2024/1689

12.7.2024

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2024/1689

ze dne 13. června 2024,

kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) 2020/1828 (akt o umělé inteligenci)

(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 Evropské centrální banky [2],

s ohledem na stanovisko Výboru regionů [3],

v souladu s řádným legislativním postupem [4],

vzhledem k těmto důvodům:

(1) Účelem tohoto nařízení je zlepšit fungování vnitřního trhu stanovením jednotného právního rámce, zejména pro vývoj, uvádění na trh, uvádění do provozu a používání systémů umělé inteligence (dále jen „systémy AI“) v Unii v souladu s hodnotami Unie, podporovat zavádění důvěryhodné umělé inteligence (dále jen „AI“) zaměřené na člověka a zároveň zajistit vysokou úroveň ochrany zdraví, bezpečnosti a základních práv zakotvených v Listině základních práv Evropské unie (dále jen „Listina“), včetně demokracie, právního státu a ochrany životního prostředí, chránit před škodlivými účinky systémů AI v Unii, jakož i podporovat inovace. Toto nařízení zajišťuje volný přeshraniční pohyb zboží a služeb založených na AI, čímž brání členským státům ukládat omezení vývoje, uvádění na trh a používání systémů AI, pokud to není tímto nařízením výslovně povoleno.

(2) Toto nařízení by mělo být uplatňováno v souladu s hodnotami Unie zakotvenými v Listině, usnadňovat ochranu fyzických osob, podniků, demokracie, právního státu a životního prostředí a zároveň podporovat inovace a zaměstnanost a zajistit Unii vedoucí postavení při zavádění důvěryhodné AI.

(3) Systémy AI mohou být snadno zaváděny v celé řadě hospodářských odvětví a složek společnosti, a to i napříč hranicemi, a mohou být snadno v oběhu v celé Unii. Některé členské státy již zkoumají možnost přijetí vnitrostátních pravidel, která by zajišťovala, že AI bude důvěryhodná a 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 mohou snížit právní jistotu pro provozovatele, kteří systémy AI vyvíjejí, dovážejí nebo používají. Proto je třeba zajistit jednotnou a vysokou úroveň ochrany v celé Unii s cílem dosáhnout důvěryhodnosti AI a zároveň zabránit rozdílům, které jsou překážkou volného oběhu, inovací, zavádění a využívání systémů AI a souvisejících produktů a služeb na vnitřním trhu, a stanovit za tímto účelem jednotné povinnosti provozovatelů

[1] Úř. věst. C 517, 22.12.2021, s. 56.
[2] Úř. věst. C 115, 11.3.2022, s. 5.
[3] Úř. věst. C 97, 28.2.2022, s. 60.
[4] Postoj Evropského parlamentu ze dne 13. března 2024 (dosud nezveřejněný v Úředním věstníku) a rozhodnutí Rady ze dne 21. května 2024.

a zaručit jednotnou ochranu naléhavých důvodů obecného zájmu a práv osob na celém vnitřním trhu na základě článku 114 Smlouvy o fungování Evropské unie (dále jen „Smlouva o fungování EU“). V rozsahu, v němž toto nařízení obsahuje zvláštní pravidla ochrany fyzických osob v souvislosti se zpracováním osobních údajů, která se týkají omezení, pokud jde o používání systémů AI pro biometrickou identifikaci na dálku pro účely vymáhání práva, používání systémů AI k posouzení rizik fyzických osob pro účely vymáhání práva a používání systémů AI pro biometrickou kategorizaci pro účely vymáhání práva, je vhodné, aby se toto nařízení ve vztahu k těmto zvláštním pravidlům zakládalo na článku 16 Smlouvy o fungování EU. S ohledem na tato zvláštní pravidla a na použití článku 16 Smlouvy o fungování EU je vhodné provést konzultace s Evropským sborem pro ochranu osobních údajů.

(4) AI je rychle se vyvíjející skupina technologií, které se podílejí na široké škále hospodářských, environmentálních a společenských přínosů v celém spektru průmyslových odvětví a sociálních aktivit. Díky zlepšení predikcí, optimalizaci provozu, přidělování zdrojů a personalizaci digitálních řešení dostupných pro jednotlivce a organizace může používání AI poskytnout podnikům klíčové konkurenční výhody a podpořit sociálně a environmentálně prospěšné výsledky, například v oblasti zdravotnictví, zemědělství, bezpečnosti potravin, vzdělávání a odborné přípravy, sdělovacích prostředků, sportu, kultury, správy infrastruktury, energetiky, dopravy a logistiky, veřejných služeb, bezpečnosti, spravedlnosti, účinného využívání zdrojů a energetické účinnosti, monitorování životního prostředí, ochrany a obnovy biologické rozmanitosti a ekosystémů a zmírňování změny klimatu a přizpůsobování se této změně.

(5) AI může zároveň v závislosti na okolnostech týkajících se jejího konkrétního uplatňování, používání a úrovně technologického rozvoje vytvářet rizika a působit újmu veřejným zájmům a základním právům, které jsou chráněny právem Unie. Tato újma může být hmotná nebo nehmotná, včetně újmy fyzické, psychické, společenské nebo ekonomické.

(6) Vzhledem k velkému dopadu, který může mít AI na společnost, a jelikož je třeba budovat důvěru, je nezbytné, aby AI i její regulační rámec byly rozvíjeny v souladu s hodnotami Unie zakotvenými v článku 2 Smlouvy o Evropské unii (dále jen „Smlouva o EU“), základními právy a svobodami zakotvenými ve Smlouvách a v souladu s článkem 6 Smlouvy o EU v Listině. Základním předpokladem je, aby byla AI technologií zaměřenou na člověka. Měla by být nástrojem pro lidi, jehož konečným cílem je zvýšit kvalitu života lidí.

(7) V zájmu zajištění jednotné a vysoké úrovně ochrany veřejných zájmů, pokud jde o zdraví, bezpečnost a základní práva, by měla být pro vysoce rizikové systémy AI stanovena společná pravidla. Tato pravidla by měla být v souladu s Listinou, nediskriminační a v souladu se závazky Unie v oblasti mezinárodního obchodu. Měla by rovněž zohlednit evropské prohlášení o digitálních právech a zásadách pro digitální dekádu a Etické pokyny pro zajištění důvěryhodnosti UI vydané Expertní skupinou na vysoké úrovni pro umělou inteligenci (AI HLEG).

(8) Je proto nezbytné zavést právní rámec Unie, kterým se stanoví harmonizovaná pravidla pro AI, s cílem podpořit vývoj, používání a zavádění AI na vnitřním trhu, který by zároveň splňoval vysokou úroveň ochrany veřejných zájmů, jako je například zdraví a bezpečnost a ochrana základních práv, včetně demokracie, právního státu a ochrany životního prostředí, která jsou uznávána a chráněna právem Unie. K dosažení tohoto cíle by měla být stanovena pravidla, která budou regulovat uvádění určitých systémů AI na trh a do provozu, jakož i jejich používání, a tím zajišťovat bezproblémové fungování vnitřního trhu a umožňovat, aby tyto systémy měly prospěch ze zásady volného pohybu zboží a služeb. Uvedená pravidla by měla být jasná a spolehlivá, pokud jde o ochranu základních práv, měla by podporovat nová inovativní řešení a umožňovat evropský ekosystém veřejných a soukromých subjektů vytvářejících systémy AI v souladu s hodnotami Unie, jakož i využívat potenciál digitální transformace ve všech regionech Unie. Stanovením těchto pravidel, jakož i opatření na podporu inovací se zvláštním zaměřením na malé a střední podniky, včetně podniků začínajících, podporuje toto nařízení cíl, kterým je prosazování evropského přístupu k AI zaměřeného na člověka a čelná pozice Unie v celosvětovém kontextu, pokud jde o rozvoj bezpečné, důvěryhodné a etické AI, jak stanovila Evropská rada ([5]), a zajišťuje ochranu etických zásad, jak výslovně požadoval Evropský parlament ([6]).

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

(9) Harmonizační pravidla Unie použitelná pro uvádění na trh, uvádění do provozu a používání vysoce rizikových systémů AI by měla být stanovena v souladu s nařízením Evropského parlamentu a Rady (ES) č. 765/2008 ([7]), rozhodnutím Evropského parlamentu a Rady č. 768/2008/ES ([8]) a nařízením Evropského parlamentu a Rady (EU) 2019/1020 ([9]) („nový legislativní rámec pro uvádění výrobků na trh"). Harmonizovaná pravidla stanovená v tomto nařízení by se měla vztahovat na všechna odvětví a v souladu s přístupem nového legislativního rámce by jimi nemělo být dotčeno stávající právo Unie, zejména v oblasti ochrany údajů, ochrany spotřebitele, základních práv, zaměstnanosti, ochrany pracovníků a bezpečnosti výrobků, které toto nařízení doplňuje. V důsledku toho zůstávají všechna práva a ochrana, které toto právo Unie stanoví pro spotřebitele a další osoby, na něž mohou mít systémy AI nepříznivý dopad, a to i pokud jde o náhradu možné škody podle směrnice Rady 85/374/EHS ([10]), nadále nedotčeny a plně použitelné. Kromě toho by tudíž v souvislosti se zaměstnaností a ochranou pracovníků nemělo být tímto nařízením dotčeno právo Unie v oblasti sociální politiky a vnitrostátní pracovní právo, a to v souladu s právem Unie, pokud jde o podmínky zaměstnávání a pracovní podmínky, včetně bezpečnosti a ochrany zdraví při práci a vztahu mezi zaměstnavateli a pracovníky. Tímto nařízením by rovněž neměl být dotčen výkon základních práv uznávaných členskými státy a na úrovni Unie, včetně práva na stávku nebo práva přijmout jiná opatření na základě zvláštních systémů členských států v oblasti pracovněprávních vztahů, jakož i právo sjednávat, uzavírat a vymáhat kolektivní smlouvy nebo vést kolektivní akce v souladu s vnitrostátním právem. Tímto nařízením by neměla být dotčena ustanovení, jejichž účelem je zlepšit pracovní podmínky při práci prostřednictvím platforem, stanovená ve směrnici Evropského parlamentu a Rady o zlepšení pracovních podmínek při práci prostřednictvím platforem. Kromě toho je cílem tohoto nařízení posílit účinnost těchto stávajících práv a ochrany, že stanoví zvláštní požadavky a povinnosti, mimo jiné pokud jde o transparentnost, technickou dokumentaci a vedení záznamů o systémech AI. Povinnosti uložené různým provozovatelům zapojeným do hodnotového řetězce AI podle tohoto nařízení by se navíc měly uplatňovat, aniž by bylo dotčeno vnitrostátní právo v souladu s právem Unie, jehož účinkem je omezení používání určitých systémů AI, pokud toto právo nespadá do oblasti působnosti tohoto nařízení nebo sleduje jiné legitimní cíle veřejného zájmu než ty, které sleduje toto nařízení. Tímto nařízením by například neměly být dotčeny vnitrostátní pracovní právo a právní předpisy na ochranu nezletilých osob, tedy osob mladších 18 let, s ohledem na obecnou připomínku UNCRC č. 25 (2021) o právech dětí v souvislosti s digitálním prostředím, pokud se netýkají konkrétně systémů AI a sledují jiné legitimní cíle veřejného zájmu.

(10) Základní právo na ochranu osobních údajů je chráněno zejména nařízeními Evropského parlamentu a Rady (EU) 2016/679 ([11]) a (EU) 2018/1725 ([12]) a směrnicí Evropského parlamentu a Rady (EU) 2016/680 ([13]). Směrnice Evropského parlamentu a Rady 2002/58/ES ([14]) navíc chrání soukromý život a důvěrný charakter sdělení, mimo jiné stanovením podmínek pro uchovávání jakýchkoli osobních a neosobních údajů v koncových zařízeních a přístup k těmto údajům z takových zařízení. Uvedené právní akty Unie poskytují základ pro udržitelné a odpovědné zpracování údajů, včetně případů, kdy datové soubory zahrnují kombinaci osobních a neosobních údajů. Tímto nařízením není dotčeno uplatňování stávajícího práva Unie upravujícího zpracování osobních údajů, včetně úkolů a pravomocí nezávislých dozorových orgánů příslušných pro sledování dodržování těchto nástrojů. Tímto nařízením nejsou dotčeny povinnosti poskytovatelů systémů AI a zavádějících subjektů v jejich úloze správců nebo zpracovatelů údajů vyplývající z práva Unie nebo vnitrostátního práva o ochraně osobních údajů, pokud návrh, vývoj nebo používání systémů AI zahrnuje zpracování osobních údajů. Je rovněž vhodné vyjasnit, že subjekty údajů

([7]) Nařízení Evropského parlamentu a Rady (ES) č. 765/2008 ze dne 9. července 2008, kterým se stanoví požadavky na akreditaci a kterým se zrušuje nařízení (EHS) č. 339/93 (Úř. věst. L 218, 13.8.2008, s. 30).

([8]) 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).

([9]) 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 (Úř. věst. L 169, 25.6.2019, s. 1).

([10]) Směrnice Rady 85/374/EHS ze dne 25. července 1985 o sbližování právních a správních předpisů členských států týkajících se odpovědnosti za vadné výrobky (Úř. věst. L 210, 7.8.1985, s. 29).

([11]) 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).

([12]) 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).

([13]) 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 (Úř. věst. L 119, 4.5.2016, s. 89).

([14]) Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích) (Úř. věst. L 201, 31.7.2002, s. 37).

nadále požívají všech práv a záruk, které jim tyto 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 AI stanovená v rámci tohoto nařízení by měla usnadnit účinné provádění a umožnit výkon práv subjektů údajů a dalších prostředků ochrany zaručených právními předpisy Unie v oblasti ochrany osobních údajů a dalších základních práv.

(11) Tímto nařízením by neměla být dotčena ustanovení týkající se odpovědnosti poskytovatelů zprostředkovatelských služeb stanovená v nařízení Evropského parlamentu a Rady (EU) 2022/2065 ([15]).

(12) Pojem „systém AI“ v tomto nařízení by měl být jasně definován a úzce sladěn s činností mezinárodních organizací zabývajících se AI, aby byla zajištěna právní jistota, aby bylo usnadněno sbližování pravidel na mezinárodní úrovni a široké přijetí a současně aby byla poskytnuta flexibilita umožňující přizpůsobit se rychlému technologickému vývoji v této oblasti. Tato definice by kromě toho měla být založena na klíčových vlastnostech systémů AI, které je odlišují od jednodušších tradičních softwarových systémů nebo programovacích přístupů, a neměla by se vztahovat na systémy, které jsou založeny na pravidlech vymezených výhradně fyzickými osobami k automatickému provádění operací. Jednou z klíčových vlastností systémů AI je jejich schopnost odvozování. Schopností odvozování se rozumí proces získávání výstupů, jako jsou predikce, obsah, doporučení nebo rozhodnutí, které mohou ovlivnit fyzické a virtuální prostředí, a schopnost systémů AI derivovat modely nebo algoritmy, nebo oboje, ze vstupů nebo dat. Mezi techniky, které umožňují odvozování při současném budování systému AI, patří přístupy strojového učení, které se učí z dat, jak dosáhnout určitých cílů, a přístupy založené na logice a poznatcích, které ze zakódovaných poznatků nebo symbolického znázornění odvozují úkol, který má být vyřešen. Schopnost odvozování systému AI přesahuje rámec základního zpracování údajů tím, že umožňuje učení, uvažování nebo modelování. Pojem „strojové“ odkazuje na skutečnost, že systémy AI fungují prostřednictvím strojů. Odkaz na explicitní nebo implicitní cíle zdůrazňuje, že systémy AI mohou fungovat na základě explicitně definovaných cílů nebo cílů implicitních. Cíle systému AI se mohou v konkrétním kontextu lišit od zamýšleného účelu systému AI. Pro účely tohoto nařízení by se prostředím měl rozumět kontext, v němž systémy AI fungují, zatímco výstupy generované systémem AI odrážejí různé funkce vykonávané systémy AI a zahrnují predikci, obsah, doporučení nebo rozhodnutí. Systémy AI jsou navrženy tak, aby fungovaly s různou úrovní samostatnosti, což znamená, že jejich činnost je alespoň do určité míry nezávislá na zapojení člověka a jsou při ní schopny alespoň do určité míry fungovat bez lidského zásahu. Přizpůsobivostí, kterou by systém AI mohl vykazovat po zavedení, se rozumí schopnost samoučení, která umožňuje, aby se systém během používání měnil. Systémy AI lze používat samostatně nebo jako komponent 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).

(13) Pojem „zavádějící subjekt“ uvedený v tomto nařízení by měl být vykládán jako jakákoli fyzická nebo právnická osoba, včetně veřejného orgánu, agentury nebo jiného subjektu, která v rámci své pravomoci používá systém AI, s výjimkou případů, kdy je tento systém AI používán při osobní neprofesionální činnosti. V závislosti na typu systému AI může používání systému ovlivňovat jiné osoby než zavádějící subjekt.

(14) Pojem „biometrické údaje“ používaný v tomto nařízení by měl být vykládán s ohledem na pojem „biometrické údaje“ vymezený v čl. 4 bodu 14 nařízení (EU) 2016/679, čl. 3 bodu 18 nařízení (EU) 2018/1725 a čl. 3 bodu 13 směrnice (EU) 2016/680. Biometrické údaje mohou umožnit autentizaci, identifikaci či kategorizaci fyzických osob a rozpoznávání jejich emocí.

(15) Pojem „biometrická identifikace“ uvedený v tomto nařízení by měl být vymezen jako automatizované rozpoznání fyzických, fyziologických a behaviorálních lidských rysů, jako jsou obličej, pohyb očí, tvar těla, hlas, řeč, chůze, držení těla, srdeční frekvence, krevní tlak, zápach, stisk kláves, pro účely zjištění totožnosti jednotlivce porovnáním biometrických údajů dané osoby s uloženými biometrickými údaji jednotlivců v referenční databázi, a to bez ohledu na to, zda daný jedinec poskytl svůj souhlas, či nikoli. To nezahrnuje systémy AI určené k biometrickému ověřování, včetně autentizace, jejichž jediným účelem je potvrdit, zda je konkrétní fyzická osoba osobou, za niž se prohlašuje, a potvrdit totožnost fyzické osoby za jediným účelem, kterým je získání přístupu ke službě, odblokování zařízení nebo získání bezpečnostního přístupu k prostorám.

([15]) Nařízení Evropského parlamentu a Rady (EU) 2022/2065 ze dne 19. října 2022 o jednotném trhu digitálních služeb a o změně směrnice 2000/31/ES (nařízení o digitálních službách) (Úř. věst. L 277, 27.10.2022, s. 1).

(16) Pojmem „biometrická kategorizace“ uvedeným v tomto nařízení by se mělo rozumět zařazení fyzických osob do zvláštních kategorií na základě jejich biometrických údajů. Tyto zvláštní kategorie se mohou týkat aspektů, jako je pohlaví, věk, barva vlasů, barva očí, tetování, behaviorální nebo osobnostní rysy, jazyk, náboženské vyznání, příslušnost k národnostní menšině, sexuální nebo politická orientace. To nezahrnuje systémy biometrické kategorizace, které jsou čistě vedlejším prvkem neoddělitelně spjatým s jinou obchodní službou, což znamená, že tento prvek nelze z objektivních technických důvodů použít bez hlavní služby a začlenění tohoto prvku nebo funkce není prostředkem k obcházení použitelnosti pravidel stanovených v tomto nařízení. Takovým vedlejším prvkem by mohly být například filtry kategorizující rysy obličeje nebo těla používané na on-line tržištích, neboť je lze použít pouze ve vztahu k hlavní službě, která spočívá v prodeji výrobku, přičemž spotřebiteli umožní zobrazit si náhled na výrobek na sobě samém a pomůže mu rozhodnout se o nákupu. Filtry používané v rámci služeb online sociálních sítí, které kategorizují rysy obličeje nebo těla tak, aby uživatelé mohli doplňovat nebo upravovat obrázky nebo videa, by rovněž mohly být považovány za vedlejší prvek, neboť takový filtr nelze použít bez hlavní služby sociální sítě spočívající ve sdílení obsahu online.

(17) Pojem „systém biometrické identifikace na dálku“ uvedený v tomto nařízení by měl být definován funkčně jako systém AI určený k identifikaci fyzických osob, a to obvykle na dálku, bez jejich aktivního zapojení prostřednictvím porovnání biometrických údajů dané osoby s biometrickými údaji obsaženými v referenční databázi, bez ohledu na konkrétní technologii, procesy nebo typy použitých biometrických údajů. Tyto systémy biometrické identifikace na dálku se obvykle používají ke snímání vícero osob nebo jejich chování současně, s cílem významně usnadnit identifikaci osob bez jejich aktivního zapojení. To nezahrnuje systémy AI určené k biometrickému ověřování, včetně autentizace, jejichž jediným účelem je potvrdit, zda je konkrétní fyzická osoba osobou, za niž se prohlašuje, a potvrdit totožnost fyzické osoby za jediným účelem, kterým je získání přístupu ke službě, odblokování zařízení nebo získání bezpečnostního přístupu k prostorám. Uvedené 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 bez jejich aktivního zapojení, 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 AI 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 „následně,“ 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.

