádnou výzkumnou ani vývojovou činnost týkající se systémů UI.

8. Toto nařízení se nevztahuje na povinnosti uživatelů, kteří jsou fyzickými osobami a používají systémy UI v rámci čistě osobní neprofesionální činnosti, s výjimkou článku 52.

[31] Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu) (Úř. věst. L 178, 17.7.2000, s. 1).

Článek 3

Definice

Pro účely tohoto nařízení se rozumí:

1) „systémem umělé inteligence“ (systém UI) systém, který je navržen tak, aby fungoval s prvky autonomie, a který na základě strojových nebo člověkem poskytnutých dat a vstupů odvozuje, jak dosáhnout daného souboru cílů pomocí strojového učení nebo přístupů založených na logice a znalostech, a vytváří systémové výstupy, jako je obsah (generativní systémy UI), predikce, doporučení nebo rozhodnutí, které ovlivňují prostředí, s nimiž systém UI komunikuje;

1a) „životním cyklem systému UI“ doba trvání systému UI od návrhu až po ukončení činnosti. Aniž jsou dotčeny pravomoci orgánů dozoru nad trhem, může k takovému ukončení činnosti dojít kdykoli během fáze monitorování po uvedení na trh na základě rozhodnutí poskytovatele a znamená to, že systém nelze dále používat. Životní cyklus systému UI je rovněž ukončen podstatnou změnou systému UI provedenou poskytovatelem nebo jinou fyzickou nebo právnickou osobou, v kterémžto případě se podstatně změněný systém UI považuje za nový systém UI.

1b) „obecným systémem umělé inteligence“ systém umělé inteligence, který má nehledě na způsob svého uvedení na trh nebo do provozu, a to i jako software s otevřeným zdrojovým kódem, podle svého poskytovatele zajišťovat obecně platné funkce, jako je rozpoznávání obrazů a řeči, vytváření audio- a videozáznamu, vyhledávání určitých vzorců, odpovídání na dotazy, překlad a další; obecný systém umělé inteligence se může používat v celé řadě situací a může být součástí mnoha jiných systémů umělé inteligence;

2) „poskytovatelem“ fyzická nebo právnická osoba, veřejný orgán, agentura nebo jiný subjekt, které vyvíjejí nebo nechávají vyvíjet systém UI a uvádějí tento systém na trh nebo do provozu pod svým vlastním jménem nebo ochrannou známkou, ať už za úplatu, nebo zdarma;

3) [vypouští se];

3a) „malým a středním podnikem“ podnik vymezený v příloze doporučení Komise 2003/361/ES o definici mikropodniků, malých a středních podniků;

4) „uživatelem“ jakákoli fyzická nebo právnická osoba, včetně veřejného orgánu, agentury nebo jiného subjektu, které v rámci své pravomoci systém využívají;

5) „zplnomocněným zástupcem“ jakákoli fyzická nebo právnická osoba fyzicky přítomná nebo usazená v Unii, která obdržela od poskytovatele systému UI písemné pověření k tomu, aby jeho jménem plnila povinnosti a prováděla postupy stanovené tímto nařízením, a toto ověření přijala;

5a) „výrobcem produktu“ výrobce ve smyslu kteréhokoli z harmonizačních právních předpisů Unie uvedených v příloze II;

6) „dovozcem“ jakákoli fyzická nebo právnická osoba fyzicky přítomná nebo usazená v Unii, která uvádí na trh systém UI označený jménem nebo ochrannou známkou fyzické nebo právnické osoby usazené mimo Unii;

7) „distributorem“ fyzická nebo právnická osoba v dodavatelském řetězci, jiná než poskytovatel nebo dovozce, která dodává systém UI na trh Unie;

8) „provozovatelem“ poskytovatel, výrobce produktu, uživatel, zplnomocněný zástupce, dovozce nebo distributor;

9) „uvedením na trh“ první dodání systému UI na trh Unie;

10) „dodáním na trh“ dodání systému UI k distribuci nebo použití na trhu Unie v rámci obchodní činnosti, ať už za úplatu, nebo zdarma;

11) „uvedením do provozu“ dodání systému UI k prvnímu použití přímo uživateli nebo pro vlastní použití v Unii za určeným účelem;

12) „určeným účelem“ použití systému UI určené poskytovatelem, včetně konkrétního kontextu a podmínek použití, které jsou uvedeny v informacích dodaných poskytovatelem v návodu k použití, v propagačních nebo prodejních materiálech a prohlášeních, jakož i v technické dokumentaci;

13) „důvodně předvídatelným nesprávným použitím“ použití systému UI způsobem, který není v souladu s jeho určeným účelem, avšak může vyplývat z důvodně předvídatelného lidského chování nebo z interakce s jinými systémy;

14) „bezpečnostní součástí produktu nebo systému“ součást produktu nebo systému, která plní bezpečnostní funkci pro daný produkt nebo systém, případně jejíž porucha nebo chybné fungování ohrožuje zdraví a bezpečnost osob nebo majetku;

15) „návodem k použití“ informace poskytnuté poskytovatelem, které uživatele informují zejména o určeném účelu a řádném použití daného systému UI;

16) „stažením systému UI z oběhu“ jakékoli opatření, jehož cílem je dosáhnout, aby byl systém UI zpřístupněný uživatelům navrácen poskytovateli nebo vyřazen z provozu či aby bylo znemožněno jeho používání;

17) „stažením systému UI z trhu“ jakékoli opatření, jehož cílem je zabránit, aby byl systém UI, který se nachází v dodavatelském řetězci, zpřístupněn na trhu;

18) „výkonností systému UI“ schopnost systému UI dosáhnout svého určeného účelu;

19) „posuzováním shody“ postup ověřování toho, zda byly splněny požadavky stanovené v hlavě III kapitole 2 tohoto nařízení týkající se vysoce rizikového systému UI;

20) „oznamujícím orgánem“ vnitrostátní orgán odpovědný za stanovení a provádění postupů nezbytných pro posuzování, jmenování a oznamování subjektů posuzování shody a za jejich monitorování;

21) „subjektem posuzování shody“ subjekt, který vykonává činnosti posuzování shody jakožto třetí strana, včetně testování, certifikace a inspekce;

22) „oznámeným subjektem“ subjekt posuzování shody určený v souladu s tímto nařízením a dalšími příslušnými harmonizačními právními předpisy Unie;

23) „podstatnou změnou“ změna systému UI po jeho uvedení na trh nebo do provozu, která ovlivňuje soulad systému UI s požadavky stanovenými v hlavě III kapitole 2 tohoto nařízení nebo vede ke změně určeného účelu, podle kterého byl systém UI posuzován. U vysoce rizikových systémů UI, které se po uvedení na trh nebo do provozu dále učí, nepředstavují změny takového vysoce rizikového systému UI a jeho výkonnosti podstatnou změnu, pokud byly poskytovatelem stanoveny předem v okamžiku počátečního posouzení shody a jsou součástí informací obsažených v technické dokumentaci uvedené v bodě 2 písm. f) přílohy IV.

24) „označením shody CE“ nebo „označením CE“ označení, kterým poskytovatel vyjadřuje, že systém UI je ve shodě s požadavky stanovenými v hlavě III kapitole 2 nebo v článku 4b tohoto nařízení a v dalších příslušných právních aktech Unie harmonizujících uvádění produktů na trh („harmonizační právní předpisy Unie“), které upravují jeho umísťování;

25) „systémem monitorování po uvedení na trh“ veškeré činnosti prováděné poskytovateli systémů UI s cílem shromažďovat a přezkoumávat zkušenosti získané v souvislosti s využíváním systémů UI, které dodávají na trh nebo uvádějí do provozu za účelem určení potřeby okamžitého uplatnění jakýchkoliv nezbytných nápravných nebo preventivních opatření;

26) „orgánem dozoru nad trhem“ vnitrostátní orgán provádějící činnosti a přijímající opatření podle nařízení (EU) 2019/1020;

27) „harmonizovanou normou“ evropská norma podle definice v čl. 2 odst. 1 písm. c) nařízení (EU) č. 1025/2012;

28) „společnou specifikací“ soubor technických specifikací ve smyslu čl. 2 bodu 4 nařízení (EU) č. 1025/2012, který poskytuje prostředky ke splnění určitých požadavků stanovených v tomto nařízením;

29) „tréninkovými daty“ data používaná pro trénování systému UI přizpůsobováním jeho parametrů, které se lze naučit;

30) „daty pro ověřování platnosti“ data používaná pro vyhodnocení trénovaného systému UI a pro vyladění jeho parametrů, které se nelze naučit, a jeho procesu učení, mimo jiné s cílem zabránit přeučení; přičemž soubor dat pro ověřování platnosti může být samostatný soubor dat nebo součást souboru tréninkových dat, ať už jako pevné, nebo variabilní rozdělení;

31) „testovacími daty“ data používaná k zajištění nezávislého vyhodnocení trénovaného a ověřeného systému UI za účelem potvrzení očekávané výkonnosti tohoto systému před jeho uvedením na trh nebo do provozu;

32) „vstupními daty“ data poskytovaná systému UI nebo přímo získaná tímto systémem, na jejichž základě tento systém vytváří výstup;

33) „biometrickými údaji“ osobní údaje vyplývající z konkrétního technického zpracování, týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, například zobrazení obličeje nebo daktyloskopické údaje;

34) „systémem rozpoznávání emocí“ systém UI pro účely zjišťování nebo odvozování psychických stavů, emocí nebo záměrů fyzických osob na základě jejich biometrických údajů;

35) „systémem biometrické kategorizace“ systém UI pro účely zařazení fyzických osob do určitých kategorií na základě jejich biometrických údajů;

36) „systémem biometrické identifikace na dálku“ systém UI pro účely identifikace fyzických osob obvykle na dálku bez jejich aktivního zapojení na základě porovnání biometrických údajů dané osoby s biometrickými údaji obsaženými v úložišti referenčních údajů;

37) „systémem biometrické identifikace na dálku, v reálném čase““ systém biometrické identifikace na dálku, kdy zachycení biometrických údajů, porovnání a identifikace probíhá okamžitě nebo téměř okamžitě;

38) [vypouští se]

39) „veřejně přístupným místem“ jakékoli fyzické místo ve veřejném nebo soukromém vlastnictví přístupné neurčenému počtu fyzických osob bez ohledu na to, zda byly předem stanoveny určité podmínky nebo okolnosti přístupu, a bez ohledu na potenciální omezení kapacity;

40) „donucovacím orgánem“

a) jakýkoliv veřejný orgán příslušný k prevenci, vyšetřování, odhalování či stíhání trestných činů či výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení, nebo

b) jakýkoliv jiný orgán nebo subjekt pověřený právem členského státu plnit veřejnou funkci a vykonávat veřejnou moc pro účely prevence, vyšetřování, odhalování či stíhání trestných činů či výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení;

41) „prosazováním práva“ činnosti prováděné donucovacími orgány nebo jejich jménem za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení;

42) [vypouští se]

43) „příslušným vnitrostátním orgánem“ kterýkoli z následujících orgánů: oznamující orgán a orgán dozoru nad trhem. Pokud jde o systémy UI uvedené do provozu nebo používané orgány, institucemi a jinými subjekty EU, plní evropský inspektor ochrany údajů povinnosti, které jsou v členských státech svěřeny příslušnému vnitrostátnímu orgánu, a v relevantních případech se jakýkoli odkaz v tomto nařízení na příslušné vnitrostátní orgány nebo orgány dozoru nad trhem považuje za odkaz na evropského inspektora ochrany údajů;

44) „závažným incidentem“ incident nebo chybné fungování systému UI, které přímo nebo nepřímo vedou k některému z těchto následků:

a) smrt určité osoby nebo závažné poškození zdraví určité osoby;

b) závažné a nevratné narušení správy a provozu kritické infrastruktury;

c) porušení povinností vyplývajících z práva Unie, jejichž cílem je ochrana základních práv;

d) závažné poškození majetku nebo životního prostředí.

45) „kritickou infrastrukturou“ jednotka, systém nebo jeho část, které jsou nezbytné k poskytování služby, jež má zásadní význam pro zachování životně důležitých společenských funkcí nebo hospodářské činnosti ve smyslu čl. 2 odst. 4 a 5 směrnice [...] o odolnosti kritických subjektů;

46) „osobními údaji“ údaje definované v čl. 4 bodě 1) nařízení (EU) 2016/679;

47) „neosobními údaji“ údaje jiné než osobní údaje definované v čl. 4 bodě 1) nařízení (EU) 2016/679;

48) „testováním v reálných podmínkách“ dočasné testování systému UI pro jeho určený účel v reálných podmínkách mimo laboratoř nebo jinak simulované prostředí za účelem shromažďování spolehlivých údajů a posuzování a ověřování shody systému UI s požadavky tohoto nařízení; testování v reálných podmínkách se nepovažuje za uvedení systému UI na trh nebo do provozu ve smyslu tohoto nařízení, pokud jsou splněny všechny podmínky podle článku 53 nebo článku 54a;

49) „plánem testování v reálných podmínkách“ dokument, který popisuje cíle, metodiku, zeměpisnou oblast, populaci a časový rozsah, monitorování, organizaci a provádění testování v reálných podmínkách;

50) „subjektem“ pro účely testování v reálných podmínkách fyzická osoba, která se účastní testování v reálných podmínkách;

51) „informovaným souhlasem“ svobodný a dobrovolný projev vůle subjektu účastnit se konkrétního testování v reálných podmínkách poté, co byl informován o všech aspektech testování, které jsou relevantní pro rozhodnutí subjektu účastnit se; v případě nezletilých osob a nezpůsobilých subjektů udělí informovaný souhlas jejich zákonně ustanovený zástupce;

52) „regulačním pískovištěm UI“ konkrétní rámec zřízený příslušným vnitrostátním orgánem, který poskytovatelům nebo potenciálním poskytovatelům systémů UI nabízí možnost vyvíjet, školit, ověřovat a testovat inovativní systém UI, případně v reálných podmínkách, podle konkrétního plánu po omezenou dobu pod regulačním dohledem.

Článek 4

Prováděcí akty

Za účelem zajištění jednotných podmínek pro provádění tohoto nařízení, pokud jde o přístupy ke strojovému učení a přístupy založené na logice a znalostech uvedené v čl. 3 odst. 1, může Komise přijmout prováděcí akty za účelem upřesnění technických prvků těchto přístupů s přihlédnutím k tržnímu a technologickému vývoji. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 74 odst. 2.

HLAVA IA

OBECNÉ SYSTÉMY UI

Článek 4a

Soulad obecných systémů UI s tímto nařízením

1. Aniž jsou dotčeny články 5, 52, 53 a 69 tohoto nařízení, obecné systémy UI musí splňovat pouze požadavky a povinnosti stanovené v článku 4b.

2. Tyto požadavky a povinnosti se uplatní bez ohledu na to, zda je obecný systém UI uváděn na trh nebo do provozu jako předem vyškolený model a zda má uživatel obecného systému UI provést další doladění modelu.

Článek 4b

Požadavky na obecné systémy UI a povinnosti provozovatelů těchto systémů

1. Obecné systémy UI, které mohou být používány jako vysoce rizikové systémy UI nebo jako součásti vysoce rizikových systémů UI ve smyslu článku 6, musí nejpozději 18 měsíců po vstupu tohoto nařízení v platnost splňovat požadavky stanovené v hlavě III kapitole 2 tohoto nařízení ode dne použitelnosti prováděcích aktů přijatých Komisí přezkumným postupem podle čl. 74 odst. 2. Tyto prováděcí akty upřesní a přizpůsobí uplatňování požadavků stanovených v hlavě III kapitole 2 na obecné systémy UI s ohledem na jejich vlastnosti, technickou proveditelnost, specifika hodnotového řetězce UI a vývoj trhu a technologií. Při plnění těchto požadavků se zohlední obecně uznávaný stav techniky.

2. Poskytovatelé obecných systémů UI uvedení v odstavci 1 plní ode dne použitelnosti prováděcích aktů uvedených v odstavci 1 povinnosti stanovené v čl. 16 písm. aa), e), f), g), i) a j) a článcích 25, 48 a 61.

3. Pro účely plnění povinností stanovených v článku 16e se poskytovatelé řídí postupem posuzování shody založeným na vnitřní kontrole, který je stanovený v příloze VI bodech 3 a 4.

4. Poskytovatelé těchto systémů rovněž uchovávají technickou dokumentaci uvedenou v článku 11 pro potřebu příslušných vnitrostátních orgánů po dobu deseti let od uvedení obecného systému UI na trh Unie nebo do provozu v Unii.

5. Poskytovatelé obecných systémů UI spolupracují s jinými poskytovateli, kteří mají v úmyslu uvést tyto systémy do provozu nebo na trh Unie jako vysoce rizikové systémy UI nebo jako součásti vysoce rizikových systémů UI, a poskytují jim nezbytné informace, aby jim umožnili splnit povinnosti podle tohoto nařízení. Tato spolupráce mezi poskytovateli zachovává podle potřeby práva duševního vlastnictví a důvěrné obchodní informace nebo obchodní tajemství v souladu s článkem 70. Za účelem zajištění jednotných podmínek pro provedení tohoto nařízení, pokud jde o informace, které mají sdílet poskytovatelé obecných systémů UI, může Komise přezkumným postupem podle čl. 74 odst. 2 přijmout prováděcí akty.

6. Při plnění požadavků a povinností uvedených v odstavcích 1, 2 a 3:

– jakýkoli odkaz na určený účel se považuje za odkaz na možné použití obecných systémů UI jako vysoce rizikových systémů UI nebo jako součástí vysoce rizikových systémů UI ve smyslu článku 6;

– jakýkoli odkaz na požadavky na vysoce rizikové systémy UI v hlavě III kapitole II se považuje pouze za odkaz na požadavky stanovené v tomto článku.

Článek 4c

Výjimky z článku 4b

1. Článek 4b se nepoužije, pokud poskytovatel v návodu k použití nebo v informacích přiložených k obecnému systému UI výslovně vyloučil všechna vysoce riziková použití.

2. Toto vyloučení se provede v dobré víře a nepovažuje se za odůvodněné, pokud má poskytovatel dostatečné důvody se domnívat, že systém může být zneužit.

3. Pokud poskytovatel zjistí, že došlo ke zneužití na trhu, nebo je o něm informován, přijme veškerá nezbytná a přiměřená opatření, aby takovému dalšímu zneužití zabránil, zejména s ohledem na rozsah zneužití a závažnost souvisejících rizik.

HLAVA II

ZAKÁZANÉ POSTUPY V OBLASTI UMĚLÉ INTELIGENCE

Článek 5

1. Zakazují se následující postupy v oblasti umělé inteligence:

   a) uvádění na trh, uvádění do provozu nebo používání systémů UI, které využívají podprahových technik mimo vědomí osob s cílem podstatně ovlivnit chování těchto osob tak, že to dotčené osobě nebo jiné osobě způsobuje nebo by s přiměřenou pravděpodobností mohlo způsobit fyzickou nebo psychickou újmu;

   b) uvádění na trh, uvádění do provozu nebo používání systémů UI, které využívají zranitelnosti určité skupiny osob v důsledku jejich věku, zdravotního postižení nebo specifické sociální nebo ekonomické situace, s cílem podstatně ovlivnit chování osoby náležející k této skupině tak, že to dotčené osobě nebo jiné osobě způsobuje nebo by s přiměřenou pravděpodobností mohlo způsobit fyzickou nebo psychickou újmu;

   c) uvádění na trh, uvádění do provozu nebo používání systémů UI pro účely hodnocení nebo klasifikace fyzických osob v určitém časovém úseku na základě jejich sociálního chování nebo známých nebo předvídaných osobních či osobnostních vlastností, přičemž výsledný sociální kredit vede k jednomu nebo oběma následujícím důsledkům:

      i) ke znevýhodňujícímu nebo nepříznivému zacházení s některými fyzickými osobami nebo skupinami těchto osob v sociálních kontextech nesouvisejících s kontextem, ve kterém byly dané údaje původně vytvořeny nebo shromážděny;

ii) ke znevýhodňujícímu nebo nepříznivému zacházení s některými fyzickými osobami nebo skupinami těchto osob, které je neodůvodněné nebo nepřiměřené jejich sociálnímu chování nebo jeho závažnosti;

d) používání systémů biometrické identifikace na dálku „v reálném čase“ na veřejně přístupných místech donucovacími orgány nebo jejich jménem pro účely prosazování práva, ledaže je to nezbytně nutné pro jeden z následujících cílů a jen do té míry, do níž je to nezbytně nutné:

i) cílené vyhledávání určitých potenciálních obětí trestných činů;

ii) prevenci konkrétního a závažného ohrožení kritické infrastruktury, života, zdraví nebo fyzické bezpečnosti fyzických osob nebo prevenci teroristických útoků;

iii) lokalizaci nebo identifikaci fyzické osoby za účelem trestního vyšetřování, stíhání nebo výkonu trestu za trestné činy uvedené v čl. 2 odst. 2 rámcového rozhodnutí Rady 2002/584/SVV[32], za které lze v dotčeném členském státě uložit trest odnětí svobody nebo ochranné opatření spojené s odnětím osobní svobody s horní hranicí sazby v délce nejméně tří let, nebo za jiné konkrétní trestné činy, za něž lze v dotčeném členském státě uložit trest odnětí svobody nebo ochranné opatření spojené s odnětím osobní svobody s horní hranicí sazby v délce nejméně pěti let, jak je stanoveno v právních předpisech tohoto členského státu.

2. Při používání systémů biometrické identifikace na dálku „v reálném čase“ na veřejně přístupných místech pro účely prosazování práva pro dosažení kteréhokoli z cílů uvedených v odst. 1 písm. d) je nutno zohlednit následující prvky:

a) povahu situace, která vede k jejich potenciálnímu použití, zejména závažnost, pravděpodobnost a rozsah újmy způsobené v případě, že by systém použit nebyl;

[32] Rámcové rozhodnutí Rady 2002/584/SVV ze dne 13. června 2002 o evropském zatýkacím rozkazu a postupech předávání mezi členskými státy (Úř. věst. L 190, 18.7.2002, s. 1).

b) důsledky používání systému pro práva a svobody všech dotčených osob, zejména závažnost, pravděpodobnost a rozsah těchto důsledků.

Použití systémů biometrické identifikace na dálku „v reálném čase“ na veřejně přístupných místech pro účely prosazování práva pro dosažení kteréhokoli z cílů uvedených v odst. 1 písm. d) musí být navíc v souladu s nezbytnými a přiměřenými zárukami a podmínkami ve vztahu k tomuto použití, zejména pokud jde o časová, zeměpisná a osobní omezení.

3. Pokud jde o odst. 1 písm. d) a odstavec 2, každé použití systému biometrické identifikace na dálku „v reálném čase“ na veřejně přístupných místech pro účely prosazování práva podléhá předchozímu povolení ze strany justičního orgánu nebo nezávislého správního orgánu členského státu, ve kterém má k tomuto použití dojít, vydanému na základě odůvodněné žádosti a v souladu s podrobnými pravidly vnitrostátního práva uvedenými v odstavci 4. V řádně odůvodněné naléhavé situaci však může být používání systému zahájeno bez povolení za předpokladu, že o takové povolení se požádá bez zbytečného odkladu během používání systému UI, a pokud je toto povolení zamítnuto, jeho používání se s okamžitým účinkem ukončí.

Příslušný justiční nebo správní orgán udělí povolení pouze v případě, že je na základě objektivních důkazů nebo jednoznačných údajů, které mu byly předloženy, přesvědčen, že použití dotčeného systému biometrické identifikace na dálku „v reálném čase“ je nezbytné a přiměřené k dosažení jednoho z cílů specifikovaných v odst. 1 písm. d), který je uveden v žádosti. Při rozhodování o žádosti zohlední příslušný justiční nebo správní orgán skutečnosti uvedené v odstavci 2.

4. Členský stát se může rozhodnout, že umožní plně nebo částečně povolit používání systémů biometrické identifikace na dálku „v reálném čase“ na veřejně přístupných místech pro účely prosazování práva v mezích a za podmínek uvedených v odst. 1 písm. d) a v odstavcích 2 a 3. Daný členský stát stanoví ve svých vnitrostátních právních předpisech nezbytná podrobná pravidla upravující žádosti o povolení uvedená v odstavci 3, vydávání a výkon těchto povolení, jakož i pro dohled a podávání zpráv o těchto povoleních. Tato pravidla rovněž stanoví, ve vztahu ke kterému cíli uvedenému v odst. 1 písm. d) a ke kterému trestnému činu uvedenému v písmenu iii) tohoto odstavce lze příslušným orgánům povolit používání těchto systémů pro účely prosazování práva.

HLAVA III

VYSOCE RIZIKOVÉ SYSTÉMY UI

KAPITOLA 1

KLASIFIKACE SYSTÉMŮ UI JAKO VYSOCE RIZIKOVÝCH

Článek 6

Klasifikační pravidla pro vysoce rizikové systémy UI

1. Systém UI, který je sám o sobě výrobkem, na nějž se vztahují harmonizační právní předpisy Unie uvedené v příloze II, je považován za vysoce rizikový, pokud se vyžaduje, aby byl podroben posouzení shody třetí stranou za účelem uvedení tohoto výrobku na trh nebo do provozu podle výše uvedených právních předpisů.

2. Systém UI, který je určen k použití jako bezpečnostní součást výrobku, na který se vztahují právní předpisy uvedené v odstavci 1, je považován za vysoce rizikový, pokud se vyžaduje, aby byl podroben posouzení shody třetí stranou za účelem uvedení tohoto výrobku na trh nebo do provozu podle výše uvedených právních předpisů. Toto ustanovení se použije bez ohledu na to, zda je systém UI uváděn na trh nebo do provozu nezávisle na výrobku.

3. Systémy UI uvedené v příloze III se považují za vysoce rizikové, pokud výstup systému není čistě doplňkový ve vztahu k příslušnému opatření nebo rozhodnutí, které má být přijato, a není proto pravděpodobné, že by vedl k významnému riziku pro zdraví, bezpečnost nebo základní práva.

Za účelem zajištění jednotných podmínek pro provedení tohoto nařízení přijme Komise nejpozději do jednoho roku od vstupu tohoto nařízení v platnost prováděcí akty, jimiž upřesní okolnosti, za nichž by výstup systémů UI uvedených v příloze III byl ve vztahu k příslušnému opatření nebo rozhodnutí, které má být přijato, čistě doplňkový. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 74 odst. 2.

Článek 7

Změny přílohy II

1. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 73 za účelem změny seznamu v příloze III přidáním vysoce rizikových systémů UI, pokud jsou splněny obě tyto podmínky:

a) systémy UI jsou určeny pro použití v kterékoli z oblastí uvedených v bodech 1 až 8 přílohy III;

b) systémy UI představují riziko újmy na zdraví a bezpečnosti nebo riziko nepříznivého dopadu na základní práva, které je z hlediska závažnosti a pravděpodobnosti výskytu stejné nebo větší než riziko újmy nebo nepříznivého dopadu, které představují vysoce rizikové systémy UI, jež jsou již uvedeny v příloze III.

2. Při posuzování toho, zda systém UI představuje riziko újmy na zdraví a bezpečnosti nebo riziko nepříznivého dopadu na základní práva stejné nebo větší než riziko újmy nebo nepříznivého dopadu, které představují vysoce rizikové systémy UI, jež jsou již uvedeny v příloze III, pro účely odstavce 1, zohlední Komise tato kritéria:

a) určený účel daného systému UI;

b) do jaké míry je daný systém UI již využíván nebo bude pravděpodobně využíván;

c) do jaké míry již používání systému UI způsobilo újmu na zdraví a bezpečnosti nebo nepříznivý dopad na základní práva nebo vzbudilo významné obavy ohledně toho, že by k této újmě nebo nepříznivému dopadu mohlo dojít, jak vyplývá ze zpráv nebo zdokumentovaných obvinění předložených příslušným vnitrostátním orgánům;

d) potenciální rozsah této újmy nebo nepříznivého dopadu, zejména pokud jde o jejich intenzitu a schopnost ovlivnit více osob;

e) do jaké míry jsou osoby, které potenciálně utrpěly újmu nebo nepříznivý dopad, závislé na výsledku vytvořeném pomocí systému UI zejména proto, že z praktických nebo právních důvodů není přiměřeně možné odmítnout účast na tomto výsledku;

f) do jaké míry se osoby, které potenciálně utrpěly újmu nebo nepříznivý dopad, nacházejí ve zranitelném postavení ve vztahu k danému uživateli systému UI, zejména v důsledku nerovnováhy sil, znalostí, ekonomických nebo sociálních podmínek nebo věku;

g) do jaké míry výsledek vytvořený systémem UI není snadno zvrátitelný, přičemž výsledky, které mají dopad na zdraví nebo bezpečnost osob, se za snadno zvrátitelné nepovažují;

h) do jaké míry stávající právní předpisy Unie stanoví:

i) účinná nápravná opatření ve vztahu k rizikům, která daný systém UI představuje, s výjimkou nároků na náhradu škody;

ii) účinná opatření vedoucí k prevenci nebo podstatné minimalizaci těchto rizik;

i) rozsah a pravděpodobnost přínosu používání UI pro jednotlivce, skupiny nebo společnost jako celek.

3. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 73 za účelem změny seznamu v příloze III odstraněním vysoce rizikových systémů UI, pokud jsou splněny obě tyto podmínky:

a) dotčený vysoce rizikový systém(systémy) UI již nepředstavuje(nepředstavují) významná rizika pro základní práva, zdraví nebo bezpečnost, a to s přihlédnutím ke kritériím uvedeným v odstavci 2;

b) vypuštěním se nesnižuje celková úroveň ochrany zdraví, bezpečnosti a základních práv podle práva Unie.

KAPITOLA 2

POŽADAVKY NA VYSOCE RIZIKOVÉ SYSTÉMY UI

Článek 8

Soulad s požadavky

1. Vysoce rizikové systémy UI musí být v souladu s požadavky stanovenými v této kapitole, přičemž je přihlíženo k obecně uznávanému stavu techniky.

2. Při zajišťování souladu s těmito požadavky se zohlední určený účel daného vysoce rizikového systému UI a systém řízení rizik uvedený v článku 9.

Článek 9

Systém řízení rizik

1. Ve vztahu k vysoce rizikovým systémům UI bude zaveden, uplatňován, zdokumentován a udržován systém řízení rizik.

2. Systém řízení rizik je chápán jako nepřetržitý opakující se proces plánovaný a prováděný v rámci celého životního cyklu vysoce rizikového systému UI, který vyžaduje pravidelnou systematickou aktualizaci. Zahrnuje následující kroky:

   a) identifikaci a analýzu známých a předvídatelných rizik v oblasti zdraví, bezpečnosti a základních práv, která mohou nejpravděpodobněji v souvislosti s určeným účelem vysoce rizikového systému UI vzniknout;

   b) [vypouští se];

   c) hodnocení dalších rizik, která mohou potenciálně vzniknout, na základě analýzy shromážděných údajů ze systému monitorování po uvedení na trh uvedeného v článku 61;

   d) přijetí vhodných opatření k řízení rizik v souladu s ustanoveními následujících odstavců.

   Rizika uvedená v tomto odstavci se týkají pouze rizik, která lze přiměřeně zmírnit nebo vyloučit vývojem nebo návrhem vysoce rizikového systému UI nebo poskytováním odpovídajících technických informací.

3. Opatření k řízení rizik uvedená v odst. 2 písm. d) věnují náležitou pozornost účinkům a možné interakci vyplývajícím z kombinovaného uplatňování požadavků stanovených v této kapitole 2 s cílem účinněji minimalizovat rizika a současně dosáhnout vhodné rovnováhy při provádění opatření ke splnění těchto požadavků.

4. Opatření k řízení rizik uvedená v odst. 2 písm. d) musí být taková, aby bylo jakékoli zbytkové riziko spojené s každým nebezpečím a rovněž celkové zbytkové riziko vysoce rizikových systémů UI považováno za přijatelné.

Při určování nejvhodnějších opatření k řízení rizik je třeba zajistit:

a) vyloučení nebo snížení rizik zjištěných a vyhodnocených podle odstavce 2, pokud možno prostřednictvím odpovídajícího návrhu a vývoje vysoce rizikového systému UI;

b) ve vhodných případech zavedení odpovídajících zmírňujících a kontrolních opatření, pokud jde o rizika, která nelze vyloučit;

c) poskytování odpovídajících informací podle článku 13, zejména pokud jde o rizika uvedená v odst. 2 písm. b) tohoto článku, a v případě potřeby zajistit pro uživatele školení.

Za účelem vyloučení nebo snížení rizik souvisejících s používáním daného vysoce rizikového systému UI by měly být náležitě zváženy technické znalosti, zkušenosti, vzdělání, školení, které může uživatel očekávat, a případně prostředí, ve kterém má být systém používán.

5. Vysoce rizikové systémy UI jsou testovány za účelem zajištění toho, aby vysoce rizikové systémy UI podávaly výkony, které budou konzistentní s jejich určeným účelem a budou v souladu s požadavky stanovenými v této kapitole.

6. Zkušební postupy mohou zahrnovat testování v reálných podmínkách v souladu s článkem 54a.

7. Testování vysoce rizikových systémů UI se provádí podle potřeby kdykoli v průběhu celého procesu vývoje a v každém případě před uvedením na trh nebo do provozu. Testování musí být provedeno na základě předem definovaných měřítek a pravděpodobnostních prahových hodnot, které jsou vhodné pro určený účel vysoce rizikového systému UI.

8. Systém řízení rizik popsaný v odstavcích 1 až 7 věnuje zvláštní pozornost tomu, zda je pravděpodobné, že k danému vysoce rizikovému systému UI budou mít přístup osoby mladší 18 let nebo zda bude mít na ně dopad.

9. V případě poskytovatelů vysoce rizikových systémů UI, na něž se vztahují požadavky týkající se vnitřních procesů řízení rizik podle příslušných odvětvových právních předpisů Unie, mohou být aspekty popsané v odstavcích 1 až 8 součástí postupů řízení rizik stanovených podle uvedeného práva.

Článek 10

Data a správa dat

1. Vysoce rizikové systémy UI, které využívají techniky zahrnující trénování modelů obsahujících data, jsou vyvíjeny na základě souborů tréninkových dat, dat pro ověřování platnosti a testovacích dat, které splňují kritéria kvality uvedená v odstavcích 2 až 5.

2. Soubory tréninkových dat, dat pro ověřování platnosti a testovacích dat podléhají příslušným postupům v oblasti správy a řízení dat. Tyto postupy se týkají zejména:

   a) příslušných možností návrhu;

   b) postupů při sběru dat;

   c) příslušných operací zpracování přípravy dat, jako jsou anotace, označování, čištění, obohacování a agregace;

d) formulace příslušných předpokladů, zejména s ohledem na informace, které mají daná data měřit a představovat;

e) předchozího posouzení dostupnosti, množství a vhodnosti potřebných souborů dat;

f) zkoumání s ohledem na potenciální zkreslení, které by mohlo ovlivnit zdraví a bezpečnost fyzických osob nebo vést k diskriminaci, kterou právo Unie zakazuje;

g) identifikace případných nedostatků nebo chyb v datech a způsobu, jak tyto nedostatky a chyby vyřešit.

3. Soubory tréninkových dat, dat pro ověřování platnosti a testovacích dat musí být v co největší možné míře relevantní, reprezentativní, bez chyb a úplné. Musí mít příslušné statistické vlastnosti, a to v relevantních případech rovněž s ohledem na osoby nebo skupiny osob, pro které má být daný vysoce rizikový systém UI používán. Tyto vlastnosti souborů dat lze splnit na úrovni jednotlivých souborů dat nebo jejich kombinací.

4. Soubory tréninkových dat, dat pro ověřování platnosti a testovacích dat zohledňují v rozsahu nezbytném pro jejich určený účel vlastnosti nebo prvky, které jsou specifické pro konkrétní zeměpisné, behaviorální nebo funkční prostředí, ve kterém má být daný vysoce rizikový systém UI používán.

5. Pokud je to nezbytně nutné pro zajištění monitorování, detekce a oprav zkreslení ve vztahu k vysoce rizikovým systémům UI, mohou poskytovatelé těchto systémů zpracovávat zvláštní kategorie osobních údajů uvedené v čl. 9 odst. 1 nařízení (EU) 2016/679, v článku 10 směrnice (EU) 2016/680 a v čl. 10 odst. 1 nařízení (EU) 2018/1725 s výhradou vhodných záruk týkajících se základních práv a svobod fyzických osob, včetně technických omezení opakovaného používání a používání nejmodernějších opatření v oblasti bezpečnosti a ochrany soukromí, jako je pseudonymizace nebo šifrování v případech, kdy anonymizace může významně ovlivnit sledovaný účel.

6. Pro vývoj vysoce rizikových systémů UI, které nevyužívají techniky zahrnující trénink modelů, se odstavce 2 až 5 použijí pouze na soubory testovacích dat.

Článek 11

Technická dokumentace

1. Technická dokumentace vysoce rizikového systému UI musí být vypracována před uvedením tohoto systému na trh nebo do provozu a musí být průběžně aktualizována.

   Technická dokumentace musí být vypracována tak, aby prokazovala, že daný vysoce rizikový systém UI splňuje požadavky stanovené v této kapitole, a aby jasným a úplným způsobem poskytovala příslušným vnitrostátním orgánům a oznámeným subjektům veškeré informace nezbytné k posouzení souladu systému UI s těmito požadavky. Obsahuje přinejmenším prvky uvedené v příloze IV nebo v případě malých a středních podniků, včetně začínajících podniků, jakoukoli rovnocennou dokumentaci, která splňuje stejné cíle, pokud to příslušný orgán nebude považovat za nevhodné.

2. Pokud je uváděn na trh nebo do provozu vysoce rizikový systém UI související s produktem, na který se vztahují právní akty uvedené v příloze II oddíle A, musí být vypracována jediná technická dokumentace obsahující všechny informace uvedené v příloze IV, jakož i informace požadované podle těchto právních aktů.

3. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 73 za účelem změny přílohy IV, je-li to nezbytné k zajištění toho, aby technická dokumentace s ohledem na technický pokrok poskytovala veškeré informace nezbytné k posouzení souladu systému s požadavky stanovenými v této kapitole.

Článek 12

Vedení záznamů

1. Vysoce rizikové systémy UI technicky umožňují automatické zaznamenávání událostí („protokoly“) po dobu životního cyklu systému.

2. Aby byla zajištěna úroveň sledovatelnosti fungování systému UI, která je přiměřená určenému účelu systému, musí schopnosti vedení protokolů umožňovat zaznamenávání událostí, které jsou relevantní pro:

   i) identifikaci situací, které mohou vést k tomu, že daný systém UI bude představovat riziko ve smyslu čl. 65 odst. 1 nebo že dojde k podstatné změně;

   ii) usnadnění monitorování po uvedení na trh uvedené v článku 61; a

   iii) sledování fungování vysoce rizikových systémů UI podle čl. 29 odst. 4.

4. U vysoce rizikových systémů UI uvedených v odst. 1 písm. a) přílohy III musí schopnosti vedení protokolů zajišťovat minimálně:

   a) záznam trvání každého použití systému (datum a čas zahájení a datum a čas ukončení každého použití);

   b) referenční databázi, s níž systém porovnává vstupní data;

   c) vstupní data, u nichž vyhledávání vedlo ke shodě;

   d) identifikaci fyzických osob podílejících se na ověřování výsledků, jak je uvedeno v čl. 14 odst. 5.

Článek 13

Transparentnost a poskytování informací uživatelům

1. Vysoce rizikové systémy UI musí být navrženy a vyvinuty tak, aby bylo jejich fungování dostatečně transparentní s cílem dosáhnout souladu s příslušnými povinnostmi uživatele a poskytovatele stanovenými v kapitole 3 této hlavy, a umožnit tak uživatelům systém náležitě pochopit a používat.

2. Vysoce rizikové systémy UI musí být opatřeny návodem k použití ve vhodném digitálním nebo jiném formátu, který obsahuje stručné, úplné, správné a jasné informace, které jsou pro uživatele relevantní, přístupné a srozumitelné.

3. Informace podle odstavce 2 uvádějí:

   a) totožnost a kontaktní údaje poskytovatele a tam, kde je to relevantní, jeho zplnomocněného zástupce;

   b) vlastnosti, schopnosti a omezení výkonnosti vysoce rizikového systému UI, včetně:

      i) jeho zamýšleného účelu, včetně konkrétního zeměpisného, behaviorálního nebo funkčního prostředí, v němž má být daný vysoce rizikový systém UI používán;

      ii) úrovně přesnosti, včetně jeho metrik, spolehlivosti a kybernetické bezpečnosti uvedené v článku 15, ve vztahu k níž byl daný vysoce rizikový systém UI testován a ověřen a kterou lze očekávat, a jakékoli známé a předvídatelné okolnosti, které mohou mít na tuto očekávanou úroveň přesnosti, spolehlivost a kybernetické bezpečnosti dopad;

      iii) jakýchkoli známých nebo předvídatelných okolností souvisejících s používáním daného vysoce rizikového systému UI v souladu s jeho určeným účelem, které mohou vést k rizikům pro zdraví a bezpečnost nebo pro základní práva podle čl. 9 odst. 2;

iv) případně jeho chování ve vztahu ke konkrétním osobám nebo skupinám osob, na něž má být systém používán;

v) případně specifikací vstupních údajů nebo jakýchkoli dalších informací příslušných z hlediska použitých souborů tréninkových dat, dat pro ověřování platnosti a testovacích dat při zohlednění určeného účelu systému UI;

vi) případně popisu očekávaného výstupu systému.

c) změny vysoce rizikového systému UI a jeho výkonnosti, které poskytovatel stanovil předem v okamžiku počátečního posouzení shody;

d) opatření v oblasti lidského dohledu uvedená v článku 14, včetně technických opatření zavedených za účelem usnadnění interpretace výstupů systémů UI ze strany uživatelů;

e) potřebné výpočetní a hardwarové zdroje, očekávanou životnost vysoce rizikového systému UI a veškerá nezbytná opatření v oblasti údržby a péče, včetně jejich frekvence, umožňující zajistit řádné fungování tohoto systému UI, včetně aktualizací softwaru;

f) popis mechanismu zahrnutého do systému UI, který v relevantních případech uživatelům umožňuje řádně shromažďovat, uchovávat a interpretovat protokoly.

Článek 14

Lidský dohled

1. Vysoce rizikové systémy UI musí být navrženy a vyvinuty takovým způsobem, a to i pomocí vhodných nástrojů rozhraní člověk-stroj, aby na ně mohly během období, kdy je daný systém UI používán, účinně dohlížet fyzické osoby.

2. Lidský dohled je zaměřen na prevenci nebo minimalizaci rizik pro zdraví, bezpečnost nebo základní práva, která mohou vzniknout při používání vysoce rizikového systému UI v souladu s jeho určeným účelem nebo za podmínek důvodně předvídatelného nesprávného použití, zejména pokud tato rizika přetrvávají bez ohledu na uplatňování dalších požadavků stanovených v této kapitole.

3. Lidský dohled je zajištěn prostřednictvím jednoho nebo všech následujících druhů opatření:

a) opatření, která identifikuje poskytovatel, a pokud je to technicky proveditelné, zabuduje je do daného vysoce rizikového systému UI před jeho uvedením na trh nebo do provozu;

b) opatření, která identifikuje poskytovatel před uvedením daného vysoce rizikového systému UI na trh nebo do provozu a u nichž je vhodné, aby je provedl uživatel.

4. Pro účely provádění odstavců 1 až 3 je vysoce rizikový systém UI poskytován uživateli takovým způsobem, aby fyzickým osobám, které jsou pověřeny lidským dohledem, umožňoval, pokud je to vhodné a přiměřené okolnostem, aby:

a) porozuměli kapacitám a omezením daného vysoce rizikového systému UI a byli schopni náležitě monitorovat jeho fungování;

b) si nadále uvědomovali možnou tendenci automatického nebo nadměrného spoléhání na výstup vysoce rizikového systému UI (dále jen „automatizační zkreslení“);

c) správně interpretovali výstup vysoce rizikového systému UI, např. dostupné interpretační nástroje a metody;

d) se v jakékoli konkrétní situaci rozhodli, že vysoce rizikový systém UI nepoužijí nebo výstup z vysoce rizikového systému UI jiným způsobem nezohlední, zruší nebo zvrátí;

e) zasáhli do fungování vysoce rizikového systému UI nebo jej přerušili tlačítkem „stop“ nebo podobným postupem.

5. U vysoce rizikových systémů UI uvedených v bodě 1 písm. a) přílohy III musí být opatření uvedená v odstavci 3 taková, aby navíc zajišťovala, že uživatel neprovede žádné kroky ani rozhodnutí na základě identifikace vyplývající z tohoto systému, pokud tato identifikace nebude samostatně ověřena a potvrzena alespoň dvěma fyzickými osobami. Požadavek na samostatné ověření nejméně dvěma fyzickými osobami se nevztahuje na vysoce rizikové systémy UI používané pro účely prosazování práva, migrace, ochrany hranic nebo azylu v případech, kdy unijní nebo vnitrostátní právo považuje uplatňování tohoto požadavku za nepřiměřené.

Článek 15

Přesnost, spolehlivost a kybernetická bezpečnost

1. Vysoce rizikové systémy UI jsou navrženy a vyvinuty tak, aby s ohledem na svůj určený účel dosahovaly odpovídající úrovně přesnosti, spolehlivosti a kybernetické bezpečnosti a aby v tomto ohledu dosahovaly konzistentních výsledků v průběhu celého svého životního cyklu.

2. Úrovně přesnosti a příslušná měřítka přesnosti vysoce rizikových systémů UI jsou oznámeny v přiloženém návodu k použití.

3. Vysoce rizikové systémy UI musí být odolné vůči chybám, poruchám nebo nesrovnalostem, které se mohou vyskytnout v daném systému nebo v prostředí, ve kterém tento systém funguje, zejména v důsledku jejich interakce s fyzickými osobami nebo jinými systémy.

   Spolehlivosti vysoce rizikových systémů UI lze dosáhnout pomocí technicky redundantních řešení, která mohou zahrnovat plány zálohování nebo zajištění proti selhání.

   Vysoce rizikové systémy UI, které se po uvedení na trh nebo do provozu dále učí, musí být vyvíjeny způsobem tak, aby se vyloučilo nebo na nejnižší možnou míru snížilo riziko, že případné zkreslené výstupy ovlivňující vstup pro budoucí operace („smyčky zpětné vazby“) budou řádně řešeny formou vhodných zmírňujících opatření.

4. Vysoce rizikové systémy UI musí být odolné proti pokusům neoprávněných třetích stran změnit jejich použití nebo výkonnost zneužitím zranitelných míst těchto systémů.

Technická řešení zaměřená na zajištění kybernetické bezpečnosti vysoce rizikových systémů UI musí odpovídat příslušným okolnostem a rizikům.

Technická řešení umožňující řešení zranitelných míst specifických pro UI zahrnují tam, kde je to vhodné, opatření pro prevenci a kontrolu útoků, které se pokoušejí manipulovat soubory tréninkových dat (tzv. data poisoning), vstupů, jejichž cílem je přimět daný model k tomu, aby udělal chybu (tzv. matoucí vzory), nebo chyb v modelech.

KAPITOLA 3

POVINNOSTI POSKYTOVATELŮ A UŽIVATELŮ VYSOCE RIZIKOVÝCH SYSTÉMŮ UI A DALŠÍCH STRAN

Článek 16

Povinnosti poskytovatelů vysoce rizikových systémů UI

Poskytovatelé vysoce rizikových systémů UI:

a) zajišťují, aby jejich vysoce rizikové systémy UI splňovaly požadavky stanovené v kapitole 2 této hlavy;

aa) uvedou na vysoce rizikovém systému UI, případně není-li to možné, podle potřeby na obalu nebo v dokumentaci, která je k vysoce rizikovému systému UI přiložena, svoje jméno, zapsaný obchodní název nebo zapsanou ochrannou známku a adresu, na které je lze kontaktovat.

b) mají zaveden systém řízení kvality, který je v souladu s článkem 17;

c) vedou dokumentaci uvedenou v článku 18;

d) pokud jsou vysoce rizikové systémy UI pod jejich kontrolou, zajišťují automatické generování protokolů těmito systémy, jak je uvedeno v článku 20;

e) zajišťují, aby byl u daného vysoce rizikového systému UI před jeho uvedením na trh nebo do provozu proveden příslušný postup posuzování shody, jak je uvedeno v článku 43;

f) dodržují povinnosti registrace uvedené v čl. 51 odst. 1;

g) přijímají nezbytná nápravná opatření podle článku 21 v případě, že daný vysoce rizikový systém UI není v souladu s požadavky stanovenými v kapitole 2 této hlavy;

h) informují příslušný vnitrostátní orgán členských států, do kterého daný systém UI dodali nebo jej uvedli do provozu, a případně oznámený subjekt o nesouladu a o případných přijatých nápravných opatřeních;

i) umisťují na své vysoce rizikové systémy UI označení CE, aby vyjádřili jejich soulad s tímto nařízením podle článku 49;

j) na žádost příslušného vnitrostátního orgánu prokazují soulad daného vysoce rizikového systému UI s požadavky stanovenými v kapitole 2 této hlavy.

Článek 17

Systém řízení kvality

1. Poskytovatelé vysoce rizikových systémů UI zavádějí systém řízení kvality, který zajišťuje soulad s tímto nařízením. Tento systém je systematicky a řádně dokumentován formou písemných politik, postupů a pokynů a obsahuje alespoň tyto aspekty:

   a) strategii pro zajištění souladu s právními předpisy, včetně souladu s postupy posuzování shody a postupy pro řízení úprav daného vysoce rizikového systému UI;

b) techniky, postupy a systematická opatření využívaná při vytváření, kontrole a ověřování návrhu vysoce rizikového systému UI;

c) techniky, postupy a systematická opatření využívaná při vývoji, kontrole a zajišťování kvality daného vysoce rizikového systému UI;

d) vyšetřovací, testovací a ověřovací postupy prováděné před vývojem vysoce rizikového systému UI, během něho a po něm, a četnost, s níž musí být prováděny;

e) technické specifikace, včetně norem, které mají být uplatňovány, a pokud nejsou příslušné harmonizované normy uplatňovány v plném rozsahu, prostředky, které mají být použity k zajištění toho, aby vysoce rizikový systém UI splňoval požadavky stanovené v kapitole 2 této hlavy;

f) systémy a postupy pro správu dat, včetně shromažďování, analýzy, označování, ukládání, filtrace, vytěžování, agregace a uchovávání dat a jakékoli další operace týkající se dat, které se provádějí před uvedením vysoce rizikových systémů UI na trh nebo do provozu a pro účely tohoto uvedení;

g) systém řízení rizik podle článku 9;

h) vytvoření, uplatňování a udržování systému monitorování po uvedení na trh v souladu s článkem 61;

i) postupy týkající se ohlašování závažného incidentu v souladu s článkem 62;

j) řešení komunikace s příslušnými vnitrostátními orgány a příslušnými orgány, včetně odvětvových orgánů, a zajišťování nebo podporu přístupu k datům, k oznámeným subjektům, k jiným provozovatelům, zákazníkům nebo k jiným zúčastněným stranám;

k) systémy a postupy pro uchovávání záznamů o veškeré příslušné dokumentaci a informacích;

l) řízení zdrojů, včetně opatření souvisejících s bezpečností dodávek;

m) rámec odpovědnosti stanovující odpovědnost vedení a ostatních zaměstnanců ve vztahu ke všem aspektům uvedeným v tomto odstavci.

2. Provádění aspektů uvedených v odstavci 1 musí být přiměřené velikosti organizace poskytovatele.

2a. V případě poskytovatelů vysoce rizikových systémů UI, na něž se vztahují povinnosti týkající se systémů řízení kvality podle příslušných odvětvových právních předpisů Unie, mohou být aspekty popsané v odstavci 1 součástí systémů řízení kvality stanovených podle uvedeného práva.

3. V případě poskytovatelů, kteří jsou finančními institucemi, na něž se vztahují požadavky týkající se jejich vnitřní správy, systémů nebo postupů podle právních předpisů Unie v oblasti finančních služeb, se povinnost zavést systém řízení kvality, s výjimkou odst. 1 písm. g), h) a i), považuje za splněnou, jsou-li dodržena pravidla týkající se systémů nebo postupů vnitřní správy podle příslušných právních předpisů Unie v oblasti finančních služeb. V této souvislosti se zohlední veškeré harmonizované normy uvedené v článku 40 tohoto nařízení.

Článek 18

Uchovávání dokumentace

1. Poskytovatel uchovává po dobu deseti let od uvedení systému UI na trh nebo do provozu pro potřebu příslušných vnitrostátních orgánů následující dokumenty:

a) technickou dokumentaci uvedenou v článku 11;

b) dokumentaci týkající se systému řízení kvality uvedenou v článku 17;

c) tam, kde je to relevantní, dokumentaci týkající se změn schválených oznámenými subjekty;

d) tam, kde je to relevantní, rozhodnutí a další dokumenty vydané oznámenými subjekty;

e) EU prohlášení o shodě podle článku 48.

1a. Každý členský stát stanoví podmínky, za nichž dokumentace uvedená v odstavci 1 zůstává k dispozici příslušným vnitrostátním orgánům po dobu stanovenou v uvedeném odstavci pro případy, kdy poskytovatel nebo jeho zplnomocněný zástupce usazený na jeho území vyhlásí úpadek nebo ukončí svou činnost před koncem tohoto období.

2. Poskytovatelé, kteří jsou finančními institucemi, na něž se vztahují požadavky týkající se jejich vnitřní správy, systémů nebo postupů podle právních předpisů Unie v oblasti finančních služeb, udržují technickou dokumentaci jako součást dokumentace vedené podle příslušných právních předpisů Unie v oblasti finančních služeb.

Článek 19

Posuzování shody

1. Poskytovatelé vysoce rizikových systémů UI zajišťují, že bude u jejich vysoce rizikových systémů UI před uvedením na trh nebo do provozu proveden příslušný postup posuzování shody v souladu s článkem 43. Pokud je po tomto posouzení shody prokázán soulad daných systémů UI s požadavky stanovenými v kapitole 2 této hlavy, vypracují poskytovatelé EU prohlášení o shodě v souladu s článkem 48 a umístí označení shody CE v souladu s článkem 49.

2. [vypouští se]

Článek 20

Automaticky generované protokoly

1. Poskytovatelé vysoce rizikových systémů UI, uvedených v čl. 12 odst. 1, uchovávají protokoly automaticky generované jejich vysoce rizikovými systémy UI v rozsahu, v jakém jsou tyto protokoly pod jejich kontrolou na základě smluvního ujednání s uživatelem nebo jinak na základě právních předpisů. Uchovávají je po dobu nejméně šesti měsíců, nestanoví-li jinak platné právní předpisy Unie nebo vnitrostátní právní předpisy, zejména právní předpisy Unie o ochraně osobních údajů.

2. Poskytovatelé, kteří jsou finančními institucemi, na něž se vztahují požadavky týkající se jejich vnitřní správy, systémů nebo postupů podle právních předpisů Unie v oblasti finančních služeb, uchovávají protokoly automaticky generované jejich vysoce rizikovými systémy UI jako součást dokumentace vedené podle příslušných právních předpisů v oblasti finančních služeb.

Článek 21

Nápravná opatření

Poskytovatelé vysoce rizikových systémů UI, kteří se domnívají nebo mají důvod se domnívat, že vysoce rizikový systém UI, který uvedli na trh nebo do provozu, není ve shodě s tímto nařízením, v příslušných případech okamžitě vyšetří příčiny ve spolupráci s ohlašujícím uživatelem a přijmou nezbytná nápravná opatření k uvedení daného systému ve shodu nebo k jeho případnému stažení z trhu či z oběhu. Náležitě informují distributory dotčeného vysoce rizikového systému UI a tam, kde je to relevantní, zplnomocněného zástupce a dovozce.

Článek 22

Informační povinnost

Pokud vysoce rizikový systém UI představuje riziko ve smyslu čl. 65 odst. 1 a toto riziko je poskytovateli systému známo, informuje tento poskytovatel okamžitě příslušné vnitrostátní orgány členských států, do kterých tento systém dodal, a tam, kde je to relevantní, oznámený subjekt, který vydal pro daný vysoce rizikový systém UI certifikát, a uvede při tom zejména informace o nesouladu a o veškerých přijatých nápravných opatřeních.

Článek 23

Spolupráce s příslušnými orgány

Poskytovatelé vysoce rizikových systémů UI předloží příslušnému vnitrostátnímu orgánu na požádání všechny informace a dokumentaci nezbytné k prokázání shody vysoce rizikového systému UI s požadavky stanovenými v kapitole 2 této hlavy, v jazyce, kterému může orgán dotčeného členského státu snadno rozumět. Na základě odůvodněné žádosti příslušného vnitrostátního orgánu mu poskytovatelé poskytnou také přístup k protokolům, uvedených v čl. 12 odst. 1, automaticky generovaným jejich vysoce rizikovým systémem UI v rozsahu, v jakém jsou tyto protokoly pod jejich kontrolou na základě smluvního ujednání s uživatelem nebo jinak na základě právních předpisů.

Článek 23a

Podmínky, za nichž se povinnosti poskytovatele vztahují na jiné osoby

1. Jakákoli fyzická nebo právnická osoba se pro účely tohoto nařízení považuje za poskytovatele nového vysoce rizikového systému UI a vztahují se na ni povinnosti poskytovatele podle článku 16, pokud nastane kterákoli z následujících okolností:

    a) uvede své jméno nebo ochrannou známku na vysoce rizikovém systému UI, který již byl uveden na trh nebo do provozu, aniž jsou dotčena smluvní ujednání, která stanoví, že povinnosti jsou rozděleny jiným způsobem;

b) [vypouští se]

c) provede podstatnou změnu vysoce rizikového systému UI již uvedeného na trh nebo do provozu;

d) mění zamýšlený účel systému UI, který není vysoce rizikový a již byl uveden na trh nebo do provozu, takovým způsobem, že se z tohoto změněného systému stává vysoce rizikový systém UI.

e) uvede na trh nebo do provozu obecný systém UI jako vysoce rizikový systém UI nebo jako součást vysoce rizikového systému UI.

2. Pokud nastanou okolnosti uvedené v odst. 1 písm. a) nebo c), není poskytovatel, který původně uvedl vysoce rizikový systém UI na trh nebo do provozu, již nadále považován za poskytovatele pro účely tohoto nařízení.

3. V případě vysoce rizikových systémů UI, které jsou bezpečnostními součástmi produktů, na něž se vztahují právní akty uvedené v příloze II oddíle A, se výrobce těchto produktů považuje za poskytovatele vysoce rizikového systému UI a vztahují se na něj povinnosti podle článku 16 podle jednoho z těchto scénářů:

i) vysoce rizikový systém UI je uváděn na trh společně s výrobkem pod jménem nebo ochrannou známkou výrobce produktu;

ii) vysoce rizikový systém UI je uveden do provozu pod jménem nebo ochrannou známkou výrobce produktu poté, co byl výrobek uveden na trh.

Článek 24

[vypouští se]

Článek 25

Zplnomocnění zástupci

1. V případě, že poskytovatelé usazení mimo Unii dodávají do Unie systémy umělé inteligence, jmenují předem zplnomocněného zástupce usazeného v Unii formou písemného pověření.

2. Zplnomocněný zástupce provádí úkoly vymezené v pověření, které obdržel od poskytovatele. Pro účely tohoto nařízení zmocňuje pověření zplnomocněného zástupce k provádění alespoň těchto úkolů:

-a) ověřit, zda bylo vypracováno EU prohlášení o shodě a technická dokumentace a zda poskytovatel provedl příslušný postup posuzování shody;

a) uchovávat pro potřebu příslušných vnitrostátních orgánů a vnitrostátních orgánů uvedených v čl. 63 odst. 7 po dobu deseti let od uvedení vysoce rizikového systému UI na trh nebo do provozu kontaktní údaje poskytovatele, jehož zplnomocněný zástupce byl jmenován, kopii EU prohlášení o shodě, technickou dokumentaci a případně certifikát vydaný oznámeným subjektem;

b) poskytnout příslušnému vnitrostátnímu orgánu na odůvodněnou žádost veškeré informace a dokumentaci, včetně té, jež se uchovává v souladu s písmenem b), nezbytné k prokázání shody vysoce rizikového systému UI s požadavky stanovenými v kapitole 2 této hlavy, včetně přístupu k protokolům, uvedených v čl. 12 odst. 1, které daný vysoce rizikový systém UI automaticky generuje, v rozsahu, v jakém jsou tyto protokoly pod kontrolou poskytovatele na základě smluvního ujednání s uživatelem nebo jinak na základě zákona;

c) spolupracovat s příslušnými vnitrostátními orgány na základě odůvodněné žádosti na veškerých opatřeních, která takový orgán v souvislosti s daným vysoce rizikovým systémem UI přijme;

d) splnit registrační povinnosti uvedené v čl. 51 odst. 1, a pokud registraci systému provádí sám poskytovatel, ověřit, zda jsou informace uvedené v příloze VIII části II bodech 1 až 11 správné.

Zplnomocněný zástupce mandát ukončí, pokud má dostatečné důvody se domnívat, že poskytovatel jedná v rozporu se svými povinnostmi podle tohoto nařízení. V takovém případě rovněž neprodleně informuje orgán dozoru nad trhem členského státu, v němž je usazen, a případně příslušný oznámený subjekt o ukončení pověření a jeho důvodech.

Zplnomocněný zástupce nese právní odpovědnost za vadné systémy UI na stejném základě a společně a nerozdílně s poskytovatelem, pokud jde o jeho potenciální odpovědnost podle směrnice Rady 85/374/EHS.

Článek 26

Povinnosti dovozců

1. Před uvedením vysoce rizikového systému UI na trh dovozci tohoto systému zajistí, aby byl systém v souladu s tímto nařízením, a to tím, že ověří, že:

a) poskytovatel daného systému UI provedl příslušný postup posuzování shody uvedený v článku 43;

b) poskytovatel vypracoval technickou dokumentaci v souladu s přílohou IV;

c) systém nese požadované označení shody CE a je k němu přiloženo EU prohlášení o shodě a návod k použití;

d) poskytovatel stanovil zplnomocněného zástupce podle článku 25.

2. Má-li dovozce dostatečné důvody se domnívat, že vysoce rizikový systém UI není ve shodě s tímto nařízením nebo že je zfalšovaný či je k němu připojena zfalšovaná dokumentace, neuvede tento systém UI na trh, dokud nebude uveden ve shodu. Pokud vysoce rizikový systém UI představuje riziko ve smyslu čl. 65 odst. 1, informuje o tom dovozce poskytovatele systému UI, zplnomocněné zástupce a orgány dozoru nad trhem.

3. Dovozci uvedou na vysoce rizikovém systému UI, případně není-li to možné, podle potřeby na obalu nebo v dokumentaci, která je k vysoce rizikovému systému UI přiložena, svoje jméno, zapsaný obchodní název nebo zapsanou ochrannou známku a adresu, na které je lze kontaktovat.

4. Dovozci zajistí, aby v době, kdy nesou za vysoce rizikový systém UI odpovědnost, tam, kde je to relevantní, skladovací nebo přepravní podmínky neohrožovaly jeho soulad s požadavky stanovenými v kapitole 2 této hlavy.

4a. Dovozci uchovávají po dobu deseti let od uvedení systému UI na trh nebo do provozu kopii případného certifikátu vydaného oznámeným subjektem o návodu k použití a EU prohlášení o shodě.

5. Dovozci poskytnou příslušným vnitrostátním orgánům na odůvodněnou žádost veškeré informace a dokumentaci, včetně informací a dokumentace uchovávaných v souladu s odstavcem 5, nezbytné k prokázání shody vysoce rizikového systému UI s požadavky stanovenými v kapitole 2 této hlavy v jazyce, který je příslušnému vnitrostátnímu orgánu snadno srozumitelný. Za tímto účelem rovněž zajistí, aby těmto orgánům mohla být zpřístupněna technická dokumentace.

5a. Dovozci spolupracují s příslušnými vnitrostátními orgány na veškerých opatřeních, která tyto orgány přijmou v souvislosti se systémem UI, jejž dovážejí.

Článek 27

Povinnosti distributorů

1. Před dodáním vysoce rizikového systému UI na trh distributoři ověří, zda je na daném vysoce rizikovém systému UI umístěno požadované označení CE, zda je k němu přiloženo EU prohlášení o shodě a návod k použití a zda poskytovatel a případně dovozce systému splnili své povinnosti stanovené v čl. 16. písm. b) a čl. 26 odst. 3.

2. Domnívá-li se distributor nebo má-li důvod se domnívat, že vysoce rizikový systém UI není ve shodě s požadavky stanovenými v kapitole 2 této hlavy, neuvede tento vysoce rizikový systém UI na trh, dokud nebude uveden ve shodu s těmito požadavky. Pokud navíc tento systém představuje riziko ve smyslu čl. 65 odst. 1, informuje o tom distributor poskytovatele, případně dovozce tohoto systému.

3. Distributoři zajistí, aby v době, kdy nesou za vysoce rizikový systém UI odpovědnost, tam, kde je to relevantní, skladovací nebo přepravní podmínky neohrožovaly soulad tohoto systému s požadavky stanovenými v kapitole 2 této hlavy.

4. Distributor, který se domnívá nebo má důvod se domnívat, že vysoce rizikový systém UI, který dodal na trh, není ve shodě s požadavky stanovenými v kapitole 2 této hlavy, přijme nápravná opatření nezbytná k uvedení tohoto systému ve shodu s těmito požadavky nebo k jeho stažení z trhu či z oběhu, případně zajistí, aby tato nápravná opatření přijal poskytovatel, dovozce nebo jakýkoli příslušný provozovatel. Představuje-li vysoce rizikový systém UI riziko ve smyslu čl. 65 odst. 1, distributor okamžitě informuje příslušné vnitrostátní orgány členských států, v nichž tento produkt za tímto účelem dodal na trh, a uvede přitom zejména podrobnosti o nesouladu a o veškerých přijatých nápravných opatřeních.

5. Na odůvodněnou žádost příslušného vnitrostátního orgánu poskytnou distributoři vysoce rizikových systémů UI tomuto orgánu všechny informace a dokumentaci týkající se činností uvedených v odstavcích 1 až 4.

5a. Distributoři spolupracují s příslušnými vnitrostátními orgány na veškerých opatřeních, která tyto orgány přijmou v souvislosti se systémem UI, jejž distribuují.

Článek 28

[vypouští se]

Článek 29

Povinnosti uživatelů vysoce rizikových systémů UI

1. Uživatelé vysoce rizikových systémů UI tyto systémy používají v souladu s návodem k použití přiloženým k těmto systémům na základě odstavců 2 a 5 tohoto článku.

1a. Uživatelé pověří lidským dohledem fyzické osoby, které k tomu mají nezbytnou způsobilost, odbornou přípravu a pravomoc.

2. Povinnostmi uvedenými v odstavcích 1 a 1a nejsou dotčeny ostatní povinnosti uživatelů podle právních předpisů Unie nebo vnitrostátních právních předpisů ani volnost uživatelů při organizaci vlastních zdrojů a činností za účelem provádění opatření v oblasti lidského dohledu uvedených poskytovatelem.

3. Aniž je dotčen odstavec 1, zajistí uživatel, aby byla vstupní data relevantní s ohledem na určený účel vysoce rizikového systému UI v rozsahu, v jakém uživatel vykonává kontrolu nad vstupními údaji.

4. Uživatelé vykonávají lidský dohled a monitorují provoz vysoce rizikového systému UI na základě návodu k použití. Pokud mají důvody se domnívat, že použití v souladu s návodem k použití může vést k tomu, že systém UI bude představovat riziko ve smyslu čl. 65 odst. 1, uvědomí o tom poskytovatele nebo distributora a používání systému pozastaví. V případě, že zjistí jakýkoliv závažný incident, rovněž informují poskytovatele nebo distributora a používání daného systému UI přeruší. V případě, že se uživateli nepodaří poskytovatele kontaktovat, použije se obdobně článek 62. Tato povinnost se nevztahuje na citlivé provozní údaje uživatelů systémů UI, kteří jsou donucovacími orgány.

V případě uživatelů, kteří jsou finančními institucemi, na něž se vztahují požadavky týkající se jejich vnitřní správy, systémů nebo postupů podle právních předpisů Unie v oblasti finančních služeb, se povinnost monitorování stanovená v prvním pododstavci považuje za splněnou, jsou-li dodržena pravidla týkající se systémů, postupů a mechanismů vnitřní správy podle příslušných právních předpisů Unie v oblasti finančních služeb.

5. Uživatelé vysoce rizikových systémů UI, uvedených v čl. 12 odst. 1, uchovávají protokoly automaticky generované jejich vysoce rizikovým systémem UI v rozsahu, v jakém jsou tyto protokoly pod jejich kontrolou. Uchovávají je po dobu nejméně šesti měsíců, nestanoví-li jinak platné právní předpisy Unie nebo vnitrostátní právní předpisy, zejména právní předpisy Unie o ochraně osobních údajů.

Uživatelé, kteří jsou finančními institucemi, na něž se vztahují požadavky týkající se jejich vnitřní správy, systémů nebo postupů podle právních předpisů Unie v oblasti finančních služeb, udržují protokoly jako součást dokumentace vedené podle příslušných právních předpisů Unie v oblasti finančních služeb.

5a. Uživatelé vysoce rizikových systémů UI, které jsou veřejnými orgány, agenturami nebo subjekty, s výjimkou donucovacích orgánů, orgánů ochrany hranic, imigračních nebo azylových orgánů, dodržují registrační povinnosti uvedené v článku 51. Pokud zjistí, že systém, který hodlají používat, nebyl zaregistrován v databázi EU uvedené v článku 60, nesmí tento systém používat a informují o tom poskytovatele nebo distributora.

6. Uživatelé vysoce rizikových systémů UI použijí informace poskytnuté podle článku 13 ke splnění své povinnosti provést posouzení vlivu na ochranu osobních údajů podle článku 35 nařízení (EU) 2016/679 nebo v relevantních případech podle článku 27 směrnice (EU) 2016/680.

6a. Uživatelé spolupracují s příslušnými vnitrostátními orgány na veškerých opatřeních, která tyto orgány přijmou v souvislosti se systémem UI, jejž distribuují.

KAPITOLA 4

OZNAMUJÍCÍ ORGÁNY A OZNÁMENÉ SUBJEKTY

Článek 30

Oznamující orgány

1. Každý členský stát jmenuje nebo určí alespoň jeden oznamující orgán odpovědný za stanovení a provádění postupů nezbytných pro posuzování, jmenování a oznamování subjektů posuzování shody a za jejich monitorování.

2. Členské státy mohou rozhodnout o tom, že posuzování a monitorování uvedené v odstavci 1 provádí vnitrostátní akreditační orgán ve smyslu nařízení (ES) č. 765/2008 a v souladu s ním.

3. Oznamující orgány musí být zřízeny, organizovány a fungovat tak, aby nedocházelo k žádným střetům zájmů se subjekty posuzování shody a aby byla chráněna objektivita a nestrannost jejich činností.

4. Oznamující orgány jsou organizovány tak, aby bylo rozhodnutí týkající se oznámení subjektů posuzování shody přijímáno příslušnými osobami, které jsou jinými osobami než osoby, které posuzování těchto subjektů prováděly.

5. Oznamující orgány nenabízejí ani neposkytují žádné činnosti, které provádějí subjekty posuzování shody, ani žádné poradenské služby na komerčním nebo konkurenčním základě.

6. Oznamující orgány zachovají důvěrnost informací získaných v souladu s článkem 70.

7. Oznamující orgány mají k dispozici přiměřený počet kvalifikovaných pracovníků, aby mohly řádně vykonávat své povinnosti.

8. [vypouští se]

Článek 31

Žádost subjektu posuzování shody o oznámení

1. Subjekty posuzování shody podávají žádost o oznámení oznamujícímu orgánu členského státu, v němž jsou usazeny.

2. Součástí žádosti o oznámení je popis činností posuzování shody, modulu nebo modulů posuzování shody a systémů UI, pro něž se subjekt posuzování shody prohlašuje za způsobilý, jakož i osvědčení o akreditaci, pokud existuje, vydané vnitrostátním akreditačním orgánem, které potvrzuje, že subjekt posuzování shody splňuje požadavky stanovené v článku 33. Přikládá se rovněž jakýkoli platný dokument týkající se stávajících jmenování žádajícího oznámeného subjektu podle jiných harmonizačních právních předpisů Unie.

3. Nemůže-li dotčený subjekt posuzování shody předložit osvědčení o akreditaci, poskytne oznamujícímu orgánu veškeré doklady nezbytné k ověření, uznání a pravidelné kontrole svého souladu s požadavky stanovenými v článku 33. U oznámených subjektů, které jsou jmenovány podle jiných harmonizačních právních předpisů Unie, lze případně pro doložení postupů jmenování podle tohoto nařízení použít veškeré dokumenty a certifikáty související s tímto jmenováním. Oznámený subjekt aktualizuje dokumentaci uvedenou v odstavcích 2 a 3, a to kdykoli dojde k významným změnám, aby umožnil orgánu odpovědnému za oznámené subjekty monitorovat a ověřovat nepřetržitý soulad se všemi požadavky stanovenými v článku 33.

Článek 32

Postup oznamování

1. Oznamující orgány mohou oznámit pouze subjekty posuzování shody, které splňují požadavky stanovené v článku 33.

2. K oznámení těchto subjektů Komisi a ostatním členským státům využijí oznamující orgány elektronický nástroj pro oznamování vyvinutý a spravovaný Komisí.

3. Oznámení uvedené v odstavci 2 musí obsahovat veškeré podrobnosti o dotčených činnostech posuzování shody, modulu nebo modulech posuzování shody a systémech UI a příslušné potvrzení o způsobilosti. Pokud se oznámení nezakládá na osvědčení o akreditaci uvedeném v čl. 31 odst. 2, poskytne oznamující orgán Komisi a ostatním členským státům podklady, které prokazují způsobilost subjektu posuzování shody, a informace o zavedených opatřeních k zajištění toho, aby byl subjekt pravidelně kontrolován a i v budoucnu splňoval požadavky stanovené v článku 33.

4. Dotčený subjekt posuzování shody může vykonávat činnosti oznámeného subjektu, pouze pokud proti tomu Komise nebo ostatní členské státy nevznesly námitky do dvou týdnů od oznámení oznamujícího orgánu, obsahuje-li osvědčení o akreditaci podle čl. 31 odst. 2, nebo do dvou měsíců od oznámení, obsahuje-li doklady podle čl. 31 odst. 3.

5. [vypouští se]

Článek 33

Požadavky týkající se oznámených subjektů

1. Oznámený subjekt se zřizuje podle vnitrostátních právních předpisů a musí mít právní subjektivitu.

2. Oznámené subjekty splňují organizační požadavky a požadavky na řízení kvality, zdroje a postupy, které jsou k plnění uvedených úkolů nezbytné.

3. Organizační struktura, rozdělení povinností, hierarchické vztahy a fungování oznámených subjektů musí být takové, aby zajišťovaly důvěru ve výkon oznámených subjektů a ve výsledky činností posuzování shody, které oznámené subjekty provádějí.

4. Oznámené subjekty jsou nezávislé na poskytovateli vysoce rizikového systému UI, u něhož provádějí činnosti posuzování shody. Oznámené subjekty jsou rovněž nezávislé na jakémkoliv jiném provozovateli, který má na posuzovaném vysoce rizikovém systému UI zájem, i na jakýchkoliv konkurentech poskytovatele.

5. Oznámené subjekty jsou organizovány a provozovány tak, aby byla zaručena nezávislost, objektivita a nestrannost jejich činností. Oznámené subjekty musí zdokumentovat a zavést strukturu a postupy pro zajištění nestrannosti a pro prosazování a uplatňování zásad nestrannosti v rámci celé své organizace, všech činností posuzování a u všech pracovníků.

6. Oznámené subjekty musí mít zavedeny zdokumentované postupy zajišťující, aby jejich pracovníci, výbory, pobočky, subdodavatelé a jakýkoliv přidružený subjekt nebo pracovníci externích subjektů zachovávali důvěrnost informací v souladu s článkem 70 získaných při provádění činností posuzování shody, s výjimkou případů, kdy je zveřejnění těchto informací ze zákona povinné. Zaměstnanci oznámených subjektů jsou povinni zachovávat služební tajemství, pokud jde o veškeré informace, které obdrželi při plnění svých úkolů podle tohoto nařízení, nikoli však ve vztahu k oznamujícím orgánům členského státu, v němž vykonávají svou činnost.

7. Oznámené subjekty mají k dispozici postupy pro provádění činností, jež řádně zohledňují velikost podniků, odvětví, v němž působí, jejich strukturu a míru složitosti daného systému UI.

8. Oznámené subjekty uzavřou vhodné pojištění odpovědnosti za škodu s ohledem na své činnosti v oblasti posuzování shody, pokud tuto odpovědnost nepřevzal členský stát, v němž se nacházejí, v souladu s vnitrostátními právními předpisy nebo pokud není tento členský stát za posuzování shody sám přímo odpovědný.

9. Oznámené subjekty musí být schopny provádět všechny úkoly, které se na ně podle tohoto nařízení vztahují, při nejvyšší úrovni profesní bezúhonnosti a náležité způsobilosti v této konkrétní oblasti bez ohledu na to, zda jsou uvedené úkoly prováděny samotnými oznámenými subjekty, nebo jejich jménem a na jejich odpovědnost.

10. Oznámené subjekty mají dostatečnou interní způsobilost, aby byly schopny účinně hodnotit úkoly, které jejich jménem provádějí externí strany. Oznámený subjekt má neustále k dispozici dostatek administrativních, technických, právních a vědeckých pracovníků se zkušenostmi a znalostmi ohledně příslušných technologií umělé inteligence, dat a datových výpočtů, jakož i požadavků uvedených v kapitole 2 této hlavy.

11. Oznámené subjekty se podílejí na koordinačních činnostech uvedených v článku 38. Rovněž se přímo účastní činnosti evropských normalizačních organizací nebo jsou v nich zastoupeny, případně zajistí, aby měly povědomí a aktuální informace o příslušných normách.

12. [vypouští se]

Článek 33a

Předpoklad shody s požadavky týkajícími se oznámených subjektů

Pokud subjekt posuzování shody prokáže svou shodu s kritérii stanovenými v příslušných harmonizovaných normách nebo jejich částech, na něž byly zveřejněny odkazy v *Úředním věstníku Evropské unie*, předpokládá se, že splňuje požadavky stanovené v článku 33 v rozsahu, v němž se harmonizované normy na tyto požadavky vztahují.

Článek 34

Dceřiné společnosti oznámených subjektů a zadávání subdodávek

1. Pokud oznámený subjekt zadá konkrétní úkoly týkající se posuzování shody subdodavateli nebo dceřiné společnosti, zajistí, že subdodavatel nebo dceřiná společnost splňuje požadavky stanovené v článku 33, a informuje o tom oznamující orgán.

2. Oznámené subjekty nesou plnou odpovědnost za úkoly provedené subdodavateli nebo dceřinými společnostmi bez ohledu na to, kde jsou tito subdodavatelé nebo dceřiné společnosti usazeni.

3. Činnosti lze zadat subdodavateli nebo dceřiné společnosti pouze se souhlasem poskytovatele.

4. Příslušné doklady týkající se posouzení kvalifikací subdodavatele nebo dceřiné společnosti a práce provedené subdodavatelem nebo dceřinou společností podle tohoto nařízení se uchovávají k dispozici oznamujícímu orgánu po dobu pěti let ode dne ukončení subdodavatelské činnosti.

Článek 34a

Povinnosti týkající se činnosti oznámených subjektů

1. Oznámené subjekty ověřují shodu daného vysoce rizikového systému UI v souladu s postupy posuzování shody uvedenými v článku 43.

2. Oznámené subjekty provádějí činnosti, přičemž zároveň zabraňují zbytečné zátěži pro poskytovatele a řádně zohledňují velikost podniku, odvětví, v němž působí, jeho strukturu a míru složitosti daného vysoce rizikového systému UI. Oznámený subjekt však musí dodržovat míru přísnosti a úroveň ochrany, jež jsou vyžadovány, aby byl vysoce rizikový systém UI v souladu s požadavky tohoto nařízení.

3. Oznámené subjekty na požádání zpřístupní a předloží veškerou příslušnou dokumentaci, včetně dokumentace poskytovatelů oznamujícímu orgánu uvedenému v článku 30 s cílem umožnit tomuto orgánu provádět činnosti související s posuzováním, jmenováním, oznamováním a monitorováním a usnadnit posuzování uvedené v této kapitole.

Článek 35

Identifikační čísla a seznamy oznámených subjektů jmenovaných podle tohoto nařízení

1. Komise oznámeným subjektům přiděluje identifikační číslo. Přidělí jim jediné číslo i v případě, že je daný subjekt oznámen podle několika aktů Unie.

2. Komise zveřejní seznam subjektů oznámených podle tohoto nařízení, včetně identifikačních čísel, která jim byla přidělena, a činností, pro něž byly oznámeny. Komise zajistí, aby byl tento seznam průběžně aktualizován.

Článek 36

Změny v oznámeních

1. Oznamující orgán oznámí Komisi a ostatním členským státům veškeré významné změny oznámení učiněných oznámeným subjektem prostřednictvím elektronického nástroje pro oznamování uvedeného v čl. 32 odst. 2.

2. Postupy popsané v článcích 31 a 32 se použijí na rozšíření rozsahu oznámení. V případě jiných změn oznámení, než jsou rozšíření jeho rozsahu, se použijí postupy stanovené v následujících odstavcích.

Pokud se oznámený subjekt rozhodne svou činnost v oblasti posuzování shody ukončit, co nejdříve a v případě plánovaného ukončení jeden rok předtím, než svou činnost ukončí, informuje oznamující orgán a dotčené poskytovatele. Po ukončení činnosti oznámeného subjektu mohou certifikáty zůstat dočasně v platnosti po dobu devíti měsíců za podmínky, že jiný oznámený subjekt písemně potvrdí, že za systémy UI, na něž se tyto certifikáty vztahují, převezme odpovědnost. Nový oznámený subjekt provede úplné posouzení systémů UI, jichž se dotkne konec uvedené lhůty před vydáním nových certifikátů pro tyto systémy. Pokud oznámený subjekt ukončil svou činnost, oznamující orgán jmenování zruší.

3. Pokud má oznamující orgán dostatečné důvody se domnívat, že oznámený subjekt již nesplňuje požadavky stanovené v článku 33 nebo neplní své povinnosti, oznamující orgán za předpokladu, že měl oznámený subjekt příležitost oznámit svá stanoviska, omezí, pozastaví nebo případně zruší oznámení podle toho, jak je neplnění těchto požadavků nebo povinností závažné. Neprodleně o tom informuje Komisi a ostatní členské státy.

4. Pokud bylo jeho jmenování pozastaveno, omezeno nebo zcela či částečně zrušeno, daný oznámený subjekt o tom nejpozději do 10 dnů uvědomí dotčené výrobce.

5. V případě omezení, pozastavení nebo zrušení oznámení učiní oznamující orgán náležité kroky, aby zajistil, že spisy dotčeného oznámeného subjektu jsou vedeny a na vyžádání zpřístupněny oznamujícím orgánům v jiných členských státech, jakož i orgánům dozoru nad trhem.

6. V případě omezení, pozastavení nebo zrušení jmenování oznamující orgán:

   a) posoudí dopad na certifikáty vydané oznámeným subjektem;

   b) předloží zprávu o svých zjištěních Komisi a ostatním členským státům do tří měsíců poté, co oznámil změny oznámení;

   c) požádá oznámený subjekt, aby v přiměřeném časovém období stanoveném tímto orgánem pozastavil nebo zrušil veškeré certifikáty, které byly neoprávněně vydány, s cílem zajistit shodu systémů UI, jež jsou na trhu;

   d) informuje Komisi a členské státy o certifikátech, jejichž pozastavení nebo zrušení požaduje;

e) poskytne příslušným vnitrostátním orgánům členského státu, v němž má poskytovatel své sídlo, veškeré příslušné informace o certifikátech, u nichž bylo požadováno pozastavení nebo zrušení. Tento příslušný orgán přijme v případě potřeby vhodná opatření s cílem zabránit možnému ohrožení zdraví, bezpečnosti nebo základních práv.

7. S výjimkou neoprávněně vydaných certifikátů a v případě, že bylo jmenování pozastaveno nebo omezeno, zůstávají certifikáty platné za těchto okolností:

a) oznamující orgán do jednoho měsíce od pozastavení nebo omezení potvrdí, že v souvislosti s certifikáty, jichž se pozastavení nebo omezení týká, neexistuje ohrožení zdraví, bezpečnosti nebo základních práv a oznamující orgán stanoví harmonogram a předpokládaná opatření za účelem nápravy nedostatků, jež byly příčinou pozastavení nebo omezení, nebo

b) oznamující orgán subjekty potvrdí, že v průběhu pozastavení či omezení nebudou vydávány, pozměňovány nebo opětovně vydávány žádné certifikáty, jichž se pozastavení či omezení týká, a uvede, zda je oznámený subjekt i nadále způsobilý monitorovat a být odpovědný za stávající certifikáty vydané na období pozastavení nebo omezení. V případě, že orgán odpovědný za oznámené subjekty rozhodne, že oznámený subjekt není způsobilý podporovat stávající vydané certifikáty, poskytovatel příslušným vnitrostátním orgánům členského státu, v němž má poskytovatel systému, na nějž se certifikát vztahuje, své sídlo, poskytne do tří měsíců od pozastavení nebo omezení písemné potvrzení o tom, že jiný kvalifikovaný oznámený subjekt dočasně přebírá funkce oznámeného subjektu v oblasti monitorování a po dobu pozastavení nebo omezení nese za certifikáty nadále odpovědnost.

8. S výjimkou neoprávněně vydaných certifikátů a v případě, že bylo jmenování zrušeno, zůstanou certifikáty v platnosti po dobu devíti měsíců za těchto podmínek:

a) pokud příslušný vnitrostátní orgán členského státu, v němž má poskytovatel systému UI, na nějž se certifikát vztahuje, své sídlo, potvrdí, že v souvislosti s dotčenými systémy není ohroženo zdraví, bezpečnost a základní práva, a rovněž

b) jiný oznámený subjekt písemně potvrdí, že převezme za dané systémy okamžitou odpovědnost a že dokončí jejich posouzení do dvanácti měsíců od zrušení jmenování.