(18) Pojem „systém rozpoznávání emocí“ uvedený v tomto nařízení by měl být vymezen jako systém AI pro účely zjišťování nebo odvozování emocí nebo záměrů fyzických osob na základě jejich biometrických údajů. Tento pojem odkazuje na emoce nebo záměry, jako je štěstí, smutek, hněv, překvapení, znechucení, pocit trapnosti, rozrušení, stud, opovržení, spokojenost a pobavenost. Nezahrnuje fyzické stavy, jako je bolest nebo únava, včetně například systémů používaných při zjišťování stavu únavy profesionálních pilotů nebo řidičů za účelem předcházení nehodám. Nezahrnuje ani pouhé zjištění snadno viditelných výrazů, gest nebo pohybů, pokud neslouží k zjišťování nebo odvozování emocí. Uvedenými výrazy mohou být základní výrazy obličeje, jako je mračení se nebo úsměv, nebo gesta, jako je pohyb rukou, paží nebo hlavy, nebo charakteristiky hlasu daného člověka, jako je zvýšený hlas nebo šepot.

(19) Pro účely tohoto nařízení by se pod pojmem „veřejně přístupný prostor“ měl rozumět jakýkoli fyzický prostor, který je přístupný neurčenému počtu fyzických osob, bez ohledu na to, zda je daný prostor v soukromém, nebo veřejném vlastnictví, bez ohledu na činnost, pro kterou může být prostor využíván, jako je obchodní činnost, například obchody, restaurace, kavárny; služby, například banky, profesní činnosti, pohostinství; sport, například plavecké bazény, tělocvičny, stadiony; doprava, například zastávky autobusu a metra a železniční nádraží, letiště, dopravní prostředky; zábava, například kina, divadla, muzea, koncertní a konferenční haly nebo volný čas či jiné, například veřejné komunikace a náměstí, parky, lesy, hřiště. Prostor by měl být klasifikován jako veřejně přístupný i v případě, že přístup podléhá 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. Prostor by naopak neměl být považován za veřejně přístupný, pokud je přístup omezen na konkrétní a vymezené fyzické osoby buď prostřednictvím práva Unie, nebo vnitrostátního práva přímo souvisejícího s veřejnou ochranou a bezpečností, nebo prostřednictvím jasného projevu vůle osobou, která má v daném prostoru příslušnou pravomoc. Samotná faktická možnost přístupu (jako jsou

odemčené dveře nebo otevřená brána v plotu) neznamená, že prostor je veřejně přístupný, existují-li indikace nebo okolnosti naznačující opak, jako jsou značky 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 prostory, které nejsou veřejně přístupné. Veřejně přístupné prostory by neměly zahrnovat věznice ani stanoviště hraniční kontroly. Některé další prostory mohou zahrnovat jak veřejně nepřístupné, tak veřejně přístupné 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.

(20) Aby bylo možné dosáhnout co největších přínosů systémů AI a zároveň chránit základní práva, zdraví a bezpečnost a umožnit demokratickou kontrolu, měli by poskytovatelé, zavádějící subjekty a dotčené osoby získat v tomto ohledu prostřednictvím gramotnosti v oblasti AI nezbytné povědomí, které jim umožní činit ohledně systémů AI informovaná rozhodnutí. Povědomí o těchto otázkách se může lišit s ohledem na příslušný kontext a může obnášet pochopení správného uplatňování technických prvků během fáze vývoje systému AI, opatření, která mají být uplatňována během jeho používání, vhodné způsoby výkladu výstupů systému AI a v případě dotčených osob poznatky nezbytné k pochopení toho, jak na ně budou mít rozhodnutí přijatá s pomocí AI dopad. V souvislosti s uplatňováním tohoto nařízení by prostřednictvím gramotnosti v oblasti AI měli mít všichni příslušní aktéři v hodnotovém řetězci AI poznatky potřebné k zajištění náležitého dodržování ustanovení tohoto nařízení a jeho řádného prosazování. Kromě toho by široké provádění opatření týkajících se gramotnosti v oblasti AI a zavedení vhodných následných opatření mohlo přispět ke zlepšení pracovních podmínek a v konečném důsledku podpořit konsolidaci a inovaci v oblasti důvěryhodné AI v Unii. Evropská rada pro umělou inteligenci (dále jen „rada“) by měla podpořit Komisi s cílem prosazovat nástroje gramotnosti v oblasti AI, informovanost veřejnosti a pochopení přínosů, rizik, záruk, práv a povinností, jež s používáním systémů AI souvisejí. Ve spolupráci s příslušnými zúčastněnými stranami by Komise a členské státy měly usnadnit vypracování dobrovolných kodexů chování pro zvýšení gramotnosti v oblasti AI, pokud jde o osoby, které se zabývají vývojem, provozem a používáním AI.

(21) 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 AI nediskriminačním způsobem bez ohledu na to, zda jsou usazeni v Unii, nebo ve třetí zemi, a na subjekty zavádějící systémy AI usazené v Unii.

(22) Určité systémy AI by s ohledem na svou digitální povahu měly spadat do oblasti působnosti tohoto nařízení i tehdy, pokud nejsou uvedeny na trh nebo do provozu v Unii nebo pokud nejsou používány v Unii. Jedná se například o případ, kdy provozovatel usazený v Unii smluvně zadává určité služby provozovateli usazenému ve třetí zemi v souvislosti s činností, kterou má provádět systém AI, jejž by bylo možno kvalifikovat jako vysoce rizikový. Za těchto okolností by systém AI, který provozovatel používá ve třetí zemi, mohl zpracovávat údaje zákonně shromážděné v Unii a přesunuté z Unie a poskytovat zadávajícímu provozovateli v Unii výstup z tohoto systému AI vyplývající z uvedeného zpracování, aniž by byl tento systém AI 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 subjekty zavádějící systémy AI, kteří jsou usazeni ve třetí zemi, pokud jsou výstupy vytvořené těmito systémy zamýšleny k používání 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 spolupráce nebo mezinárodních dohod uzavřených na unijní nebo vnitrostátní úrovni za účelem spolupráce v oblasti vymáhání práva a justiční spolupráce s Unií nebo členskými státy, pokud daná třetí země či mezinárodní organizace poskytne přiměřené záruky, pokud jde o ochranu základních práv a svobod fyzických osob. V příslušných případech se může jednat o činnosti subjektů pověřených třetími zeměmi prováděním zvláštních úkolů na podporu této spolupráce v oblasti vymáhání práva a justiční spolupráce. Tyto rámce pro spolupráci či dohody byly uzavřeny dvoustranně mezi členskými státy a třetími zeměmi nebo mezi Evropskou unií, Europolem a dalšími agenturami Unie a třetími zeměmi a mezinárodními organizacemi. Orgány příslušné pro dohled nad donucovacími a justičními orgány podle tohoto nařízení by měly posoudit, zda tyto rámce pro spolupráci nebo mezinárodní dohody obsahují přiměřené záruky, pokud jde o ochranu základních práv

a svobod fyzických osob. Přijímající vnitrostátní orgány 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.

(23) Toto nařízení by se mělo vztahovat také na orgány, instituce a jiné subjekty Unie, pokud jednají jako poskytovatel systému AI nebo subjekt zavádějící tento systém.

(24) Pokud, a v míře v jaké jsou systémy AI uvedeny na trh nebo do provozu nebo jsou používány se změnami těchto systémů nebo bez nich pro vojenské nebo 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 Smlouvy o Evropské unii, tak specifiky obranné politiky členských států a společné obranné politiky Unie, na něž se vztahuje hlava V kapitola 2 Smlouvy o Evropské unii a jež podléhají mezinárodnímu právu veřejnému, což je pak vhodnější právní rámec pro regulaci systémů AI v kontextu použití smrticí síly a jiných systémů AI 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 Smlouvy o Evropské unii 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 AI 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 vymáhání práva nebo pro účely veřejné bezpečnosti, do oblasti působnosti tohoto nařízení by spadal. V takovém případě by subjekt, který systém AI používá pro jiné než vojenské nebo obranné účely nebo účely národní bezpečnosti, měl zajistit soulad systému AI s tímto nařízením, pokud systém dosud v souladu s tímto nařízením není. Systémy AI uváděné na trh nebo do provozu pro vyloučené účely, tedy vojenské nebo obranné účely nebo účely národní bezpečnosti, a jeden nebo více účelů, které vyloučeny nejsou, jako jsou civilní účely či vymáhání práva, do oblasti působnosti tohoto nařízení spadají a poskytovatelé těchto systémů by měli zajistit soulad s tímto nařízením. V těchto případech by skutečností, že systém AI může spadat do oblasti působnosti tohoto nařízení, neměla být dotčena možnost, aby subjekty provádějící činnosti v oblasti národní bezpečnosti nebo obranné a vojenské činnosti, bez ohledu na typ subjektu, který tyto činnosti provádí, používaly systémy AI pro účely národní bezpečnosti nebo vojenské a obranné účely, jejichž použití je z oblasti působnosti tohoto nařízení vyloučeno. Systém AI uváděný na trh pro civilní účely nebo pro účely vymáhání práva, který se používá se změnami nebo bez nich pro vojenské nebo obranné účely nebo pro účely národní bezpečnosti, by do oblasti působnosti tohoto nařízení spadat neměl, a to bez ohledu na typ subjektu, který tyto činnosti provádí.

(25) Toto nařízení by mělo podporovat inovace, respektovat svobodu vědy a nemělo by narušovat činnosti v oblasti výzkumu a vývoje. Je proto nezbytné vyloučit z jeho oblasti působnosti systémy a modely AI, které byly speciálně vyvinuty a uvedeny do provozu výhradně za účelem vědeckého výzkumu a vývoje. Kromě toho je nezbytné zajistit, aby toto nařízení nemělo žádný jiný vliv na činnost v oblasti vědeckého výzkumu a vývoje systémů AI před jejich uvedením na trh nebo do provozu. Pokud jde o činnost v oblasti výzkumu, testování a vývoje zaměřenou na produkty a týkající se systémů nebo modelů AI, ustanovení tohoto nařízení by se rovněž neměla použít před uvedením těchto systémů a modelů do provozu nebo na trh. Tímto vyloučením není dotčena povinnost dodržovat toto nařízení, pokud je systém AI spadající do oblasti působnosti tohoto nařízení uveden na trh nebo do provozu jako výsledek této výzkumné a vývojové činnosti, ani uplatňování ustanovení o regulačních sandboxech pro AI a testování v reálných podmínkách. Aniž je dotčeno vyloučení, pokud jde o systémy AI speciálně vyvinuté a uvedené do provozu výhradně za účelem vědeckého výzkumu a vývoje, měla by se ustanovení tohoto nařízení i nadále vztahovat rovněž na jakýkoli jiný systém AI, který může být použit k provádění jakékoli výzkumné a vývojové činnosti. Za všech okolností by měla být veškerá výzkumná a vývojová činnost prováděna v souladu s uznávanými etickými a profesními normami vědeckého výzkumu a v souladu s platným právem Unie.

(26) Aby bylo možné zavést přiměřený a účinný soubor závazných pravidel pro systémy AI, 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 AI vytvářet. Je proto nezbytné zakázat některé nepřijatelné postupy v oblasti AI a stanovit požadavky na vysoce rizikové systémy AI a povinnosti příslušných provozovatelů, jakož i povinnosti transparentnosti pro určité systémy AI.

(27) Ačkoli přístup založený na posouzení rizik je základem pro přiměřený a účinný soubor závazných pravidel, je důležité připomenout Etické pokyny pro zajištění důvěryhodnosti UI z roku 2019, které vypracovala nezávislá Expertní skupina na vysoké úrovni pro AI jmenovaná Komisí. V těchto pokynech vypracovala uvedená skupina sedm nezávazných etických zásad týkajících se AI, které mají pomoci zajistit, aby byla AI důvěryhodná a vyhovovala požadavkům etiky. Předmětných sedm zásad obsahuje lidský faktor a dohled; technickou spolehlivost a bezpečnost; ochranu soukromí a správu dat; transparentnost; rozmanitost, nediskriminaci a spravedlnost; dobré sociální a environmentální podmínky; odpovědnost. Aniž jsou dotčeny právně závazné požadavky tohoto nařízení a jakékoli jiné použitelné právo předpisů Unie, přispívají uvedené pokyny k navrhování soudržné, důvěryhodné AI zaměřené na člověka v souladu s Listinou a s hodnotami, na nichž je Unie založena. Podle pokynů skupiny AI HLEG lidský faktor a dohled spočívá v tom, že systémy AI jsou vyvíjeny a používány jako nástroj, který slouží lidem, respektuje lidskou důstojnost a osobní autonomii a který funguje způsobem, jenž může být řádně ovládán a kontrolován člověkem. Technická spolehlivost a bezpečnost znamená, že systémy AI jsou vyvíjeny a používány takovým způsobem, jenž zajistí jejich spolehlivost v případě problémů a odolnost vůči pokusům změnit jejich použití nebo výkonnost tak, aby bylo umožněno protiprávní použití třetími stranami, a jímž je minimalizována neúmyslná újma. Ochranou soukromí a správou dat se rozumí, že systémy AI jsou vyvíjeny a používány v souladu s pravidly pro ochranu soukromí a osobních údajů při současném zpracovávání údajů, které splňují vysoké standardy kvality a integrity. Transparentností se rozumí, že systémy AI jsou vyvíjeny a používány tak, aby umožňovaly patřičnou sledovatelnost a vysvětlitelnost, aby lidé byli informováni o tom, že komunikují nebo interagují se systémem AI, a aby zavádějící subjekty byly řádně informovány o schopnostech a omezeních daného systému AI a dotčené osoby o svých právech. Rozmanitostí, zákazem diskriminace a spravedlností se rozumí, že systémy AI jsou vyvíjeny a používány tak, aby zahrnovaly nejrůznější aktéry a podporovaly rovný přístup, genderovou rovnost a kulturní rozmanitost a zároveň bránily diskriminačním dopadům a nespravedlivé zaujatosti, které jsou podle práva Unie a členských států zakázány. Dobrými sociálními a environmentálními podmínkami se rozumí, že systémy AI jsou vyvíjeny a používány udržitelným způsobem šetrným k životnímu prostředí, jakož i ve prospěch všech lidí při současném sledování a posuzování dlouhodobých dopadů na jednotlivce, společnost a demokracii. Uplatňování těchto zásad by se mělo pokud možno promítnout v rámci navrhování a používání modelů AI. V každém případě by měly sloužit jako základ pro vypracování kodexů chování podle tohoto nařízení. Všechny zúčastněné strany, včetně průmyslu, akademické obce, občanské společnosti a normalizačních organizací, se vyzývají, aby uvedené etické zásady ve vhodných případech zohledňovaly při vypracovávání dobrovolných osvědčených postupů a norem.

(28) Přestože využívání AI přináší celou řadu výhod, AI může být i zneužita a stát se zdrojem nových a výkonných nástrojů umožňujících praktiky spočívající v manipulaci, vykořisťování a sociální kontrole. Tyto praktiky jsou mimořádně škodlivé a nekalé a měly by být zakázány, neboť jsou v rozporu s hodnotami Unie, jimiž je úcta k lidské důstojnosti, svoboda, rovnost, demokracie a právní stát, a se základními právy zakotvenými v Listině, včetně práva na zákaz diskriminace, na ochranu údajů a soukromí a práv dítěte.

(29) Manipulativní techniky založené na AI lze použít k přesvědčování osob k nežádoucímu chování nebo k jejich klamání tím, že je podněcují k přijímání rozhodnutí tak, že je podkopávána a narušována jejich autonomie, rozhodování a svobodná volba. Uvádění na trh nebo do provozu nebo používání určitých systémů AI s cílem podstatně ovlivnit lidské chování nebo s takovým účinkem, kdy je pravděpodobné, že bude dotčeným osobám způsobena značná újma, zejména pokud jde o dostatečně významné nepříznivé dopady na fyzické či psychické zdraví nebo finanční zájmy, je obzvláště nebezpečné, a proto by mělo být zakázáno. Tyto systémy AI využívají podprahové signály, jako jsou zvukové a obrazové stimuly a videostimuly, které člověk není schopen vnímat, neboť jsou mimo rámec lidského vnímání, nebo jiné manipulativní nebo klamavé techniky, které narušují nebo oslabují autonomii, schopnost rozhodování nebo svobodnou volbu člověka tak, že tento vliv vědomě nezaznamená, nebo pokud si jej uvědomí, přesto se nechá oklamat nebo není schopen tyto techniky ovlivnit nebo jim odolat. To by mohlo být usnadněno například rozhraními stroj–mozek nebo virtuální realitou, neboť umožňují větší kontrolu nad tím, jakým stimulům je jedinec vystaven, pokud mohou tyto stimuly značnou měrou a výrazně škodlivým způsobem narušit jejich chování. Systémy AI mohou kromě toho zneužívat zranitelnost jednotlivců či určité skupiny osob i jiným způsobem, z důvodu jejich věku, zdravotního postižení ve smyslu směrnice Evropského parlamentu a Rady (EU) 2019/882 ([16]) nebo zvláštní sociální nebo ekonomické situace, v jejímž důsledku mohou být tyto osoby, jako jsou osoby žijící v extrémní chudobě nebo etnické nebo náboženské menšiny, více zranitelné vůči zneužívání. Tyto systémy mohou být uváděny na trh nebo do provozu nebo používány s cílem podstatně ovlivnit chování určitého jednotlivce nebo s takovým účinkem, a to takovým způsobem, že je dotčenému jednotlivci nebo jiné osobě nebo skupinám osob způsobena značná újma nebo lze takovou újmu důvodně předpokládat, přičemž se může

([16]) Směrnice Evropského parlamentu a Rady (EU) 2019/882 ze dne 17. dubna 2019 o požadavcích na přístupnost u výrobků a služeb (Úř. věst. L 151, 7.6.2019, s. 70).

jednat i o újmy, které v průběhu času kumulují; proto by měly být tyto systémy zakázány. Může se stát, že úmysl ovlivnit chování není možné předpokládat, pokud je takovéto ovlivnění způsobeno faktory mimo systém AI, které jsou mimo kontrolu poskytovatele nebo zavádějícího subjektu, konkrétně pokud jde o faktory, které nemusí být rozumně předvídatelné, a tudíž je poskytovatel nebo subjekt zavádějící systém AI nemohou zmírnit. V každém případě nemusí mít poskytovatel nebo zavádějící subjekt v úmyslu způsobit značnou újmu, pokud tato újma vyplývá z manipulativních nebo vykořisťujících praktik založených na AI. Zákazy těchto praktik AI se doplňují ustanovení obsažená ve směrnici Evropského parlamentu a Rady 2005/29/ES ([17]), 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 AI, nebo jinak. Zákazy manipulativních a vykořisťujících praktik stanovené 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 platným právem a lékařskými normami, například pokud jde o výslovný souhlas osob nebo jejich právních zástupců. Kromě toho by za škodlivé manipulativní praktiky založené na AI neměly být samy o sobě považovány běžné a legitimní obchodní praktiky, například v oblasti reklamy, které jsou v souladu s platným právem.

(30) Měly by být zakázány systémy biometrické kategorizace, které jsou založeny na biometrických údajích fyzických osob, jako je obličej nebo otisky prstů jednotlivců, za účelem odvozování či vyvozování politických názorů jednotlivců, členství v odborových organizacích, náboženského nebo filozofického přesvědčení, rasy, sexuálního života nebo sexuální orientace. Tento zákaz by se neměl vztahovat na zákonné označování, filtrování nebo kategorizaci souborů biometrických údajů získaných v souladu s právem Unie nebo vnitrostátním právem na základě biometrických údajů, jako je třídění zobrazení podle barvy vlasů nebo očí, které lze použít například v oblasti vymáhání práva.

(31) Systémy AI umožňující hodnocení sociálního kreditu fyzických osob ze strany veřejných či 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 AI hodnotí nebo klasifikují fyzické osoby nebo skupiny fyzických osob na základě vícedatových bodů týkajících se jejich sociálního chování v různých kontextech nebo známých, odvozených či předvídaných osobních či osobnostních vlastností v průběhu určitého časového období. Sociální kredit získaný na základě těchto systémů AI může vést ke znevýhodňujícímu nebo nepříznivému zacházení s fyzickými osobami nebo s celými skupinami fyzických 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 AI, které tyto nepřijatelné postupy hodnocení zahrnují a vedou k takovým znevýhodňujícím nebo nepříznivým výsledkům, by proto měly být zakázány. Tímto zákazem by neměly být dotčeny zákonné postupy posuzování fyzických osob prováděné za zvláštním účelem v souladu s unijním či vnitrostátním právem.

(32) Využívání systémů AI pro biometrickou identifikaci fyzických osob na dálku „v reálném čase“ ve veřejně přístupných prostorech pro účely vymáhání práva obzvláště zasahuje 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. Technické nepřesnosti systémů AI určených pro biometrickou identifikaci fyzických osob na dálku mohou vést ke zkresleným výsledkům a mít diskriminační účinky. Tyto případné zkreslené výsledky a diskriminační účinky jsou obzvláště relevantní, pokud jde o věk, etnickou příslušnost, rasu, pohlaví nebo zdravotní postižení. 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 vymáhání práva nebo jsou jimi dotčeny.

(33) Používání těchto systémů pro účely vymáhání 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 určitých obětí trestných činů, včetně pohřešovaných osob, některé případy ohrožení života nebo fyzické bezpečnosti fyzických osob nebo hrozby teroristického útoku a lokalizaci nebo identifikaci pachatelů nebo osob podezřelých ze spáchání trestných činů uvedených v příloze tohoto nařízení, pokud lze za tyto trestné činy uložit v dotčeném členském státě trest odnětí

([17]) Směrnice Evropského parlamentu a Rady 2005/29/ES ze dne 11. května 2005 o nekalých obchodních praktikách vůči spotřebitelům na vnitřním trhu a o změně směrnice Rady 84/450/EHS, směrnic Evropského parlamentu a Rady 97/7/ES, 98/27/ES a 2002/65/ES a nařízení Evropského parlamentu a Rady (ES) č. 2006/2004 (směrnice o nekalých obchodních praktikách) (Úř. věst. L 149, 11.6.2005, s. 22).

svobody s horní hranicí v délce nejméně čtyři roky nebo ochranné opatření spojené se zbavením osobní svobody ve stejné délce v souladu s právem tohoto členského státu. Tato hranice pro trest odnětí svobody nebo ochranné opatření spojené se zbavením osobní svobody v souladu s vnitrostátním právem přispívá k zajištění toho, že použití systémů biometrické identifikace na dálku v reálném čase bude možno potenciálně odůvodnit jen dostatečnou závažností daného trestného činu. Kromě toho je seznam trestných činů uvedený v příloze tohoto nařízení založen na seznamu 32 trestných činů uvedených v rámcovém rozhodnutí Rady 2002/584/SVV ([18]), přičemž je zohledněna skutečnost, že některé z těchto trestných činů budou v praxi pravděpodobně relevantnější než jiné v tom smyslu, že nezbytnost a přiměřenost využívání biometrické identifikace na dálku v reálném čase může být pravděpodobně velmi různorodá jak z hlediska praktické snahy o lokalizaci či identifikaci pachatelů jednotlivých trestných činů uvedených na seznamu nebo osob podezřelých z jejich spáchání, tak s ohledem na pravděpodobné rozdíly v závažnosti, pravděpodobnosti a rozsahu způsobené újmy nebo možných negativních důsledků. Bezprostřední ohrožení života nebo fyzické bezpečnosti fyzických osob by mohlo být rovněž důsledkem vážného narušení kritické infrastruktury ve smyslu čl. 2 bodu 4 směrnice Evropského parlamentu a Rady (EU) 2022/2557 ([19]), pokud by narušení nebo zničení této kritické infrastruktury vedlo k bezprostřednímu ohrožení života nebo fyzické bezpečnosti určité osoby, a to i v důsledku vážného narušení poskytování základních dodávek obyvatelstvu nebo výkonu základních funkcí státu. 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 osob, které během kontroly totožnosti buď odmítnou být identifikovány, nebo nejsou schopny uvést či prokázat svou totožnost, aniž by tyto orgány byly podle tohoto nařízení povinny získat předchozí povolení. Může se jednat například o osobu zapojenou do trestného činu, která není ochotna nebo z důvodu nehody nebo zdravotního stavu schopna sdělit svou totožnost donucovacím orgánům.

(34) 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 žádosti, o důsledky užití těchto systémů pro práva a svobody všech dotčených osob a o záruky a podmínky zajištěné při tomto použití. Kromě toho by používání systémů biometrické identifikace na dálku v reálném čase ve veřejně přístupných prostorech pro účely vymáhání práva mělo být nasazeno pouze k potvrzení totožnosti konkrétně cílené fyzické osoby a mělo by být omezeno na to, co je nezbytně nutné, pokud jde o dobu, jakož i zeměpisný a osobní rozsah, zejména s ohledem na důkazy nebo údaje týkající se daných hrozeb, obětí nebo pachatele. Používání systému biometrické identifikace na dálku v reálném čase ve veřejně přístupných prostorech by mělo být povoleno pouze v případě, že příslušný donucovací orgán dokončil posouzení dopadů na základní práva, a nestanoví-li toto nařízení jinak, zaregistroval systém v databázi podle tohoto nařízení. Pro každý případ použití v každé z výše uvedených situací by mělo být vhodné využití referenční databáze osob.

(35) Každé použití systému biometrické identifikace na dálku v reálném čase ve veřejně přístupných prostorech pro účely vymáhání práva by mělo podléhat výslovnému a konkrétnímu povolení justičního orgánu nebo nezávislého správního orgánu členského státu, jehož rozhodnutí je závazné. Toto povolení by mělo být v zásadě získáno před použitím systému AI za účelem identifikace určité osoby nebo osob. Výjimky z tohoto pravidla by měly být povoleny v řádně odůvodněných situacích z důvodu naléhavosti, tedy v situacích, kdy je potřeba použít dotčené systémy tak naléhavá, že je fakticky a objektivně nemožné získat povolení před zahájením tohoto použití. V těchto naléhavých situacích by použití systému AI mělo být omezeno na absolutně nezbytné minimum a mělo by podléhat příslušným zárukám a podmínkám, které stanoví vnitrostátní právo a které konkrétně určuje v souvislosti s každým jednotlivým případem naléhavého použití samotný donucovací orgán. Kromě toho by měl donucovací orgán v uvedených situacích o toto povolení požádat a uvést důvody, proč o ně nemohl požádat dříve, bez zbytečného odkladu, nejpozději však do 24 hodin. Je-li takové povolení zamítnuto, mělo by být použití systémů biometrické identifikace v reálném čase spojené s tímto povolením zastaveno s okamžitým účinkem a veškeré údaje související s tímto použitím by měly být vyřazeny a vymazány. Uvedené údaje zahrnují vstupní údaje přímo získané systémem

([18]) 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).

([19]) Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES (Úř. věst. L 333, 27.12.2022, s. 164).

AI v průběhu jeho používání, jakož i výsledky a výstupy použití spojeného s tímto povolením. Neměly by zahrnovat vstupy, které jsou zákonně získány v souladu s jiným unijním nebo vnitrostátním právem. Výlučně na základě výstupu systému biometrické identifikace na dálku by každopádně nemělo být přijato žádné rozhodnutí, které má pro určitou osobu nepříznivé právní účinky.

(36) Aby mohl plnit své úkoly v souladu s požadavky stanovenými v tomto nařízení a ve vnitrostátních předpisech, měl by být příslušný orgán dozoru nad trhem a vnitrostátní orgán pro ochranu osobních údajů o každém použití systému biometrické identifikace v reálném čase informován. Orgány dozoru nad trhem a vnitrostátní orgány pro ochranu osobních údajů, které byly o tomto použití informovány, by měly k používání systémů biometrické identifikace v reálném čase předložit Komisi výroční zprávu.

(37) 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 v případě, že se dotčený členský stát rozhodl výslovně stanovit možnost povolit toto použití v podrobných pravidlech svého vnitrostátního práva, a v míře stanovené tamtéž. 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. Tato vnitrostátní pravidla by měla být oznámena Komisi do 30 dnů od přijetí.

(38) Používání systémů AI pro biometrickou identifikaci fyzických osob na dálku v reálném čase ve veřejně přístupných prostorech pro účely vymáhání 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 Smlouvy o fungování Evropské unie, 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 dotčených biometrických údajů vyčerpávajícím způsobem upravovalo. Toto použití a zpracování by proto mělo být možné jen v případě, že je slučitelné s rámcem stanoveným tímto nařízením, a mimo tento rámec by neměl existovat prostor pro to, aby příslušné orgány, pokud jednají za účelem vymáhání práva, tyto systémy používaly a zpracovávaly v souvislosti s nimi uvedené údaje z důvodů uvedených v článku 10 směrnice (EU) 2016/680. V této souvislosti není cílem tohoto nařízení poskytnout právní základ pro zpracování osobních údajů podle článku 8 směrnice (EU) 2016/680. Na používání systémů biometrické identifikace na dálku v reálném čase na veřejně přístupných prostorech pro jiné účely než vymáhání práva, a to i příslušnými orgány, by se však zvláštní rámec stanovený tímto nařízením pro používání uvedených systémů pro účely vymáhání práva vztahovat neměl. Toto použití pro jiné účely než vymáhání práva by proto nemělo podléhat požadavku na povolení podle tohoto nařízení a použitelným podrobným pravidlům vnitrostátního práva, která mohou toto povolení uvést v účinnost.

(39) Jakékoli zpracování biometrických údajů a dalších osobních údajů související s používáním systémů AI pro účely biometrické identifikace jinak než v souvislosti s používáním systémů biometrické identifikace na dálku v reálném čase ve veřejně přístupných prostorech pro účely vymáhání práva podle tohoto nařízení by mělo i nadále splňovat všechny požadavky vyplývající z článku 10 směrnice (EU) 2016/680. Pro jiné účely než vymáhání práva zakazují čl. 9 odst. 1 nařízení (EU) 2016/679 a čl. 10 odst. 1 nařízení (EU) 2018/1725 zpracování biometrických údajů s výhradou omezených výjimek stanovených v uvedených článcích Vnitrostátní orgány pro ochranu osobních údajů již při uplatňování čl. 9 odst. 1 nařízení (EU) 2016/679 vydaly rozhodnutí, jejichž předmětem byl zákaz použití biometrické identifikace na dálku pro jiné účely než pro účely vymáhání práva.

(40) 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 prvním pododstavci písm. g) v rozsahu, v němž se vztahují na používání systémů biometrické kategorizace k činnostem v oblasti policejní spolupráce a justiční spolupráce v trestních věcech, v čl. 5 odst. 1 prvním pododstavci písm. d) v rozsahu, v němž se vztahují na použití systémů AI, na něž se vztahuje uvedené ustanovení, v čl. 5 odst. 1 prvním pododstavci písm. h), v čl. 5 odst.2 až 6 a v čl. 26 odst. 10 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 upravujícími formy justiční spolupráce v trestních věcech nebo policejní spolupráce, v jejichž rámci musí být dodržována ustanovení stanovená na základě článku 16 Smlouvy o fungování EU.

(41) 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 čl. 5 odst. 1 prvním pododstavci písm. g) v rozsahu, v němž se vztahují na používání systémů biometrické kategorizace k činnostem v oblasti policejní spolupráce a justiční spolupráce v trestních věcech, v čl. 5 odst. 1 prvním pododstavci písm. d) v rozsahu, v němž se vztahují na použití systémů AI, na něž se vztahuje uvedené ustanovení, v čl. 5 odst. 1 prvním pododstavci písm. h), v čl. 5

odst.2 až 6 a čl. 26 odst. 10 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.

(42) V souladu s presumpcí neviny by fyzické osoby v Unii měly být vždy posuzovány podle svého skutečného chování. Fyzické osoby by nikdy neměly být posuzovány na základě chování předvídaného AI pouze na základě jejich profilování, osobnostních rysů nebo charakteristik, jako je státní příslušnost, místo narození, místo bydliště, počet dětí, výše dluhu nebo typ vozidla, aniž by na základě objektivních ověřitelných skutečností existovalo důvodné podezření, že se dotčená osoba podílí na trestné činnosti, a aniž by bylo provedeno posouzení člověkem. Proto by mělo být zakázáno provádět posouzení rizik ve vztahu k fyzickým osobám za účelem posouzení pravděpodobnosti spáchání trestného činu těmito osobami nebo předvídání skutečného nebo potenciálního trestného činu pouze na základě profilování těchto osob nebo posouzení jejich osobnostních rysů a charakteristik. V každém případě se tento zákaz nevztahuje na analýzy rizik, které nejsou založeny na profilování jednotlivců nebo na osobnostních rysech a charakteristikách jednotlivců, jako jsou systémy AI využívající analýzu rizik k posouzení pravděpodobnosti finančních podvodů ze strany podniků na základě podezřelých transakcí nebo nástroje analýzy rizik, které umožňují předvídat pravděpodobnost lokalizace omamných látek nebo nezákonného zboží celními orgány, například na základě známých tras využívaných k obchodování s těmito látkami či zbožím, a tyto analýzy jím nejsou dotčeny.

(43) Uvádění na trh nebo do provozu pro tento konkrétní účel nebo používání systémů AI, které vytvářejí nebo rozšiřují databáze rozpoznávání obličeje prostřednictvím necíleného získávání zobrazení obličeje z internetu nebo záznamů CCTV, by mělo být zakázáno, protože tato praxe přispívá k pocitu hromadného sledování a může vést k hrubému porušování základních práv, včetně práva na soukromí.

(44) Existují vážné obavy ohledně vědeckého základu systémů AI, jejichž cílem je zjišťovat nebo odvozovat emoce, zejména z toho důvodu, že vyjádření emocí se v jednotlivých kulturách a situacích značně liší, a dokonce i u téhož jednotlivce. Mezi hlavní nedostatky těchto systémů patří omezená spolehlivost, nedostatečná specifičnost a omezená možnost zobecňování. Systémy AI, které zjišťují nebo odvozují emoce nebo záměry fyzických osob na základě jejich biometrických údajů, proto mohou vést k diskriminačním výsledkům a mohou zasahovat do práv a svobod dotčených osob. Vzhledem k nerovnováze moci v kontextu práce nebo vzdělávání ve spojení s invazivní povahou těchto systémů by tyto systémy mohly vést ke znevýhodňujícímu nebo nepříznivému zacházení s některými fyzickými osobami nebo celými skupinami fyzických osob. Uvádění na trh, uvádění do provozu nebo používání systémů AI určených k použití za účelem zjišťování emočního stavu jednotlivců v situacích souvisejících s prací a vzděláváním by proto mělo být zakázáno. Tento zákaz by se neměl vztahovat na systémy AI uváděné na trh výhradně z lékařských nebo bezpečnostních důvodů, jako jsou systémy určené k terapeutickému použití.

(45) Tímto nařízením by neměly být dotčeny postupy, které jsou zakázány právem Unie, včetně práva v oblasti ochrany údajů, nediskriminace, ochrany spotřebitele a hospodářské soutěže.

(46) Vysoce rizikové systémy AI by měly být uváděny na trh Unie, do provozu nebo používány pouze v případě, že splňují určité závazné požadavky. Tyto požadavky by měly zajistit, aby vysoce rizikové systémy AI, 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. Na základě nového legislativního rámce, jak je objasněno ve sdělení Komise „Modrá příručka“ k provádění pravidel EU pro výrobky (2022) ([20]), je obecným pravidlem, že na jeden produkt může být použitelný více než jeden právní akt náležející mezi harmonizační právní předpis Unie, jako jsou nařízení Evropského parlamentu a Rady (EU) 2017/745 ([21]) a 2017/746 ([22]) nebo směrnice Evropského parlamentu a Rady 2006/42/ES ([23]), neboť k dodání na trh nebo uvedení do provozu může dojít pouze v případě, že je produkt v souladu se všemi platnými harmonizačními právními předpisy Unie. Aby byla zajištěna soudržnost

([20]) Úř. věst. C 247, 29.6.2022, s. 1.

([21]) 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).

([22]) 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).

([23]) 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).

a zabránilo se zbytečné administrativní zátěži nebo nákladům, poskytovatelé produktu, který obsahuje jeden nebo více vysoce rizikových systémů AI, na něž se vztahují požadavky tohoto nařízení a harmonizačních právních předpisů Unie uvedených v příloze tohoto nařízení, by měli být flexibilní, pokud jde o přijímání provozních rozhodnutí o tom, jak optimálně zajistit soulad produktu obsahujícího jeden nebo více systémů AI se všemi platnými požadavky harmonizačních právních předpisů Unie. Označení systémů AI jako vysoce rizikové by mělo být omezeno na systémy, které mají významný škodlivý dopad na zdraví, bezpečnost a základní práva osob v Unii, a tímto omezením by se mělo minimalizovat jakékoli případné omezení mezinárodního obchodu.

(47) Systémy AI by mohly mít nepříznivý dopad na zdraví a bezpečnost osob, zejména pokud tyto systémy fungují jako bezpečnostní komponenty. 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 produkty bezpečné a jinak vyhovující, je důležitá náležitá prevence a zmírňování bezpečnostních rizik, která mohou případně vyplývat z produktu jako celku v důsledku jeho digitálních prvků, včetně systémů AI. 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 jsou život a zdraví vystaveny obzvláště vysokému riziku, by měly být stále sofistikovanější diagnostické systémy a systémy podporující lidská rozhodnutí spolehlivé a přesné.

(48) Pro klasifikaci určitého systému AI jako vysoce rizikového je zvláště relevantní míra nepříznivého dopadu takového systému AI na základní práva chráněná Listinou. Tato práva zahrnují právo na lidskou důstojnost, respektování soukromého a rodinného života, ochranu osobních údajů, svobodu projevu a informací, svobodu shromažďování a sdružování, právo na nediskriminaci, právo na vzdělání, ochranu spotřebitele, práva pracovníků, práva osob se zdravotním postižením, genderovou rovnost, práva duševního vlastnictví, 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 skutečnost, že v článku 24 Listiny a v Úmluvě OSN o právech dítěte jsou zakotvena zvláštní práva dětí, dále rozpracovaná ve vztahu k digitálnímu prostředí v obecné připomínce č. 25 k Úmluvě o právech dítěte, přičemž oba dokumenty vyžadují zohlednění zranitelnosti dětí a poskytnutí takové ochrany a péče, která je nezbytná pro jejich blaho. Při posuzování závažnosti újmy, kterou může systém AI 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.

(49) Pokud jde o vysoce rizikové systémy AI, které jsou bezpečnostními komponentami produktů nebo systémů, případně které jsou samy produkty nebo systémy spadajícími do působnosti nařízení Evropského parlamentu a Rady (ES) č. 300/2008 ([24]), nařízení Evropského parlamentu a Rady (EU) č. 167/2013 ([25]), nařízení Evropského parlamentu a Rady (EU) č. 168/2013 ([26]), směrnice Evropského parlamentu a Rady 2014/90/EU ([27]), směrnice Evropského parlamentu a Rady (EU) 2016/797 ([28]), nařízení Evropského parlamentu a Rady (EU) 2018/858 ([29]), nařízení Evropského parlamentu a Rady (EU) 2018/1139 ([30]) a nařízení Evropského parlamentu a Rady (EU)

([24]) 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).

([25]) 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).

([26]) 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).

([27]) 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).

([28]) 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).

([29]) 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).

([30]) 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).

2019/2144 ([31]), je vhodné tyto akty pozměnit s cílem zajistit, aby Komise při přijímání jakýchkoli relevantních aktů v přenesené pravomoci nebo prováděcích aktů na základě výše uvedených aktů zohledňovala povinné požadavky na vysoce rizikové systémy AI 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.

(50) Pokud jde o systémy AI, které jsou bezpečnostními komponentami produktů nebo jsou produkty samy o sobě a které spadají do oblasti působnosti některých harmonizačních právních předpisů Unie uvedených v příloze tohoto nařízení, je vhodné je podle tohoto nařízení klasifikovat jako vysoce rizikové, pokud u dotyčného produktu provádí postup posuzování shody subjekt, který činnosti posuzování shody vykonává 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* a automobilový průmysl a letectví.

(51) Klasifikace určitého systému AI jako vysoce rizikového podle tohoto nařízení by neměla nutně znamenat, že produkt, jehož je daný systém AI bezpečnostní komponentou, případně tento samotný systém AI 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 (EU) 2017/745 a (EU) 2017/746, kde je pro produkty se středním a vysokým rizikem vyžadováno posuzování shody subjektem, který vykonává činnosti posuzování shody jakožto třetí strana.

(52) Pokud jde o samostatné systémy AI, konkrétně vysoce rizikové systémy AI s výjimkou těch, které představují bezpečnostní komponenty produktů nebo které jsou samy produkty, je vhodné je klasifikovat jako vysoce rizikové, pokud s ohledem na zamýšlený 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 AI, k jejichž přijímání by měla být Komise zmocněna prostřednictvím aktů v přenesené pravomoci s cílem zohlednit rychlé tempo technologického vývoje, jakož i možné změny v používání systémů AI.

(53) Je rovněž důležité vyjasnit, že mohou existovat zvláštní případy, kdy systémy AI uvedené v předem vymezených oblastech specifikovaných v tomto nařízení nezakládají významné riziko poškození právních zájmů, které jsou v těchto oblastech chráněny, protože nemají podstatný vliv na rozhodování nebo tyto zájmy podstatně nepoškozují. Pro účely tohoto nařízení by se systémem AI, který nemá podstatný vliv na výsledek rozhodování, měl rozumět systém AI, který nemá vliv na podstatu, a tím ani na výsledek rozhodování, ať už jde o lidské, nebo automatizované rozhodování. Systém AI, který podstatně neovlivňuje výsledek rozhodování, by mohl zahrnovat situace, kdy je splněna jedna nebo více z následujících podmínek. Prvním takovou podmínkou by mělo být, že je daný systém AI určen k plnění úzce vymezeného procedurálního úkolu, jako je systém AI, který přeměňuje nestrukturovaná data na data strukturovaná, systém AI, který třídí příchozí dokumenty do kategorií, nebo systém AI, který se používá k odhalování duplicit mezi velkým počtem žádostí. Tyto úkoly jsou natolik úzké a omezené povahy, že představují pouze omezená rizika, která se použitím systému AI v kontextu uvedeném na seznamu v příloze tohoto nařízení

([31]) 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).

jako vysoce rizikové použití nezvyšují. Druhou podmínkou by mělo být, že úkol prováděný daným systémem AI je určen ke zlepšení výsledku dříve dokončené lidské činnosti, která může být relevantní pro účely vysoce rizikového použití uvedeného v seznamu v příloze tohoto nařízení. Vzhledem k těmto vlastnostem přidává takový systém AI pouze další vrstvu k lidské činnosti, a riziko je tudíž nízké. Tato podmínka by se například vztahovala na systémy AI, které mají zdokonalit formulace použité v dříve vypracovaných dokumentech, například z hlediska odborného vyjadřování, akademického stylu nebo přizpůsobení textu určitému sdělení značky. Třetí podmínkou by mělo být, že je daný systém AI určen k odhalování vzorců rozhodování nebo odchylek od předchozích vzorců rozhodování. Riziko by bylo sníženo, protože použití takového systému AI následuje po dříve dokončeném lidském posouzení, které jím nemá být bez řádného lidského přezkumu nahrazeno ani ovlivněno. Mezi takové systémy AI patří například ty, které mohou být při určitém způsobu známkování ze strany učitele použity k následné kontrole, zda se učitel od tohoto způsobu známkování mohl odchýlit, a upozornit tak na možné nesrovnalosti nebo anomálie. Čtvrtou podmínkou by mělo být, že je daný systém AI určen k plnění úkolu, který je pouze přípravou k posouzení relevantnímu pro účely systémů AI uvedených v příloze tohoto nařízení, a možný dopad výstupu systému z hlediska rizika, jež pro následné posouzení představuje, je tudíž velmi nízký. Tato podmínka se vztahuje mimo jiné na inteligentní řešení pro zpracování souborů, která zahrnují různé funkce jako indexování, vyhledávání, zpracování textu a řeči nebo propojení dat s jinými zdroji údajů, nebo systémy AI používané pro překlad výchozích dokumentů. V každém případě by se mělo mít za to, že tyto systémy AI používané v případech vysoce rizikového použití uvedených v příloze tohoto nařízení představují významné riziko poškození zdraví, bezpečnosti nebo základních práv, pokud systém AI zahrnuje profilování ve smyslu čl. 4 bodu. 4 nařízení (EU) 2016/679, čl. 3 bodu 4 směrnice (EU) 2016/680 nebo čl. 3 bodu 5 nařízení 2018/1725. Aby byla zajištěna sledovatelnost a transparentnost, měl by poskytovatel, který se na základě výše uvedených podmínek domnívá, že určitý systém AI vysoce rizikový není, vypracovat dokumentaci o posouzení před uvedením tohoto systému na trh nebo do provozu a měl by tuto dokumentaci na požádání poskytnout příslušným vnitrostátním orgánům. Tento poskytovatel by měl mít povinnost zaregistrovat systém AI v databázi EU zřízené podle tohoto nařízení. Jako další pokyny pro praktické provádění podmínek, podle nichž systémy AI uvedené v příloze tohoto nařízení vysoce rizikové výjimečně nejsou, by Komise měla po konzultaci s radou poskytnout pokyny upřesňující toto praktické provádění doplněné komplexním seznamem praktických příkladů použití vysoce rizikových systémů AI a příkladů použití systémů AI, jež vysoce rizikové nejsou.