Za podmínek stanovených v prvním pododstavci může příslušný vnitrostátní orgán členského státu, v němž má poskytovatel systému, na který se certifikát vztahuje, své sídlo, prodloužit prozatímní platnost certifikátů o další tříměsíční období, která celkově nepřesáhnou dvanáct měsíců.

Příslušný vnitrostátní orgán nebo oznámený subjekt přebírající funkce oznámeného subjektu, kterého se týká změna oznámení, o tom okamžitě informuje Komisi, ostatní členské státy a ostatní oznámené subjekty.

Článek 37

Zpochybnění způsobilosti oznámených subjektů

1. Komise v případě potřeby vyšetří všechny případy, u nichž jsou důvody pochybovat o tom, zda oznámený subjekt splňuje požadavky uvedené v článku 33.

2. Oznamující orgán předloží Komisi na vyžádání všechny informace týkající se oznámení dotčeného oznámeného subjektu.

3. Komise zajistí, aby se se všemi důvěrnými informacemi získanými v průběhu jejího šetření podle tohoto článku nakládalo jako s důvěrnými v souladu s článkem 70.

4. Pokud Komise zjistí, že oznámený subjekt nesplňuje nebo přestal splňovat požadavky uvedené v článku 33, informuje o důvodech tohoto zjištění oznamující orgán a požádá jej, aby přijal nezbytná nápravná opatření, včetně případného pozastavení, omezení nebo zrušení jmenování. Pokud oznamující orgán nezbytná nápravná opatření nepřijme, může Komise prostřednictvím prováděcích aktů oznámení pozastavit, omezit nebo zrušit. Tento prováděcí akt se přijme přezkumným postupem uvedeným v čl. 74 odst. 2.

Článek 38

Koordinace oznámených subjektů

1. Komise zajistí, aby v souvislosti s vysoce rizikovými systémy UI byla mezi oznámenými subjekty zabývajícími se postupy posuzování shody podle tohoto nařízení zavedena a řádně prováděna náležitá koordinace a spolupráce, která se provádí formou odvětvové skupiny oznámených subjektů.

2. Oznamující orgán zajistí, aby se jím oznámené subjekty účastnily práce této skupiny, a to přímo nebo prostřednictvím určených zástupců.

Článek 39

Subjekty posuzování shody třetích zemí

K provádění činnosti oznámených subjektů podle tohoto nařízení mohou být oprávněny subjekty posuzování shody zřízené podle práva třetí země, se kterou Unie uzavřela dohodu, za předpokladu, že splňují požadavky podle článku 33.

KAPITOLA 5

NORMY, POSUZOVÁNÍ SHODY, CERTIFIKÁTY, REGISTRACE

Článek 40

Harmonizované normy

1. Předpokládá se, že vysoce rizikové nebo obecné systémy UI, které jsou ve shodě s harmonizovanými normami nebo jejich částmi, na něž byly zveřejněny odkazy v *Úředním věstníku Evropské unie*, jsou ve shodě s požadavky stanovenými v kapitole 2 této hlavy nebo případně s požadavky stanovenými v článcích 4a a 4b v rozsahu, v jakém se tyto normy na dané požadavky vztahují.

2. Komise při podání žádosti o normalizaci evropským normalizačním organizacím v souladu s článkem 10 nařízení (EU) č. 1025/2012 upřesní, že normy mají být soudržné, jasné a navržené tak, aby se zaměřovaly zejména na splnění těchto cílů:

   a) zajistit, aby systémy UI uváděné na trh nebo do provozu v Unii byly bezpečné, respektovaly hodnoty Unie a posilovaly otevřenou strategickou autonomii Unie;

   b) podporovat investice a inovace v oblasti UI, mimo jiné zvyšováním právní jistoty, jakož i konkurenceschopnost a růst trhu Unie;

   c) zlepšovat správu zapojující více zúčastněných stran a reprezentovat všechny relevantní evropské zúčastněné strany (např. průmysl, malé a střední podniky, občanskou společnost, výzkumné pracovníky);

   d) přispívat k posílení celosvětové spolupráce v oblasti normalizace UI, která je v souladu s hodnotami a zájmy Unie.

   Komise požádá evropské normalizační organizace, aby doložily, že ke splnění uvedených cílů vynakládají maximální úsilí.

Článek 41

Společné specifikace

1. Komisi je svěřena pravomoc přijímat, po konzultaci s radou pro UI uvedenou v článku 56, prováděcí akty, kterými se stanoví společné technické specifikace pro požadavky uvedené v kapitole 2 této hlavy, a to přezkumným postupem podle čl. 74 odst. 2 nebo případně v souladu s požadavky uvedenými v článcích 4a a 4b, pokud jsou splněny tyto podmínky:

   a) v *Úředním věstníku Evropské unie* není zveřejněn odkaz na harmonizované normy, které se vztahují na příslušné hlavní obavy týkající se bezpečnosti nebo základních práv v souladu s nařízením (EU) č. 1025/2012;

   b) Komise požádala podle čl. 10 odst. 1 nařízení č. 1025/2012 jednu nebo více evropských normalizačních organizací, aby vypracovaly harmonizovanou normu pro požadavky stanovené v kapitole 2 této hlavy;

   c) žádná z evropských normalizačních organizací nepřijala žádost uvedenou v písmenu b), harmonizované normy řešící tuto žádost nebyly doručeny ve lhůtě stanovené v souladu s čl. 10 odst. 1 nařízení č. 1025/2012 nebo tyto normy nejsou v souladu se žádostí.

1a. Před vypracováním návrhu prováděcího aktu informuje Komise výbor uvedený v článku 22 nařízení (EU) č. 1025/2012, že se domnívá, že jsou splněny podmínky uvedené v odstavci 1.

2. Během včasné přípravy návrhu prováděcího aktu, kterým se stanoví společná specifikace, plní Komise cíle uvedené v čl. 40 odst. 2 a shromažďuje názory příslušných subjektů nebo skupin odborníků zřízených podle příslušných odvětvových právních předpisů Unie. Na základě této konzultace připraví Komise návrh prováděcího aktu.

3. Předpokládá se, že vysoce rizikové nebo obecné systémy UI, které jsou ve shodě s obecnými specifikacemi uvedenými v odstavci 1, jsou ve shodě s požadavky stanovenými v kapitole 2 této hlavy, případně s požadavky stanovenými v článcích 4a a 4b v rozsahu, v jakém se tyto obecné specifikace na uvedené požadavky vztahují.

4. Jsou-li odkazy na harmonizovanou normu zveřejněny v *Úředním věstníku Evropské unie*, zrušují se prováděcí akty uvedené v odstavci 1, které se vztahuje na požadavky stanovené v kapitole 2 této hlavy nebo požadavky stanovené v článcích 4a a 4b.

5. Pokud se členský stát domnívá, že společná specifikace nesplňuje zcela požadavky stanovené v kapitole 2 této hlavy nebo případně požadavky stanovené v článcích 4a a 4b, uvědomí o tom Komisi spolu s podrobným vysvětlením a Komise tyto informace posoudí a případně změní prováděcí akt, kterým se daná společná specifikace stanoví.

Článek 42

Předpoklad shody s určitými požadavky

1. U vysoce rizikových systémů UI, které byly trénovány a testovány na údajích zohledňujících konkrétní zeměpisné, behaviorální nebo funkční prostředí, ve kterém mají být používány, se předpokládá, že jsou v souladu s příslušnými požadavky stanovenými v čl. 10 odst. 4.

2. Má se za to, že vysoce rizikové či obecné systémy UI, které byly certifikovány nebo pro které bylo vydáno prohlášení o shodě v rámci systému kybernetické bezpečnosti podle nařízení Evropského parlamentu a Rady (EU) 2019/881[33] a odkaz na něž byl zveřejněn v *Úředním věstníku Evropské unie*, jsou v souladu s požadavky na kybernetickou bezpečnost stanovenými v článku 15 tohoto nařízení, pokud se tento certifikát o kybernetické bezpečnosti nebo prohlášení o shodě, případně jejich části, na tyto požadavky vztahují.

Článek 43

Posuzování shody

1. V případě vysoce rizikových systémů UI uvedených v bodě 1 přílohy III, u nichž poskytovatel při prokazování souladu vysoce rizikového systému UI s požadavky stanovenými v kapitole 2 této hlavy použil harmonizované normy uvedené v článku 40, nebo tam, kde je to relevantní, společné specifikace uvedené v článku 41, si poskytovatel zvolí jeden z následujících postupů:

   a) postup posuzování shody založený na vnitřní kontrole podle přílohy VI, nebo

   b) postup posuzování shody založený na posouzení systému řízení kvality a posouzení technické dokumentace za účasti oznámeného subjektu podle přílohy VII.

   Pokud poskytovatel při prokazování souladu vysoce rizikového systému UI s požadavky stanovenými v kapitole 2 této hlavy nepoužil harmonizované normy uvedené v článku 40 nebo je použil pouze částečně, případně pokud tyto harmonizované normy neexistují a společné specifikace uvedené v článku 41 nejsou k dispozici, uplatňuje poskytovatel postup posuzování shody podle přílohy VII.

[33] Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“) (Úř. věst. L 151, 7.6.2019, s. 1).

Pro účely postupu posuzování shody uvedeného v příloze VII si poskytovatel může zvolit kterýkoli z oznámených subjektů. Je-li však systém určen k uvedení do provozu donucovacími, imigračními nebo azylovými orgány, jakož i institucemi, orgány nebo agenturami EU, jedná jako oznámený subjekt orgán dozoru nad trhem uvedený v čl. 63 odst. 5, případně 6.

2. U vysoce rizikových systémů UI uvedených v bodech 2 až 8 přílohy III a u obecných systémů UI uvedených v hlavě 1a uplatňují poskytovatelé postup posuzování shody založený na vnitřní kontrole uvedené v příloze VI, který nestanoví zapojení oznámeného subjektu.

3. U vysoce rizikových systémů UI, na které se vztahují právní akty uvedené v příloze II oddílu A, uplatňuje poskytovatel příslušné posouzení shody, které stanoví uvedené právní akty. Na tyto vysoce rizikové systémy UI se vztahují požadavky stanovené v kapitole 2 této hlavy, které jsou součástí uvedeného posouzení. Použijí se rovněž body 4.3, 4.4, 4.5 a pátý odstavec bodu 4.6 přílohy VII.

Pro účely tohoto posouzení jsou oznámené subjekty, které byly oznámeny podle těchto právních aktů, oprávněny kontrolovat shodu vysoce rizikových systémů UI s požadavky stanovenými v kapitole 2 této hlavy, pokud byl posouzen soulad těchto oznámených subjektů s požadavky stanovenými v čl. 33 odst. 4, 9 a 10 v rámci postupu pro oznamování podle těchto právních aktů.

Pokud právní akty uvedené v příloze II oddíle A umožňují výrobci produktu neúčastnit se posuzování shody třetí stranou za předpokladu, že tento výrobce uplatnil všechny harmonizované normy pokrývající všechny příslušné požadavky, může tento výrobce tuto možnost využít pouze v případě, že uplatnil rovněž harmonizované normy, nebo tam, kde je to relevantní, společné specifikace uvedené v článku 41, které pokrývají požadavky stanovené v kapitole 2 této hlavy.

4. [vypouští se]

5. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 73, aby bylo s ohledem na technický pokrok možné aktualizovat přílohy VI a VII.

6. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci za účelem změny odstavců 1 a 2 s cílem podrobit vysoce rizikové systémy UI uvedené v bodech 2 až 8 přílohy III postupu posuzování shody uvedenému v příloze VII nebo jejích částech. Komise přijímá tyto akty v přenesené pravomoci s přihlédnutím k účinnosti postupu posuzování shody založeného na vnitřní kontrole podle přílohy VI v oblasti prevence nebo minimalizace rizik pro zdraví, bezpečnost a ochranu základních práv, která tyto systémy představují, jakož i k dostupnosti přiměřených kapacit a zdrojů mezi oznámenými subjekty.

Článek 44

Certifikáty

1. Certifikáty vydané oznámenými subjekty v souladu s přílohou VII se vyhotovují v jazyce, který je snadno srozumitelný příslušným orgánům v členském státě, v němž je oznámený subjekt usazen.

2. Certifikáty jsou platné po dobu v nich uvedenou, která nesmí překročit délku pěti let. Na základě žádosti poskytovatele může být platnost certifikátu prodlužována o další období, z nichž žádné nepřekročí délku pěti let, a to na základě nového posouzení v souladu s příslušnými postupy posuzování shody. Veškeré dodatky k certifikátu zůstávají v platnosti, pokud je platný certifikát, k němuž se vztahují.

3. Pokud oznámený subjekt zjistí, že systém UI již nesplňuje požadavky uvedené v kapitole 2 této hlavy, pozastaví s ohledem na zásadu proporcionality platnost certifikátu nebo ho zruší či jinak omezí, dokud není vhodnými nápravnými opatřeními přijatými poskytovatelem tohoto systému v rámci příslušné lhůty stanovené oznámeným subjektem zajištěno dosažení souladu s těmito požadavky. Oznámený subjekt své rozhodnutí zdůvodní.

Článek 45

Odvolání proti rozhodnutím oznámených subjektů

Proti rozhodnutím oznámených subjektů je možné se odvolat.

Článek 46

Informační povinnosti oznámených subjektů

1. Oznámené subjekty informují oznamující orgán:

   a) o veškerých certifikátech Unie o posouzení technické dokumentace, o veškerých dodatcích k těmto certifikátům a o schváleních systému řízení kvality vydaných v souladu s požadavky přílohy VII;

   b) o veškerých zamítnutích, omezeních, pozastaveních a zrušeních certifikátu Unie o posouzení technické dokumentace nebo o schváleních systému řízení kvality vydaných v souladu s požadavky přílohy VII;

   c) o všech okolnostech majících vliv na působnost nebo podmínky oznámení;

   d) o každé žádosti o informace týkající se činností posuzování shody, kterou obdržely od orgánů dozoru nad trhem;

   e) na vyžádání o činnostech posuzování shody vykonaných v rámci působnosti jejich oznámení a o jakékoli jiné vykonané činnosti, včetně přeshraničních činností a zadávání subdodávek.

2. Každý oznámený subjekt informuje ostatní oznámené subjekty:

   a) o schváleních systému kvality, která zamítl, pozastavil či zrušil, a na požádání o schváleních systému kvality, která vydal;

b) o EU certifikátech posouzení technické dokumentace nebo jakýchkoli jejich dodatcích, které zamítl, zrušil, pozastavil či jinak omezil, a na požádání o certifikátech a/nebo dodatcích k nim, které vydal.

3. Každý oznámený subjekt poskytne jiným oznámeným subjektům, které vykonávají obdobné činnosti posuzování shody a zabývají se stejnými systémy UI, příslušné informace o otázkách týkajících se negativních a na vyžádání pozitivních výsledků posuzování shody.

4. Povinnosti uvedené v odstavcích 1 až 3 jsou plněny v souladu s článkem 70.

Článek 47

Odchylka od postupu posuzování shody

1. Odchylně od článku 43 a na základě řádně odůvodněné žádosti může kterýkoli orgán dozoru nad trhem povolit uvedení konkrétních vysoce rizikových systémů UI na trh nebo do provozu na území dotčeného členského státu z výjimečných důvodů veřejné bezpečnosti nebo ochrany života a zdraví osob, ochrany životního prostředí a ochrany klíčových průmyslových a infrastrukturních aktiv. Toto povolení se uděluje na omezenou dobu, dokud jsou prováděny nezbytné postupy posuzování shody, při zohlednění výjimečných důvodů opodstatňujících odchylku. Dokončení těchto postupů bude provedeno bez zbytečného odkladu.

1a. V řádně odůvodněné naléhavé situaci z výjimečných důvodů veřejné bezpečnosti nebo v případě konkrétního, podstatného a bezprostředního ohrožení života nebo fyzické bezpečnosti fyzických osob mohou donucovací orgány nebo orgány civilní ochrany uvést do provozu konkrétní vysoce rizikový systém UI bez povolení uvedeného v odstavci 1, pokud je o takové povolení požádáno bez zbytečného odkladu v průběhu používání nebo po něm, a jestliže je toto povolení zamítnuto, jeho používání se s okamžitým účinkem ukončí a všechny výsledky a výstupy tohoto použití se okamžitě zničí.

2. Povolení uvedené v odstavci 1 bude vydáno jen tehdy, pokud orgán dozoru nad trhem dospěje k závěru, že daný vysoce rizikový systém UI splňuje požadavky kapitoly 2 této hlavy. Orgán dozoru nad trhem informuje Komisi a ostatní členské státy o každém povolení vydaném podle odstavce 1. Tato povinnost se nevztahuje na citlivé provozní údaje týkající se činnosti donucovacích orgánů.

3. [vypouští se]

4. [vypouští se]

5. [vypouští se]

6. V případě vysoce rizikových systémů UI souvisejících s produkty, na něž se vztahují harmonizační právní předpisy Unie uvedené v příloze II oddíle A, se použijí pouze postupy pro odchylky od posuzování shody stanovené v uvedených právních předpisech.

Článek 48

EU prohlášení o shodě

1. Poskytovatel vypracuje pro každý systém UI písemné nebo elektronicky podepsané EU prohlášení o shodě a po dobu deseti let od uvedení systému UI na trh nebo do provozu je uchovává pro potřebu příslušných vnitrostátních orgánů. V EU prohlášení o shodě je uveden systém UI, pro nějž bylo vypracováno. Kopie EU prohlášení o shodě bude na vyžádání předložena dotčeným příslušným vnitrostátním orgánům.

2. EU prohlášení o shodě stanoví, že dotyčný vysoce rizikový systém UI splňuje požadavky stanovené v kapitole 2 této hlavy. EU prohlášení o shodě obsahuje informace stanovené v příloze V a je přeloženo do jazyka, který je snadno srozumitelný příslušným vnitrostátním orgánům v členském státě nebo členských státech, v nichž je vysoce rizikový systém UI dodáván na trh.

3. Pokud se na vysoce rizikové systémy AI vztahují jiné harmonizační právní předpisy Unie, které také vyžadují EU prohlášení o shodě, vypracuje se jediné EU prohlášení o shodě s ohledem na všechny právní předpisy Unie, které se vztahují na daný vysoce rizikový systém UI. Toto prohlášení musí obsahovat veškeré informace požadované pro identifikaci harmonizačních právních předpisů Unie, k nimž se prohlášení vztahuje.

4. Vypracováním EU prohlášení o shodě přebírá poskytovatel odpovědnost za soulad s požadavky stanovenými v kapitole 2 této hlavy. Poskytovatel toto EU prohlášení o shodě podle potřeby průběžně aktualizuje.

5. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 73 za účelem aktualizace obsahu EU prohlášení o shodě uvedeného v příloze V s cílem zavést prvky, které mohou být nutné s ohledem na technický pokrok.

Článek 49

Označení shody CE

1. Označení shody CE podléhá obecným zásadám uvedeným v článku 30 nařízení (ES) č. 765/2008.

2. Označení CE se viditelně, čitelně a nesmazatelně umístí na daný vysoce rizikový systém UI. Pokud to není možné nebo to nelze s ohledem na charakter vysoce rizikového systému UI zaručit, umístí se podle potřeby na obal nebo na průvodní doklady.

3. Tam, kde je to relevantní, následuje za označením CE identifikační číslo oznámeného subjektu odpovědného za postupy posuzování shody stanovené v článku 43. Identifikační číslo je rovněž uvedeno ve všech propagačních materiálech, které uvádí, že daný vysoce rizikový systém UI splňuje požadavky na označení CE.

Článek 50

[vypouští se]

Článek 51

Registrace příslušných provozovatelů a vysoce rizikových systémů UI uvedených v příloze III

1. Před uvedením vysoce rizikového systému UI obsaženého v příloze III na trh nebo do provozu, s výjimkou vysoce rizikových systémů UI uvedených v příloze III bodech 1, 6 a 7 v oblasti prosazování práva, migrace, azylu a řízení ochrany hranic a vysoce rizikových systémů UI uvedených v příloze III bodě 2, se poskytovatel a případně zplnomocněný zástupce zaregistrují do databáze EU uvedené v článku 60. Poskytovatel nebo případně zplnomocněný zástupce rovněž do této databáze zaregistruje své systémy.

2. Před použitím vysoce rizikového systému UI uvedeného v příloze III se uživatelé vysoce rizikových systémů UI, které jsou veřejnými orgány, agenturami nebo subjekty, nebo subjekty jednajícími jejich jménem, zaregistrují do databáze EU uvedené v článku 60 a vyberou systém, který hodlají používat.

   Povinnosti stanovené v předchozím pododstavci se nevztahují na donucovací orgány, orgány ochrany hranic, imigrační nebo azylové orgány či agentury nebo subjekty působící v uvedených oblastech, které používají vysoce rizikové systémy UI uvedené v příloze III bodě 2, ani na subjekty jednající jejich jménem.

HLAVA IV

POVINNOSTI TRANSPARENTNOSTI PRO POSKYTOVATELE A UŽIVATELE URČITÝCH SYSTÉMŮ UI

Článek 52

Povinnosti transparentnosti pro poskytovatele a uživatele určitých systémů UI

1. Poskytovatelé zajistí, že systémy UI určené k interakci s fyzickými osobami budou navrhovány a vyvíjeny tak, aby byly fyzické osoby informovány o tom, že komunikují se systémem UI, není-li to zřejmé z pohledu fyzické osoby, která je přiměřeně informovaná, pozorná a obezřetná, při zohlednění okolností a kontextu použití. S výhradou příslušných záruk týkajících se práv a svobod třetích stran se tato povinnost nevztahuje na systémy UI, které jsou ze zákona oprávněny odhalovat trestné činy, předcházet jim, vyšetřovat je a stíhat, s výjimkou případů, kdy jsou tyto systémy k dispozici veřejnosti za účelem hlášení trestných činů.

2. Uživatelé systému biometrické kategorizace musí o fungování tohoto systému informovat fyzické osoby, které jsou mu vystaveny. Tato povinnost se nevztahuje na systémy UI používané pro biometrickou kategorizaci, kterým zákon umožňuje odhalovat trestné činy, předcházet jim a vyšetřovat je, s výhradou příslušných záruk týkajících se práv a svobod třetích stran.

2a. Uživatelé systému rozpoznávání emocí musí o fungování tohoto systému informovat fyzické osoby, které jsou mu vystaveny. Tato povinnost se nevztahuje na systémy UI používané pro rozpoznávání emocí, kterým zákon umožňuje odhalovat trestné činy, předcházet jim a vyšetřovat je, s výhradou příslušných záruk týkajících se práv a svobod třetích stran.

3. Uživatelé systému UI vytvářejícího obrazový, zvukový nebo video obsah, který se znatelně podobá existujícím osobám, objektům, místům nebo jiným subjektům nebo událostem a který by se určité osobě mohl nepravdivě jevit jako autentický nebo pravdivý (tzv. deep fake), případně manipulujícího s takovým obsahem, zveřejní, že tento obsah byl uměle vytvořen nebo s ním bylo manipulováno.

První pododstavec se však nepoužije, pokud toto použití povoluje zákon pro účely odhalování, prevence, vyšetřování a stíhání trestných činů nebo pokud je obsah součástí zjevně tvůrčího, satirického, uměleckého nebo fiktivního díla nebo programu, s výhradou příslušných záruk týkajících se práv a svobod třetích osob.

3a. Informace uvedené v odstavcích 1 až 3 se fyzickým osobám poskytují jasným a rozlišitelným způsobem nejpozději v době první interakce nebo expozice.

4. Odstavci 1, 2, 2a a 3 a 3a nejsou dotčeny požadavky a povinnosti stanovené v hlavě III tohoto nařízení a nejsou jimi dotčeny jiné povinnosti týkající se transparentnosti pro uživatele systémů UI stanovené v právu Unie nebo vnitrostátním právu.

HLAVA V

OPATŘENÍ NA PODPORU INOVACÍ

Článek 53

Regulační pískoviště UI

-1a. Příslušné vnitrostátní orgány mohou zřídit regulační pískoviště UI pro vývoj, trénování, testování a validaci inovativních systémů UI pod přímým dohledem a vedením a s přímou podporou příslušného vnitrostátního orgánu předtím, než jsou tyto systémy uvedeny na trh nebo do provozu. Tato regulační pískoviště mohou zahrnovat testování v reálných podmínkách pod dohledem příslušných vnitrostátních orgánů.

-1b. [vypouští se]

-1c Příslušné vnitrostátní orgány případně spolupracují s dalšími relevantními orgány a mohou umožnit zapojení dalších subjektů do ekosystému UI.

-1d. Tímto článkem nejsou dotčena jiná regulační pískoviště zřízená podle vnitrostátních právních předpisů nebo právních předpisů Unie, a to ani v případech, kdy produkty nebo služby, které jsou v nich testovány, souvisejí s používáním inovativních systémů UI. Členské státy zajistí odpovídající úroveň spolupráce mezi orgány vykonávajícími dohled nad těmito jinými pískovišti a příslušnými vnitrostátními orgány.

1. [vypouští se]

1a. [vypouští se]

1b. Cílem zřízení regulačních pískovišť UI podle tohoto nařízení je přispět k jednomu nebo několika z těchto cílů:

a) podporovat inovace a konkurenceschopnost a usnadňovat vývoj ekosystému UI;
b) usnadnit a urychlit přístup systémů UI na trh Unie, zejména pokud jsou poskytovány malými a středními podniky, včetně začínajících podniků;
c) zlepšit právní jistotu a přispět ke sdílení osvědčených postupů prostřednictvím spolupráce s orgány zapojenými do regulačního pískoviště UI s cílem zajistit budoucí soulad s tímto nařízením a případně s dalšími právními předpisy Unie a členských států;
d) přispívat k regulačnímu učení založenému na důkazech.

2. [vypouští se]

2a. Přístup k regulačním pískovištím UI je otevřen všem poskytovatelům nebo potenciálním poskytovatelům systému UI, kteří splňují kritéria způsobilosti a výběru uvedená v odst. 6 písm. a) a kteří byli vybráni příslušnými vnitrostátními orgány na základě výběrového řízení uvedeného v odst. 6 písm. b). Poskytovatelé nebo potenciální poskytovatelé mohou rovněž podávat žádosti společně s uživateli nebo jinými příslušnými třetími stranami.

Účast na regulačním pískovišti UI je omezena na dobu, která je přiměřená složitosti a rozsahu projektu. Tuto lhůtu může příslušný vnitrostátní orgán prodloužit.

Účast na regulačním pískovišti UI je založena na zvláštním plánu uvedeném v odstavci 6 tohoto článku, na němž se podle potřeby dohodnou účastník (účastníci) s příslušným vnitrostátním orgánem (příslušnými vnitrostátními orgány).

3. Účast na regulačních pískovištích UI nebudou mít vliv na pravomoci v oblasti dohledu a nápravy příslušející orgánům vykonávajícím dohled nad pískovištěm. Tyto orgány jsou při výkonu svých pravomocí dohledu v mezích příslušných právních předpisů flexibilní, přičemž při uplatňování právních ustanovení na konkrétní projekt pískoviště UI využijí své diskreční pravomoci s cílem podpořit v Unii inovace v oblasti UI.

Za předpokladu, že účastník (účastníci) dodržuje (dodržují) plán pískoviště UI a podmínky pro svou účast uvedené v odst. 6 písm. c) a řídí se v dobré víře pokyny orgánů, neuloží orgány žádné správní pokuty za porušení platných právních předpisů Unie nebo členského státu, včetně ustanovení tohoto nařízení, týkajících se systému UI, nad nímž je v rámci pískoviště vykonáván dohled.

4. Podle platných právních předpisů Unie a členských států v oblasti odpovědnosti účastníci i nadále odpovídají za veškeré škody způsobené v průběhu jejich účasti na regulačním pískovišti UI.

4a. Na žádost poskytovatele nebo potenciálního poskytovatele systému UI poskytne příslušný vnitrostátní orgán případně písemný doklad o činnostech, které byly v rámci pískoviště úspěšně provedeny. Příslušný vnitrostátní orgán rovněž předloží výstupní zprávu s podrobným popisem činností prováděných v rámci pískoviště a souvisejících výsledků, jakož i výsledků učení. Tyto písemné doklady a výstupní zprávu by mohly orgány dozoru nad trhem nebo případně oznámené subjekty zohlednit v souvislosti s postupy posuzování shody nebo kontrolami dozoru nad trhem.

S výhradou ustanovení o důvěrnosti v článku 70 a se souhlasem účastníků pískoviště UI jsou Evropská komise a rada pro UI oprávněny nahlížet do výstupních zpráv a podle potřeby je zohlední při plnění svých úkolů podle tohoto nařízení. Pokud s tím účastník i příslušný vnitrostátní orgán výslovně souhlasí, může být výstupní zpráva zpřístupněna veřejnosti prostřednictvím jednotné informační platformy uvedené v čl. 55 odst. 3 písm. b).