(54) Vzhledem k tomu, že zvláštní kategorii osobních údajů představují biometrické údaje, je vhodné klasifikovat jako vysoce rizikové několik případů kritického použití biometrických systémů, pokud je jejich používání povoleno podle příslušného práva Unie a vnitrostátního práva. Technické nepřesnosti systémů AI určených pro biometrickou identifikaci fyzických osob na dálku mohou vést ke zkresleným výsledkům a mít diskriminační účinky. Riziko takto předpojatých výsledků a diskriminačních účinků je obzvláště relevantní ve vztahu k věku, etnické příslušnosti, rase, pohlaví nebo zdravotnímu postižení. Systémy biometrické identifikace na dálku by proto s ohledem na rizika, která představují, měly být klasifikovány jako vysoce rizikové. Taková klasifikace se nevztahuje na systémy AI určené k biometrickému ověřování, včetně autentizace, jejichž jediným účelem je potvrdit, zda je konkrétní fyzická osoba osobou, za niž se prohlašuje, a systémy, které se používají k potvrzení totožnosti fyzické osoby za jediným účelem, kterým je získání přístupu ke službě, odblokování zařízení nebo získání bezpečného přístupu k prostorám. Kromě toho by jako vysoce rizikové měly být klasifikovány systémy AI určené k použití pro biometrickou kategorizaci podle citlivých atributů nebo vlastností chráněných podle čl. 9 odst. 1 nařízení (EU) 2016/679 na základě biometrických údajů, pokud nejsou tímto nařízením zakázány, a systémy rozpoznávání emocí, které nejsou tímto nařízením zakázány. Biometrické systémy, které jsou určeny k použití výhradně za účelem podpory opatření v oblasti kybernetické bezpečnosti a ochrany osobních údajů, by za vysoce rizikové systémy AI považovány být neměly.

(55) Pokud jde o správu a provoz kritické infrastruktury, je vhodné klasifikovat jako vysoce rizikové takové systémy AI, které jsou určeny k použití jako bezpečnostní komponenty při řízení a provozu kritické digitální infrastruktury, jak je uvedeno v bodu 8 přílohy směrnice (EU) 2022/2557, 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 provozu sociálních a hospodářských činností. Bezpečnostní komponenty 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 komponent může přímo vést k ohrožení fyzické

integrity kritické infrastruktury, a tím i k ohrožení zdraví a bezpečnosti osob a majetku. Komponenty určené k použití výhradně pro účely kybernetické bezpečnosti by neměly být považovány za bezpečnostní komponenty. Mezi příklady bezpečnostních komponent takové kritické infrastruktury mohou patřit systémy pro monitorování tlaku vody nebo systémy řízení požárního poplachu ve střediscích cloud computingu.

(56) Ve vzdělávání je zavádění systémů AI důležité pro podporu vysoce kvalitního digitálního vzdělávání a odborné přípravy a pro to, aby všichni účastníci vzdělávání a učitelé mohli získat a sdílet nezbytné digitální dovednosti a kompetence, včetně mediální gramotnosti a kritického myšlení, a mohli se tak aktivně zapojit do ekonomiky, společnosti a demokratických procesů. Jako vysoce rizikové by však měly být klasifikovány systémy AI používané ve vzdělávání nebo v odborné přípravě, zejména při určování přístupu osob do školských institucí a programů nebo institucí nebo programů odborného vzdělávání, jejich přijímání nebo přidělování do těchto institucí nebo programů na všech úrovních nebo pro hodnocení výsledků učení osob, pro posouzení vhodné úrovně vzdělávání jednotlivce a věcného vlivu úrovně vzdělávání a odborné přípravy, které tito jedinci obdrží, nebo pro určení přístupu nebo pro monitorování a detekci zakázaného chování studentů během testů, neboť takovéto systémy mohou určovat vzdělávací a profesní průběh života určité osoby, a tím mohou ovlivňovat její schopnost zajišťovat si živobytí. Pokud budou tyto systémy navrženy a používány nesprávně, mohou být mimořádně invazivní a mohou porušovat právo na vzdělávání a odbornou přípravu i právo nebýt diskriminován a fixovat historické vzorce diskriminace, například vůči ženám, určitým věkovým skupinám, osobám se zdravotním postižením nebo osobám určitého rasového nebo etnického původu nebo sexuální orientace.

(57) Jako vysoce rizikové by měly být klasifikovány rovněž systémy AI používané při zaměstnávání, řízení pracovníků a při přístupu k samostatné výdělečné činnosti, zejména při náboru a výběru osob, při rozhodováních ovlivňujících podmínky pracovního poměru, povýšení a ukončení smluvních pracovněprávních vztahů, při přidělování úkolů na základě individuálního chování, osobnostních rysů či vlastností a při monitorování nebo hodnocení osob ve smluvních pracovněprávních vztazích, protože mohou významně ovlivnit budoucí kariérní vyhlídky, živobytí těchto osob a práva pracovníků. Příslušné smluvní pracovněprávní vztahy by měly smysluplně zahrnovat zaměstnance a osoby poskytující služby prostřednictvím platforem, jak je uvedeno v pracovním programu Komise na rok 2021. 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 AI používané k monitorování výkonnosti a chování těchto osob mohou rovněž ohrožovat jejich základní práva na ochranu údajů a soukromí.

(58) Další oblastí, ve které si používání systémů AI 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. Zejména fyzické osoby, které žádají o základní dávky sociálního zabezpečení a veřejné asistenční služby u veřejných orgánů, případně kterým jsou tyto dávky a služby poskytovány, konkrétně služby zdravotní péče, dávky sociálního zabezpečení, sociální služby zajišťující ochranu v takových případech, jako je mateřství, nemoc, pracovní úrazy, závislost nebo stáří, jakož i v případě ztráty zaměstnání a sociální pomoci a pomoci v oblasti bydlení, jsou zpravidla na těchto dávkách a službách závislé a nacházejí se ve vztahu k odpovědným orgánům ve zranitelném postavení. Jsou-li systémy AI používány k určování toho, zda by tyto orgány měly tyto dávky a služby poskytnout, 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, a měly by proto být klasifikovány jako vysoce rizikové. Toto nařízení by však nemělo bránit rozvoji a používání inovativních přístupů ve veřejné správě, pro kterou by mohlo být širší používání vyhovujících a bezpečných systémů AI prospěšné, pokud tyto systémy nepředstavují vysoké riziko pro právnické a fyzické osoby. Kromě toho by jako vysoce rizikové systémy AI by měly být klasifikovány systémy AI 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 AI používané pro tyto účely mohou vést k diskriminaci mezi osobami nebo skupinami a mohou fixovat historické vzorce diskriminace, například na základě rasového nebo etnického původu, genderu, zdravotního postižení, věku a sexuální orientace, nebo mohou vytvářet nové formy diskriminačních dopadů. Systémy AI stanovené právem Unie pro účely odhalování podvodů při nabízení finančních služeb a pro účely obezřetnosti za účelem výpočtu kapitálových požadavků úvěrových institucí a pojišťoven, by však neměly být podle tohoto nařízení považovány za vysoce rizikové. Kromě toho systémy AI určené k použití pro posuzování rizik a stanovování cen ve vztahu

k fyzickým osobám pro účely zdravotního a životního pojištění mohou mít rovněž významný dopad na živobytí osob, a pokud nejsou řádně navrženy, vyvinuty a používány, mohou porušovat jejich základní práva a mohou mít závažné důsledky pro život a zdraví lidí, včetně finančního vyloučení a diskriminace. A konečně by měly být jako vysoce rizikové klasifikovány rovněž systémy AI používané pro hodnocení a klasifikaci tísňových volání fyzických osob nebo při dispečinku pohotovostních služeb nebo stanovení priorit při tomto dispečinku, včetně policie, hasičů a lékařské pomoci, jakož i systémy třídění pacientů ve zdravotnictví, protože rozhodují v situacích, které jsou velmi kritické pro život a zdraví osob a jejich majetek.

(59) Opatření donucovacích orgánů zahrnující určitá použití systémů AI se s ohledem na jejich úlohu a odpovědnost 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 AI nebyl trénován na vysoce kvalitních datech, nesplňuje odpovídající požadavky na výkonnost, 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 ochranu a na spravedlivý proces, jakož i právo na obhajobu a presumpce neviny, zejména pokud tyto systémy AI nejsou dostatečně transparentní, vysvětlitelné a zdokumentované. Je proto vhodné klasifikovat jako vysoce rizikové celou řadu systémů AI určených k použití v kontextu vymáhání práva, kde je přesnost, spolehlivost a transparentnost obzvláště důležitá, pokud je jejich používání povoleno podle příslušného práva Unie a vnitrostátního práva, s cílem zabránit nepříznivým dopadům, zachovat důvěru veřejnosti a zajistit odpovědnost a účinné opravné prostředky. S ohledem na povahu činností a na rizika s nimi spojená by tyto vysoce rizikové systémy AI měly zahrnovat zejména systémy AI určené k použití donucovacími orgány nebo jejich jménem nebo orgány, institucemi nebo jinými subjekty Unie na podporu donucovacích orgánů při posuzování rizika, že se fyzická osoba stane obětí trestných činů, jako jsou polygrafy a podobné nástroje, k vyhodnocování spolehlivosti důkazů v průběhu vyšetřování nebo stíhání trestných činů, a pokud to není zakázáno tímto nařízením, k posuzování rizika protiprávního jednání nebo opakovaného protiprávního jednání fyzické osoby, a to nejen na základě profilování fyzických osob, ani na základě posuzování osobnostních a povahových rysů nebo předchozí trestné činnosti fyzických osob nebo skupin, k profilování v průběhu odhalování, vyšetřování nebo stíhání trestných činů. Systémy AI výslovně určené k použití daňovými a celními orgány při správním řízení, jakož i finančními zpravodajskými jednotkami provádějícími administrativní úkoly při analýze informací podle práva Unie proti praní peněz, by neměly být klasifikovány jako vysoce rizikové systémy AI používané donucovacími orgány za účelem prevence, odhalování, vyšetřování a stíhání trestných činů. Využívání nástrojů AI donucovacími orgány a dalšími relevantními orgány by se nemělo stát faktorem nerovnosti nebo vyloučení. Dopad používání nástrojů AI na práva podezřelých osob na obhajobu by neměl být opomíjen, zejména pokud jde o obtíže při získávání důležitých informací o fungování těchto systémů a související problémy při vznesení námitek proti jejich výsledkům u soudu, zejména ze strany vyšetřovaných fyzických osob.

(60) Systémy AI používané 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 AI 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 klasifikovat jako vysoce rizikové ty systémy AI, které jsou určeny k použití příslušnými orgány veřejné moci nebo jejich jménem nebo orgány, institucemi nebo jinými subjekty Unie pověřenými úkoly v oblasti migrace, azylu a řízení ochrany hranic, jako jsou například polygrafy a podobné nástroje, pokud je jejich používání povoleno podle příslušného práva Unie a vnitrostátního práva, 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, včetně souvisejícího posouzení spolehlivosti důkazů, pro účely odhalování, uznávání nebo identifikace fyzických osob v souvislosti s migrací, azylem a řízením ochrany hranic, s výjimkou ověřování cestovních dokladů.Systémy AI v oblasti migrace, azylu a řízení ochrany hranic, na které se vztahuje toto nařízení, by měly splňovat příslušné procesní požadavky stanovené nařízením Evropského parlamentu a Rady (ES) č. 810/2009 ([32]), směrnicí Evropského parlamentu a Rady 2013/32/EU ([33]) a dalším

([32]) 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).

([33]) 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).

příslušným právem Unie. Členské státy nebo orgány, instituce nebo jiné subjekty Unie by za žádných okolností neměly používat systémy AI při migraci, azylu a řízení ochrany hranic jako prostředek k obcházení svých mezinárodních závazků vyplývajících z Úmluvy OSN o právním postavení uprchlíků, která byla podepsána v Ženevě dne 28. července 1951, ve znění protokolu ze dne 31. ledna 1967, ani by tyto systémy neměly být využívány k jakémukoli porušování zásady nenavracení nebo k odepření bezpečných a účinných legálních cest na území Unie, včetně práva na mezinárodní ochranu.

(61) Určité systémy AI 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 ochranu a na spravedlivý proces. Jako vysoce rizikové je vhodné kvalifikovat systémy AI určené k použití justičním orgánem nebo jeho jménem, jejichž cílem je poskytovat pomoc justičním orgánům při zkoumání a výkladu skutečností a práva a při uplatňování práva na konkrétní soubor skutečností, zejména z důvodu řešení rizik možného zkreslení, chyb a neprůhlednosti. Systémy AI určené k použití subjekty pro alternativní řešení sporů pro tyto účely by měly být rovněž považovány za vysoce rizikové, pokud výsledky postupů alternativního řešení sporů mají pro strany právní účinky. Využívání nástrojů AI může podpořit rozhodovací pravomoci soudců nebo nezávislost soudnictví, ale nemělo by je nahrazovat, neboť konečné rozhodnutí musí i nadále přijímat člověk. Klasifikace systémů AI jako vysoce rizikových by se však neměla vztahovat na systémy AI 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.

(62) Aniž jsou dotčena pravidla stanovená v nařízení Evropského parlamentu a Rady (EU) 2024/900 ([34]) a s cílem řešit rizika nepřiměřeného vnějšího zasahování do volebního práva zakotveného v článku 39 Listiny a nepříznivých dopadů na demokracii a právní stát by systémy AI, které jsou určeny k ovlivňování výsledku voleb nebo referenda nebo hlasování fyzických osob ve volbách nebo referendech, měly být klasifikovány jako vysoce rizikové systémy AI, s výjimkou systémů AI, jejichž výstupu nejsou fyzické osoby přímo vystaveny, jako jsou nástroje používané k organizaci, optimalizaci a strukturování politických kampaní z administrativního a logistického hlediska.

(63) Skutečnost, že daný systém AI je podle tohoto nařízení klasifikován jako vysoce rizikový systém AI, by neměla být vykládána v tom smyslu, že používání tohoto systému je zákonné podle jiných aktů práva Unie nebo podle vnitrostátního práva slučitelného 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 používání 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, v relevantních případech včetně zvláštních kategorií osobních údajů, není-li v tomto nařízení konkrétně stanoveno jinak.

(64) Ke zmírnění rizik, která vyplývají z vysoce rizikových systémů AI uváděných na trh nebo do provozu, a k zajištění vysoké úrovně důvěryhodnosti by měly být na vysoce rizikové systémy AI uplatňovány určité povinné požadavky s přihlédnutím k zamýšlenému účelu a v souvislosti s používáním systému AI a v souladu se systémem řízení rizik, který stanoví poskytovatel. Opatření přijatá poskytovateli za účelem splnění povinných požadavků tohoto nařízení by měla zohledňovat obecně uznávaný současný stav v oblasti AI a měla by být přiměřená a účinná pro splnění cílů tohoto nařízení. Na základě nového legislativního rámce, jak je objasněno v oznámení Komise, „Modrá příručka“ k provádění pravidel EU pro výrobky (2022), je obecným pravidlem, že na jeden produkt může být použitelný více než jeden právní akt náležející mezi harmonizační právní předpis Unie, neboť k dodání na trh nebo uvedení do provozu může dojít pouze v případě, když je produkt v souladu se všemi platnými harmonizačními právními předpisy Unie. Nebezpečí spojená se systémy AI, na něž se vztahují požadavky tohoto nařízení, se vztahují k jiným aspektům než stávající harmonizační právní předpisy Unie, a proto požadavky tohoto nařízení doplní stávající soubor harmonizačních právních předpisů Unie. Například produkty v podobě strojních zařízení nebo zdravotnických prostředků obsahující systém AI mohou představovat rizika, na která se nevztahují základní

([34]) Nařízení Evropského parlamentu a Rady (EU) 2024/900 ze dne 13. března 2024 o transparentnosti a cílení politické reklamy (Úř. věst. L, 2024/900, 20.3.2024, ELI: http://data.europa.eu/eli/reg/2024/900/oj).

požadavky na ochranu zdraví a bezpečnost stanovené v příslušných harmonizovaných právních předpisech Unie, neboť toto odvětvové právo se nezabývá riziky specifickými pro systémy AI. To vyžaduje současné a doplňkové použití různých legislativních aktů. Aby byla zajištěna soudržnost a zabránilo se zbytečné administrativní zátěži nebo zbytečným nákladům, poskytovatelé produktu, který obsahuje jeden nebo více vysoce rizikových systémů AI, na něž se vztahují požadavky tohoto nařízení a harmonizačních právních předpisů Unie založených na novém legislativním rámci a uvedené v příloze tohoto nařízení, by měli být flexibilní, pokud jde o přijímání provozních rozhodnutí o tom, jak optimálně zajistit soulad produktu obsahujícího jeden nebo více systémů AI se všemi platnými požadavky harmonizovaných právních předpisů Unie. Tato flexibilita by mohla obnášet například rozhodnutí poskytovatele začlenit část nezbytných procesů testování a podávání zpráv, informací a dokumentace požadovaných podle tohoto nařízení do již existující dokumentace a postupů požadovaných podle stávajících harmonizačních právních předpisů Unie založených na novém legislativním rámci a uvedených v příloze tohoto nařízení. Tím by neměla být nijak dotčena povinnost poskytovatele dodržovat všechny platné požadavky.

(65) Systém řízení rizik by měl spočívat v nepřetržitém opakujícím se procesu, který je plánovaný a probíhá během celého životního cyklu vysoce rizikového systému AI. Tento proces by měl být zaměřen na identifikaci a zmírnění příslušných rizik systémů AI pro zdraví, bezpečnost a základní práva. Systém řízení rizik by měl být pravidelně přezkoumáván a aktualizován, aby byla zajištěna jeho trvalá účinnost, jakož i odůvodněnost a dokumentace veškerých významných rozhodnutí a opatření přijatých podle tohoto nařízení. Tento proces by měl zajistit, aby poskytovatel identifikoval rizika nebo nepříznivé dopady a zavedl opatření ke zmírnění známých a rozumně předvídatelných rizik systémů AI pro zdraví, bezpečnost a základní práva s ohledem na jeho zamýšlený účel a rozumně předvídatelné nesprávné použití, včetně možných rizik vyplývajících z interakce mezi systémem AI a prostředím, v němž působí. Systém řízení rizik by měl přijmout nejvhodnější opatření k řízení rizik s ohledem na nejnovější vývoj v oblasti AI. Při identifikaci nejvhodnějších opatření k řízení rizik by měl poskytovatel zdokumentovat a vysvětlit provedené volby a případně zapojit odborníky a externí zúčastněné strany. Při identifikaci rozumně předvídatelného nesprávného použití vysoce rizikových systémů AI by měl poskytovatel zahrnout způsoby použití systémů AI, které sice nejsou přímo pokryty zamýšleným účelem a nejsou uvedeny v návodu k použití, nicméně lze důvodně očekávat, že vyplynou ze snadno předvídatelného lidského chování v souvislosti se specifickými vlastnostmi a používáním konkrétního systému AI. V návodu k použití poskytnutém poskytovatelem by měly být uvedeny jakékoli známé nebo předvídatelné okolnosti související s používáním daného vysoce rizikového systému AI v souladu s jeho zamýšleným účelem nebo za podmínek rozumně předvídatelného nesprávného použití, které mohou vést k rizikům pro zdraví a bezpečnost nebo pro základní práva. Účelem je zajistit, aby si jich byl zavádějící subjekt při používání vysoce rizikového systému AI vědom a zohlednil je. Pro identifikaci a provádění opatření ke zmírnění rizik v případě předvídatelného nesprávného použití vysoce rizikového systému AI podle tohoto nařízení by nemělo být nutné, aby poskytovatel v zájmu řešení předvídatelného nesprávného použití přistupoval ke zvláštním dodatečným školením. Poskytovatelé se však vyzývají, aby taková dodatečná opatření v oblasti školení zvážili, bude-li to pro omezení rozumně předvídatelného použití nezbytné a vhodné.

(66) Na vysoce rizikové systémy AI by se měly vztahovat požadavky týkající se řízení rizik, kvality a významu použitých souborů dat, technické dokumentace a uchovávání záznamů, transparentnosti a poskytování informací zavádějícím subjektům, lidského dohledu a spolehlivosti, přesnosti a kybernetické bezpečnosti. Tyto požadavky jsou nezbytným předpokladem účinného zmírňování rizik pro zdraví, bezpečnost a základní práva. Jelikož nejsou žádná další opatření méně omezující obchod rozumně dostupná, tyto požadavky nejsou bezdůvodným omezením obchodu.

(67) Při poskytování struktury a zajišťování výkonnosti celé řady systémů AI mají zásadní úlohu vysoce kvalitní data a přístup k nim, zejména pokud jsou používány techniky zahrnující trénování modelů s cílem zajistit, aby vysoce rizikový systém AI fungoval dle předpokladu a bezpečně a aby se nestal zdrojem diskriminace, kterou právo Unie zakazuje. Soubory vysoce kvalitních trénovacích, validačních a testovacích dat vyžadují zavedení vhodných postupů správy a řízení dat. Soubory trénovacích, validačních a testovacích dat, včetně štítků, by měly být relevantní, dostatečně reprezentativní a v nejvyšší možné míře bez chyb a úplné s ohledem na zamýšlený účel systému. Aby se usnadnil soulad s právem Unie v oblasti ochrany údajů, jako je nařízení (EU) 2016/679, měly by postupy správy a řízení dat v případě osobních údajů zahrnovat transparentnost původního účelu shromažďování údajů. Soubory dat by měly mít rovněž odpovídající statistické vlastnosti, a to i pokud jde o osoby nebo skupiny osob, ve vztahu k nimž má být vysoce rizikový systém AI používán, se zvláštním zaměřením na zmírnění možných zkreslení v souborech dat, které by mohly ovlivnit zdraví a bezpečnost osob, mít negativní dopad na základní práva nebo vést k diskriminaci zakázané právem Unie, zejména pokud výstupy dat ovlivňují vstupy pro budoucí operace (dále jen

„smyčky zpětné vazby“). Zkreslení mohou být například inherentní součástí základních datových souborů, zejména pokud jsou používána historická data, která byla generována při zavádění systémů v reálných podmínkách.Výsledky poskytnuté systémy AI by mohly být ovlivněny takovýmito zkresleními, která mají tendenci se postupně zvyšovat, a tudíž zachovávat a posilovat existující diskriminaci, zejména v případě osob patřících k určitým zranitelným skupinám, včetně rasových nebo etnických skupin. Požadavek, aby soubory dat byly v nejvyšší možné míře úplné a bez chyb, by neměl mít vliv na používání technik ochrany soukromí v souvislosti s vývojem a testováním systémů AI. Soubory dat by měly především v rozsahu nezbytném pro jejich zamýšlený účel zohledňovat rysy, vlastnosti nebo prvky, které jsou specifické pro konkrétní zeměpisné, kontextuální, behaviorální nebo funkční prostředí, ve kterém má být systém AI používán. Požadavky týkající se správy dat lze splnit využitím služeb třetích stran, které nabízejí certifikované služby dodržování předpisů, včetně ověřování správy dat, integrity datového souboru a postupů trénování, validace a testování dat, pokud je zajištěn soulad s požadavky na data podle tohoto nařízení.

(68) Při vývoji a posuzování vysoce rizikových systémů AI by některé subjekty, jako jsou poskytovatelé, oznámené subjekty a další příslušné subjekty, například evropská centra pro digitální inovace, pokusná zkušební zařízení a výzkumní pracovníci, měly mít přístup k vysoce kvalitním datovým souborům ve svých příslušných oborech činnosti, které souvisejí s tímto nařízením, a měly by je využívat. Zásadní význam pro zajištění důvěryhodného, odpovědného a nediskriminačního přístupu k vysoce kvalitním datům pro účely trénování, validace a testování systémů AI 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 AI 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, validace a testování systémů AI mohou podporovat rovněž odpovídající příslušné orgány, včetně odvětvových, které poskytují nebo podporují přístup k datům.

(69) Během celého životního cyklu systému AI musí být zaručeno právo na soukromí a na ochranu osobních údajů. V tomto ohledu se při zpracování osobních údajů použijí zásady minimalizace údajů a záměrné a standardní ochrany údajů, jak jsou stanoveny v právu Unie v oblasti ochrany údajů. Opatření přijatá poskytovateli k zajištění souladu s těmito zásadami mohou zahrnovat nejen anonymizaci a šifrování, ale také používání technologie, která umožňuje vnášet algoritmy do dat a umožňuje trénování systémů AI bez předávání mezi stranami nebo kopírování samotných nezpracovaných nebo strukturovaných dat, aniž jsou dotčeny požadavky na správu dat stanovené v tomto nařízení.

(70) V zájmu ochrany práva jiných osob před diskriminací, která by mohla vyplynout ze zkreslení v rámci systémů AI, by poskytovatelé v rozsahu nezbytně nutném pro účely zajištění odhalování a nápravy zkreslení ve vztahu k vysoce rizikovým systémům AI, s výhradou vhodných záruk chránících základní práva a svobody fyzických osob a po uplatnění všech platných podmínek stanovených v tomto nařízení vedle podmínek stanovených v nařízení (EU) 2016/679 a (EU) 2018/1725 a směrnici (EU) 2016/680, měli mít výjimečně 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.

(71) Pro sledovatelnost těchto systémů, ověření souladu s požadavky tohoto nařízení, jakož i sledování jejich provozu a monitorování po uvedení na trh má zásadní význam, aby byly k dispozici srozumitelné informace o tom, jak byly vysoce rizikové systémy AI 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 AI s příslušnými požadavky a usnadnění monitorování po uvedení na trh. Tyto informace by měly zahrnovat obecné vlastnosti, schopnosti a omezení tohoto systému, použité algoritmy, data, postupy při trénování, testování a validaci, jakož i dokumentaci příslušného systému řízení rizik, a měly by být vypracovány jasným a srozumitelným způsobem. Technická dokumentace by měla být řádně aktualizována po celou dobu životního cyklu systému AI. Kromě toho by vysoce rizikové systémy AI měly technicky umožňovat automatické zaznamenávání událostí prostřednictvím protokolů po celou dobu životnosti systému.

(72) S cílem řešit obavy týkající se neprůhlednosti a složitosti některých systémů AI a pomoci zavádějícím subjektům plnit jejich povinnosti podle tohoto nařízení by měla být vyžadována transparentnost u vysoce rizikových systémů AI před jejich uvedením na trh nebo do provozu. Vysoce rizikové systémy AI by měly být navrženy tak, aby zavádějícím subjektům umožnily pochopit, jak systém AI funguje, vyhodnotit jeho funkčnost a porozumět jeho silným stránkám a omezením. K vysoce rizikovým systémům AI by měly být přiloženy příslušné informace ve formě návodu k použití. Tyto informace by měly zahrnovat vlastnosti, schopnosti a omezení výkonnosti systému AI. Měly by obsahovat informace o možných známých a předvídatelných okolnostech souvisejících s používáním vysoce rizikového systému AI, včetně činnosti zavádějícího subjektu, která může ovlivnit chování a výkonnost systému, za nichž může systém AI vést k rizikům pro zdraví, bezpečnost a základní práva, o změnách, které poskytovatel předem stanovil a posoudil z hlediska shody, a o příslušných opatřeních v oblasti lidského dohledu, včetně opatření k usnadnění interpretace výstupů systému AI zavádějícími subjekty. Transparentnost, včetně přiloženého návodu k použití, by měla zavádějícím subjektům pomoci při používání systému a podporovat jejich informované rozhodování. Zavádějící subjekty by měly být mimo jiné lépe schopny správně zvolit systém, který mají v úmyslu používat, s ohledem na povinnosti, které se na ně vztahují, měly by být poučeny o zamýšleném a vyloučeném použití a měly by systém AI používat správně a podle potřeby. Pro zvýšení srozumitelnosti a přístupnosti informací uvedených v návodu k použití, by měly být případně uvedeny ilustrační příklady, například omezení a zamýšlená a vyloučená použití systému AI. Poskytovatelé by měli zajistit, aby veškerá dokumentace, včetně návodu k použití, obsahovala smysluplné, komplexní, přístupné a srozumitelné informace s přihlédnutím k potřebám a předvídatelným znalostem cílových zavádějících subjektů. Návod k použití by měl být k dispozici v jazyce, který je pro cílové zavádějící subjekty snadno srozumitelný, jak určí příslušný členský stát.

(73) Vysoce rizikové systémy AI by měly být navrhovány a vyvíjeny tak, aby na jejich fungování mohly dohlížet fyzické osoby, aby bylo zajištěno, že budou používány zamýšleným způsobem, a aby jejich dopady byly řešeny během celého životního cyklu systému. 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, 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 lidským dohledem pověřeny, měly odbornou způsobilost, odbornou přípravu a pravomoci nezbytné k výkonu této funkce. Je rovněž nezbytné zajistit, aby vysoce rizikové systémy AI případně zahrnovaly mechanismy, které vedou a informují fyzickou osobu, jež byla lidským dohledem pověřena, aby mohla činit informovaná rozhodnutí, zda, kdy a jak zasáhnout, aby se zabránilo negativním důsledkům nebo rizikům, nebo systém zastavit, pokud nefunguje tak, jak má. Vzhledem k závažným důsledkům pro konkrétní osoby v případě nesprávné shody některých systémů biometrické identifikace je vhodné stanovit požadavek na posílený lidský dohled nad těmito systémy, aby zavádějící subjekt nemohl přijmout žádné opatření nebo rozhodnutí na základě identifikace vyplývající ze systému, pokud ji samostatně neověřily a nepotvrdily alespoň dvě fyzické osoby. Těmito osobami by mohli být zástupci jednoho nebo více subjektů a mohla by mezi ně patřit osoba, 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. Vzhledem ke zvláštnostem oblastí vymáhání práva, migrace, ochrany hranic a azylu by se tento požadavek neměl uplatňovat v případech, kdy právo Unie nebo vnitrostátní právo považuje uplatňování tohoto požadavku za nepřiměřené.

(74) Vysoce rizikové systémy AI by měly po celou dobu svého životního cyklu fungovat konzistentně a splňovat příslušnou úroveň přesnosti, spolehlivosti a kybernetické bezpečnosti s ohledem na svůj zamýšlený účel a v souladu s obecně uznávaným nejnovějším vývojem. Komise a příslušné organizace a zúčastněné strany se vyzývají, aby náležitě zohledňovaly zmírnění rizik a negativních dopadů systémů AI. V přiloženém návodu k použití by měla být uvedena očekávaná úroveň metrik výkonnosti. Poskytovatelé se vyzývají, aby tyto informace zavádějícím subjektům sdělili jasným a snadno srozumitelným způsobem, bez nedorozumění nebo zavádějících prohlášení. Cílem práva Unie týkajícího se legální metrologie, včetně směrnic Evropského parlamentu a Rady 2014/31/EU ([35]) a 2014/32/EU ([36]), je zajistit přesnost měření a přispět k transparentnosti a poctivosti obchodních transakcí. V této souvislosti by Komise měla ve spolupráci s příslušnými zúčastněnými stranami a organizacemi, jako jsou metrologické a srovnávací orgány, případně podporovat vývoj referenčních hodnot a metodik měření pro systémy AI. Komise by přitom měla vzít na vědomí mezinárodní partnery pracující v oblasti metrologie a příslušných ukazatelů měření týkajících se AI a spolupracovat s nimi.

([35]) Směrnice Evropského parlamentu a Rady 2014/31/EU ze dne 26. února 2014 o harmonizaci právních předpisů členských států týkajících se dodávání vah s neautomatickou činností na trh (Úř. věst. L 96, 29.3.2014, s. 107).

([36]) Směrnice Evropského parlamentu a Rady 2014/32/EU ze dne 26. února 2014 o harmonizaci právních předpisů členských států týkajících se dodávání měřidel na trh (Úř. věst. L 96, 29.3.2014, s. 149).

(75) U vysoce rizikových systémů AI je klíčovým požadavkem technická spolehlivost. Tyto systémy by měly 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). Proto by měla být přijata technická a organizační opatření k zajištění spolehlivosti vysoce rizikových systémů AI, obnášející například navrhování a vývoj vhodných technických řešení pro prevenci nebo minimalizaci škodlivého nebo jinak nežádoucího chování. Tato technická řešení mohou zahrnovat 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 AI.

(76) Zásadní úlohu při zajišťování odolnosti systémů AI 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 AI mohou využívat aspekty, jež jsou pro AI specifické, například soubory trénovacích dat (například tzv. data poisoning) nebo trénované modely (například nepřátelské útoky nebo odvozování členství), nebo zneužívat slabých míst digitálních aktiv daného systému AI nebo příslušné infrastruktury IKT. Pro zajištění úrovně kybernetické bezpečnosti odpovídající těmto rizikům by proto poskytovatelé vysoce rizikových systémů AI měli přijmout vhodná opatření, jako jsou bezpečnostní kontroly, případně současně zohlednit i příslušnou infrastrukturu IKT.

(77) Aniž jsou dotčeny požadavky týkající se spolehlivosti a přesnosti stanovené v tomto nařízení, mohou vysoce rizikové systémy AI, které spadají do oblasti působnosti nařízení Evropského parlamentu a Rady o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky, v souladu s uvedeným nařízením prokázat soulad s požadavky na kybernetickou bezpečnost podle tohoto nařízení splněním základních požadavků na kybernetickou bezpečnost stanoveným v uvedeném nařízení. Pokud vysoce rizikové systémy AI splňují základní požadavky nařízení Evropského parlamentu a Rady o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky, měly by být považovány za vyhovující požadavkům na kybernetickou bezpečnost stanoveným v tomto nařízení, pokud je splnění těchto požadavků prokázáno v EU prohlášení o shodě nebo jeho částech vydaném podle uvedeného nařízení. Za tímto účelem by posouzení kybernetických bezpečnostních rizik spojených s produktem s digitálními prvky klasifikovanými podle tohoto nařízení jako vysoce rizikový systém AI, prováděné podle nařízení Evropského parlamentu a Rady o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky, mělo zohlednit rizika pro kybernetickou odolnost systému AI, pokud jde o pokusy neoprávněných třetích stran změnit jeho používání, chování nebo výkonnost, včetně zranitelných míst specifických pro AI, jako jsou „tzv. data poisoning“ nebo nepřátelské útoky, jakož i příslušná rizika pro základní práva, jak vyžaduje toto nařízení.

(78) Postup posuzování shody stanovený tímto nařízením by se měl použít ve vztahu k základním požadavkům na kybernetickou bezpečnost produktu s digitálními prvky, na něž se vztahuje nařízení Evropského parlamentu a Rady o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a který je podle tohoto nařízení klasifikován jako vysoce rizikový systém AI. Toto pravidlo by však nemělo vést ke snížení potřebné míry jistoty u kritických produktů s digitálními prvky, na něž se vztahuje nařízení Evropského parlamentu a Rady o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky. Odchylně od tohoto pravidla se proto vysoce rizikové systémy AI, které spadají do oblasti působnosti tohoto nařízení a jsou rovněž považovány za důležité a kritické produkty s digitálními prvky podle nařízení Evropského parlamentu a Rady o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky, na něž se vztahuje postup posuzování shody založený na interní kontrole stanovený v příloze tohoto nařízení, řídí ustanoveními nařízení Evropského parlamentu a Rady o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky o posuzování shody, pokud jde o základní požadavky uvedeného nařízení na kybernetickou bezpečnost. V tomto případě by se na všechny ostatní aspekty, na něž se vztahuje toto nařízení, měla použít příslušná ustanovení o posuzování shody založená na interní kontrole uvedená v příloze tohoto nařízení. Na základě poznatků a odborných znalostí agentury ENISA týkajících se politiky kybernetické bezpečnosti a úkolů svěřených agentuře ENISA podle nařízení Evropského parlamentu a Rady 2019/881 ([37]) by Komise měla v otázkách souvisejících s kybernetickou bezpečností systémů AI s agenturou ENISA spolupracovat.

([37]) 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. 15).

(79) Je vhodné, aby za uvedení vysoce rizikového systému AI 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.

(80) Unie a členské státy jsou jakožto signatáři Úmluvy Organizace spojených národů o právech osob se zdravotním postižením ze zákona povinny chránit osoby se zdravotním postižením před diskriminací a podporovat jejich rovnost, zajistit, aby osoby se zdravotním postižením měly na rovnoprávném základě s ostatními přístup k informačním a komunikačním technologiím a systémům, a zaručit respektování soukromí osob se zdravotním postižením. Vzhledem k rostoucímu významu a nárůstu používání systémů AI by uplatňování zásad univerzálního designu na veškeré nové technologie a služby mělo zajistit plný a rovný přístup každému, na koho mohou mít technologie AI vliv nebo kdo je používá, včetně osob se zdravotním postižením, a to způsobem, který by plně zohlednil jejich přirozenou důstojnost a rozmanitost. Je proto nutné, aby poskytovatelé zajistili plný soulad s požadavky na přístupnost, včetně směrnice Evropského parlamentu a Rady (EU) 2016/2102 ([38]) a směrnice (EU) 2019/882. Poskytovatelé by měli zajistit soulad s těmito požadavky již od fáze návrhu. Nezbytná opatření by proto měla být v co největší míře začleněna již do návrhu vysoce rizikového systému AI.

(81) Poskytovatel by měl zavést spolehlivý systém řízení kvality, zajistit provedení požadovaného postupu posuzování shody, vypracovat příslušnou dokumentaci a zavést spolehlivý systém monitorování po uvedení na trh. Poskytovatelé vysoce rizikových systémů AI, na něž se vztahují povinnosti týkající se systémů řízení kvality podle příslušného odvětvového práva Unie, by měli mít možnost zahrnout prvky systému řízení kvality stanovené v tomto nařízení do stávajícího systému řízení kvality stanoveného v tomto jiném odvětvovém právu Unie. Doplňkovost mezi tímto nařízením a stávajícím odvětvovým právem Unie by měla být rovněž zohledněna v budoucích normalizačních činnostech nebo pokynech přijatých Komisí. Veřejné orgány, které uvádějí do provozu vysoce rizikové systémy AI pro vlastní potřebu, mohou přijímat a provádět pravidla pro systém řízení kvality jako součást systému řízení kvality přijatého na vnitrostátní nebo regionální úrovni, případně s přihlédnutím ke zvláštnostem daného odvětví a k pravomocím a organizaci dotyčného veřejného orgánu.

(82) 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 AI. Poskytovatelé usazení ve třetích zemích by proto v případě, že dodávají do Unie systémy AI, měly předem jmenovat formou písemného pověření svého zplnomocněného zástupce usazeného v Unii. Tento zplnomocněný zástupce hraje klíčovou roli při zajišťování shody vysoce rizikových systémů AI uváděných na trh nebo do provozu v Unii uvedenými poskytovateli, kteří v Unii usazeni nejsou, a vystupuje jako jejich kontaktní osoba usazená v Unii.

(83) S ohledem na povahu a složitost hodnotového řetězce systémů AI a v souladu s novým legislativním rámcem je nezbytné zajistit právní jistotu a usnadnit soulad s tímto nařízením. Je proto zapotřebí vyjasnit úlohu a konkrétní povinnosti příslušných provozovatelů v celém tomto hodnotovém řetězci, jako jsou dovozci a distributoři, kteří mohou přispívat k vývoji systémů AI. 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.

(84) V zájmu zajištění právní jistoty je nezbytné vyjasnit, že za určitých zvláštních podmínek by každý distributor, dovozce, zavádějící subjekt nebo jiná třetí strana měli být považováni za poskytovatele vysoce rizikového systému AI, a proto by měli převzít všechny příslušné povinnosti. Tak by tomu mělo být v případě, že daná strana připojí své jméno, název nebo ochrannou známku k vysoce rizikovému systému AI, který již byl uveden na trh nebo do provozu, aniž jsou dotčena smluvní ujednání stanovující jiné rozdělení povinností. Mělo by tomu tak být i v případě, kdy tato strana podstatně změní vysoce rizikový systém AI, který již byl uveden na trh nebo do provozu, přičemž v důsledku této změny daný systém AI zůstává vysoce rizikovým systémem AI v souladu tímto nařízením, nebo pokud změní zamýšlený účel systému AI, včetně obecného systému AI, který nebyl klasifikován jako vysoce rizikový a již byl uveden na trh nebo do provozu, přičemž v důsledku této změny se daný systém AI stává vysoce rizikovým systémem AI v souladu s tímto nařízením. Uvedená ustanovení by se měla použít, aniž by byla dotčena konkrétnější ustanovení zavedená v některých harmonizačních právních předpisech Unie založených na novém legislativním rámci, s nimiž by se toto nařízení mělo společně uplatňovat. Například čl. 16 odst. 2 nařízení (EU)

([38]) Směrnice Evropského parlamentu a Rady (EU) 2016/2102 ze dne 26. října 2016 o přístupnosti internetových stránek a mobilních aplikací subjektů veřejného sektoru (Úř. věst L 327, 2.12.2016, s. 1).