4b. Regulační pískoviště UI jsou navržena a zavedena tak, aby případně usnadňovala přeshraniční spolupráci mezi příslušnými vnitrostátními orgány.

5. Příslušné vnitrostátní orgány zveřejňují výroční zprávy o provádění regulačních pískovišť AI, včetně osvědčených postupů, získaných zkušeností a doporučení o jejich uspořádání a případně o uplatňování tohoto nařízení a dalších právních předpisů Unie, nad nimiž je prováděn dohled v rámci daného pískoviště. Tyto výroční zprávy se předkládají radě pro UI, která zveřejní souhrn všech osvědčených postupů, získaných zkušeností a doporučení. Tato povinnost zveřejňovat výroční zprávy se nevztahuje na citlivé provozní údaje týkající se činností donucovacích orgánů, orgánů ochrany hranic, imigračních nebo azylových orgánů. Komise a rada pro UI při plnění svých úkolů podle tohoto nařízení v případě potřeby zohlední výroční zprávy.

5b. Komise zajistí, aby informace o regulačních pískovištích UI, včetně těch, která byla zřízena podle tohoto článku, byly dostupné prostřednictvím jednotné informační platformy uvedené v čl. 55 odst. 3 písm. b).

6. Způsob a podmínky pro zřízení a provoz regulačních pískovišť UI podle tohoto nařízení se přijímají prostřednictvím prováděcích aktů, a to přezkumným postupem podle čl. 74 odst. 2.

Způsob a podmínky v co největší míře posilují flexibilitu příslušných vnitrostátních orgánů při zřizování a provozu jejich regulačních pískovišť UI, podporují inovace a regulační učení a zejména zohledňují zvláštní okolnosti a kapacity zúčastněných malých a středních podniků, včetně začínajících podniků.

Uvedené prováděcí akty obsahují společné hlavní zásady týkající se těchto otázek:

a) způsobilost a výběr pro účast na regulačním pískovišti UI;
b) postup pro podávání žádostí, účast, monitorování, ukončení účasti, jakož i ukončení samotného regulačního pískoviště UI, včetně plánu pískoviště a výstupní zprávy;
c) podmínky vztahující se na účastníky.

7. Pokud příslušné vnitrostátní orgány zvažují povolit testování v reálných podmínkách, nad nímž je vykonáván dohled v rámci regulačního pískoviště UI zřízeného podle tohoto článku, výslovně se s účastníky dohodnou na podmínkách tohoto testování, a zejména na vhodných zárukách s cílem chránit základní práva, zdraví a bezpečnost. V případě potřeby spolupracují s dalšími příslušnými vnitrostátními orgány s cílem zajistit jednotné postupy v celé Unii.

Článek 54

Další zpracování osobních údajů pro účely vývoje určitých systémů UI ve veřejném zájmu v rámci regulačního pískoviště UI

1. V regulačním pískovišti UI mohou být zpracovávány osobní údaje zákonně shromážděné pro jiné účely, a to s cílem vyvíjet, testovat a trénovat určité inovativní systémy UI v daném pískovišti za následujících kumulativních podmínek:

   a) inovativní systémy UI budou vyvinuty veřejným orgánem nebo jinou veřejnoprávní či soukromoprávní fyzickou nebo právnickou osobou za účelem ochrany podstatného veřejného zájmu v jedné nebo více z následujících oblastí:

      i) [vypouští se]

      ii) veřejná bezpečnost a zdraví, včetně prevence, tlumení a léčby nemocí a zlepšení systémů zdravotní péče;

      iii) ochrana a zlepšování kvality životního prostředí, včetně ekologické transformace, zmírňování změny klimatu a přizpůsobování se jí;

      iv) energetická udržitelnost, doprava a mobilita;

      v) účinnost a kvalita veřejné správy a veřejných služeb;

      vi) kybernetická bezpečnost a odolnost kritické infrastruktury.

   b) zpracovávané údaje jsou nezbytné pro splnění jednoho nebo více požadavků uvedených v hlavě III kapitole 2, pokud tyto požadavky nelze účinně splnit zpracováním anonymizovaných, syntetických nebo jiných neosobních údajů;

c) existují účinné monitorovací mechanismy umožňující identifikovat, zda mohou během experimentování v pískovišti vzniknout jakákoli vysoká rizika pro práva a svobody subjektů údajů, uvedená v článku 35 nařízení (EU) 2016/679 a článku 39 nařízení (EU) 2018/1725, jakož i mechanismus reakce umožňující okamžité zmírnění těchto rizik a v případě potřeby i zastavení zpracování;

d) veškeré osobní údaje, které mají být zpracovány v rámci pískoviště, se nacházejí ve funkčně odděleném, izolovaném a chráněném prostředí pro zpracování údajů pod kontrolou účastníků a mají k nim přístup pouze oprávněné osoby;

e) žádné zpracovávané osobní údaje nejsou přenášeny, převáděny ani jinak zpřístupněny třetím stranám, které nejsou účastníky pískoviště, ledaže k takovému zveřejnění dojde v souladu s nařízením (EU) 2016/679 nebo případně s nařízením 2018/725 a všichni účastníci s tím souhlasí;

f) žádné zpracování osobních údajů v rámci pískoviště neovlivní uplatňování práv subjektů údajů stanovených v právních předpisech Unie o ochraně osobních údajů, zejména v článku 22 nařízení (EU) 2016/679 a článku 24 nařízení (EU) 2018/1725;

g) veškeré osobní údaje zpracovávané v rámci pískoviště jsou chráněny prostřednictvím vhodných technických a organizačních opatření a vymazány, jakmile skončí účast na pískovišti nebo doba uchovávání osobních údajů;

h) protokoly o zpracování osobních údajů v rámci pískoviště jsou uchovávány po dobu účasti na pískovišti, nestanoví-li právní předpisy Unie nebo vnitrostátní právní předpisy jinak;

i) úplný a podrobný popis postupu a zdůvodnění trénování, testování a validace systému UI je uchováván společně s výsledky testování jako součást technické dokumentace v příloze IV;

j) zveřejnění stručného shrnutí projektu UI vyvinutého v pískovišti, jeho cílů a očekávaných výsledků na internetových stránkách příslušných orgánů. Tato povinnost se nevztahuje na citlivé provozní údaje týkající se činností donucovacích orgánů, orgánů ochrany hranic, imigračních nebo azylových orgánů.

1a. Pro účely prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkon trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení pod dozorem a v pravomoci donucovacích orgánů, vychází zpracování osobních údajů v regulačních pískovištích UI z právních předpisů konkrétního členského státu nebo Unie a podléhá stejným kumulativním podmínkám uvedeným v odstavci 1.

2. Odstavcem 1 nejsou dotčeny právní předpisy Unie nebo členských států, které stanoví základ pro zpracování osobních údajů, které je nezbytné pro účely vývoje, testování a trénování inovativních systémů UI, nebo jakýkoli jiný právní základ v souladu s právem Unie o ochraně osobních údajů.

Článek 54a

Testování vysoce rizikových systémů UI v reálných podmínkách mimo regulační pískoviště UI

1. Testování systémů UI v reálných podmínkách mimo regulační pískoviště UI mohou provádět poskytovatelé nebo potenciální poskytovatelé vysoce rizikových systémů UI uvedených v příloze III v souladu s ustanoveními tohoto článku a plánem testování v reálném provozu uvedeným v tomto článku.

Podrobné prvky plánu testování v reálných podmínkách se upřesní v prováděcích aktech přijatých Komisí přezkumným postupem podle čl. 74 odst. 2.

Tímto ustanovením nejsou dotčeny právní předpisy Unie nebo členských států týkající se testování vysoce rizikových systémů UI v reálných podmínkách v souvislosti s produkty, na něž se vztahují právní předpisy uvedené v příloze II.

2. Kdykoli před uvedením systému UI na trh nebo do provozu mohou poskytovatelé nebo potenciální poskytovatelé provádět testování vysoce rizikových systémů UI uvedených v příloze III v reálných podmínkách, a to samostatně nebo v partnerství s jedním nebo více potenciálními uživateli.

3. Testováním vysoce rizikových systémů UI v reálných podmínkách podle tohoto článku není dotčen etický přezkum, který může být vyžadován vnitrostátními právními předpisy nebo právními předpisy Unie.

4. Poskytovatelé nebo potenciální poskytovatelé mohou provádět testování v reálných podmínkách pouze tehdy, jsou-li splněny všechny tyto podmínky:

a) poskytovatel nebo potenciální poskytovatel vypracoval plán testování v reálných podmínkách a předložil jej orgánu dozoru nad trhem v členském státě (členských státech), v němž má být testování v reálných podmínkách provedeno;

b) orgán dozoru nad trhem v členském státě (členských státech), v němž má být testování v reálných podmínkách provedeno, nevznesl do 30 dnů od předložení plánu proti testování námitky;

c) poskytovatel nebo potenciální poskytovatel s výjimkou vysoce rizikových systémů UI uvedených v příloze III bodech 1, 6 a 7 v oblasti prosazování práva, migrace, azylu a řízení ochrany hranic a vysoce rizikových systémů UI uvedených v příloze III bodě 2 zaregistroval testování v reálných podmínkách v databázi EU uvedené v čl. 60 odst. 5a s uvedením celounijního jedinečného identifikačního čísla a informací stanovených v příloze VIIIa;

d) poskytovatel nebo potenciální poskytovatel provádějící testování v reálných podmínkách je usazen v Unii nebo pro účely testování v reálných podmínkách jmenoval právního zástupce, který je usazen v Unii;

e) údaje shromážděné a zpracované pro účely testování v reálných podmínkách se nepředávají do zemí mimo Unii, ledaže předávání a zpracování poskytuje záruky, jež jsou rovnocenné zárukám stanoveným právními předpisy Unie;

f) testování v reálných podmínkách netrvá déle, než je nezbytné k dosažení jeho cílů, a v žádném případě ne déle než 12 měsíců;

g) osoby, jež na základě svého věku, tělesného nebo mentálního postižení patří do zranitelných skupin, jsou náležitě chráněny;

h) [vypouští se]

i) pokud poskytovatel nebo potenciální poskytovatel uspořádá testování v reálných podmínkách ve spolupráci s jedním nebo více potenciálními uživateli, tito uživatelé byli informováni o všech aspektech testování, které jsou relevantní pro jejich rozhodnutí účastnit se, a obdrželi příslušné pokyny o tom, jak systém UI uvedený v článku 13 používat; poskytovatel nebo potenciální poskytovatel a uživatel (uživatelé) uzavřou dohodu, v níž upřesní své úlohy a povinnosti s cílem zajistit soulad s ustanoveními týkajícími se testování v reálných podmínkách podle tohoto nařízení a dalšími platnými právními předpisy Unie a členských států;

j) subjekty testování v reálných podmínkách udělily informovaný souhlas v souladu s článkem 54b, nebo v případě prosazování práva, pokud by získání informovaného souhlasu bránilo testování systému UI, samotné testování a výsledek testování v reálných podmínkách nemá na subjekt hodnocení negativní dopad;

k) na testování v reálných podmínkách účinně dohlíží poskytovatel nebo potenciální poskytovatel a uživatel (uživatelé) spolu s osobami, které mají jak odpovídající kvalifikaci v příslušné oblasti, tak nezbytnou kapacitu, odbornou přípravu a pravomoc k plnění svých úkolů;

l) predikce, doporučení nebo rozhodnutí systému UI lze účinně zvrátit nebo nezohlednit.

5. Kterýkoli subjekt testování v reálných podmínkách nebo případně jeho zákonně ustanovený zástupce může odvoláním svého informovaného souhlasu od testování kdykoli odstoupit, aniž by tím došel jakékoliv újmy a aniž by byl povinen poskytnout jakékoliv odůvodnění. Odvolání informovaného souhlasu neovlivní již provedené činnosti ani využití údajů získaných na základě informovaného souhlasu před jeho odvoláním.

6. Veškeré závažné incidenty zjištěné v průběhu testování v reálných podmínkách se oznámí vnitrostátnímu orgánu dozoru nad trhem v souladu s článkem 62 tohoto nařízení. Poskytovatel nebo potenciální poskytovatel přijme okamžitá zmírňující opatření nebo, pokud to není možné, testování v reálných podmínkách pozastaví, dokud k tomuto zmírnění nedojde, nebo jej jiným způsobem ukončí. Po takovém ukončení testování v reálných podmínkách stanoví poskytovatel nebo potenciální poskytovatel postup pro okamžité stažení systému UI z oběhu.

7. Poskytovatelé nebo potenciální poskytovatelé oznámí vnitrostátnímu orgánu dozoru nad trhem v členském státě (členských státech), v němž má být testování v reálných podmínkách provedeno, že testování v reálných podmínkách bylo pozastaveno nebo ukončeno, a jaké jsou konečné výsledky.

8. Podle platných právních předpisů Unie a členských států o odpovědnosti nesou poskytovatel nebo potenciální poskytovatel odpovědnost za veškeré škody způsobené v průběhu jejich účasti na testování v reálných podmínkách.

Článek 54b

Informovaný souhlas s účastí na testování v reálných podmínkách mimo regulační pískoviště UI

1. Pro účely testování v reálných podmínkách podle článku 54a subjekt testování dobrovolně udělí před svou účastí na tomto testování informovaný souhlas, a to poté, co řádně obdržel stručné, jasné, relevantní a srozumitelné informace týkající se:

i) povahy a cíle testování v reálných podmínkách a možných obtíží, které mohou být s jeho účastí spojeny;

ii) podmínek, za nichž má být testování v reálných podmínkách provedeno, včetně předpokládané doby trvání účasti subjektu;

iii) práv subjektu a záruk týkajících se jeho účasti, zejména jeho práva odmítnout účast a práva kdykoliv od testování v reálných podmínkách odstoupit, aniž by tím došel jakékoliv újmy a byl povinen poskytnout jakékoliv odůvodnění;

iv) způsobů žádosti o zrušení nebo nezohlednění predikcí, doporučení nebo rozhodnutí systému UI;

v) celounijního jedinečného identifikačního čísla testování v reálných podmínkách v souladu s čl. 54a odst. 4c a kontaktních údajů poskytovatele nebo jeho právního zástupce, od něhož lze získat další informace.

2. Informovaný souhlas musí být datován a zdokumentován a jeho kopie musí být poskytnuta subjektu nebo jeho právnímu zástupci.

Článek 55

Podpůrná opatření pro provozovatele, zejména malé a střední podniky, včetně začínajících podniků

1. Členské státy učiní tato opatření:

a) poskytovat malým a středním podnikům, včetně začínajících podniků, přednostní přístup k regulačním pískovištím UI v rozsahu, v jakém splňují kritéria způsobilosti a výběru;

b) organizovat konkrétní činnosti zaměřené na zvyšování povědomí a odbornou přípravu, pokud jde o uplatňování tohoto nařízení, přizpůsobené potřebám malých a středních podniků, včetně začínajících podniků, a případně místních veřejných orgánů;

c) případně zřídit vyhrazený kanál pro komunikaci s malými a středními podniky, včetně začínajících podniků, a v případě potřeby s místními veřejnými orgány, který bude poskytovat poradenství a reagovat na dotazy týkající se provádění tohoto nařízení, a to i v souvislosti s účastí na regulačních pískovištích UI.

2. Při stanovování poplatků za posuzování shody podle článku 43 jsou zohledňovány zvláštní zájmy a potřeby malých a středních podniků, včetně začínajících podniků, přičemž tyto poplatky se snižují úměrně jejich velikosti, velikosti trhu a dalším příslušným ukazatelům.

3. Komise učiní tato opatření:

a) na žádost rady pro UI poskytnout standardizované vzory pro oblasti, na něž se vztahuje toto nařízení;

b) vytvořit a udržovat jednotnou informační platformu poskytující snadno použitelné informace v souvislosti s tímto nařízením všem hospodářským subjektům v celé Unii;

c) organizovat vhodné komunikační kampaně s cílem zvýšit povědomí o povinnostech vyplývajících z tohoto nařízení;

d) vyhodnocovat a podporovat sbližování osvědčených postupů při zadávacím řízení v souvislosti se systémy UI.

Článek 55a

Výjimky pro specifické provozovatele

1. Povinnosti stanovené v článku 17 tohoto nařízení se nevztahují na mikropodniky definované v čl. 2 odst. 3 přílohy doporučení Komise 2003/361/ES týkající se definice mikropodniků a malých a středních podniků, pokud tyto podniky nemají partnerské podniky nebo propojené podniky ve smyslu článku 3 téže přílohy.

2. Odstavec 1 nelze vykládat tak, že tyto provozovatele osvobozuje od plnění jakýchkoli jiných požadavků a povinností stanovených v tomto nařízení, včetně požadavků a povinností stanovených v článcích 9, 61 a 62.

3. Požadavky a povinnosti týkající se obecných systémů UI stanovené v článku 4b se nevztahují na mikropodniky a malé a střední podniky, pokud tyto podniky nemají partnerské nebo propojené podniky ve smyslu článku 3 přílohy doporučení Komise 2003/361/ES týkající se definice mikropodniků a malých a středních podniků.

HLAVA VI

SPRÁVA

KAPITOLA 1

EVROPSKÁ RADA PRO UMĚLOU INTELIGENCI

Článek 56

Zřízení a struktura Evropské rady pro umělou inteligenci

1. Zřizuje se „Evropská rada pro umělou inteligenci“ (dále jen „rada“).

2. Rada se skládá z jednoho zástupce každého členského státu. Evropský inspektor ochrany údajů se účastní jako pozorovatel. Na zasedání rady je rovněž přítomna Komise, která se však neúčastní hlasování.

   Rada může v jednotlivých případech přizvat na zasedání další vnitrostátní a unijní orgány, subjekty nebo odborníky z členských států a Unie v případě, že jsou pro ně projednávané otázky relevantní.

2a. Členský stát jmenuje svého zástupce na dobu tří let, přičemž tuto dobu lze jednou prodloužit.

2aa. Členské státy zajistí, aby jejich zástupci v radě:

   i) měli ve svém členském státě příslušné kompetence a pravomoci, a mohli se tak aktivně podílet na plnění úkolů rady uvedených v článku 58;

   ii) byli určeni jako jediné kontaktní osoby pro radu a případně, s ohledem na potřeby členských států, jako jediné kontaktní osoby pro zúčastněné strany;

iii) měli pravomoc usnadňovat jednotnost a koordinaci mezi příslušnými vnitrostátními orgány ve svém členském státě, pokud jde o provádění tohoto nařízení, mimo jiné shromažďováním příslušných údajů a informací pro účely plnění svých úkolů v rámci rady.

3. Určení zástupci členských států přijmou jednací řád rady dvoutřetinovou většinou.

Jednací řád zejména stanoví postupy pro výběrové řízení, dobu trvání mandátu předsedy a jeho konkrétní úkoly, způsoby hlasování a organizaci činností rady a jejích podskupin.

Rada zřídí stálou podskupinu jakožto platformu pro zúčastněné strany, která bude radě poskytovat poradenství ve všech otázkách souvisejících s prováděním tohoto nařízení, včetně přípravy prováděcích aktů a aktů v přenesené pravomoci. Za tímto účelem jsou k účasti v této podskupině přizvány organizace zastupující zájmy poskytovatelů a uživatelů systémů UI, včetně malých a středních podniků a začínajících podniků, jakož i organizace občanské společnosti, zástupci dotčených osob, výzkumní pracovníci, normalizační organizace, oznámené subjekty, laboratoře a zkušební a experimentální zařízení. Rada zřídí dvě stálé podskupiny, které poskytnou platformu pro spolupráci a výměnu mezi orgány dozoru nad trhem a oznamujícími orgány v otázkách týkajících se dozoru nad trhem a oznámených subjektů.

Rada může podle potřeby zřizovat další stálé nebo dočasné podskupiny pro účely zkoumání konkrétních otázek. Zúčastněné strany uvedené v předchozím pododstavci mohou být případně přizvány do těchto podskupin nebo na jejich zvláštní zasedání jako pozorovatelé.

3a. Rada je organizována a provozována tak, aby byla zaručena objektivita a nestrannost jejích činností.

4. Radě předsedá jeden ze zástupců členských států. Na žádost předsedy svolává Komise zasedání a připravuje pořad jednání v souladu s úkoly rady podle tohoto nařízení a s jejím jednacím řádem. Komise poskytuje administrativní a analytickou podporu činnostem rady podle tohoto nařízení.

Článek 57

[vypouští se]

Článek 58

Úkoly rady

Rada poskytuje poradenství a je nápomocna Komisi a členským státům s cílem usnadnit jednotné a účinné uplatňování tohoto nařízení. Za tímto účelem může rada zejména:

a) shromažďovat a sdílet technické a regulační odborné znalosti a osvědčené postupy mezi členskými státy;

b) přispívat k harmonizaci správní praxe v členských státech, a to i v souvislosti s odchylkou od postupů posuzování shody podle článku 47, fungováním regulačních pískovišť a testováním v reálných podmínkách podle článků 53, 54 a 54a;

c) na žádost Komise nebo z vlastního podnětu vydávat doporučení a písemná stanoviska k veškerým relevantním záležitostem souvisejícím s prováděním tohoto nařízení a s jeho jednotným a účinným uplatňováním, a to i:

   i) k technickým specifikacím nebo stávajícím normám týkajícím se požadavků stanovených v hlavě III kapitole 2;

   ii) k používání harmonizovaných norem nebo společných specifikací uvedených v článcích 40 a 41;

iii) k přípravě pokynů, včetně pokynů pro stanovení správních pokut uvedených v článku 71;

d) poskytovat Komisi poradenství týkající se případné potřeby učinit změnu přílohy III v souladu s články 4 a 7, s přihlédnutím k příslušným dostupným důkazům a nejnovějšímu vývoji v technologické oblasti;

e) poskytovat Komisi poradenství při přípravě aktu v přenesené pravomoci nebo prováděcího aktu podle tohoto nařízení;

f) podle potřeby spolupracovat s příslušnými orgány EU, skupinami a sítěmi odborníků, zejména v oblasti bezpečnosti produktů, kybernetické bezpečnosti, hospodářské soutěže, digitálních a mediálních služeb, finančních služeb, kryptoměn, ochrany spotřebitele, dat a základních práv;

g) podporovat Komisi a poskytovat jí příslušné poradenství při vypracovávání pokynů uvedených v článku 58a nebo vypracování takových pokynů požadovat;

h) napomáhat práci orgánů dozoru nad trhem a ve spolupráci a se souhlasem dotčených orgánů dozoru nad trhem prosazovat a podporovat přeshraniční šetření v oblasti dozoru nad trhem, a to i s ohledem na vznik rizik systémové povahy, která mohou vyplývat ze systémů UI;

i) přispívat k posuzování potřeb v oblasti odborné přípravy zaměstnanců členských států podílejících se na provádění tohoto nařízení;

j) poskytovat Komisi poradenství ve vztahu k mezinárodním záležitostem týkajícím se umělé inteligence.

KAPITOLA 1A

POKYNY KOMISE

Článek 58a

Pokyny Komise k provádění tohoto nařízení

1. Na žádost členských států nebo rady či z vlastního podnětu vydá Komise pokyny k praktickému provádění tohoto nařízení, a zejména k:

   i) uplatňování požadavků podle článků 8 až 15;

   ii) zakázaným postupům podle článku 5;

   iii) praktickému provádění ustanovení týkajících se podstatné změny;

   iv) praktickému uplatňování jednotných podmínek uvedených v čl. 6 odst. 3, včetně příkladů týkajících se vysoce rizikových systémů UI uvedených v příloze III;

   v) praktickému provádění povinností transparentnosti stanovených v článku 52;

   vi) vztahu mezi tímto nařízením a dalšími příslušnými právními předpisy Unie, a to i pokud jde o jednotnost při jejich prosazování.

Při vydávání těchto pokynů věnuje Komise zvláštní pozornost potřebám malých a středních podniků, včetně začínajících podniků, místních veřejných orgánů a odvětví, kterých se toto nařízení s největší pravděpodobností dotkne.

KAPITOLA 2

PŘÍSLUŠNÉ VNITROSTÁTNÍ ORGÁNY

Článek 59

Určení příslušných vnitrostátních orgánů

1. [vypouští se]

2. Pro účely tohoto nařízení každý členský stát zřídí nebo určí alespoň jeden oznamující orgán a alespoň jeden orgán dozoru nad trhem jakožto příslušné vnitrostátní orgány. Tyto příslušné vnitrostátní orgány jsou organizovány tak, aby chránily objektivitu a nestrannost svých činností a úkolů. Jsou-li dodrženy tyto základní principy, mohou být takové činnosti a úkoly prováděny jedním nebo několika určenými orgány v souladu s organizačními potřebami členského státu.

3. Členské státy informují Komisi o tom, který orgán nebo které orgány určily.

4. Členské státy zajistí, aby příslušným vnitrostátním orgánům byly poskytnuty odpovídající finanční zdroje, technické vybavení, jakož i kvalifikované lidské zdroje, které jim umožní efektivně plnit úkoly podle tohoto nařízení.

5. Do *[jednoho roku po vstupu tohoto nařízení v platnost]* a poté šest měsíců před uplynutím lhůty uvedené v čl. 84 odst. 2 informují členské státy Komisi o stavu finančních zdrojů, technického vybavení a lidských zdrojů příslušných vnitrostátních orgánů s hodnocením jejich přiměřenosti. Komise předá tyto informace radě k projednání a případným doporučením.

6. Komise usnadňuje výměnu zkušeností mezi příslušnými vnitrostátními orgány.

7. Příslušné vnitrostátní orgány mohou poskytovat poradenství ohledně provádění tohoto nařízení, a to i poradenství přizpůsobené pro poskytovatele z řad malých a středních podniků, včetně začínajících podniků. Kdykoli mají příslušné vnitrostátní orgány v úmyslu poskytnout pokyny a rady týkající se systému UI v oblastech, na které se vztahují jiné právní předpisy Unie, provedou podle potřeby konzultaci s vnitrostátními orgány příslušnými podle těchto právních předpisů Unie. Členské státy mohou rovněž zřídit jedno ústřední kontaktní místo pro komunikaci s provozovateli.

8. Pokud orgány, instituce a subjekty Unie spadají do oblasti působnosti tohoto nařízení, jedná jako orgán příslušný pro dohled nad nimi evropský inspektor ochrany údajů.

HLAVA VII

DATABÁZE EU OBSAHUJÍCÍ VYSOCE RIZIKOVÉ SYSTÉMY UI UVEDENÉ V PŘÍLOZE III

Článek 60

Databáze EU obsahující vysoce rizikové systémy UI uvedené v příloze III

1. Komise ve spolupráci s členskými státy zřizuje a udržuje databázi EU obsahující informace uvedené v odstavci 2 ohledně příslušných poskytovatelů a vysoce rizikových systémů UI uvedených v příloze III a registrovaných v souladu s články 51 a 54a. Při stanovování funkčních specifikací této databáze konzultuje Komise radu pro UI.

2. Údaje uvedené v příloze VIII části I vloží do databáze EU poskytovatelé, zplnomocnění zástupci a případně příslušní uživatelé při své registraci. Údaje uvedené v příloze VIII části II bodech 1 až 11 vloží do databáze EU poskytovatelé nebo případně zplnomocněný zástupce v souladu s článkem 51. Údaje uvedené v příloze VIII části II bodě 12 automaticky generuje databáze na základě informací poskytnutých příslušnými uživateli podle čl. 51 odst. 2. Údaje uvedené v příloze VIIIa vloží do databáze potenciální poskytovatelé nebo poskytovatelé v souladu s článkem 54a.

3. [vypouští se]

4. Databáze EU neobsahuje žádné osobní údaje, s výjimkou informací uvedených v příloze VIII, a není jí dotčen článek 70.

5. Správcem databáze EU je Komise. Poskytovatelům, potenciálním poskytovatelům a uživatelům zpřístupní přiměřenou technickou a administrativní podporu.

5a. Informace obsažené v databázi EU registrované v souladu s článkem 51 jsou přístupné veřejnosti. Informace registrované v souladu s článkem 54a jsou přístupné pouze orgánům dozoru nad trhem a Komisi, pokud potenciální poskytovatel nebo poskytovatel nedal souhlas k tomu, aby tyto informace byly rovněž zpřístupněny veřejnosti.

HLAVA VIII

MONITOROVÁNÍ PO UVEDENÍ NA TRH, SDÍLENÍ INFORMACÍ, DOZOR NAD TRHEM

KAPITOLA 1

MONITOROVÁNÍ PO UVEDENÍ NA TRH

Článek 61

Monitorování po uvedení na trh prováděné poskytovateli a plán monitorování po uvedení vysoce rizikových systémů UI na trh

1. Poskytovatelé zavádějí a dokumentují systém monitorování po uvedení na trh způsobem, který je přiměřený rizikům daného vysoce rizikového systému UI.

2. Aby mohl poskytovatel vyhodnocovat soulad systémů UI s požadavky stanovenými v hlavě III kapitole 2 během jejich celého životního cyklu, systém monitorování po uvedení na trh shromažďuje, dokumentuje a analyzuje příslušné údaje o výkonnosti vysoce rizikových systémů UI, které mohou být poskytnuty uživateli nebo shromažďovány prostřednictvím jiných zdrojů. Tato povinnost se nevztahuje na citlivé provozní údaje uživatelů systémů UI, kteří jsou donucovacími orgány.

3. Systém monitorování po uvedení na trh je založen na plánu monitorování po uvedení na trh. Plán monitorování po uvedení na trh je součástí technické dokumentace uvedené v příloze IV. Komise přijme prováděcí akt, kterým se stanoví podrobná ustanovení zavádějící vzor plánu monitorování po uvedení na trh a seznam prvků, které mají být do tohoto plánu zahrnuty.

4. U vysoce rizikových systémů UI, na které se vztahují právní akty uvedené v příloze II oddíle A, u nichž je systém a plán monitorování po uvedení na trh podle daných právních předpisů již stanoven, se dokumentace monitorování po uvedení na trh připravená podle těchto právních předpisů považuje za dostatečnou, použije-li se vzor uvedený v odstavci 3.

První pododstavec se vztahuje také na vysoce rizikové systémy UI uvedené v bodě 5 přílohy III, které jsou uvedeny na trh nebo do provozu finančními institucemi, na něž se vztahují požadavky týkající se jejich vnitřní správy, systémů nebo postupů podle právních předpisů Unie v oblasti finančních služeb.

KAPITOLA 2

SDÍLENÍ INFORMACÍ O ZÁVAŽNÝCH INCIDENTECH

Článek 62

Ohlašování závažných incidentů

1. Poskytovatelé vysoce rizikových systémů UI uváděných na trh Unie ohlašují jakýkoli závažný incident orgánům dozoru nad trhem v členských státech, v nichž k tomuto incidentu došlo.

Toto oznámení musí být učiněno neprodleně poté, co poskytovatel zjistí příčinnou souvislost mezi daným systémem UI a daným závažným incidentem nebo přiměřenou pravděpodobnost této souvislosti, v každém případě však nejpozději do patnácti dnů poté, co se poskytovatelé o daném závažném incidentu dozvěděli.

2. Po obdržení oznámení týkajícího se závažného incidentu uvedeného v čl. 3 odst. 44 písm. c) informuje příslušný orgán dozoru nad trhem vnitrostátní veřejné orgány nebo subjekty veřejného sektoru uvedené v čl. 64 odst. 3. Komise vypracuje zvláštní pokyny s cílem usnadnit plnění povinností stanovených v odstavci 1. Tyto pokyny jsou vydány nejpozději dvanáct měsíců po vstupu tohoto nařízení v platnost.

3. U vysoce rizikových systémů UI podle bodu 5 přílohy III uváděných na trh nebo do provozu poskytovateli, kteří jsou finančními institucemi, na něž se vztahují požadavky týkající se jejich vnitřní správy, systémů nebo postupů podle právních předpisů Unie v oblasti finančních služeb, se oznamování závažných incidentů omezuje na incidenty, které jsou uvedeny v čl. 3 odst. 44 písm. c).

4. U vysoce rizikových systémů UI, které jsou bezpečnostními součástmi zařízení nebo jsou samy zařízeními, na něž se vztahuje nařízení (EU) 2017/745 a nařízení (EU) 2017/746, se oznamování závažných incidentů omezuje na incidenty, které jsou uvedeny v čl. 3 odst. 44 písm. c), a provádí se u příslušného vnitrostátního orgánu zvoleného pro tento účel členskými státy, v nichž k danému incidentu došlo.

KAPITOLA 3

PROSAZOVÁNÍ PRÁVA

Článek 63

Dozor nad trhem a kontrola systémů UI na trhu Unie

1. Na systémy UI upravené tímto nařízením se vztahuje nařízení (EU) 2019/1020. Pro účely účinného prosazování tohoto nařízení však platí, že:

   a) jakýkoli odkaz na hospodářský subjekt podle nařízení (EU) 2019/1020 je třeba chápat tak, že zahrnuje všechny provozovatele uvedené v článku 2 tohoto nařízení;

   b) jakýkoli odkaz na výrobek podle nařízení (EU) 2019/1020 je třeba chápat tak, že zahrnuje všechny systémy UI spadající do oblasti působnosti tohoto nařízení.

2. V rámci svých oznamovacích povinností podle čl. 34 odst. 4 nařízení (EU) 2019/1020 podávají orgány dozoru nad trhem Komisi zprávy o výsledcích příslušných činností v oblasti dozoru nad trhem podle tohoto nařízení.

3. U vysoce rizikových systémů UI souvisejících s výrobky, na které se vztahují právní akty uvedené v příloze II oddíle A, je orgánem dozoru nad trhem pro účely tohoto nařízení orgán odpovědný za činnosti v oblasti dozoru nad trhem určený podle uvedených právních aktů nebo, v odůvodněných případech a za předpokladu, že je zajištěna koordinace, jiný příslušný orgán určený členským státem.

   Postupy uvedené v článcích 65, 66, 67 a 68 tohoto nařízení se nepoužijí na systémy UI související s produkty, na něž se vztahují právní akty uvedené v příloze II oddíle A, pokud jsou v těchto právních aktech už stanoveny postupy se stejným cílem. V takovém případě se místo toho použijí dané odvětvové postupy.

4. U vysoce rizikových systémů UI uváděných na trh, do provozu nebo využívaných finančními institucemi, na něž se vztahují právní předpisy Unie v oblasti finančních služeb, je orgánem dozoru nad trhem pro účely tohoto nařízení příslušný vnitrostátní orgán odpovědný za finanční dohled nad těmito institucemi podle uvedených právních předpisů, pokud je uvedení na trh, do provozu nebo používání systému UI v přímé souvislosti s poskytováním těchto finančních služeb.

   Odchylně od předchozího pododstavce může členský stát v odůvodněných případech a za předpokladu, že je zajištěna koordinace, určit pro účely tohoto nařízení jiný příslušný orgán jako orgán dozoru nad trhem.

   Vnitrostátní orgány dozoru nad trhem odpovědné za dohled nad úvěrovými institucemi, na něž se vztahuje směrnice 2013/36/EU a které se účastní jednotného mechanismu dohledu zřízeného nařízením Rady č. 1204/2013, by měly neprodleně podat Evropské centrální bance zprávu o veškerých informacích zjištěných v průběhu svých činností v oblasti dozoru nad trhem, které by mohly mít potenciální význam pro úkoly Evropské centrální banky v oblasti obezřetnostního dohledu podle uvedeného nařízení.

5. Pokud jde o vysoce rizikové systémy UI uvedené v bodě 1 písm. a), pokud se tyto systémy používají pro účely prosazování práva dle bodů 6, 7 a 8 přílohy III, určí členské státy jako orgány dozoru nad trhem pro účely tohoto nařízení buď vnitrostátní orgány vykonávající dohled nad činností donucovacích orgánů, orgánů ochrany hranic, imigračních, azylových nebo justičních orgánů, nebo příslušné dozorové úřady pro ochranu údajů podle směrnice (EU) 2016/680 či nařízení 2016/679. Činnosti v oblasti dozoru nad trhem nijak neovlivní nezávislost justičních orgánů ani jinak nezasahují do jejich činnosti při výkonu jejich soudní pravomoci.

6. Pokud orgány, instituce a subjekty Unie spadají do oblasti působnosti tohoto nařízení, jedná jako jejich orgán dozoru nad trhem evropský inspektor ochrany údajů.

7. Členské státy usnadňují koordinaci mezi orgány dozoru nad trhem určenými podle tohoto nařízení a dalšími příslušnými vnitrostátními orgány nebo subjekty, které dohlížejí na uplatňování harmonizačních právních předpisů Unie uvedených v příloze II nebo jiných právních předpisů Unie, které by mohly být relevantní pro vysoce rizikové systémy UI uvedené v příloze III.

8. Aniž jsou dotčeny pravomoci stanovené nařízením (EU) 2019/1020 a je-li to relevantní a omezené na to, co je nezbytné pro plnění jejich úkolů, orgánům dozoru nad trhem je poskytovatelem udělen plný přístup k dokumentaci, jakož i k souborům tréninkových, validačních a testovacích dat používaných pro vývoj vysoce rizikového systému UI, a to i, v příslušných případech a s výhradou bezpečnostních záruk, prostřednictvím aplikačních programovacích rozhraní (API) nebo jiných vhodných technických prostředků a nástrojů umožňujících dálkový přístup.

9. Orgánům dozoru nad trhem se na základě odůvodněné žádosti a pouze tehdy, jsou-li splněny tyto kumulativní podmínky, poskytne přístup ke zdrojovému kódu vysoce rizikového systému UI:

a) přístup ke zdrojovému kódu je nezbytný k posouzení shody vysoce rizikového systému UI s požadavky stanovenými v hlavě III kapitole 2 a

b) postupy testování či auditu a ověřování na základě dat a dokumentace poskytnuté poskytovatelem byly vyčerpány nebo se ukázaly jako nedostatečné.

10. S veškerými informacemi a dokumentací získanými orgány dozoru nad trhem podle tohoto článku se nakládá v souladu s povinnostmi zachování důvěrnosti stanovenými v článku 70.

11. Stížnosti může příslušnému orgánu dozoru nad trhem podat jakákoli fyzická nebo právnická osoba, která má důvod se domnívat, že došlo k porušení ustanovení tohoto nařízení.

V souladu s čl. 11 odst. 3 písm. e) a odst. 7 písm. a) nařízení (EU) 2019/1020 se stížnosti zohlední pro účely provádění činností dozoru nad trhem a vyřizují se v souladu se specializovanými postupy, které pro tyto účely stanoví orgány dozoru nad trhem.

Článek 63a

Dohled nad testováním v reálných podmínkách vykonávaný orgány dozoru nad trhem

1. Orgány dozoru nad trhem mají kompetence a pravomoci k zajištění toho, aby bylo testování v reálných podmínkách v souladu s tímto nařízením.

2. Pokud se testování v reálných podmínkách provádí u systémů UI, nad nimiž je vykonáván dohled v rámci regulačního pískoviště UI podle článku 54, ověří orgány dozoru nad trhem v rámci své dozorčí úlohy týkající se regulačního pískoviště UI soulad s ustanoveními článku 54a. Tyto orgány mohou případně povolit, aby testování v reálných podmínkách provedl poskytovatel nebo potenciální poskytovatel odchylně od podmínek stanovených v čl. 54a odst. 4 písm. f) a g).

3. Byl-li orgán dozoru nad trhem potenciálním poskytovatelem, poskytovatelem nebo jakoukoli třetí stranou informován o závažném incidentu nebo má-li jiné důvody se domnívat, že podmínky stanovené v článcích 54a a 54b nejsou splněny, může na svém území případně přijmout kterékoli z těchto rozhodnutí:

a) pozastavit nebo ukončit testování v reálných podmínkách;

b) požadovat, aby poskytovatel nebo potenciální poskytovatel a uživatel (uživatelé) změnili jakýkoli aspekt testování v reálných podmínkách.

4. Pokud orgán dozoru nad trhem přijal rozhodnutí uvedené v odstavci 3 tohoto článku nebo vznesl námitku ve smyslu čl. 54a odst. 4 písm. b), musí být v rozhodnutí nebo námitce uvedeno jejich odůvodnění, jakož i způsoby a podmínky, za nichž může poskytovatel nebo potenciální poskytovatel toto rozhodnutí nebo tuto námitku napadnout.

5. Pokud orgán dozoru nad trhem přijal rozhodnutí uvedené v odstavci 3 tohoto článku, sdělí případně důvody tohoto rozhodnutí orgánům dozoru nad trhem ostatních členských států, v nichž byl systém UI testován v souladu s plánem testování.

Článek 64

Pravomoci orgánů chránících základní práva

1. [vypouští se]

2. [vypouští se]

3. Vnitrostátní veřejné orgány nebo subjekty veřejného sektoru, které dohlížejí na dodržování povinností stanovených v právních předpisech Unie na ochranu základních práv, včetně práva na nediskriminaci, v souvislosti s používáním vysoce rizikových systémů UI uvedených v příloze III, případně je vymáhají, jsou oprávněny vyžádat si jakoukoli dokumentaci vytvořenou nebo vedenou podle tohoto nařízení a mít k ní přístup, pokud je přístup k této dokumentaci nezbytný k plnění pravomocí vyplývajících z jejich pověření v rámci jejich příslušnosti. Příslušný veřejný orgán nebo subjekt veřejného sektoru o každé této žádosti informuje orgán dozoru nad trhem dotčeného členského státu.

4. Každý členský stát určí do tří měsíců po vstupu tohoto nařízení v platnost veřejné orgány nebo subjekty veřejného sektoru uvedené v odstavci 3 a zveřejní jejich seznam. Členské státy oznámí tento seznam Komisi a všem ostatním členským státům a průběžně jej aktualizují.

5. Pokud dokumentace uvedená v odstavci 3 není dostatečná k tomu, aby bylo možné zjistit, zda došlo k porušení povinností podle právních předpisů Unie, jejichž cílem je ochrana základních práv, může veřejný orgán nebo subjekt veřejného sektoru uvedený v odstavci 3 podat orgánu dozoru nad trhem odůvodněnou žádost o uspořádání testů vysoce rizikového systému UI technickými prostředky. Orgán dozoru nad trhem uspořádá tyto testy, do nichž bude dožadující veřejný orgán nebo subjekt veřejného sektoru významně zapojen, v přiměřené lhůtě po podání žádosti.

6. S veškerými informacemi a dokumentací získanými vnitrostátními veřejnými orgány nebo subjekty veřejného sektoru uvedenými v odstavci 3 podle ustanovení tohoto článku se nakládá v souladu s povinnostmi zachování důvěrnosti stanovenými v článku 70.

Článek 65

Postup nakládání se systémy UI, které představují riziko, na vnitrostátní úrovni

1. Systémy UI, které představují riziko, jsou považovány za výrobek představující riziko podle čl. 3 bodu 19 nařízení (EU) 2019/1020, pokud jde o rizika pro zdraví, bezpečnost nebo základní práva osob.

2. Pokud má orgán dozoru nad trhem členského státu dostatečné důvody domnívat se, že systém UI představuje riziko podle odstavce 1, provede hodnocení dotčeného systému UI z hlediska jeho souladu se všemi požadavky a povinnostmi stanovenými v tomto nařízení. Pokud jsou zjištěna rizika týkající se základních práv, informuje orgán dozoru nad trhem rovněž příslušné vnitrostátní veřejné orgány nebo subjekty veřejného sektoru uvedené v čl. 64 odst. 3. Příslušní provozovatelé podle potřeby spolupracují s orgány dozoru nad trhem a s dalšími vnitrostátními veřejnými orgány nebo subjekty veřejného sektoru uvedenými v čl. 64 odst. 3.

   Pokud v průběhu tohoto hodnocení orgán dozoru nad trhem zjistí, že systém UI nesplňuje požadavky a povinnosti stanovené tímto nařízením, neprodleně vyzve příslušného provozovatele, aby přijal veškerá vhodná nápravná opatření k uvedení systému UI do souladu nebo k jeho stažení z trhu nebo z oběhu ve lhůtě, kterou může orgán dozor nad trhem stanovit.

   Orgán dozoru nad trhem o tom informuje příslušný oznámený subjekt. Na opatření uvedená v druhém pododstavci se použije článek 18 nařízení (EU) 2019/1020.

3. Domnívá-li se orgán dozoru nad trhem, že se nesoulad netýká pouze území jeho členského státu, neprodleně informuje Komisi a ostatní členské státy o výsledcích hodnocení a o opatřeních, která má provozovatel na jeho žádost přijmout.

4. Provozovatel zajistí, aby byla přijata všechna vhodná nápravná opatření ohledně všech dotčených systémů UI, které dodal na trh v celé Unii.

5. Pokud provozovatel systému UI ve lhůtě uvedené v odstavci 2 nepřijme přiměřená nápravná opatření, přijme orgán dozoru nad trhem všechna vhodná dočasná opatření k omezení nebo zákazu dodávání systému UI na trh svého členského státu nebo k zajištění toho, že je tento produkt stažen z trhu nebo z oběhu. O takových opatřeních tento orgán neprodleně informuje Komisi a ostatní členské státy.

6. Součástí oznámení uvedeného v odstavci 5 jsou všechny dostupné podrobnosti, zejména informace nezbytné pro identifikaci nevyhovujícího systému UI, údaje o původu systému UI, povaze nesouladu a souvisejícího rizika, povaze a době trvání opatření přijatých na vnitrostátní úrovni a stanoviska příslušného poskytovatele. Orgány dozoru nad trhem zejména uvedou, zda je důvodem nesouladu jeden nebo více těchto nedostatků:

(-a) nedodržení zákazu postupů v oblasti umělé inteligence uvedených v článku 5;

a) vysoce rizikový systém UI nesplňuje požadavky uvedené v hlavě III kapitole 2;

b) nedostatky v harmonizovaných normách nebo ve společných specifikacích uvedených v článcích 40 a 41, na nichž je založen předpoklad shody.

c) nesoulad s ustanoveními uvedenými v článku 52;

d) nesoulad obecných systémů UI s požadavky a povinnostmi uvedenými v článku 4a;

7. Orgány dozoru nad trhem členských států jiné než orgán dozoru nad trhem členského státu, který zahájil tento postup, neprodleně informují Komisi a ostatní členské státy o veškerých opatřeních, která přijaly, a o všech doplňujících údajích týkajících se nesouladu dotčeného systému UI, které mají k dispozici, a v případě nesouhlasu s oznámeným vnitrostátním opatřením o svých námitkách.

8. Jestliže do tří měsíců od přijetí oznámení uvedeného v odstavci 5 nevznese žádný členský stát ani Komise námitku proti předběžnému opatření přijatému členským státem, považuje se uvedené opatření za odůvodněné. Tím nejsou dotčena procesní práva dotčeného provozovatele v souladu s článkem 18 nařízení (EU) 2019/1020. Lhůta uvedená v první větě tohoto odstavce se zkracuje na 30 dnů v případě nedodržení zákazu postupů v oblasti umělé inteligence podle článku 5.

9. Orgány dozoru nad trhem všech členských států poté zajistí, aby byla v souvislosti s dotčeným systémem AI bezodkladně přijata náležitá restriktivní opatření, například stažení daného produktu z jejich trhů.

Článek 66

Ochranný postup Unie

1. Pokud do tří měsíců od obdržení oznámení uvedeného v čl. 65 odst. 5 nebo do třiceti dnů v případě nedodržení zákazu postupů v oblasti umělé inteligence podle článku 5 vznese některý členský stát námitky proti opatření přijatému jiným členským státem nebo pokud se Komise domnívá, že je dané opatření v rozporu s právem Unie, zahájí Komise neprodleně konzultaci s příslušným orgánem dozoru nad trhem a provozovatelem nebo provozovateli členského státu a provede hodnocení tohoto vnitrostátního opatření. Na základě výsledků tohoto hodnocení Komise rozhodne, zda je vnitrostátní opatření odůvodněné či nikoli, a to do devíti měsíců nebo 60 dnů v případě nedodržení zákazu postupů v oblasti umělé inteligence podle článku 5, počínaje oznámením podle čl. 65 odst. 5. Toto rozhodnutí oznámí Komise dotčenému členskému státu. O rozhodnutí rovněž uvědomí ostatní členské státy.

2. Pokud Komise považuje opatření přijaté orgánem dozoru nad trhem dotčeného členského státu za odůvodněné, orgány dozoru nad trhem všech členských států zajistí, aby byla v souvislosti s dotčeným systémem UI přijata vhodná omezující opatření, jako je neprodlené stažení systému UI z daného trhu, a informují o tom Komisi. Pokud Komise považuje vnitrostátní opatření za neodůvodněné, orgán dozoru nad trhem dotčeného členského státu toto opatření zruší a uvědomí o tom Komisi.

3. Pokud je vnitrostátní opatření považováno za odůvodněné a je-li nesoulad systému UI přisuzován nedostatkům v harmonizovaných normách nebo společných specifikacích, jak je uvedeno v článcích 40 a 41 tohoto nařízení, použije Komise postup stanovený v článku 11 nařízení (EU) č. 1025/2012.

Článek 67

Vyhovující vysoce rizikové nebo obecné systémy UI, které představují riziko

1. Pokud orgán dozoru nad trhem členského státu po provedení hodnocení podle článku 65 zjistí, že ačkoli je vysoce rizikový nebo obecný systém UI v souladu s tímto nařízením, představuje riziko pro zdraví nebo bezpečnost osob či pro základní práva, vyzve příslušného provozovatele, aby přijal veškerá vhodná opatření k zajištění toho, aby dotčený systém UI, pokud bude uveden na trh nebo do provozu, dále nepředstavoval toto riziko, nebo aby byl tento systém UI neprodleně stažen z trhu nebo z oběhu ve lhůtě, kterou může členský stát stanovit.

2. Poskytovatel nebo jiní příslušní provozovatelé zajistí, aby byla přijata nápravná opatření ve vztahu ke všem dotčeným systémům UI, které dodali na trh v rámci celé Unie, ve lhůtě stanovené orgánem dozoru nad trhem členského státu uvedeného v odstavci 1.

3. Tento členský stát o tom neprodleně informuje Komisi a ostatní členské státy. Tato informace musí obsahovat všechny dostupné podrobnosti, zejména údaje nezbytné pro identifikaci dotčeného systému UI, údaje o jeho původu a dodavatelském řetězci, údaje o povaze souvisejícího rizika a údaje o povaze a době trvání opatření přijatých na vnitrostátní úrovni.

4. Komise neprodleně zahájí konzultaci s dotčenými členskými státy a s příslušným provozovatelem a vyhodnotí přijatá vnitrostátní opatření. Na základě výsledků tohoto hodnocení Komise rozhodne, zda jsou opatření odůvodněná či nikoli, a pokud je to nutné, navrhne vhodná opatření.

5. Rozhodnutí Komise je určeno dotčenému členskému státu, přičemž všechny ostatní členské státy jsou o daném rozhodnutí uvědomeny.

Článek 68

Formální nesoulad

1. Orgán dozoru nad trhem daného členského státu požádá příslušného provozovatele, aby ve lhůtě, kterou může orgán dozor nad trhem stanovit, odstranil dotčený nesoulad, pokud zjistí jeden z těchto nedostatků:

   a) označení CE bylo umístěno v rozporu s článkem 49;

   b) označení CE nebylo umístěno;

   c) nebylo vypracováno EU prohlášení o shodě;

   d) EU prohlášení o shodě nebylo vypracováno správně;

   e) identifikační číslo oznámeného subjektu, který je tam, kde je to relevantní, zapojen do postupu posuzování shody, nebylo umístěno.

2. Pokud nesoulad uvedený v odstavci 1 nadále trvá, přijme dotčený členský stát všechna vhodná opatření a omezí nebo zakáže dodávání vysoce rizikového systému UI na trh, nebo zajistí, aby byl tento systém stažen z oběhu nebo z trhu.

Článek 68a

Zkušební zařízení Unie v oblasti umělé inteligence

1. Komise určí jedno nebo více zkušebních zařízení Unie v oblasti umělé inteligence podle článku 21 nařízení (EU) 2019/1020.

2. Aniž jsou dotčeny činnosti zkušebních zařízení Unie uvedené v čl. 21 odst. 6 nařízení (EU) 2019/1020, poskytují zkušební zařízení Unie uvedená v odstavci 1 na žádost rady nebo orgánů dozoru nad trhem rovněž nezávislé technické nebo vědecké poradenství.

Článek 68a

Centrální skupina nezávislých odborníků

1. Na žádost rady pro UI přijme Komise prostřednictvím prováděcího aktu ustanovení o vytvoření, udržování a financování centrální skupiny nezávislých odborníků na podporu činností v oblasti prosazování práva podle tohoto nařízení.

2. Odborníci jsou vybíráni Komisí a zařazeni do centrální skupiny na základě aktuálních vědeckých nebo technických odborných znalostí v oblasti umělé inteligence, s náležitým ohledem na technické oblasti, na něž se vztahují požadavky a povinnosti stanovené v tomto nařízení, jakož i na činnosti orgánů dozoru nad trhem podle článku 11 nařízení (EU) 2019/1020. Komise určí počet členů odborníků v této skupině na základě aktuálních potřeb.

3. Odborníci mohou mít tyto úkoly:

a) poskytovat orgánům dozoru nad trhem poradenství a podporovat jejich činnost, a to na jejich žádost;

b) podporovat přeshraniční šetření v oblasti dozoru nad trhem podle čl. 58 písm. h), aniž jsou dotčeny pravomoci orgánů dozoru nad trhem;

c) poskytovat poradenství a podporovat Komisi při plnění jejích povinností v souvislosti s ochrannou doložkou podle článku 66.

4. Odborníci plní své úkoly nestranně a objektivně a zajišťují důvěrnost informací a údajů získaných při plnění svých úkolů a činností. Každý odborník vypracuje prohlášení o střetu zájmů, které je veřejně dostupné. Komise zavede systémy a postupy s cílem řídit případné střety zájmů a zabránit jim.

5. Za poradenství a podporu odborníků mohou být členské státy povinny hradit poplatky. Strukturu a výši poplatků, jakož i rozsah a strukturu nahraditelných nákladů přijme Komise prostřednictvím prováděcího aktu uvedeného v odstavci 1, přičemž zohlední cíle náležitého provádění tohoto nařízení, nákladovou efektivnost a nutnost zajistit, aby všechny členské státy měly k odborníkům účinný přístup.

6. Komise podle potřeby usnadní členským státům včasný přístup k odborníkům a zajistí, aby kombinace podpůrných činností prováděných zkušebními zařízeními Unie podle článku 68a a odborníky podle tohoto článku byla účinně organizována a přinášela co nejlepší přidanou hodnotu.

HLAVA IX

KODEXY CHOVÁNÍ

Článek 69

Kodexy chování v případě dobrovolného uplatňování konkrétních požadavků

1. Komise a členské státy usnadňují vypracovávání kodexů chování, které mají v co největší míře podpořit dobrovolné uplatňování jednoho či více požadavků stanovených v hlavě III kapitole 2 tohoto nařízení na jiné než vysoce rizikové systémy UI, při zohlednění dostupných technických řešení umožňujících uplatňování těchto požadavků.

2. Komise a členské státy usnadňují vypracovávání kodexů chování, které mají podpořit dobrovolné uplatňování konkrétních požadavků týkajících se například udržitelnosti z hlediska životního prostředí, a to i v souvislosti s energeticky účinným programováním, přístupnosti pro osoby se zdravotním postižením, zapojení zúčastněných stran do návrhu a vývoje systémů UI a rozmanitosti vývojových týmů na všechny systémy UI na základě jasných cílů a klíčových ukazatelů výkonnosti umožňujících měřit dosahování těchto cílů. Pokud jde o povinnosti uživatelů ve vztahu k systémům UI, Komise a členské státy rovněž případně usnadní vypracování kodexů chování použitelných na dobrovolném základě.

3. Kodexy chování použitelné na dobrovolném základě mohou být vypracovány jednotlivými poskytovateli systémů UI nebo organizacemi, které je zastupují, případně poskytovateli i organizacemi, a to i za účasti uživatelů a veškerých zúčastněných stran a jejich zastupujících organizací, či případně uživateli s ohledem na jejich povinnosti. Kodexy chování se mohou vztahovat na jeden nebo více systémů UI s přihlédnutím k podobnosti určeného účelu daných systémů.

4. Při podpoře a usnadňování vypracovávání kodexů chování uvedených v tomto článku zohlední Komise a členské státy konkrétní zájmy a potřeby poskytovatelů z řad malých a středních podniků, včetně začínajících podniků.

HLAVA X

DŮVĚRNOST A SANKCE

Článek 70

Důvěrnost

1. Příslušné vnitrostátní orgány, oznámené subjekty, Komise, rada a veškeré další fyzické nebo právnické osoby zapojené do používání tohoto nařízení zavádějí v souladu s právními předpisy Unie a vnitrostátními právními předpisy vhodná technická a organizační opatření s cílem zajistit důvěrnost informací a údajů, které získají při provádění svých úkolů a činností, takovým způsobem, aby chránily zejména:

a) práva duševního vlastnictví a důvěrné obchodní informace nebo obchodní tajemství fyzických nebo právnických osob, včetně zdrojového kódu s výjimkou případů, na které se vztahuje článek 5 směrnice 2016/943 o ochraně nezveřejněného know-how a obchodních informací (obchodního tajemství) před jejich neoprávněným získáním, využitím a zpřístupněním;

b) účinné provádění tohoto nařízení, zejména za účelem inspekcí, šetření nebo auditů;

c) veřejný zájem a zájem národní bezpečnosti;

d) integritu trestního nebo správního řízení;

e) integritu utajovaných informací v souladu s právními předpisy Unie a vnitrostátními právními předpisy.