2017/745, 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 AI, které jsou zdravotnickými prostředky ve smyslu uvedeného nařízení.

(85) Obecné systémy AI mohou být samy o sobě používány jako vysoce rizikové systémy AI nebo mohou být součástí jiných vysoce rizikových systémů AI. Vzhledem k zvláštní povaze těchto systémů a v zájmu zajištění spravedlivého rozdělení odpovědností v celém hodnotovém řetězci AI bez ohledu na to, zda mohou být dané systémy jinými poskytovateli používány jako vysoce rizikové systémy AI jako takové, nebo jako součásti vysoce rizikových systémů AI, a není-li v tomto nařízení stanoveno jinak, měli by poskytovatelé těchto systémů úzce spolupracovat s poskytovateli příslušných vysoce rizikových systémů AI, aby mohli plnit příslušné povinnosti podle tohoto nařízení, a s příslušnými orgány zřízenými podle tohoto nařízení.

(86) Pokud by poskytovatel, který původně uvedl systém AI na trh nebo do provozu, za podmínek stanovených v tomto nařízení již neměl být považován za poskytovatele pro účely tohoto nařízení a pokud výslovně nevyloučil změnu systému AI na vysoce rizikový systém AI, měl by tento bývalý poskytovatel přesto úzce spolupracovat, zpřístupnit nezbytné informace a poskytnout rozumně očekávaný technický přístup a další pomoc, které jsou nezbytné pro splnění povinností stanovených v tomto nařízení, zejména pokud jde o soulad s posuzováním shody vysoce rizikových systémů AI.

(87) Kromě toho pokud vysoce rizikový systém AI, který je bezpečnostní komponentou produktu, jenž spadá do oblasti působnosti harmonizačních právních předpisů Unie založených na novém legislativním rámci, není uveden na trh nebo do provozu nezávisle na tomto produktu, měl by výrobce produktu definovaného v uvedených právních předpisech splňovat povinnosti poskytovatele stanovené v tomto nařízení, a zejména zajistit, aby systém AI zabudovaný do konečného produktu splňoval požadavky tohoto nařízení.

(88) V celém hodnotovém řetězci AI mnoho stran často dodává systémy, nástroje a služby AI, ale také komponenty nebo procesy, které poskytovatel začleňuje do systému AI s různými cíli, včetně trénování modelu, opětovného trénování modelu, testování a hodnocení modelu, integrace do softwaru nebo jiných aspektů vývoje modelu. Tyto strany hrají důležitou úlohu v hodnotovém řetězci ve vztahu k poskytovateli vysoce rizikového systému AI, do něhož jsou jejich systémy, nástroje, služby, součásti nebo procesy AI začleňovány, a měly by na základě písemné dohody tomuto poskytovateli poskytnout nezbytné informace, schopnosti, technický přístup a další pomoc na základě obecně uznávaného stavu techniky, aby poskytovatel mohl plně plnit povinnosti stanovené v tomto nařízení, aniž by byla ohrožena jejich práva duševního vlastnictví nebo obchodní tajemství.

(89) Třetí strany, které zpřístupňují veřejnosti nástroje, služby, procesy nebo součásti AI jiné než obecné modely AI, by neměly být povinny dodržovat požadavky vztahující se k odpovědnosti vůči celému hodnotovému řetězci AI, zejména vůči poskytovateli, který tyto nástroje, služby, procesy nebo součásti AI použil nebo začlenil, pokud jsou zpřístupněny na základě svobodné a otevřené licence. Vývojáři svobodných nástrojů, služeb, procesů nebo komponent AI a s otevřeným zdrojovým kódem jiných než obecné modely AI by měli být vybízeni, aby zavedli široce přijaté dokumentační postupy, například modelové karty a datové listy, jako způsob rychlejšího sdílení informací v celém hodnotovém řetězci AI, což umožní podporu důvěryhodných systémů AI v Unii.

(90) Komise by mohla vypracovat a doporučit dobrovolné vzorové smluvní podmínky mezi poskytovateli vysoce rizikových systémů AI a třetími stranami, které dodávají nástroje, služby, komponenty nebo procesy, jež jsou ve vysoce rizikových systémech AI používány nebo jsou do nich integrovány, a v celém hodnotovém řetězci tak usnadnit spolupráci. Při vypracovávání dobrovolných vzorových smluvních podmínek by Komise měla také zohlednit možné smluvní požadavky použitelné v konkrétních odvětvích nebo obchodních případech.

(91) Vzhledem k povaze systémů AI 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 AI v reálných podmínkách, je vhodné stanovit konkrétní odpovědnost zavádějících subjektů. Zavádějící subjekty by zejména měly přijmout vhodná technická a organizační opatření, aby zajistily, že budou vysoce rizikové systémy AI používat v souladu s návodem k použití, a měly by být stanoveny některé další povinnosti týkající se monitorování fungování systémů AI a případně uchovávání záznamů. Zavádějící subjekty by dále měly zajistit, aby osoby pověřené uplatňováním návodů k použití a lidským dohledem, jak je stanoveno v tomto nařízení, měly nezbytnou

způsobilost, zejména odpovídající úroveň gramotnosti, odborné přípravy a pravomoci v oblasti AI, aby mohly tyto úkoly řádně plnit. Těmito povinnostmi by neměly být dotčeny jiné povinnosti zavádějících subjektů v souvislosti s vysoce rizikovými systémy AI podle práva Unie nebo vnitrostátního práva.

(92) Tímto nařízením nejsou dotčeny povinnosti zaměstnavatelů týkající se informování zaměstnanců nebo informování zaměstnanců a projednávání se zaměstnanci nebo jejich zástupci podle práva a praxe Unie nebo vnitrostátního práva a praxe, včetně směrnice Evropského parlamentu a Rady 2002/14/ES ([39]), o rozhodnutích o uvedení do provozu nebo používání systémů AI. Je i nadále nezbytné zajistit informování zaměstnanců a jejich zástupců o plánovaném zavádění vysoce rizikových systémů AI na pracovišti v případech, kdy nejsou splněny podmínky pro tyto povinnosti týkající se informování nebo informování a projednávání stanovené v jiných právních nástrojích. Toto právo na informace je navíc doplňkové a nezbytné k dosažení cíle ochrany základních práv, na němž je toto nařízení založeno. Proto by měl být v tomto nařízení stanoven požadavek na informování, aniž by byla dotčena stávající práva zaměstnanců.

(93) Rizika spojená se systémy AI mohou vyplývat ze způsobu, jakým jsou tyto systémy navrhovány, avšak mohou rovněž vzniknout v souvislosti s tím, jak jsou tyto systémy používány. Subjekty zavádějící vysoce rizikový systém AI proto hrají zásadní úlohu při zajišťování ochrany základních práv a doplňují povinnosti poskytovatele při vývoji systému AI. Zavádějící subjekty mají nejlepší předpoklady k tomu, aby posoudily, jak bude vysoce rizikový systém AI konkrétně používán, a mohou proto identifikovat potenciální rizika, která se ve fázi vývoje nepředpokládala, a to díky přesnější znalosti kontextu používání a osob nebo skupin osob, na které bude mít systém pravděpodobně dopad, včetně zranitelných skupin. Subjekty zavádějící vysoce rizikové systémy AI uvedené v příloze tohoto nařízení rovněž hrají zásadní úlohu při informování fyzických osob a měly by při přijímání rozhodnutí nebo pomoci při přijímání rozhodnutí týkajících se fyzických osob v příslušných případech tyto fyzické osoby informovat, že jsou použití vysoce rizikového systému AI vystaveny. Tyto informace by měly zahrnovat zamýšlený účel a druh přijímaných rozhodnutí. Zavádějící subjekt by měl rovněž informovat danou fyzickou osobu o jejím právu na vysvětlení uvedeném v tomto nařízení. Pokud jde o vysoce rizikové systémy AI používané pro účely vymáhání práva, měla by být tato povinnost provedena v souladu s článkem 13 směrnice (EU) 2016/680.

(94) Jakékoli zpracování biometrických údajů související s používáním systémů AI pro biometrickou identifikaci pro účely vymáhání práva musí být v souladu s článkem 10 směrnice (EU) 2016/680, který takové zpracování povoluje pouze ve zcela nezbytných případech, s výhradou vhodných záruk pro práva a svobody subjektů údajů, a pokud je povoleno právem Unie nebo členského státu. Je-li takové použití povoleno, musí rovněž splňovat zásady stanovené v čl. 4 odst. 1 směrnice (EU) 2016/680, včetně zákonnosti, spravedlnosti a transparentnosti, účelového omezení, přesnosti a omezení uložení.

(95) Aniž je dotčeno platné právo Unie, zejména nařízení (EU) 2016/679 a směrnice (EU) 2016/680, vzhledem k rušivé povaze systémů následné biometrické identifikace na dálku by používání systémů následné biometrické identifikace na dálku mělo podléhat zárukám. Systémy následné biometrické identifikace by měly být vždy používány způsobem, který je přiměřený, legitimní a nezbytně nutný, a tudíž cílený, pokud jde o osoby, které mají být identifikovány, místo, časový rozsah, a založeny na uzavřeném souboru údajů legálně získaných videozáznamů. V žádném případě by systémy následné biometrické identifikace na dálku neměly být používány v rámci vymáhání práva, aby vedly k nerozlišujícímu sledování. Podmínky pro následnou biometrickou identifikaci na dálku by v žádném případě neměly sloužit jako základ pro obcházení podmínek zákazu a přísných výjimek pro biometrickou identifikaci na dálku v reálném čase.

(96) Aby byla účinně zajištěna ochrana základních práv, měly by subjekty zavádějící vysoce rizikové systémy AI, které jsou veřejnoprávními subjekty, nebo soukromé subjekty poskytující veřejné služby a subjekty zavádějící určité vysoce rizikové systémy AI uvedené v příloze tohoto nařízení, jako jsou bankovní nebo pojišťovací subjekty, provést před jejich uvedením do provozu posouzení dopadů na základní práva. Služby důležité pro jednotlivce, které jsou veřejné povahy, mohou poskytovat i soukromé subjekty. Soukromé subjekty poskytující takové veřejné služby jsou spojeni s úkoly ve veřejném zájmu, například v oblastech vzdělávání, zdravotní péče, sociálních služeb, bydlení či výkonu spravedlnosti. Cílem posouzení dopadů na základní práva je, aby zavádějící subjekt určil konkrétní rizika pro práva jednotlivců nebo skupin jednotlivců, která mohou být dotčena, a určil opatření, která je třeba přijmout v případě naplnění tohoto rizika. Posouzení dopadů by mělo být provedeno před prvním zavedením vysoce

([39]) Směrnice Evropského parlamentu a Rady 2002/14/ES ze dne 11. března 2002, kterou se stanoví obecný rámec pro informování zaměstnanců a projednávání se zaměstnanci v Evropském společenství (Úř. věst. L 80, 23.3.2002, s. 29).

rizikového systému AI a mělo by být aktualizováno, pokud se zavádějící subjekt domnívá, že se kterýkoli z relevantních faktorů změnil. Posouzení dopadů by mělo určit příslušné procesy zavádějícího subjektu, v nichž bude vysoce rizikový systém AI používán v souladu s jeho zamýšleným účelem, a mělo by zahrnovat popis časového období a četnosti, v nichž má být systém používán, jakož i konkrétní kategorie fyzických osob a skupin, které budou pravděpodobně dotčeny v konkrétním kontextu použití. Posouzení by mělo rovněž zahrnovat identifikaci konkrétních rizik újmy, která by mohla mít dopad na základní práva těchto osob nebo skupin. Při provádění tohoto posouzení by měl zavádějící subjekt zohlednit informace relevantní pro řádné posouzení dopadu, mimo jiné včetně informací uvedených poskytovatelem vysoce rizikového systému AI v návodu k použití. S ohledem na zjištěná rizika by zavádějící subjekty měly určit opatření, která je třeba přijmout v případě naplnění těchto rizik, například systémy správy a řízení v tomto konkrétním kontextu použití včetně opatření pro lidský dohled v souladu s návodem k použití nebo postupů pro vyřizování stížností a zjednávání nápravy, neboť taková opatření by mohla přispět ke zmírnění rizik pro základní práva v konkrétních případech použití. Po provedení tohoto posouzení dopadů by měl zavádějící subjekt informovat příslušný orgán dozoru nad trhem. Za účelem shromáždění relevantních informací nezbytných k provedení posouzení dopadů by subjekty zavádějící vysoce rizikový systém AI, zejména pokud jsou systémy AI používány ve veřejném sektoru, mohly do provádění těchto posouzení dopadů a navrhování opatření, která je třeba přijmout v případě naplnění rizik, případně zapojit příslušné zúčastněné strany, včetně zástupců skupin osob, které by mohly být systémem AI dotčeny, nezávislých odborníků a organizací občanské společnosti. Evropský úřad pro umělou inteligenci (dále jen „úřad pro AI“) by měl vypracovat vzor dotazníku s cílem usnadnit dodržování předpisů a snížit administrativní zátěž pro zavádějící subjekty.

(97) Měl by být jasně definován pojem „obecné modely AI“ a měl by být odlišen od pojmu „systémy AI“, aby byla zajištěna právní jistota. Definice by měla být založena na klíčových funkčních vlastnostech obecného modelu AI, zejména na obecnosti a schopnosti kompetentně plnit širokou škálu různých úkolů. Tyto modely jsou obvykle trénovány na velkém množství dat, a to prostřednictvím různých metod, jako je učení s učitelem, bez učitele nebo posilované učení. Obecné modely AI mohou být uváděny na trh různými způsoby, mimo jiné prostřednictvím knihoven, aplikačních programovacích rozhraní (API), jako přímé stahování nebo jako fyzická kopie. Tyto modely lze dále upravovat nebo dolaďovat do nových modelů. Ačkoli jsou modely AI základními součástmi systémů AI, nepředstavují samy o sobě systémy AI. Modely AI vyžadují doplnění dalších součástí, jako je například uživatelské rozhraní, aby se z nich staly systémy AI. Modely AI jsou obvykle začleněny do systémů AI a tvoří jejich součást. Toto nařízení stanoví zvláštní pravidla pro obecné modely AI a pro obecné modely AI, které představují systémová rizika, jež by se měla použít i v případě, že jsou tyto modely začleněny nebo jsou součástí systému AI. Mělo by se mít za to, že povinnosti poskytovatelů obecných modelů AI by měly platit, jakmile budou obecné modely AI uvedeny na trh. Pokud poskytovatel obecného modelu AI do svého vlastního systému AI, který je dodáván na trh nebo uváděn do provozu, začlení vlastní model, měl by být tento model považován za uvedený na trh, a proto by se kromě povinností pro systémy AI měly i nadále uplatňovat povinnosti stanovené v tomto nařízení pro modely. Povinnosti stanovené pro modely by se v žádném případě neměly vztahovat na případy, kdy se vlastní model používá pro čistě interní postupy, které nejsou nezbytné pro poskytování produktu nebo služby třetím stranám, a kdy nejsou dotčena práva fyzických osob. Vzhledem k jejich možným výrazně negativním účinkům by se na obecné modely AI se systémovým rizikem vždy měly vztahovat příslušné povinnosti podle tohoto nařízení. Definice by se neměla vztahovat na modely AI používané před jejich uvedením na trh výhradně za účelem výzkumu, vývoje a tvorby prototypů. Tím není dotčena povinnost dodržovat toto nařízení, pokud je model v návaznosti na tyto činnosti na trh uveden.

(98) Jelikož obecná povaha modelu by mohla být mimo jiné určena také počtem parametrů, modely s alespoň miliardou parametrů a trénované s velkým množstvím dat za použití rozsáhlé sebekontroly by měly být považovány za modely, které vykazují značnou obecnost a kompetentně plní širokou škálu specifických úkolů.

(99) Typickým příkladem obecného modelu AI jsou velké generativní modely AI, umožňující flexibilní tvorbu obsahu (například ve formě textu, zvuku, obrázků nebo videa), který může snadno plnit širokou škálu specifických úkolů.

(100) Je-li obecný model AI začleněn do systému AI nebo je jeho součástí, měl by být tento systém považován za obecný systém AI, pokud je tento systém díky tomuto začlenění schopen sloužit různým účelům. Obecný systém AI se může používat přímo nebo může být součástí jiných systémů AI.

(101) Poskytovatelé obecných modelů AI mají v celém hodnotovém řetězci AI zvláštní úlohu a odpovědnost, neboť modely, které poskytují, mohou tvořit základ pro řadu navazujících systémů, často poskytovaných navazujícími poskytovateli, kteří musejí těmto modelům a jejich schopnostem dobře rozumět, a to jak pro účely začlenění těchto modelů do vlastních produktů, tak v zájmu plnění svých povinností podle tohoto nebo jiných nařízení. Proto by měla být stanovena přiměřená opatření v oblasti transparentnosti, včetně vypracování a aktualizace dokumentace a poskytování informací o obecném modelu AI pro jeho používání navazujícími poskytovateli. Poskytovatel obecného modelu AI by měl technickou dokumentaci připravit a aktualizovat, aby ji na požádání zpřístupnil úřadu pro AI a příslušným vnitrostátním orgánům. Minimální soubor prvků, které mají být v takové dokumentaci obsaženy, by měl být stanoven v konkrétních přílohách tohoto nařízení. Komise by měla být zmocněna měnit tyto přílohy prostřednictvím aktů v přenesené pravomoci s ohledem na vývoj technologií.

(102) Software a data, včetně modelů, zpřístupněné na základě svobodné licence s otevřeným zdrojovým kódem, která umožňuje jejich otevřené sdílení a v jejichž rámci mohou uživatelé k nim nebo jejich změněným verzím volně přistupovat, používat je, upravovat a přerozdělovat, mohou přispět k výzkumu a inovacím na trhu a mohou hospodářství Unie poskytnout významné příležitosti k růstu. Obecné modely AI zpřístupněné na základě svobodných licencí s otevřeným zdrojovým kódem by měly být považovány za modely zajišťující vysokou úroveň transparentnosti a otevřenosti, pokud jsou jejich parametry, včetně vah, informací o architektuře modelu a informací o používání modelů veřejně dostupné. Licence by měla být považována za svobodnou s otevřeným zdrojovým kódem i v případě, že umožňuje uživatelům provozovat, kopírovat, distribuovat, studovat, měnit a vylepšovat software a data, včetně modelů za podmínky, že je připsána původnímu poskytovateli modelu a že jsou dodrženy totožné nebo srovnatelné podmínky distribuce.

(103) Svobodné komponenty AI s otevřeným zdrojovým kódem zahrnují software a data, včetně modelů a obecných modelů AI, nástrojů, služeb nebo procesů systému AI. Svobodné komponenty AI s otevřeným zdrojovým kódem lze poskytovat prostřednictvím různých kanálů, včetně jejich vývoje na otevřených úložištích. Pro účely tohoto nařízení by se výjimky poskytované pro svobodné komponenty AI s otevřeným zdrojovým kódem neměly vztahovat na součásti AI, které jsou poskytovány za cenu nebo jinak zpeněženy, včetně poskytování technické podpory nebo jiných služeb souvisejících s předmětnou komponentou AI, a to i prostřednictvím softwarové platformy, nebo používání osobních údajů z jiných důvodů než výhradně za účelem zlepšení bezpečnosti, kompatibility nebo interoperability softwaru, s výjimkou transakcí mezi mikropodniky. Zpřístupnění komponent AI prostřednictvím otevřených úložišť by samo o sobě nemělo představovat zpeněžení.

(104) Na poskytovatele obecných modelů AI, které jsou zpřístupňovány na základě svobodné licence s otevřeným zdrojovým kódem a jejichž parametry, včetně vah, informací o architektuře modelu a informací o používání modelu, jsou veřejně dostupné, by se měly vztahovat výjimky, pokud jde o požadavky týkající se transparentnosti kladené na obecné modely AI, ledaže je lze považovat za modely představující systémové riziko; v takovém případě by okolnost, že model je transparentní a doprovázený licencí s otevřeným zdrojovým kódem, neměla být považována za dostatečný důvod pro upuštění od souladu s povinnostmi podle tohoto nařízení. V každém případě vzhledem k tomu, že zpřístupnění obecných modelů AI na základě svobodné licence s otevřeným zdrojovým kódem nemusí nutně odhalit podstatné informace o souboru dat použitém pro trénování nebo doladění modelu a o tom, jak bylo zajištěno dodržování autorského práva, neměla by se výjimka stanovená pro obecné modely AI z dodržování požadavků souvisejících s transparentností týkat povinnosti vypracovat shrnutí obsahu použitého pro trénování modelu a povinnosti zavést politiku dodržování autorského práva Unie, zejména pokud jde o identifikaci a dodržování výhrad práv podle čl. 4 odst. 3 směrnice Evropského parlamentu a Rady (EU) 2019/790 ([40]).

(105) Obecné modely AI, zejména velké generativní modely AI schopné vytvářet text, obrázky a další obsah, představují jedinečné inovační příležitosti, ale také výzvy pro umělce, autory a další tvůrce i pro způsoby, jimiž je jejich tvůrčí obsah vytvářen, distribuován, používán a zužitkováván. Vývoj a trénování těchto modelů vyžaduje přístup k obrovskému množství textů, obrázků, videí a dalších dat. V této souvislosti mohou být pro vyhledávání a analýzu takového obsahu, který může být chráněn autorským právem a právy s ním souvisejícími, hojně využívány techniky vytěžování textů a dat. Jakékoli užití obsahu chráněného autorským právem vyžaduje svolení dotčeného nositele práv, pokud neplatí výjimky a omezení z autorských práv. Směrnice (EU) 2019/790 zavedla výjimky a omezení umožňující za určitých podmínek rozmnožování a extrakce děl nebo jiných předmětů ochrany pro účely vytěžování

([40]) Směrnice Evropského parlamentu a Rady (EU) 2019/790 ze dne 17. dubna 2019 o autorském právu a právech s ním souvisejících na jednotném digitálním trhu a o změně směrnic 96/9/ES a 2001/29/ES (Úř. věst. L 130, 17.5.2019, s. 92).

textů a dat. Podle těchto pravidel se nositelé práv mohou rozhodnout, že si práva ke svým dílům nebo jiným předmětům ochrany vyhradí, aby zabránili vytěžování textů a dat, pokud vytěžování neprobíhá pro účely vědeckého výzkumu. Jestliže byla práva na výjimku výslovně a vhodným způsobem vyhrazena, musí poskytovatelé obecných modelů AI od nositelů práv získat povolení, pokud chtějí vytěžování textů a dat u těchto děl provádět.

(106) Poskytovatelé, kteří uvádějí na trh Unie obecné modely AI, by měli zajistit dodržování příslušných povinností stanovených v tomto nařízení. Za tímto účelem by poskytovatelé obecných modelů AI měli zavést politiky k dodržování práva Unie v oblasti autorského práva a práv s ním souvisejících, zejména s cílem identifikovat a dodržovat výhradu práv vyjádřenou nositeli práv podle čl. 4 odst. 3 směrnice (EU) 2019/790. Každý poskytovatel, který uvádí na trh Unie obecný model AI, by měl tuto povinnost splnit bez ohledu na jurisdikci, v níž dochází k úkonům souvisejícím s autorským právem, na jejichž základě se tyto obecné modely AI trénují. Toto je nezbytné k zajištění rovných podmínek mezi poskytovateli obecných modelů AI, kdy by žádný poskytovatel neměl být schopen získat konkurenční výhodu na trhu Unie tím, že bude uplatňovat nižší standardy autorského práva, než jaké jsou v Unii stanoveny.

(107) V zájmu zvýšení transparentnosti dat, která se používají v předběžném trénování a trénování obecných modelů AI, včetně textů a dat chráněných autorským právem, je vhodné, aby poskytovatelé těchto modelů vypracovali a zveřejnili dostatečně podrobné shrnutí obsahu, jenž byl pro trénování obecného modelu AI použit. Při řádném zohlednění potřeby chránit obchodní tajemství a důvěrné obchodní informace by toto shrnutí mělo být ve svém rozsahu obecně komplexní, a nikoli technicky podrobné, aby stranám s oprávněnými zájmy, včetně nositelů autorských práv, usnadnilo výkon a prosazování jejich práv podle práva Unie, a například by v něm tak měly být uvedeny hlavní sady nebo soubory dat, které byly při trénování modelu použity, jako jsou rozsáhlé soukromé nebo veřejné databáze nebo datové archivy, a mělo by v něm být obsaženo narativní vysvětlení jiných použitých zdrojů údajů. Je vhodné, aby úřad pro AI poskytl vzor takového shrnutí, který by měl být jednoduchý a účinný a měl by poskytovateli umožnit poskytnout požadované shrnutí v podobě souvislého textu.

(108) Pokud jde o povinnost poskytovatelů obecných modelů AI zavést politiku dodržování autorského práva Unie a o jejich povinnost zveřejnit shrnutí obsahu použitého pro trénování, měl by úřad pro AI sledovat, zda daný poskytovatel tyto povinnosti splnil, aniž by z hlediska dodržování autorského práva ověřoval nebo přistupoval k posuzování trénovacích dat podle jednotlivých činností. Tímto nařízením není dotčeno prosazování pravidel v oblasti autorského práva, jak je stanoveno v právu Unie.

(109) Dodržování povinností, které se vztahují na poskytovatele obecných modelů AI, by mělo být úměrné a přiměřené typu poskytovatele modelu, aniž by tyto povinnosti musely dodržovat osoby, které vyvíjejí nebo používají modely pro nekomerční účely nebo pro účely vědeckého výzkumu; tyto osoby by měly být nicméně vybízeny k tomu, aby uvedené požadavky plnily dobrovolně. Aniž je dotčeno právo Unie v oblasti autorského práva, dodržování těchto povinností by mělo náležitě zohlednit velikost poskytovatele a umožnit zjednodušené způsoby jejich dodržování malým a středním podnikům, včetně podniků začínajících, přičemž tyto způsoby by neměly představovat nadměrné náklady a neměly by od používání takových modelů odrazovat. V případě změny nebo doladění modelu by povinnosti poskytovatelů obecných modelů AI měly být omezeny na tuto změnu nebo doladění, například doplněním již existující technické dokumentace o informace o změnách, včetně nových zdrojů trénovacích dat, jako prostředku ke splnění povinností hodnotového řetězce stanovených v tomto nařízení.

(110) Obecné modely AI by mohly představovat systémová rizika, která zahrnují mimo jiné jakékoli skutečné nebo rozumně předvídatelné negativní dopady v souvislosti se závažnými haváriemi, narušením kritických odvětví a závažnými důsledky pro veřejné zdraví a bezpečnost; jakékoli skutečné nebo rozumně předvídatelné negativní dopady na demokratické procesy, veřejnou a hospodářskou bezpečnost; šíření nezákonného, nepravdivého nebo diskriminačního obsahu. Systémová rizika by měla být chápána tak, že se zvyšují se schopnostmi a dosahem modelu, mohou vzniknout během celého životního cyklu modelu a jsou ovlivněna podmínkami zneužití, spolehlivostí modelu, poctivostí modelu a bezpečností modelu, úrovní autonomie modelu, jeho přístupem

k nástrojům, novými nebo kombinovanými způsoby, strategiemi zpřístupňování a distribuce, potenciálem k odstranění ochranných opatření a dalšími faktory. Mezinárodní přístupy dosud zejména zjistily, že je třeba zaměřit pozornost na rizika vyplývající z možného úmyslného zneužití nebo z nezamýšlených problémů s ovládáním souvisejících se sladěním s lidským záměrem; chemická, biologická, radiologická a jaderná rizika, například způsoby snížení překážek v přístupu, a to i pokud jde o vývoj zbraní, pořizování konstrukce nebo použití; mohou být umožněny ofenzivní kybernetické schopnosti, jako jsou způsoby odhalování zranitelností, zneužívání nebo operační využití; účinky interakce a používání nástrojů, například schopnost ovládat fyzické systémy a zasahovat do kritické infrastruktury; rizika, že modely budou vytvářet kopie sebe sama neboli se „samoreplikovat“ nebo že budou trénovat jiné modely; způsoby, jakými mohou modely vést ke škodlivé předpojatosti a diskriminaci s rizikem pro jednotlivce, komunity nebo společnosti; napomáhání dezinformacím nebo poškozování soukromí s ohrožením demokratických hodnot a lidských práv; riziko, že by konkrétní událost mohla vést k řetězové reakci se značnými negativními dopady, které by mohly ovlivnit až celé město, celou oblast činnosti nebo celou komunitu.

(111) Je vhodné stanovit metodiku klasifikace obecných modelů AI jako obecných modelů AI se systémovými riziky. Vzhledem k tomu, že systémová rizika vyplývají ze schopností s obzvláště velkým dopadem, měl by být obecný model AI považován za model představující systémová rizika, pokud má schopnosti s velkým dopadem, hodnocené na základě vhodných technických nástrojů a metodik, nebo významný dopad na vnitřní trh v důsledku svého dosahu. Schopnostmi s velkým dopadem v obecných modelech AI se rozumí schopnosti, které odpovídají schopnostem zaznamenaným v nejpokročilejších obecných modelech AI nebo je překračují. Po uvedení modelu na trh nebo při interakci zavádějících subjektů s modelem by bylo možné lépe porozumět celé škále schopností modelu. Podle aktuálního stavu vývoje v době vstupu tohoto nařízení v platnost je jednou z relevantních aproximací schopností modelu kumulativní množství výpočetních operací použité pro trénování obecného modelu AI, měřené při operacích s pohyblivou řádovou čárkou. Kumulativní množství výpočetních operací použitých pro trénování zahrnuje výpočty používané v rámci činností a metod, které jsou určeny k posílení schopností modelu před zavedením, jako je předběžné trénování, vytváření syntetických dat a doladění. Proto by měla být stanovena počáteční prahová hodnota operací s pohyblivou řádovou čárkou, která v případě, že ji určitý obecný model AI splňuje, vede k domněnce, že daný model je obecným modelem AI se systémovými riziky. Tato prahová hodnota by měla být v průběhu času upravována tak, aby odrážela technologické a průmyslové změny, jako jsou algoritmická zlepšení nebo zvýšená účinnost hardwaru, a měla by být doplněna referenčními hodnotami a ukazateli schopnosti modelu. Za tímto účelem by měl úřad pro AI spolupracovat s vědeckou obcí, průmyslem, občanskou společností a dalšími odborníky. Prahové hodnoty, jakož i nástroje a referenční hodnoty pro posuzování schopností s velkým dopadem by měly být silnými prediktory obecnosti, jejích schopností a souvisejícího systémového rizika obecných modelů AI a mohly by zohledňovat způsob, jakým bude daný model uveden na trh, nebo počet uživatelů, na něž může mít vliv. Za účelem doplnění tohoto systému by Komise měla mít možnost přijímat individuální rozhodnutí určující obecný model AI jako obecný model AI se systémovým rizikem, pokud se zjistí, že tento model má schopnosti nebo dopad odpovídající těm, které jsou zachyceny stanovenou prahovou hodnotou. Toto rozhodnutí by mělo být přijato na základě celkového posouzení kritérií pro určování obecných modelů AI se systémovým rizikem stanovených v příloze tohoto nařízení, jako je kvalita nebo velikost souboru trénovacích dat, počet podnikatelských a koncových uživatelů, způsoby jejich vstupů a výstupů, úroveň autonomie a škálovatelnosti nebo nástroje, k nimž má přístup. Komise by měla zohlednit odůvodněnou žádost poskytovatele, jehož model byl určen jako obecný model AI se systémovým rizikem, a může rozhodnout o přehodnocení, zda lze mít nadále za to, že tento model představuje systémová rizika.

(112) Je rovněž třeba vyjasnit postup pro klasifikaci obecných modelů AI se systémovými riziky. Za obecný model AI se systémovým rizikem by měl být předběžně považován obecný model AI, který splňuje příslušnou prahovou hodnotu pro schopnosti s velkým dopadem. Pokud určitý obecný model AI splnil podmínky dávající vyvstat takové předběžné domněnce nebo pokud začne být zřejmé, že tyto podmínky splní, měl by poskytovatel tuto skutečnost nejpozději do dvou týdnů oznámit úřadu pro AI. To je obzvláště důležité ve vztahu k prahové hodnotě operací s pohyblivou řádovou čárkou, protože trénování obecných modelů AI vyžaduje značné plánování, které zahrnuje předběžné přidělování výpočetních zdrojů, a poskytovatelé obecných modelů AI jsou proto schopni zjistit již před ukončením trénování, zda jejich model prahové hodnoty dosáhne. V souvislosti s tímto oznámením by poskytovatel měl být schopen prokázat, že vzhledem ke svým specifickým vlastnostem daný obecný model AI výjimečně nepředstavuje systémová rizika, a neměl by proto být jako obecný model AI se systémovými riziky klasifikován. Tyto informace jsou cenné pro úřad pro AI, aby mohl předvídat uvádění obecných modelů AI se systémovými riziky

na trh, a poskytovatelé tak mohou začít s úřadem pro AI již zkraje spolupracovat. Tyto informace jsou obzvláště důležité, pokud jde o obecné modely AI, které mají být zpřístupněny jako modely s otevřeným zdrojovým kódem, jelikož po zveřejnění modelu s otevřeným zdrojovým kódem může být provádění nezbytných opatření k zajištění souladu s povinnostmi podle tohoto nařízení obtížnější.

(113) Pokud se Komise dozví, že určitý obecný model AI splňuje požadavky na to, aby byl klasifikován jako obecný model AI se systémovým rizikem, což dříve buď nebylo známo, nebo o této skutečnosti příslušný poskytovatel Komisi neinformoval, měla by mít Komise pravomoc jej takto označit. Mělo by být zajištěno systémem kvalifikovaných výstrah, aby byl úřad pro AI informován vědeckou komisí o obecných modelech AI, které by případně měly být klasifikovány jako obecné modely AI se systémovým rizikem, a to nad rámec monitorovacích činností úřadu pro AI.

(114) Poskytovatelé obecných modelů AI, které představují systémová rizika, by měli kromě povinností stanovených poskytovatelům obecných modelů AI podléhat povinnostem zaměřeným na identifikaci a zmírnění těchto rizik a na zajištění odpovídající úrovně ochrany kybernetické bezpečnosti bez ohledu na to, zda jsou dotyčné modely poskytovány jako modely samostatné, nebo jsou začleněny do určitého systému nebo produktu AI. Za účelem dosažení těchto cílů by toto nařízení mělo vyžadovat, aby poskytovatelé prováděli nezbytná hodnocení modelů, zejména před jejich prvním uvedením na trh, včetně provádění a dokumentace kontradiktorního testování modelů, případně i prostřednictvím interního nebo nezávislého externího testování. Kromě toho by poskytovatelé obecných modelů AI se systémovými riziky měli systémová rizika průběžně posuzovat a zmírňovat, například zavedením politik řízení rizik, jako jsou procesy odpovědnosti a správy, prováděním monitorování po uvedení na trh, přijímáním vhodných opatření v průběhu celého životního cyklu modelu a prostřednictvím spolupráce s příslušnými subjekty v celém hodnotovém řetězci AI.

(115) Poskytovatelé obecných modelů AI se systémovými riziky by měli posuzovat a zmírňovat možná systémová rizika. Pokud navzdory úsilí o identifikaci a prevenci rizik souvisejících s obecným modelem AI, která mohou představovat rizika systémová, vývoj nebo používání modelu způsobí závažný incident, měl by poskytovatel obecného modelu AI bez zbytečného odkladu incident sledovat a oznámit veškeré relevantní informace a případná nápravná opatření Komisi a příslušným vnitrostátním orgánům. Poskytovatelé by dále během celého životního cyklu daného modelu měli zajišťovat náležitou úroveň ochrany jeho kybernetické bezpečnosti a případně jeho fyzické infrastruktury. Ochrana kybernetické bezpečnosti související se systémovými riziky spojenými se zneužitím nebo útoky by měla řádně zohledňovat nahodilý únik modelu, neoprávněné zpřístupnění, obcházení bezpečnostních opatření a obranu před kybernetickými útoky, neoprávněným přístupem nebo krádeží modelu. Tato ochrana by mohla být usnadněna zajištěním modelových vah, algoritmů, serverů a datových souborů, například prostřednictvím provozních bezpečnostních opatření pro bezpečnost informací, specifických politik kybernetické bezpečnosti, odpovídajících technických a zavedených řešení a kontrol kybernetického a fyzického přístupu, které odpovídají příslušným okolnostem a souvisejícím rizikům.

(116) Úřad pro AI by měl podporovat a usnadňovat vypracování, přezkum a úpravu kodexů správné praxe s přihlédnutím k mezinárodním přístupům. K účasti by mohli být přizváni všichni poskytovatelé obecných modelů AI. Aby bylo zajištěno, že kodexy správné praxe odrážejí aktuální stav vývoje a náležitě zohledňují různorodý soubor perspektiv, měl by úřad pro AI při vypracovávání těchto kodexů spolupracovat s příslušnými vnitrostátními orgány a případně by mohl konzultovat organizace občanské společnosti a další příslušné zúčastněné strany a odborníky, včetně vědecké komise. Kodexy správné praxe by se měly vztahovat na povinnosti poskytovatelů obecných modelů AI a obecných modelů, které představují systémová rizika. Kromě toho, pokud jde o systémová rizika, měly by kodexy správné praxe pomoci stanovit taxonomii rizik týkající se druhu a povahy systémových rizik na úrovni Unie, včetně jejich zdrojů. Kodexy správné praxe by se měly rovněž zaměřit na konkrétní posouzení rizik a opatření k jejich zmírnění.

(117) Kodexy správné praxe by měly představovat ústřední nástroj pro řádné dodržování povinností stanovených tímto nařízením pro poskytovatele obecných modelů AI. Poskytovatelé by měli mít možnost kodexy správné praxe využívat, aby dodržování povinností prokázali. Komise může prostřednictvím prováděcích aktů rozhodnout o schválení kodexu správné praxe a o jeho obecné platnosti v rámci Unie, nebo případně o stanovení společných pravidel pro plnění příslušných povinností, pokud v době, kdy se toto nařízení stane použitelným, nemůže být kodex správné praxe dokončen nebo jej úřad pro AI nepovažuje za vhodný. Jakmile je zveřejněna harmonizovaná

norma a úřad pro AI ji posoudí jako vhodnou k pokrytí příslušných povinností, měl by soulad s evropskou harmonizovanou normou poskytnout poskytovatelům předpoklad shody. Poskytovatelé obecných modelů AI by dále měli být schopni prokázat soulad přiměřenými alternativními prostředky, nejsou-li kodexy správné praxe nebo harmonizované normy k dispozici nebo rozhodnou-li se je tito poskytovatelé nevyužít.

(118) Toto nařízení upravuje systémy AI a modely AI tím, že ukládá určité požadavky a povinnosti relevantním účastníkům trhu, kteří je uvádějí na trh, do provozu nebo používají v Unii, a doplňuje tak povinnosti poskytovatelů zprostředkovatelských služeb, kteří tyto systémy nebo modely začleňují do svých služeb upravených nařízením (EU) 2022/2065. Pokud jsou tyto systémy nebo modely začleněny do určených velmi velkých online platforem nebo velmi velkých internetových vyhledávačů, podléhají rámci pro řízení rizik stanovenému v nařízení (EU) 2022/2065. V důsledku by se tak příslušné povinnosti podle tohoto nařízení měly považovat za splněné, pokud se v těchto modelech neobjeví a nejsou identifikována významná systémová rizika, na něž se nařízení (EU) 2022/2065 nevztahuje. V tomto rámci jsou poskytovatelé velmi velkých online platforem a velmi velkých internetových vyhledávačů povinni posoudit potenciální systémová rizika vyplývající z navrhování, fungování a využívání jejich služeb, včetně toho, jak může k těmto rizikům přispět návrh algoritmických systémů používaných v určité službě, jakož i systémová rizika vyplývající z možného zneužití. Tito poskytovatelé jsou rovněž povinni přijmout vhodná zmírňující opatření při dodržování základních práv.

(119) Vzhledem k rychlému tempu inovací a technologickému vývoji digitálních služeb v oblasti působnosti různých nástrojů práva Unie, zejména s ohledem na používání a vnímání ze strany jejich příjemců, mohou být systémy AI, na něž se toto nařízení vztahuje, poskytovány jako zprostředkovatelské služby nebo jejich části ve smyslu nařízení (EU) 2022/2065, které by mělo být vykládáno technologicky neutrálním způsobem. Systémy AI lze například využít k poskytování internetových vyhledávačů, a to zejména do té míry, že systém AI, jako je online chatbot, v zásadě provádí vyhledávání na všech internetových stránkách, poté výsledky začleňuje do svých stávajících znalostí a využívá aktualizované znalosti k vytvoření jediného výstupu, který kombinuje různé zdroje informací.

(120) Kromě toho jsou pro usnadnění účinného provádění nařízení (EU) 2022/2065 obzvláště důležité povinnosti, které toto nařízení ukládá poskytovatelům a subjektům zavádějícím systémy AI, aby bylo možné odhalit a zveřejnit, že výstupy těchto systémů jsou uměle generovány nebo s nimi bylo manipulováno. To platí zejména pro povinnost poskytovatelů velmi velkých online platforem nebo velmi velkých internetových vyhledávačů identifikovat a jejich povinnost zmírňovat systémová rizika, která mohou vyplývat z šíření obsahu, který byl uměle vytvořen nebo s nímž bylo manipulováno, zejména riziko skutečných nebo předvídatelných negativních dopadů na demokratické procesy, občanský diskurz a volební procesy, a to i prostřednictvím dezinformací.

(121) Klíčovou úlohu při poskytování technických řešení zajišťujících dodržování tohoto nařízení poskytovatelům by měla hrát normalizace, v souladu s aktuálním stavem vývoje, aby se podpořily inovace a konkurenceschopnost a růst na jednotném trhu. 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 čl. 2 odst. 1 písm. c) nařízení Evropského parlamentu a Rady (EU) č. 1025/2012 ([41]). Proto by mělo být podporováno vyvážené zastoupení zájmů se zapojením všech příslušných zúčastněných stran do tvorby norem, zejména malých a středních podniků, spotřebitelských organizací a zúčastněných stran v oblasti životního prostředí a v sociální oblasti v souladu s články 5 a 6 nařízení (EU) č. 1025/2012. Aby se usnadnilo dodržování předpisů, měla by Komise žádosti o normalizaci vydávat bez zbytečného odkladu. Při přípravě žádosti o normalizaci by Komise měla konzultovat poradní fórum a radu s cílem shromáždit příslušné odborné znalosti. Pokud však příslušné odkazy na harmonizované normy neexistují, měla by mít Komise možnost stanovit prostřednictvím prováděcích aktů a po konzultaci s poradním fórem společné specifikace pro určité požadavky podle tohoto nařízení. Společná specifikace by měla být výjimečným záložním řešením, které usnadní povinnost poskytovatele splnit požadavky tohoto nařízení, pokud žádost o normalizaci nebyla přijata žádnou z evropských normalizačních organizací nebo pokud příslušné harmonizované normy dostatečně neřeší obavy týkající se základních práv nebo pokud harmonizované

([41]) 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).

normy nejsou v souladu s žádostí nebo pokud při přijímání vhodné harmonizované normy dochází ke zpoždění. Pokud je toto zpoždění při přijímání harmonizované normy způsobeno technickou složitostí dané normy, Komise by před posuzováním možnosti stanovit společné specifikace měla tuto skutečnost zohlednit. Komise vyzývá, aby při vypracovávání společných specifikací spolupracovala s mezinárodními partnery a mezinárodními normalizačními orgány.