2. Aniž je dotčen odstavec 1, informace vyměňované důvěrně mezi příslušnými vnitrostátními orgány a mezi příslušnými vnitrostátními orgány a Komisí se nezpřístupní bez předchozí dohody s příslušným vnitrostátním orgánem, který informace poskytl, a uživatelem, pokud jsou vysoce rizikové systémy UI uvedené v bodech 1, 6 a 7 přílohy III používány donucovacími orgány, orgány ochrany hranic, imigračními nebo azylovými orgány a jejich zveřejnění by ohrozilo zájmy veřejné a vnitrostátní bezpečnosti. Tato povinnost výměny informací se nevztahuje na citlivé provozní údaje týkající se činností donucovacích orgánů, orgánů ochrany hranic, imigračních nebo azylových orgánů.

Pokud jsou uvedené donucovací, imigrační nebo azylové orgány poskytovateli vysoce rizikových systémů UI uvedených v bodech 1, 6 a 7 přílohy III, technická dokumentace uvedená v příloze IV zůstává v prostorách těchto orgánů. Tyto orgány zajistí, aby orgány dozoru nad trhem uvedené v čl. 63 odst. 5 a 6 mohly případně na požádání okamžitě získat přístup k této dokumentaci nebo obdržet její kopii. K této dokumentaci nebo k jakékoli její kopii mají přístup pouze pracovníci orgánu dozoru nad trhem, kteří mají bezpečnostní prověrku na odpovídající úrovni.

3. Ustanoveními odstavců 1 a 2 nejsou dotčena práva a povinnosti Komise, členských států a jejich příslušných orgánů, jakož i oznámených subjektů ohledně vzájemného informování a šíření výstrah, a to i v souvislosti s přeshraniční spoluprací, ani povinnosti dotčených stran poskytovat informace podle trestního práva členských států.

Článek 71

Sankce

1. Členské státy stanoví v souladu s podmínkami uvedenými v tomto nařízení pravidla pro ukládání sankcí, včetně správních pokut za porušení tohoto nařízení, a přijmou veškerá opatření nezbytná k zajištění jejich řádného a účinného uplatňování. Stanovené sankce musí být účinné, přiměřené a odrazující. Zohledňují zejména velikost a zájmy poskytovatelů z řad malých a středních podniků, včetně začínajících podniků, a jejich ekonomickou životaschopnost. Rovněž zohlední, zda se systém UI používá v souvislosti s osobní jinou než profesionální činností.

2. Členské státy neprodleně oznámí Komisi uvedená pravidla a opatření a veškeré následné změny, které se jich týkají.

3. Za nedodržení kteréhokoli zákazu postupů v oblasti umělé inteligence podle článku 5 se uloží správní pokuty až do výše 30 000 000 EUR, nebo, dopustí-li se porušení společnost, až do výše 6 % jejího celkového ročního obratu celosvětově za předchozí finanční rok podle toho, která hodnota je vyšší. V případě malých a středních podniků, včetně začínajících podniků, činí tyto pokuty až 3 % jejich ročního obratu celosvětově za předchozí finanční rok.

4. Za porušení následujících ustanovení týkajících se provozovatelů nebo oznámených subjektů se uloží správní pokuty až do výše 20 000 000 EUR nebo, dopustí-li se porušení společnost, až do výše 4 % jejího celkového ročního obratu celosvětově za předchozí finanční rok podle toho, která hodnota je vyšší:

-a) povinnosti poskytovatelů podle článků 4b a 4c;

a) povinnosti poskytovatelů podle článku 16;

b) povinnosti některých dalších osob podle článku 23a;

c) povinnosti zplnomocněných zástupců podle článku 25;

d) povinnosti dovozců podle článku 26;

e) povinnosti distributorů podle článku 27;

f) povinnosti uživatelů podle čl. 29 odst. 1 až 6a;

g) požadavky a povinnosti oznámených subjektů podle článku 33, čl. 34 odst. 1, čl. 34 odst. 3 a 4 a článku 34a;

h) povinnosti transparentnosti pro poskytovatele a uživatele podle článku 52.

V případě malých a středních podniků, včetně začínajících podniků, činí tyto pokuty až 2 % jejich ročního obratu celosvětově za předchozí finanční rok.

5. Za poskytnutí nesprávných, neúplných nebo zavádějících informací oznámeným subjektům a příslušným vnitrostátním orgánům v reakci na žádost se uloží správní pokuty až do výše 10 000 000 EUR, nebo, dopustí-li se porušení společnost, až do výše 2 % jejího celkového ročního obratu celosvětově za předchozí finanční rok podle toho, která hodnota je vyšší. V případě malých a středních podniků, včetně začínajících podniků, činí tyto pokuty až 1 % jejich ročního obratu celosvětově za předchozí finanční rok.

6. Při rozhodování o výši správní pokuty v jednotlivých případech se zohlední všechny příslušné okolnosti konkrétní situace s náležitým přihlédnutím k následujícím okolnostem:

a) povaha, závažnost a doba trvání porušení těchto ustanovení a jeho následky;

aa) zda k porušení došlo úmyslně nebo z nedbalosti;

ab) veškerá opatření učiněná provozovatelem za účelem nápravy daného porušení a zmírnění jeho možných nežádoucích účinků;

b) zda již byly stejnému provozovateli za stejné protiprávní jednání uloženy správní pokuty jinými orgány dozoru nad trhem v jiných členských státech;

ba) zda již jiné orgány uložily témuž provozovateli správní pokuty za porušení jiných právních předpisů Unie nebo vnitrostátních právních předpisů, pokud tato porušení vyplývají ze stejné činnosti nebo opomenutí, které představuje příslušné porušení tohoto aktu;

c) velikost a roční obrat provozovatele, který se porušení dopustil, a jeho podíl na trhu;

d) jakákoliv jiná přitěžující nebo polehčující okolnost vztahující se na okolnosti daného případu, jako jsou získaný finanční prospěch či zamezení ztrátám, přímo či nepřímo vyplývající z porušení.

7. Každý členský stát stanovuje pravidla týkající se toho, zda a do jaké míry je možno ukládat správní pokuty veřejným orgánům a subjektům veřejného sektoru usazeným v daném členském státě.

8. V závislosti na právním systému členských států lze pravidla pro správní pokuty použít tak, aby pokuty byly ukládány příslušnými vnitrostátními soudy nebo jinými orgány dle úpravy platné v těchto členských státech. Uplatňování těchto pravidel v uvedených členských státech má rovnocenný účinek.

9. Na výkon pravomocí orgánu dozoru nad trhem podle tohoto článku se vztahují vhodné procesní záruky v souladu s právem Unie a členského státu, včetně účinné soudní ochrany a spravedlivého procesu.

Článek 72

Správní pokuty ukládané orgánům, institucím a subjektům Unie

1. Evropský inspektor ochrany údajů může ukládat správní pokuty orgánům, institucím a subjektům Unie, které spadají do oblasti působnosti tohoto nařízení. Při rozhodování o tom, zda uložit správní pokutu, a rozhodování o výši správní pokuty v jednotlivých případech se zohlední všechny příslušné okolnosti konkrétní situace s náležitým přihlédnutím k následujícím okolnostem:

   a) povaha, závažnost a doba trvání porušení těchto ustanovení a jeho následky;

   b) spolupráce s evropským inspektorem ochrany údajů za účelem nápravy daného porušení a zmírnění jeho možných nežádoucích účinků, včetně splnění případných opatření, která dříve nařídil evropský inspektor ochrany údajů dotčené instituci, orgánu nebo subjektu Unie v souvislosti s touž záležitostí;

   c) všechna podobná předchozí porušení ze strany orgánu, instituce nebo subjektu Unie.

2. Za nedodržení kteréhokoli zákazu postupů v oblasti umělé inteligence podle článku 5 se uloží správní pokuty až do výše 500 000 EUR.

3. Za nesoulad systému UI s jakýmikoli požadavky nebo povinnostmi podle tohoto nařízení s výjimkou těch, které jsou stanoveny v článcích 5 a 10, se uloží správní pokuty až do výše 250 000 EUR.

4. Před přijetím rozhodnutí podle tohoto článku poskytne evropský inspektor ochrany údajů orgánu, instituci nebo subjektu Unie, se kterým vede řízení, příležitost vyjádřit své stanovisko k záležitosti týkající se daného možného porušení. Evropský inspektor ochrany údajů zakládá své rozhodnutí pouze na prvcích a okolnostech, ke kterým se dotčené osoby mohly vyjádřit. Případní stěžovatelé jsou do řízení úzce zapojeni.

5. Při řízení se plně dodrží právo dotčených stran na obhajobu. Musí mít přístup do spisu evropského inspektora ochrany údajů, s výhradou oprávněného zájmu jednotlivců nebo podniků na ochraně jejich osobních údajů nebo obchodního tajemství.

6. Prostředky vybrané ukládáním pokut podle tohoto článku jsou příjmem souhrnného rozpočtu Unie.

HLAVA XI

PŘENESENÍ PRAVOMOCI A POSTUP PROJEDNÁVÁNÍ VE VÝBORU

Článek 73

Výkon přenesené pravomoci

1. Pravomoc přijímat akty v přenesené pravomoci je svěřena Komisi za podmínek stanovených v tomto článku.

2. Pravomoc přijímat akty v přenesené pravomoci uvedená v čl. 7 odst. 1 a 3, čl. 11 odst. 3, čl. 43 odst. 5 a 6 a v čl. 48 odst. 5 je svěřena Komisi na období pěti let od [*vstupu tohoto nařízení v platnost*].

Komise vypracuje zprávu o výkonu přenesení pravomoci nejpozději devět měsíců před koncem tohoto pětiletého období. Přenesení pravomoci se automaticky prodlužuje o stejně dlouhá období, pokud Evropský parlament ani Rada nevysloví proti tomuto prodloužení námitku nejpozději tři měsíce před koncem každého z těchto období.

3. Evropský parlament nebo Rada mohou přenesení pravomocí uvedené v čl. 7 odst. 1 a 3, čl. 11 odst. 3, čl. 43 odst. 5 a 6 a v čl. 48 odst. 5 kdykoli zrušit. Rozhodnutím o zrušení se ukončuje přenesení pravomoci v něm blíže určené. Rozhodnutí nabývá účinku prvním dnem po zveřejnění v *Úředním věstníku Evropské unie* nebo k pozdějšímu dni, který je v něm upřesněn. Nedotýká se platnosti již platných aktů v přenesené pravomoci.

4. Přijetí aktu v přenesené pravomoci Komise neprodleně oznámí současně Evropskému parlamentu a Radě.

5. Akt v přenesené pravomoci přijatý podle čl. 7 odst. 1 a 3, čl. 11 odst. 3, čl. 43 odst. 5 a 6 a čl. 48 odst. 5 vstoupí v platnost, pouze pokud proti němu Evropský parlament nebo Rada nevysloví námitky ve lhůtě tří měsíců ode dne, kdy jim byl tento akt oznámen, nebo pokud Evropský parlament i Rada před uplynutím této lhůty informují Komisi o tom, že námitky nevysloví. Z podnětu Evropského parlamentu nebo Rady se tato lhůta prodlouží o tři měsíce.

Článek 74

Postup projednávání ve výboru

1. Komisi je nápomocen výbor. Tento výbor je výborem ve smyslu nařízení (EU) č. 182/2011.

2. Odkazuje-li se na tento odstavec, použije se článek 5 nařízení (EU) č. 182/2011.

HLAVA XII

ZÁVĚREČNÁ USTANOVENÍ

Článek 75

Změna nařízení (ES) č. 300/2008

V čl. 4 odst. 3 nařízení (ES) č. 300/2008 se doplňuje nový pododstavec, který zní:

„Při přijímání podrobných prováděcích opatření týkajících se technických specifikací a postupů pro schvalování a používání bezpečnostního vybavení ve vztahu k systémům umělé inteligence ve smyslu nařízení Evropského parlamentu a Rady (EU) YYY/XX [o umělé inteligenci]*, se zohledňují požadavky uvedené v kapitole 2 hlavě III uvedeného nařízení.

_____

* nařízení (EU) YYY/XX [o umělé inteligenci] (Úř. věst. …).“

Článek 76

Změna nařízení (EU) č. 167/2013

V čl. 17 odst. 5 nařízení (EU) č. 167/2013 se doplňuje nový pododstavec, který zní:

„Při přijímání aktů v přenesené pravomoci podle prvního pododstavce týkajících se systémů umělé inteligence, které představují bezpečnostní součásti ve smyslu nařízení Evropského parlamentu a Rady (EU) YYY/XX [o umělé inteligenci]*, se zohledňují požadavky uvedené v hlavě III kapitole 2 uvedeného nařízení.

_____

* nařízení (EU) YYY/XX [o umělé inteligenci] (Úř. věst. …).“

Článek 77

Změna nařízení (EU) č. 168/2013

V čl. 22 odst. 5 nařízení (EU) č. 168/2013 se doplňuje nový pododstavec, který zní:

„Při přijímání aktů v přenesené pravomoci podle prvního pododstavce týkajících se systémů umělé inteligence, které představují bezpečnostní součásti ve smyslu nařízení Evropského parlamentu a Rady (EU) YYY/XX [o umělé inteligenci]*, se zohledňují požadavky uvedené v hlavě III kapitole 2 uvedeného nařízení.

_____

* nařízení (EU) YYY/XX [o umělé inteligenci] (Úř. věst. …).“

Článek 78

Změna směrnice 2014/90/EU

V článku 8 směrnice 2014/90/EU se doplňuje nový odstavec, který zní:

„4. Pro systémy umělé inteligence, které představují součásti ve smyslu nařízení Evropského parlamentu a Rady (EU) YYY/XX [o umělé inteligenci]* zohlední Komise při provádění svých činností podle odstavce 1 a při přijímání technických specifikací a zkušebních norem v souladu s odstavci 2 a 3 požadavky stanovené v hlavě III kapitole 2 uvedeného nařízení.

_____

* nařízení (EU) YYY/XX [o umělé inteligenci] (Úř. věst. …).“

Článek 79

Změny směrnice (EU) 2016/797

V článku 5 směrnice (EU) 2016/797 se doplňuje nový odstavec, který zní:

„12. Při přijímání aktů v přenesené pravomoci podle odstavce 1 a prováděcích aktů podle odstavce 11 týkajících se systémů umělé inteligence, které představují bezpečnostní součásti ve smyslu nařízení Evropského parlamentu a Rady (EU) YYY/XX [o umělé inteligenci]* se zohledňují požadavky uvedené v hlavě III kapitole 2 uvedeného nařízení.

_____

* nařízení (EU) YYY/XX [o umělé inteligenci] (Úř. věst. …).“

Článek 80

Změna nařízení (EU) 2018/858

V článku 5 nařízení (EU) 2018/858 se doplňuje nový odstavec, který zní:

„4. Při přijímání aktů v přenesené pravomoci podle odstavce 3 týkajících se systémů umělé inteligence, které představují bezpečnostní součásti ve smyslu nařízení Evropského parlamentu a Rady (EU) YYY/XX [o umělé inteligenci] *, se zohledňují požadavky uvedené v hlavě III kapitole 2 uvedeného nařízení.

_____

* nařízení (EU) YYY/XX [o umělé inteligenci] (Úř. věst. …).“

Článek 81

Změna nařízení (EU) 2018/1139

Nařízení (EU) 2018/1139 se mění takto:

1) V článku 17 se doplňuje nový odstavec, který zní:

„3. Aniž je dotčen odstavec 2, zohledňují se při přijímání prováděcích aktů podle odstavce 1 týkajících se systémů umělé inteligence, které představují bezpečnostní součásti ve smyslu nařízení Evropského parlamentu a Rady (EU) YYY/XX [*o umělé inteligenci*]*, požadavky uvedené v hlavě III kapitole 2 uvedeného nařízení.

_____

* nařízení (EU) YYY/XX [o umělé inteligenci] (Úř. věst. …).“

2) V článku 19 se doplňuje nový odstavec, který zní:

„4. Při přijímání aktů v přenesené pravomoci podle odstavců 1 a 2 týkajících se systémů umělé inteligence, které představují bezpečnostní součásti ve smyslu nařízení (EU) YYY/XX [o umělé inteligenci], se zohledňují požadavky uvedené v hlavě III kapitole 2 uvedeného nařízení.“

3) V článku 43 se doplňuje nový odstavec, který zní:

„4. Při přijímání prováděcích aktů podle odstavce 1 týkajících se systémů umělé inteligence, které představují bezpečnostní součásti ve smyslu nařízení (EU) YYY/XX [o umělé inteligenci], se zohledňují požadavky uvedené v hlavě III kapitole 2 uvedeného nařízení.“

4) V článku 47 se doplňuje nový odstavec, který zní:

„3. Při přijímání aktů v přenesené pravomoci podle odstavců 1 a 2 týkajících se systémů umělé inteligence, které představují bezpečnostní součásti ve smyslu nařízení (EU) YYY/XX [o umělé inteligenci], se zohledňují požadavky uvedené v hlavě III kapitole 2 uvedeného nařízení.“

5) V článku 57 se doplňuje nový odstavec, který zní:

„Při přijímání těchto prováděcích aktů týkajících se systémů umělé inteligence, které představují bezpečnostní součásti ve smyslu nařízení (EU) YYY/XX [o umělé inteligenci], se zohledňují požadavky uvedené v hlavě III kapitole 2 uvedeného nařízení.“

6) V článku 58 se doplňuje nový odstavec, který zní:

„3. Při přijímání aktů v přenesené pravomoci podle odstavců 1 a 2 týkajících se systémů umělé inteligence, které představují bezpečnostní součásti ve smyslu nařízení (EU) YYY/XX [o umělé inteligenci], se zohledňují požadavky uvedené v hlavě III kapitole 2 uvedeného nařízení.“

Článek 82

Změna nařízení (EU) 2019/2144

V článku 11 nařízení (EU) 2019/2144 se doplňuje nový odstavec, který zní:

„3. Při přijímání prováděcích aktů podle odstavce 2 týkajících se systémů umělé inteligence, které představují bezpečnostní součásti ve smyslu nařízení Evropského parlamentu a Rady (EU) YYY/XX [o umělé inteligenci]*, se zohledňují požadavky uvedené v hlavě III kapitole 2 uvedeného nařízení.

_____

* nařízení (EU) YYY/XX [o umělé inteligenci] (Úř. věst. …).“

Článek 83

Systémy UI, které již byly uvedeny na trh nebo do provozu

1. Toto nařízení se nevztahuje na systémy UI, které jsou součástmi rozsáhlých informačních systémů zřízených právními akty uvedenými v příloze IX a které byly uvedeny na trh nebo do provozu před [*12 měsíci od data použitelnosti tohoto nařízení uvedeného v čl. 85 odst. 2)*], pokud nahrazení nebo změna těchto právních aktů nevede k významné změně návrhu nebo určeného účelu dotčeného systému UI nebo dotčených systémů UI.

   Požadavky stanovené v tomto nařízení se tam, kde je to relevantní, zohlední při hodnocení všech rozsáhlých informačních systémů zřízených právními akty uvedenými v příloze IX, které se má provádět v souladu s těmito příslušnými akty.

2. Toto nařízení se vztahuje na vysoce rizikové systémy UI jiné než ty, jež upravuje odstavec 1, které byly uvedeny na trh nebo do provozu před [*datem použitelnosti tohoto nařízení uvedeným v čl. 85 odst. 2*], pouze pokud po uvedeném datu dojde k významným změnám návrhu nebo určeného účelu těchto systémů.

Článek 84

Hodnocení a přezkum

1. [vypouští se]

1b. Komise posuzuje potřebu změny seznamu uvedeného v příloze III každých 24 měsíců od vstupu tohoto nařízení v platnost a do konce období přenesení pravomoci. Závěry tohoto posouzení se předloží Evropskému parlamentu a Radě.

2. Do [*tří let od data použitelnosti tohoto nařízení uvedeného v čl. 85 odst. 2*] a poté každé čtyři roky předloží Komise Evropskému parlamentu a Radě zprávu o hodnocení a přezkumu tohoto nařízení. Tyto zprávy se zveřejní.

3. Zprávy uvedené v odstavci 2 věnují obzvláštní pozornost následujícím skutečnostem:

   a) stavu finančních zdrojů, technického vybavení a lidských zdrojů příslušných vnitrostátních orgánů určených na účinné plnění úkolů, kterými byly tyto orgány pověřeny podle tohoto nařízení;

   b) stavu sankcí, a zejména správních pokut uvedených v čl. 71 odst. 1, které členské státy uplatňují v případě porušení ustanovení tohoto nařízení.

4. Do [*tří let od data použitelnosti tohoto nařízení uvedeného v čl. 85 odst. 2*] a poté případně každé čtyři roky zhodnotí Komise dopad a účinnost dobrovolných kodexů chování, které mají podpořit uplatňování požadavků stanovených v hlavě III kapitole 2 na všechny systémy UI kromě vysoce rizikových systémů UI, a případně dalších požadavků na systémy UI, včetně požadavků týkajících se udržitelnosti životního prostředí.

5. Pro účely odstavců 1 až 4 poskytuje rada, členské státy a příslušné vnitrostátní orgány Komisi na její žádost příslušné informace.

6. Při provádění hodnocení a přezkumů podle odstavců 1 až 4 zohlední Komise postoje a zjištění rady, Evropského parlamentu, Rady a dalších příslušných subjektů nebo zdrojů.

7. Komise v případě potřeby předloží vhodné návrhy na změnu tohoto nařízení, zejména s přihlédnutím k vývoji technologií a dosaženému pokroku v informační společnosti.

Článek 85

Vstup v platnost a použitelnost

1. Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

2. Toto nařízení se použije [36 měsíců od vstupu tohoto nařízení v platnost].

3. Odchylně od odstavce 2:

   a) hlava III kapitola 4 a hlava VI se použijí ode dne [dvanáct měsíců od vstupu tohoto nařízení v platnost];

   b) článek 71 se použije ode dne [dvanáct měsíců od vstupu tohoto nařízení v platnost].

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V Bruselu dne

Za Evropský parlament	*Za Radu*
předseda/předsedkyně	*předseda/předsedkyně*

PŘÍLOHA I

[vypouští se]

PŘÍLOHA II

SEZNAM HARMONIZAČNÍCH PRÁVNÍCH PŘEDPISŮ UNIE

Oddíl A – Seznam harmonizačních právních předpisů Unie vycházejících z nového legislativního rámce

1. Směrnice Evropského parlamentu a Rady 2006/42/ES ze dne 17. května 2006 o strojních zařízeních a o změně směrnice 95/16/ES (Úř. věst. L 157, 9.6.2006, s. 24) [zrušená nařízením o strojních zařízeních]

2. Směrnice Evropského parlamentu a Rady 2009/48/ES ze dne 18. června 2009 o bezpečnosti hraček (Úř. věst. L 170, 30.6.2009, s. 1)

3. Směrnice Evropského parlamentu a Rady 2013/53/EU ze dne 20. listopadu 2013 o rekreačních plavidlech a vodních skútrech a o zrušení směrnice 94/25/ES (Úř. věst. L 354, 28.12.2013, s. 90)

4. Směrnice Evropského parlamentu a Rady 2014/33/EU ze dne 26. února 2014 o harmonizaci právních předpisů členských států týkajících se výtahů a bezpečnostních komponent pro výtahy (Úř. věst. L 96, 29.3.2014, s. 251)

5. Směrnice Evropského parlamentu a Rady 2014/34/EU ze dne 26. února 2014 o harmonizaci právních předpisů členských států týkajících se zařízení a ochranných systémů určených k použití v prostředí s nebezpečím výbuchu (Úř. věst. L 96, 29.3.2014, s. 309)

6. Směrnice Evropského parlamentu a Rady 2014/53/EU ze dne 16. dubna 2014 o harmonizaci právních předpisů členských států týkajících se dodávání rádiových zařízení na trh a zrušení směrnice 1999/5/ES (Úř. věst. L 153, 22.5.2014, s. 62)

7. Směrnice Evropského parlamentu a Rady 2014/68/EU ze dne 15. května 2014 o harmonizaci právních předpisů členských států týkajících se dodávání tlakových zařízení na trh (Úř. věst. L 189, 27.6.2014, s. 164)

8. Nařízení Evropského parlamentu a Rady (EU) 2016/424 ze dne 9. března 2016 o lanových dráhách a o zrušení směrnice 2000/9/ES (Úř. věst. L 81, 31.3.2016, s. 1)

9. Nařízení Evropského parlamentu a Rady (EU) 2016/425 ze dne 9. března 2016 o osobních ochranných prostředcích a o zrušení směrnice Rady 89/686/EHS (Úř. věst. L 81, 31.3.2016, s. 51)

10. Nařízení Evropského parlamentu a Rady (EU) 2016/426 ze dne 9. března 2016 o spotřebičích plynných paliv a o zrušení směrnice 2009/142/ES (Úř. věst. L 81, 31.3.2016, s. 99)

11. Nařízení Evropského parlamentu a Rady (EU) 2017/745 ze dne 5. dubna 2017 o zdravotnických prostředcích, změně směrnice 2001/83/ES, nařízení (ES) č. 178/2002 a nařízení (ES) č. 1223/2009 a o zrušení směrnic Rady 90/385/EHS a 93/42/EHS (Úř. věst. L 117, 5.5.2017, s. 1)

12. Nařízení Evropského parlamentu a Rady (EU) 2017/746 ze dne 5. dubna 2017 o diagnostických zdravotnických prostředcích in vitro a o zrušení směrnice 98/79/ES a rozhodnutí Komise 2010/227/EU (Úř. věst. L 117, 5.5.2017, s. 176)

Oddíl B – Seznam jiných harmonizačních právních předpisů Unie

1. Nařízení Evropského parlamentu a Rady (ES) č. 300/2008 ze dne 11. března 2008 o společných pravidlech v oblasti ochrany civilního letectví před protiprávními činy a o zrušení nařízení (ES) č. 2320/2002 (Úř. věst. L 97, 9.4.2008, s. 72)

2. Nařízení Evropského parlamentu a Rady (EU) č. 168/2013 ze dne 15. ledna 2013 o schvalování dvoukolových nebo tříkolových vozidel a čtyřkolek a dozoru nad trhem s těmito vozidly (Úř. věst. L 60, 2.3.2013, s. 52)

3. Nařízení Evropského parlamentu a Rady (EU) č. 167/2013 ze dne 5. února 2013 o schvalování zemědělských a lesnických vozidel a dozoru nad trhem s těmito vozidly (Úř. věst. L 60, 2.3.2013, s. 1)

4. Směrnice Evropského parlamentu a Rady 2014/90/EU ze dne 23. července 2014 o lodní výstroji a o zrušení směrnice Rady 96/98/ES (Úř. věst. L 257, 28.8.2014, s. 146)

5. Směrnice Evropského parlamentu a Rady (EU) 2016/797 ze dne 11. května 2016 o interoperabilitě železničního systému v Evropské unii (Úř. věst. L 138, 26.5.2016, s. 44)

6. Nařízení Evropského parlamentu a Rady (EU) 2018/858 ze dne 30. května 2018 o schvalování motorových vozidel a jejich přípojných vozidel, jakož i systémů, konstrukčních částí a samostatných technických celků určených pro tato vozidla a o dozoru nad trhem s nimi, o změně nařízení (ES) č. 715/2007 a č. 595/2009 a o zrušení směrnice 2007/46/ES (Úř. věst. L 151, 14.6.2018, s. 1) 3.

7. Nařízení Evropského parlamentu a Rady (EU) 2019/2144 ze dne 27. listopadu 2019 o požadavcích pro schvalování typu motorových vozidel a jejich přípojných vozidel a systémů, konstrukčních částí a samostatných technických celků určených pro tato vozidla z hlediska obecné bezpečnosti a ochrany cestujících ve vozidle a zranitelných účastníků silničního provozu, o změně nařízení Evropského parlamentu a Rady (EU) 2018/858 a o zrušení nařízení Evropského parlamentu a Rady (ES) č. 78/2009, (ES) č. 79/2009 a (ES) č. 661/2009 a nařízení Komise (ES) č. 631/2009, (EU) č. 406/2010, (EU) č. 672/2010, (EU) č. 1003/2010, (EU) č. 1005/2010, (EU) č. 1008/2010, (EU) č. 1009/2010, (EU) č. 19/2011, (EU) č. 109/2011, (EU) č. 458/2011, (EU) č. 65/2012, (EU) č. 130/2012, (EU) č. 347/2012, (EU) č. 351/2012, (EU) č. 1230/2012 a (EU) 2015/166 (Úř. věst. L 325, 16.12.2019, s. 1)

8. Nařízení Evropského parlamentu a Rady (EU) 2018/1139 ze dne 4. července 2018 o společných pravidlech v oblasti civilního letectví a o zřízení Agentury Evropské unie pro bezpečnost letectví, kterým se mění nařízení (ES) č. 2111/2005, (ES) č. 1008/2008, (EU) č. 996/2010, (EU) č. 376/2014 a směrnice Evropského parlamentu a Rady 2014/30/EU a 2014/53/EU a kterým se zrušuje nařízení Evropského parlamentu a Rady (ES) č. 552/2004 a (ES) č. 216/2008 a nařízení Rady (EHS) č. 3922/91 (Úř. věst. L 212, 22.8.2018, s. 1), v rozsahu projektování, výroby a uvádění na trh letadel uvedených v jeho čl. 2 odst. 1 písm. a) a b), pokud jde o bezpilotní letadla a jde-li o jejich motory, vrtule, letadlové části a vybavení pro jejich řízení na dálku

PŘÍLOHA III

VYSOCE RIZIKOVÉ SYSTÉMY UI UVEDENÉ V ČL. 6 ODST. 3

V každé z oblastí uvedených v bodech 1 až 8 se systémy UI konkrétně uvedené v každém písmeni považují za vysoce rizikové systémy UI podle čl. 6 odst. 3:

1. Biometrika:

   a) systémy biometrické identifikace na dálku.

2. Kritická infrastruktura:

   a) systémy UI určené k použití jako bezpečnostní komponenty řízení a provozu kritické digitální infrastruktury, silniční dopravy a dodávek vody, plynu, topení a elektřiny.

3. Vzdělávání a odborná příprava:

   a) systémy UI zamýšlené k určování přístupu fyzických osob ke vzdělávacím institucím či programům a institucím či programům odborné přípravy na všech úrovních nebo jejich přijetí a zařazení do těchto institucí či programů;

   b) systémy UI určené k hodnocení výsledků učení, včetně případů, kdy jsou tyto výsledky používány k řízení procesu učení fyzických osob ve vzdělávacích institucích či programech a institucích či programech odborné přípravy na všech úrovních.

4. Zaměstnanost, správa pracovníků a přístup k samostatné výdělečné činnosti:

   a) systémy UI určené k náboru nebo výběru fyzických osob, zejména k umísťování cílených nabídek zaměstnání, k analýze a třídění žádostí o zaměstnání a k hodnocení uchazečů;

b) systémy UI určené k rozhodování o postupu v zaměstnání nebo ukončení smluvních pracovněprávních vztahů, přidělování úkolů na základě individuálního chování, osobnostních rysů nebo charakteristiky a ke sledování a hodnocení výkonnosti a chování osob v rámci těchto vztahů.

5. Přístup k základním soukromým a veřejným službám a dávkám a jejich využívání:

a) systémy UI určené pro použití veřejnými orgány nebo jejich jménem za účelem hodnocení nároků fyzických osob základní na dávky a služby veřejné podpory a za účelem udělení, snížení, zrušení nebo opětovného získání těchto dávek a služeb;

b) systémy UI určené k hodnocení úvěruschopnosti fyzických osob nebo jejich úvěrového bodování, s výjimkou systémů UI uvedených do provozu poskytovateli, kteří jsou mikropodniky a malými podniky podle definice v příloze doporučení Komise 2003/361/ES, pro jejich vlastní potřebu;

c) systémy UI určené k použití za účelem vysílání nebo stanovení priority při vyslání zásahových služeb první reakce, včetně hasičů a lékařské pomoci;

d) systémy UI určené k posouzení rizika a stanovení cen v případě životního a zdravotního pojištění týkajícího se fyzických osob s výjimkou systémů UI uvedených do provozu poskytovateli, kteří jsou mikropodniky a malými podniky podle definice v příloze doporučení Komise 2003/361/ES, pro jejich vlastní potřebu.

6. Vymáhání práva:

a) systémy UI určené pro použití donucovacími orgány nebo jejich jménem s cílem posoudit riziko, že fyzická osoba spáchá či opětovně spáchá trestný čin, nebo riziko, že se fyzická osoba stane potenciální obětí trestných činů;

b) systémy UI určené pro použití donucovacími orgány nebo jejich jménem jako detektory lži a obdobné nástroje nebo za účelem zjišťování emočního stavu fyzické osoby;

c) [vypouští se]

d) systémy UI určené pro použití donucovacími orgány nebo jejich jménem za účelem hodnocení spolehlivosti důkazů v průběhu vyšetřování nebo stíhání trestných činů;

e) systémy UI určené pro použití donucovacími orgány nebo jejich jménem za účelem předvídání výskytu nebo opětovného výskytu skutečné nebo potenciální trestné činnosti na základě profilování fyzických osob podle čl. 3 bodu 4 směrnice (EU) 2016/680 nebo posuzování povahových vlastností a osobnostních rysů nebo dřívější trestné činnosti fyzických osob nebo skupin;

f) systémy UI určené pro použití donucovacími orgány nebo jejich jménem za účelem profilování fyzických osob podle čl. 3 bodu 4 směrnice (EU) 2016/680 v průběhu odhalování, vyšetřování nebo stíhání trestných činů.

g) [vypouští se]

7. Migrace, azyl a správa hraničních kontrol:

a) systémy UI určené pro použití příslušnými veřejnými orgány nebo jejich jménem jako detektory lži a obdobné nástroje nebo za účelem zjišťování emočního stavu fyzické osoby;

b) systémy UI určené pro použití příslušnými veřejnými orgány nebo jejich jménem za účelem posuzování určitého rizika, včetně bezpečnostního rizika, rizika nelegální migrace nebo zdravotního rizika, jež představuje fyzická osoba, která má v úmyslu vstoupit nebo již vstoupila na území členského státu;

c) [vypouští se]

d) systémy UI určené pro použití příslušnými veřejnými orgány nebo jejich jménem za účelem přezkoumání žádostí o azyl, o udělení víza a o povolení k pobytu a s tím souvisejících stížností, které se týkají způsobilosti fyzických osob žádajících o určitý status.

8. Správa soudnictví a demokratické procesy:

a) systémy UI určené pro použití soudním orgánem nebo jeho jménem při výkladu skutečností a práva a při uplatňování práva na konkrétní soubor skutečností.

PŘÍLOHA IV

TECHNICKÁ DOKUMENTACE podle čl. 11 odst. 1

Technická dokumentace podle čl. 11 odst. 1 obsahuje podle okolností dotyčného systému UI alespoň tyto informace:

1. Obecný popis systému UI zahrnující:

   a) jeho zamýšlený účel použití, osobu/osoby, jež systém vyvinula/vyvinuly, datum a verzi systému;

   b) jak systém UI interaguje s hardwarem nebo softwarem, který není součástí samotného systému UI, nebo jak může, tam, kde je to relevantní, být za účelem interakce s nimi použit;

   c) verze příslušného softwaru nebo firmwaru a veškeré požadavky týkající se aktualizace verze;

   d) popis všech forem, ve kterých je systém UI uveden na trh nebo do provozu (např. jako softwarový balíček, jenž je součástí hardwaru, soubor ke stažení, aplikační programovací rozhraní apod.);

   e) popis hardwaru, na kterém má systém UI pracovat;

   f) pokud je systém UI součástí produktů, fotografií nebo vyobrazení, které zobrazují vnější prvky, pak označení a vnitřní uspořádání těchto produktů;

   g) návod k použití pro uživatele a tam, kde je to relevantní, pokyny pro instalaci.

2. Podrobný popis prvků systému UI a procesu jeho vývoje zahrnující:

   a) metody a kroky provedené při vývoji systému UI, v příslušných případech včetně využití předtrénovaných systémů nebo nástrojů poskytnutých třetími stranami, a jak byly tyto systémy nebo nástroje použity, integrovány nebo upraveny poskytovatelem;

b) specifikace návrhu systému, zejména obecná logika systému UI a algoritmů; hlavní možnosti volby návrhu, včetně odůvodnění a učiněných předpokladů, také ve vztahu k osobám nebo skupinám osob, ohledně kterých má být systém používán; hlavní možnosti klasifikace; co má systém optimalizovat a význam jednotlivých parametrů; popis očekávaného výstupu systému; rozhodnutí o všech možných učiněných kompromisech, pokud jde o technická řešení přijatá za účelem dodržení požadavků stanovených v hlavě III kapitole 2;

c) popis architektury systému vysvětlující, jak na sebe komponenty softwaru vzájemně navazují nebo jsou do sebe začleněny a integrovány do celkového zpracování; výpočetní prostředky použité za účelem vývoje, trénování, testování a ověřování systému UI;

d) v příslušných případech požadavky na data ve formě informativních přehledů popisujících metody a techniky trénování a použité soubory tréninkových dat, včetně obecného popisu těchto datových souborů, informací o jejich rozsahu a hlavních vlastnostech; jakým způsobem byla data získána a vybrána; postupy označování (např. pro učení s učitelem), metody čištění údajů (např. určování odlehlých hodnot);

e) posouzení opatření lidského dohledu potřebných v souladu s článkem 14, včetně posouzení technických opatření potřebných pro usnadnění interpretace výstupů systémů UI uživateli v souladu s čl. 13 odst. 3 písm. d);

f) tam, kde je to relevantní, podrobný popis předdefinovaných změn systému UI a jeho výkonnosti, spolu se všemi příslušnými informacemi, které se týkají technických řešení přijatých k zajištění trvalého souladu systému UI s příslušnými požadavky stanovenými v hlavě III kapitole 2;

g) použité postupy ověřování a testování, včetně informací o použitých ověřovacích a testovacích údajích a jejich hlavních charakteristikách; ukazatele použité k měření přesnosti, spolehlivosti, kybernetické bezpečnosti a dodržení jiných příslušných požadavků stanovených v hlavě III kapitole 2, jakož i jejich potenciálně diskriminační dopady; testovací protokoly a všechny zprávy o testování, datované a podepsané odpovědnými osobami, a to i v souvislosti s předdefinovanými změnami uvedenými v písmeně f).

3. Podrobné informace o monitorování, fungování a kontrole systému UI, zejména pokud jde o: jeho schopnosti a omezení v oblasti výkonnosti, včetně stupňů přesnosti z hlediska konkrétních osob nebo skupin osob, ohledně kterých má být systém používán, a celková očekávaná úroveň přesnosti ve vztahu k zamýšlenému účelu použití; předvídatelné nezamýšlené výsledky a zdroje rizik pro zdraví a bezpečnost, základní práva a diskriminaci s ohledem na zamýšlený účel použití systému UI; opatření lidského dohledu potřebná v souladu s článkem 14, včetně technických opatření zavedených za účelem usnadnění interpretace výstupů systémů UI uživateli; případně specifikace vstupních dat.

4. Podrobný popis systému řízení rizik v souladu s článkem 9.

5. Popis příslušných změn systému provedených poskytovatelem v průběhu jeho životního cyklu.

6. Seznam harmonizovaných norem použitých v plném rozsahu nebo zčásti, na něž byly zveřejněny odkazy v Úředním věstníku Evropské unie; pokud žádné takové harmonizované normy nebyly použity, podrobný popis řešení přijatých za účelem splnění požadavků stanovených v hlavě III kapitole 2, včetně seznamu jiných příslušných norem a technických specifikací, které byly použity.

7. Kopii EU prohlášení o shodě.

8. Podrobný popis systému zavedeného za účelem hodnocení výkonnosti systému UI po uvedení na trh v souladu s článkem 61, včetně plánu monitorování po uvedení na trh podle čl. 61 odst. 3.

PŘÍLOHA V

EU PROHLÁŠENÍ O SHODĚ

EU prohlášení o shodě podle článku 48 obsahuje všechny tyto informace:

1. název a typ systému UI a veškeré další jednoznačné odkazy, jež umožňují identifikaci a sledovatelnost systému UI;

2. jméno a adresu poskytovatele nebo jeho zplnomocněného zástupce tam, kde je to relevantní;

3. uvedení skutečnosti že EU prohlášení o shodě se vydává na výhradní odpovědnost poskytovatele;

4. údaj o tom, že dotyčný systém UI je ve shodě s tímto nařízením a případně s veškerými jinými příslušnými právními předpisy Unie, které stanoví vydávání EU prohlášení o shodě;

5. odkazy na veškeré příslušné harmonizované normy, které byly použity, nebo na veškeré další společné specifikace, v souvislosti s nimiž se shoda prohlašuje;

6. tam, kde je to relevantní, název a identifikační číslo oznámeného subjektu, popis postupu posuzování shody a identifikace vydaného certifikátu;

7. místo a datum vydání prohlášení, jméno a funkce osoby, která je podepsala, a údaj o tom, pro koho a jménem koho je tato osoba podepsala, podpis.

PŘÍLOHA VI

POSTUP POSUZOVÁNÍ SHODY ZALOŽENÝ NA VNITŘNÍ KONTROLE

1. Postupem posuzování shody založeným na vnitřní kontrole se rozumí postup posuzování shody založený na bodech 2 až 4.

2. Poskytovatel ověří, že zavedený systém řízení kvality je v souladu s požadavky článku 17.

3. Poskytovatel přezkoumá informace obsažené v technické dokumentaci za účelem posouzení souladu systému UI s příslušnými základními požadavky stanovenými v hlavě III kapitole 2.

4. Poskytovatel rovněž ověří, že proces návrhu a vývoje systému UI a jeho monitorování po uvedení na trh podle článku 61 odpovídá technické dokumentaci.

PŘÍLOHA VII

SHODA ZALOŽENÁ NA POSOUZENÍ SYSTÉMU ŘÍZENÍ KVALITY A NA POSOUZENÍ TECHNICKÉ DOKUMENTACE

1. Úvod

Shodou založenou na posouzení systému řízení kvality a na posouzení technické dokumentace se rozumí postup posuzování shody založený na bodech 2 až 5.

2. Přehled

Schválený systém řízení kvality pro návrh, vývoj a testování systémů UI podle článku 17 se zkoumá v souladu s bodem 3 a podléhá dozoru stanovenému v bodě 5. Technická dokumentace systému UI se přezkoumá v souladu s bodem 4.

3. Systém řízení kvality

3.1. Žádost poskytovatele obsahuje:

a) jméno a adresu poskytovatele, a pokud žádost podává zplnomocněný zástupce, také jeho jméno a adresu;

b) seznam systémů UI, na něž se vztahuje tentýž systém řízení kvality;

c) technickou dokumentaci pro každý ze systémů UI, na nějž se vztahuje tentýž systém řízení kvality;

d) dokumentaci týkající se systému řízení kvality, jež zahrnuje všechny prvky uvedené v článku 17;

e) popis postupů zavedených s cílem zajistit, aby systém řízení kvality zůstal v přiměřeném a účinném stavu;

f) písemné prohlášení, že stejná žádost nebyla podána u jiného oznámeného subjektu.

3.2. Systém řízení kvality posuzuje oznámený subjekt, který určí, zda vyhovuje požadavkům podle článku 17.

Rozhodnutí se oznámí poskytovateli nebo jeho zplnomocněnému zástupci.

Oznámení musí obsahovat závěry posouzení systému řízení kvality a odůvodněné rozhodnutí o posouzení.

3.3. Schválený systém řízení kvality je poskytovatelem i nadále uplatňován a udržován tak, aby zůstal v přiměřeném a účinném stavu.

3.4. Poskytovatel informuje oznámený subjekt o každé zamýšlené změně schváleného systému řízení kvality nebo změně seznamu systémů UI, na něž se tento systém řízení kvality vztahuje.

Oznámený subjekt navrhované změny přezkoumá a rozhodne, zda změněný systém řízení kvality i nadále splňuje požadavky podle bodu 3.2, nebo zda je nutné nové posouzení.

Oznámený subjekt oznámí své rozhodnutí poskytovateli. Oznámení musí obsahovat závěry přezkoumání změn a odůvodněné rozhodnutí o posouzení.

4. Kontrola technické dokumentace

4.1. Kromě žádosti uvedené v bodě 3 poskytovatel podá oznámenému subjektu dle vlastní volby žádost o posouzení technické dokumentace týkající se systému UI, jejž poskytovatel zamýšlí uvést na trh nebo do provozu a na nějž se vztahuje systém řízení kvality uvedený v bodě 3.

4.2. Žádost musí mimo jiné obsahovat:

a) jméno a adresu poskytovatele;

b) písemné prohlášení, že stejná žádost nebyla podána u jiného oznámeného subjektu;

c) technickou dokumentaci uvedenou v příloze IV.

4.3. Oznámený subjekt technickou dokumentaci přezkoumá. Je-li to relevantní a omezené na to, co je nezbytné pro plnění jeho úkolů, je oznamovanému subjektu udělen plný přístup k používaným souborům tréninkových, validačních a testovacích dat, a to v příslušných případech a s výhradou bezpečnostních záruk i prostřednictvím aplikačních programovacích rozhraní (API) nebo jiných relevantních technických prostředků a nástrojů umožňujících dálkový přístup.

4.4. Při přezkoumávání technické dokumentace může oznámený subjekt požadovat, aby poskytovatel dodal další důkazy nebo provedl další zkoušky s cílem umožnit náležité posouzení shody systému UI s požadavky stanovenými v hlavě III kapitole 2. Není-li oznámený subjekt se zkouškami provedenými poskytovatelem spokojen, provede odpovídající zkoušky případně přímo oznámený subjekt.

4.5. Oznámeným subjektům se na základě odůvodněné žádosti a pouze tehdy, jsou-li splněny tyto kumulativní podmínky, poskytne přístup ke zdrojovému kódu systému UI:

a) přístup ke zdrojovému kódu je nezbytný k posouzení shody vysoce rizikového systému UI s požadavky stanovenými v hlavě III kapitole 2 a

b) postupy testování či auditu a ověřování na základě dat a dokumentace poskytnutých poskytovatelem byly vyčerpány nebo se ukázaly jako nedostatečné.

4.6. Rozhodnutí se oznámí poskytovateli nebo jeho zplnomocněnému zástupci. Oznámení musí obsahovat závěry posouzení technické dokumentace a odůvodněné rozhodnutí o posouzení.

Pokud je systém UI ve shodě s požadavky stanovenými v hlavě III kapitole 2, vydá oznámený subjekt certifikát EU posouzení technické dokumentace. Certifikát musí obsahovat jméno a adresu poskytovatele, závěry přezkoumání, podmínky platnosti certifikátu (existují-li) a údaje nezbytné k identifikaci systému UI.

Certifikát a jeho přílohy musí obsahovat všechny příslušné informace, jež umožňují vyhodnotit shodu systému UI a tam, kde je to relevantní, zkontrolovat systém UI při používání.

Pokud systém UI není ve shodě s požadavky stanovenými v hlavě III kapitole 2, oznámený subjekt odmítne certifikát EU posouzení technické dokumentace vydat a informuje o tom žadatele s uvedením podrobných důvodů svého odmítnutí.

Pokud systém UI nesplňuje požadavek týkající se dat použitých za účelem jeho trénování, před podáním žádosti o nové posouzení shody bude třeba opětovné trénování. V tomto případě odůvodněné rozhodnutí o posouzení, ve kterém oznámený subjekt odmítl vydat certifikát EU posouzení technické dokumentace, musí obsahovat konkrétní vyjádření ke kvalitě dat použitých za účelem trénování systému UI, a zejména o důvodech neshody.

4.7. Veškeré změny systému UI, jež by mohly ovlivnit shodu systému UI s požadavky nebo se zamýšleným účelem jeho použití, musí schválit oznámený subjekt, který vydal certifikát EU posouzení technické dokumentace. Poskytovatel musí tento oznámený subjekt informovat o svém záměru zavést jakékoli z výše uvedených změn, nebo pokud se o výskytu těchto změn dozvěděl jiným způsobem. Oznámený subjekt posoudí zamýšlené změny a rozhodne, zda uvedené změny vyžadují nové posouzení shody v souladu s čl. 43 odst. 4, nebo zda je lze vyřešit dodatkem k certifikátu EU posouzení technické dokumentace. Ve druhém z výše uvedených případů oznámený subjekt dané změny posoudí, informuje poskytovatele o svém rozhodnutí a v případě schválení změn mu vydá dodatek k certifikátu EU posouzení technické dokumentace.

5. Dozor nad schváleným systémem řízení kvality

5.1. Účelem dozoru prováděného oznámeným subjektem uvedeným v bodě 3 je ujistit se, že poskytovatel řádně plní podmínky schváleného systému řízení kvality.

5.2. Pro účely posouzení musí poskytovatel umožnit oznámenému subjektu přístup do prostor, kde se uskutečňuje návrh, vývoj a testování systémů UI. Poskytovatel dále musí s oznámeným subjektem sdílet veškeré potřebné informace.

5.3. Oznámený subjekt pravidelně provádí audity, aby se ujistil, že poskytovatel systém řízení jakosti udržuje a používá systém řízení jakosti, a předkládá poskytovateli zprávu o auditu. V souvislosti s těmito audity může oznámený subjekt provést další zkoušky systémů UI, pro něž byl vydán certifikát EU posouzení technické dokumentace.

PŘÍLOHA VIII

INFORMACE, KTERÉ MAJÍ BÝT POSKYTNUTY PŘI REGISTRACI PROVOZOVATELŮ VYSOCE RIZIKOVÝCH SYSTÉMŮ UI V SOULADU S ČLÁNKEM 51

Poskytovatelé, zplnomocnění zástupci a uživatelé, kteří jsou veřejnými orgány, agenturami nebo subjekty, předkládají informace uvedené v části I. Poskytovatelé nebo případně zplnomocnění zástupci zajistí, aby informace o jejich vysoce rizikových systémech UI uvedené v části II bodech 1 až 11 byly úplné, správné a aktuální. Informace uvedené v části II bodě 12 jsou automaticky generovány databází.

Část I. Informace týkající se provozovatelů (při jejich registraci)

-1. typ provozovatele (poskytovatel, zplnomocněný zástupce nebo uživatel);

1. jméno, adresa a další kontaktní údaje poskytovatele;

2. pokud informace předkládá jiná osoba jménem provozovatele, jméno, adresa a další kontaktní údaje této osoby;

Část II. Informace týkající se vysoce rizikového systému UI

1. jméno, adresa a další kontaktní údaje poskytovatele;

2. tam, kde je to relevantní, jméno, adresa a kontaktní údaje zplnomocněného zástupce;

3. obchodní název systému UI a veškeré další jednoznačné odkazy, jež umožňují identifikaci a sledovatelnost systému UI;

4. popis zamýšleného účelu použití systému UI;

5. status systému UI (na trhu nebo v provozu; již ne na trhu nebo v provozu, stažen z oběhu);

6. typ, číslo a datum použitelnosti certifikátu vydaného oznámeným subjektem a případně název nebo identifikační číslo tohoto oznámeného subjektu;

7. případně naskenovaná kopie certifikátu uvedeného v bodě 6;

8. členské státy, v nichž je systém UI uveden nebo byl uveden na trh, uveden do provozu nebo zpřístupněn v Unii;

9. kopie EU prohlášení o shodě podle článku 48;

10. elektronický návod k použití;

11. internetová adresa pro doplňující informace (nepovinné);

12. jméno, adresa a další kontaktní údaje uživatelů.

PŘÍLOHA VIIIa

INFORMACE PŘEDKLÁDANÉ NA VYŽÁDÁNÍ PŘI REGISTRACI VYSOCE RIZIKOVÝCH SYSTÉMŮ UI UVEDENÝCH V PŘÍLOZE III TÝKAJÍCÍ SE TESTOVÁNÍ V REÁLNÝCH PODMÍNKÁCH V SOULADU S ČLÁNKEM 54a

V souvislosti s testováním v reálných podmínkách, jež má být registrováno v souladu s článkem 54a, jsou poskytnuty a poté průběžně aktualizovány tyto informace:

1. celounijní jedinečné identifikační číslo testování v reálných podmínkách;

2. jméno a kontaktní údaje poskytovatele nebo potenciálního poskytovatele a uživatelů zapojených do testování v reálných podmínkách;

3. stručný popis systému UI, jeho zamýšlený účel a další informace nezbytné pro identifikaci systému;

4. souhrn hlavních charakteristik plánu testování v reálných podmínkách;

5. informace týkající se pozastavení nebo ukončení testování v reálných podmínkách.

PŘÍLOHA IX

PRÁVNÍ PŘEDPISY UNIE O ROZSÁHLÝCH INFORMAČNÍCH SYSTÉMECH V OBLASTI SVOBODY, BEZPEČNOSTI A PRÁVA

1. Schengenský informační systém

   a) Nařízení Evropského parlamentu a Rady (EU) 2018/1860 ze dne 28. listopadu 2018 o využívání Schengenského informačního systému při navracení neoprávněně pobývajících státních příslušníků třetích zemí (Úř. věst. L 312, 7.12.2018, s. 1)

   b) Nařízení Evropského parlamentu a Rady (EU) 2018/1861 ze dne 28. listopadu 2018 o zřízení, provozu a využívání Schengenského informačního systému (SIS) v oblasti hraničních kontrol, o změně Úmluvy k provedení Schengenské dohody a o změně a zrušení nařízení (ES) č. 1987/2006 (Úř. věst. L 312, 7.12.2018, s. 14)

   c) Nařízení Evropského parlamentu a Rady (EU) 2018/1862 ze dne 28. listopadu 2018 o zřízení, provozu a využívání Schengenského informačního systému (SIS) v oblasti policejní spolupráce a justiční spolupráce v trestních věcech, o změně a o zrušení rozhodnutí Rady 2007/533/SVV a o zrušení nařízení Evropského parlamentu a Rady (ES) č. 1986/2006 a rozhodnutí Komise 2010/261/EU (Úř. věst. L 312, 7.12.2018, s. 56)

2. Vízový informační systém

   a) Návrh nařízení Evropského parlamentu a Rady, kterým se mění nařízení (ES) č. 767/2008, nařízení (ES) č. 810/2009, nařízení (EU) 2017/2226, nařízení (EU) 2016/399, nařízení XX/2018 [nařízení o interoperabilitě] a rozhodnutí 2004/512/ES a kterým se zrušuje rozhodnutí Rady 2008/633/SVV – COM(2018) 302 final. Po přijetí nařízení spolunormotvůrci (duben/květen 2021) bude aktualizováno.

3. Systém Eurodac

a) Pozměněný návrh nařízení Evropského parlamentu a Rady o zřízení systému „Eurodac“ pro porovnávání biometrických údajů za účelem účinného uplatňování nařízení (EU) XXX/XXX [nařízení o řízení azylu a migrace] a nařízení (EU) XXX/XXX [nařízení o znovuusídlování], za účelem identifikace neoprávněně pobývajícího státního příslušníka třetí země nebo osoby bez státní příslušnosti, o podávání žádostí donucovacích orgánů členských států a Europolu o porovnání údajů s údaji systému Eurodac pro účely vymáhání práva a o změně nařízení (EU) 2018/1240 a (EU) 2019/818 – COM(2020) 614 final

4. Systém vstupu/výstupu

a) Nařízení Evropského parlamentu a Rady (EU) 2017/2226 ze dne 30. listopadu 2017, kterým se zřizuje Systém vstupu/výstupu (EES) pro registraci údajů o vstupu a výstupu a údajů o odepření vstupu, pokud jde o státní příslušníky třetích zemí překračující vnější hranice členských států, kterým se stanoví podmínky přístupu do systému EES pro účely vymáhání práva a kterým se mění Úmluva k provedení Schengenské dohody a nařízení (ES) č. 767/2008 a (EU) č. 1077/2011 (Úř. věst. L 327, 9.12.2017, s. 20)

5. Evropský systém pro cestovní informace a povolení

a) Nařízení Evropského parlamentu a Rady (EU) 2018/1240 ze dne 12. září 2018, kterým se zřizuje Evropský systém pro cestovní informace a povolení (ETIAS) a kterým se mění nařízení (EU) č. 1077/2011, (EU) č. 515/2014, (EU) 2016/399, (EU) 2016/1624 a (EU) 2017/2226 (Úř. věst. L 236, 19.9.2018, s. 1)

b) Nařízení Evropského parlamentu a Rady (EU) 2018/1241 ze dne 12. září 2018, kterým se mění nařízení (EU) 2016/794 za účelem zřízení Evropského systému pro cestovní informace a povolení (ETIAS) (Úř. věst. L 236, 19.9.2018, s. 72)

6. Evropský informační systém rejstříků trestů státních příslušníků třetích zemí a osob bez státní příslušnosti

   a) Nařízení Evropského parlamentu a Rady (EU) 2019/816 ze dne 17. dubna 2019, kterým se zřizuje centralizovaný systém pro identifikaci členských států, jež mají informace o odsouzeních státních příslušníků třetích zemí a osob bez státní příslušnosti (ECRIS-TCN), na doplnění Evropského informačního systému rejstříků trestů, a kterým se mění nařízení (EU) 2018/1726 (Úř. věst. L 135, 22.5.2019, s. 1)

7. Interoperabilita

   a) Nařízení Evropského parlamentu a Rady (EU) 2019/817 ze dne 20. května 2019, kterým se zřizuje rámec pro interoperabilitu mezi informačními systémy EU v oblasti hranic a víz (Úř. věst. L 135, 22.5.2019, s. 27)

   b) Nařízení Evropského parlamentu a Rady (EU) 2019/818 ze dne 20. května 2019, kterým se zřizuje rámec pro interoperabilitu mezi informačními systémy EU v oblasti policejní a justiční spolupráce, azylu a migrace (Úř. věst. L 135, 22.5.2019, s. 85)