(122) Aniž je dotčeno používání harmonizovaných norem a společných specifikací, je vhodné předpokládat, že poskytovatelé vysoce rizikového systému AI, který byl trénován a testován na datech odrážejících specifické zeměpisné, behaviorální, kontextuální nebo funkční prostředí, v němž má být systém AI používán, splňují příslušné opatření stanovené v rámci požadavku na správu dat stanoveného v tomto nařízení. Aniž jsou dotčeny požadavky týkající se spolehlivosti a přesnosti stanovené v tomto nařízení, mělo by se v souladu s čl. 54 odst. 3 nařízení (EU) 2019/881 předpokládat, že vysoce rizikové systémy AI, 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*, splňují požadavek tohoto nařízení na kybernetickou bezpečnost, pokud se certifikát kybernetické bezpečnosti nebo prohlášení o shodě nebo jejich části vztahují na požadavek na kybernetickou bezpečnost stanovený v tomto nařízení. Tím není dotčena dobrovolná povaha tohoto systému kybernetické bezpečnosti.

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

(124) V případě vysoce rizikových systémů AI vztahujících se k produktům upraveným stávajícími harmonizačními právními předpisy Unie na základě nového legislativního rámce je v zájmu minimalizace zátěže provozovatelů a předcházení případnému zdvojování vhodné, aby byl soulad těchto systémů AI s požadavky tohoto nařízení posuzován v rámci posuzování shody, které uvedené právo již stanovují. Použitelnost požadavků tohoto nařízení by tedy neměla mít vliv na konkrétní logiku, metodiku nebo obecnou strukturu posuzování shody podle příslušných harmonizačních právních předpisů Unie.

(125) Vzhledem ke složitosti vysoce rizikových systémů AI a rizikům, která jsou s nimi spojena, je důležité vyvinout pro vysoce rizikové systémy AI odpovídající postup posuzování shody zahrnující oznámené subjekty, tzv. posuzování shody třetí stranou. Vzhledem ke stávajícím zkušenostem profesionálních ověřovatelů před uvedením na trh v oblasti bezpečnosti produktů a k odlišné povaze souvisejících rizik je však vhodné alespoň v počáteční fázi uplatňování tohoto nařízení omezit oblast působnosti posuzování shody vysoce rizikových systémů AI 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 AI určené pro biometriku.

(126) Příslušné vnitrostátní orgány by v souladu s tímto nařízením měly, pokud je to požadováno, oznámit oznámené subjekty pro účely posouzení shody třetími stranami pod podmínkou, že splňují určitý soubor požadavků, zejména požadavku na nezávislost, způsobilost a neexistenci střetu zájmů a vhodných požadavků na kybernetickou bezpečnost. 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 přílohy I rozhodnutí č. 768/2008/ES.

(127) V souladu se závazky Unie podle Dohody Světové obchodní organizace o technických překážkách obchodu je vhodné usnadnit vzájemné uznávání výsledků posuzování shody vypracovaných příslušnými subjekty posuzování shody nezávisle na území, na němž jsou usazeny, za předpokladu, že tyto subjekty posuzování shody zřízené podle práva třetí země splňují příslušné požadavky tohoto nařízení a že Unie v tomto ohledu uzavřela dohodu. V této souvislosti by Komise měla za uvedeným účelem aktivně prozkoumat možné mezinárodní nástroje, a zejména usilovat o uzavření dohod o vzájemném uznávání se třetími zeměmi.

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

(129) Vysoce rizikové systémy AI by měly být opatřeny označením CE prokazujícím jejich shodu s tímto nařízením, aby jim byl umožněn volný pohyb v rámci vnitřního trhu. Na vysoce rizikových systémech AI začleněných do produktu by mělo být připevněno fyzické označení CE, které může být doplněno digitálním označením CE. U vysoce rizikových systémů AI poskytovaných pouze digitálně by se mělo používat digitální označení CE. Členské státy by neměly vytvářet neodůvodněné překážky uvádění na trh nebo do provozu u vysoce rizikových systémů AI, které jsou v souladu s požadavky stanovenými v tomto nařízení a jsou opatřeny označením CE.

(130) Rychlá dostupnost inovativních technologií může mít za určitých podmínek zásadní význam pro zdraví a bezpečnost osob, ochranu životního prostředí a změnu klimatu i pro společnost jako celek. Je proto vhodné, aby orgány dozoru nad trhem mohly z výjimečných důvodů veřejné bezpečnosti nebo ochrany života a zdraví fyzických osob, ochrany životního prostředí a ochrany klíčových průmyslových a infrastrukturních aktiv povolit uvedení na trh nebo do provozu v případě systémů AI, u nichž posouzení shody nebylo provedeno. V řádně odůvodněných situacích, jak je stanoveno v tomto nařízení, mohou donucovací orgány nebo orgány civilní ochrany uvést konkrétní vysoce rizikový systém AI do provozu bez povolení orgánu dozoru nad trhem, pokud je o takové povolení požádáno během používání nebo po něm bez zbytečného odkladu.

(131) Pro usnadnění práce Komise a členských států v oblasti AI a zvýšení transparentnosti vůči veřejnosti by poskytovatelé vysoce rizikových systémů AI s výjimkou těch, které se vztahují k produktům spadajícím do oblasti působnosti příslušných stávajících harmonizačních právních předpisů Unie, jakož i poskytovatelé, kteří se domnívají, že systém AI uvedený mezi příklady vysoce rizikového použití v příloze tohoto nařízení není vysoce rizikový na základě výjimky, měli mít povinnost se zaregistrovat, jakož i zaregistrovat informace o svém vysoce rizikovém systému AI do databáze EU, kterou zřídí a bude spravovat Komise. Před použitím systému AI uvedeného mezi příklady vysoce rizikového použití by se subjekty zavádějící vysoce rizikové systémy AI, které jsou veřejnými orgány, agenturami nebo subjekty, měly zaregistrovat do této databáze a vybrat systém, který hodlají používat. Ostatní zavádějící subjekty by měly mít právo tak učinit dobrovolně. Tento oddíl databáze EU by měl být veřejně přístupný, bezplatný, informace by měly být snadno dohledatelné, srozumitelné a strojově čitelné. Databáze EU by rovněž měla být uživatelsky přívětivá, například tím, že bude poskytovat funkce vyhledávání, a to i prostřednictvím klíčových slov, což umožní široké veřejnosti nalézt relevantní informace, které mají být předloženy při registraci vysoce rizikových systémů AI a o příkladech vysoce rizikového použití systémů AI stanovených v přílohách tohoto nařízení, jimž vysoce rizikové systémy AI odpovídají. Veškeré podstatné změny vysoce rizikových systémů AI by se rovněž měly zaregistrovat v databázi EU. U vysoce rizikových systémů AI v oblasti vymáhání práva, migrace, azylu a řízení ochrany hranic by registrační povinnosti měly být splněny v zabezpečeném neveřejném oddílu databáze EU. Přístup k zabezpečenému neveřejnému oddílu by měl být přísně omezen na Komisi, jakož i na orgány dozoru nad trhem, pokud jde o jejich vnitrostátní část této databáze. Vysoce rizikové systémy AI v oblasti kritické infrastruktury by měly být registrovány pouze na vnitrostátní úrovni. V souladu s nařízením 2018/1725 by správcem databáze EU pro přeshraniční výměnu informací měla být Komise. Aby byla zajištěna plná funkčnost databáze EU při jejím zavedení, měl by postup při vytváření databáze zahrnovat vytvoření funkčních specifikací ze strany Komise a nezávislou zprávu o auditu. Komise by měla při plnění svých úkolů správce údajů v databázi EU zohlednit rizika spojená s kybernetickou bezpečností. Aby byla databáze EU co nejvíce dostupná a využívaná veřejností, měla by spolu s informacemi, které jsou jejím prostřednictvím zpřístupňovány, splňovat požadavky směrnice (EU) 2019/882.

(132) Určité systémy AI 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 AI, a s výhradou cílených výjimek, které zohledňují zvláštní potřeby spojené s vymáháním práva. Zejména fyzické osoby by měly být upozorněny, že komunikují se systémem AI, není-li tato skutečnost zřejmá z pohledu fyzické osoby, která je přiměřeně informovaná, pozorná a obezřetná, při zohlednění okolností a kontextu použití. Při plnění této povinnosti by měly být zohledněny vlastnosti fyzických osob náležejících ke zranitelným skupinám vzhledem k jejich věku nebo zdravotnímu postižení, a to v rozsahu, v jakém je systém AI určen i pro komunikaci s těmito skupinami. Fyzické osoby by navíc měly být informovány v případě, že jsou vystaveny systémům AI, které zpracováním jejich biometrických údajů mohou identifikovat nebo odvodit jejich emoce nebo záměry nebo je zařadit do konkrétních kategorií. Tyto konkrétní kategorie se mohou týkat takových aspektů, jako je pohlaví, věk, barva vlasů, barva očí, tetování, osobnostní rysy, etnický původ, osobní preference a zájmy. Tyto informace a oznámení by měly být poskytovány ve formátech přístupných pro osoby se zdravotním postižením.

(133) Různé systémy AI mohou generovat velké množství syntetického obsahu, který je pro člověka stále obtížnější odlišit od autentického obsahu vytvořeného člověkem. Široká dostupnost a rostoucí schopnosti těchto systémů mají významný dopad na integritu a důvěru v informační ekosystém, neboť zvyšují nová rizika zavádějících informací a manipulace ve velkém měřítku, podvodů, vydávání se za jinou osobu a klamání spotřebitelů. Vzhledem k těmto dopadům, rychlému technologickému tempu a potřebě nových metod a technik pro vysledování původu informací je vhodné požadovat, aby poskytovatelé těchto systémů zavedli technická řešení, která umožňují označení ve strojově čitelném formátu a zjištění, že výstup vytvořil nebo s ním manipuloval systém AI, a nikoli člověk. Tyto techniky a metody by měly být dostatečně spolehlivé, interoperabilní, účinné a robusní, pokud je to technicky proveditelné, s přihlédnutím k dostupným technikám nebo kombinaci těchto technik, jako jsou vodoznaky, identifikace metadat, kryptografické metody prokazování původu a pravosti obsahu, metody vedení protokolů, otisky prstů nebo případně jiné techniky. Při plnění této povinnosti by poskytovatelé měli rovněž zohlednit specifika a omezení různých typů obsahu a příslušný technologický a tržní vývoj v této oblasti, jak se odráží v obecně uznávaném aktuálním stavu vývoje. Tyto techniky a metody lze uplatňovat na úrovni systému AI nebo na úrovni modelu AI, včetně obecných modelů AI, které generují obsah, čímž se usnadní plnění této povinnosti navazujícímu poskytovateli systému AI. V zájmu zachování proporcionality je vhodné předpokládat, že by se tato povinnost označování neměla vztahovat na systémy AI, které plní především asistenční funkci pro standardní editaci, nebo na systémy AI, které podstatně nemění vstupní údaje poskytnuté zavádějícím subjektem nebo jejich sémantiku.

(134) Kromě technických řešení používaných poskytovateli systému by zavádějící subjekty, které používají systém AI k vytváření obrazového, zvukového nebo video obsahu nebo k manipulaci s ním, přičemž tento obsah se znatelně podobá existujícím osobám, objektům, místům, subjektům nebo událostem, a určité osobě by se falešně jevil jako autentický nebo pravdivý (deep fakes), měly rovněž jasně a zřetelně uvádět, že obsah byl vytvořen uměle nebo s ním bylo manipulováno, a to tak, že odpovídajícím způsobem označí výstup umělé inteligence a zveřejní jeho umělý původ. Splnění této povinnosti týkající se transparentnosti by nemělo být vykládáno tak, že naznačuje, že používání systému AI nebo jeho výstupu brání právu na svobodu projevu a právu na svobodu umění a vědy zaručeným Listinou, zejména pokud je obsah součástí zjevně tvůrčího, satirického, uměleckého nebo fiktivního nebo obdobného díla nebo programu, s výhradou vhodných záruk práv a svobod třetích osob. V těchto případech je povinnost transparentnosti pro „deep fakes“ stanovená v tomto nařízení omezena na zveřejnění existence takového vytvořeného nebo zmanipulovaného obsahu vhodným způsobem, který nebrání zobrazení díla nebo požitku z něj, včetně jeho běžného využívání a používání, při zachování užitečnosti a kvality díla. Kromě toho je rovněž vhodné stanovit podobnou povinnost zveřejňování v souvislosti s textem vytvořeným nebo zmanipulovaným umělou inteligencí, pokud je zveřejněn za účelem informování veřejnosti o záležitostech veřejného zájmu, pokud obsah vytvořený umělou inteligencí neprošel procesem lidského přezkumu nebo redakční kontroly a redakční odpovědnost za zveřejnění obsahu nese fyzická nebo právnická osoba.

(135) Aniž je dotčena závazná povaha a plná použitelnost povinností týkajících se transparentnosti, může Komise rovněž podporovat a usnadňovat vypracování kodexů správné praxe na úrovni Unie s cílem usnadnit účinné provádění povinností týkajících se odhalování a označování uměle vytvořeného nebo zmanipulovaného obsahu, včetně podpory praktických opatření pro případné zpřístupnění detekčních mechanismů a usnadnění spolupráce s dalšími subjekty v celém hodnotovém řetězci, šíření obsahu nebo ověřování jeho pravosti a původu, aby veřejnost mohla obsah vytvořený umělou inteligencí účinně odlišit.

(136) Pro usnadnění účinného provádění nařízení (EU) 2022/2065 jsou obzvláště důležité povinnosti, které toto nařízení ukládá poskytovatelům a subjektům zavádějícím systémy AI, aby bylo možné odhalit a zveřejnit, že výstupy těchto systémů jsou uměle generovány nebo s nimi bylo manipulováno. Toto platí zejména pro povinnost poskytovatelů velmi velkých online platforem nebo velmi velkých internetových vyhledávačů identifikovat a zmírňovat systémová rizika, která mohou vyplývat z šíření obsahu, který byl uměle vytvořen nebo s nímž bylo manipulováno, zejména riziko skutečných nebo předvídatelných negativních dopadů na demokratické procesy, občanský diskurz a volební procesy, a to i prostřednictvím dezinformací. Požadavkem na označování obsahu vytvořeného systémy AI podle tohoto nařízení není dotčena povinnost uvedená v čl. 16. odst. 6 nařízení (EU) 2022/2065, podle něhož poskytovatelé hostingových služeb musejí zpracovávat oznámení o nezákonném obsahu obdržená podle čl. 16 odst. 1 uvedeného nařízení, a tento požadavek by neměl ovlivňovat posouzení a rozhodnutí o nezákonnosti konkrétního obsahu. Toto posouzení by mělo být provedeno výhradně s ohledem na pravidla upravující legalitu obsahu.

(137) Dodržování povinností týkajících se transparentnosti pro systémy AI, na něž se vztahuje toto nařízení, by nemělo být vykládáno tak, že se uvádí, že používání daného systému AI nebo jeho výstupu je podle tohoto nařízení nebo jiného práva Unie a členských států zákonné, a neměly by jím být dotčeny jiné povinnosti týkající se transparentnosti pro subjekty zavádějící systémy AI stanovené v unijním nebo vnitrostátním právu.

(138) AI je rychle se vyvíjející skupina technologií, která vyžaduje regulační dohled a bezpečný a kontrolovaný prostor pro experimentování při současném zajištění odpovědných inovací a integrace vhodných záruk a opatření ke zmírnění rizika. Aby byl zajištěn právní rámec, který inovace podporuje, obstojí i v budoucnu a je odolný vůči narušení, měly by členské státy zajistit, aby jejich příslušné vnitrostátní orgány zřídily alespoň jeden regulační sandbox pro AI na vnitrostátní úrovni s cílem usnadnit vývoj a testování inovativních systémů AI pod přísným regulačním dohledem, než budou tyto systémy uvedeny na trh nebo jiným způsobem do provozu. Členské státy by mohly tuto povinnost splnit také účastí v již existujících regulačních sandboxech nebo společným zřízením sandboxu s příslušnými orgány jednoho nebo více členských států, pokud tato účast poskytuje zúčastněným členským státům rovnocennou úroveň vnitrostátního pokrytí. Regulační sandboxy pro AI by mohly být zřízeny ve fyzické, digitální nebo hybridní podobě a mohou být určeny pro fyzické i digitální produkty. Zřizující orgány by rovněž měly zajistit, aby regulační sandboxy pro AI měly odpovídající zdroje pro své fungování, včetně finančních a lidských zdrojů.

(139) Cílem těchto regulačních sandboxů pro AI by měla být podpora inovací AI na základě vytvoření kontrolovaného experimentálního a testovacího prostředí ve fázi vývoje a před uvedením na trh, aby byl zajištěn soulad inovativních systémů AI s tímto nařízením a s dalšími příslušným právem Unie i s vnitrostátním právem. Regulační sandboxy pro AI by dále měly vést k posílení právní jistoty inovátorů, dohledu příslušných orgánů a jejich porozumění příležitostem, vznikajícím rizikům a dopadům používání AI, usnadnění regulačního učení orgánů a podniků, a to i s ohledem na budoucí úpravy právního rámce, podpora spolupráce a sdílení osvědčených postupů s orgány zapojenými do regulačního sandboxu pro AI, jakož i urychlení přístupu na trhy, mimo jiné odstraněním překážek pro malé a střední podniky včetně podniků začínajících. Regulační sandboxy pro AI by měly být široce dostupné v celé Unii a zvláštní pozornost by měla být věnována jejich dostupnosti pro malé a střední podniky, včetně podniků začínajících. Účast v regulačním sandboxu pro AI by se měla zaměřit na otázky, které zvyšují právní nejistotu pro poskytovatele a potenciální poskytovatele, pokud jde o inovace, experimentování s AI v Unii a přispívání k fakticky podloženému regulačnímu učení. Dohled nad systémy AI v regulačním sandboxu pro AI by proto měl zahrnovat jejich vývoj, trénování, testování a validaci před uvedením systémů na trh nebo do provozu, jakož i pojem podstatných změn, které mohou vyžadovat nový postup posuzování shody, a výskyt takových změn. Veškerá významná rizika, která budou zjištěna během vývoje a testování těchto systémů AI, by měla být následně náležitě zmírněna, přičemž v případě neúspěchu by měl být proces vývoje a testování pozastaven.Příslušné vnitrostátní orgány, které zřizují regulační sandboxy pro AI, 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 AI, jako jsou vnitrostátní nebo evropské normalizační organizace, oznámené subjekty, testovací a experimentální zařízení, výzkumné a experimentální laboratoře, evropská centra pro digitální inovace 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 sandboxů pro AI a rámec spolupráce mezi příslušnými orgány, které se podílejí na dohledu nad těmito sandboxy. Regulačními sandboxy pro AI zřízenými podle tohoto nařízení by nemělo být dotčeno jiné právo umožňující zřízení jiných sandboxů, jejichž cílem je zajistit soulad s jiným právem, než je toto nařízení. Příslušné orgány odpovědné za tyto jiné regulační sandboxy by případně měly zvážit přínosy používání těchto sandboxů rovněž pro účely zajištění souladu systémů AI s tímto nařízením. Na základě dohody mezi příslušnými vnitrostátními orgány a účastníky regulačního sandboxu pro AI může být v rámci regulačního sandboxu pro AI rovněž prováděno a kontrolováno testování v reálných podmínkách.

(140) Toto nařízení by mělo poskytovatelům a potenciálním poskytovatelům v regulačním sandboxu pro AI poskytnout právní základ pro to, aby v rámci regulačního sandboxu pro AI mohli k vývoji určitých systémů AI ve veřejném zájmu použít osobní údaje shromážděné pro jiné účely, a to pouze za určitých podmínek, v souladu s čl. 6 odst. 4 a čl. 9 odst. 2 písm. g) nařízení (EU) 2016/679 a s článkem 5, 6 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. Poskytovatelé a potenciální poskytovatelé by v regulačních sandboxech pro AI by měli zajistit vhodné záruky a spolupracovat s příslušnými orgány, mimo jiné postupovat podle jejich pokynů a jednat rychle a v dobré víře, aby náležitě zmírnili veškerá zjištěná významná rizika pro bezpečnost, zdraví a základní práva, která v průběhu vývoje, testování a experimentování v rámci sandboxu případně vzniknou.

(141) V zájmu urychlení procesu vývoje vysoce rizikových systémů AI uvedených v příloze tohoto nařízení 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 sandboxu pro AI. V takových případech, s ohledem na možné důsledky takového testování pro jednotlivce by však mělo být zajištěno, aby toto nařízení pro poskytovatele nebo potenciální poskytovatele zavedlo vhodné a dostatečné záruky a podmínky. Tyto záruky by měly mimo jiné zahrnovat požadavek na informovaný souhlas fyzických osob s účastí na testování v reálných podmínkách, s výjimkou vymáhání práva v případech, kdy by získání informovaného souhlasu bránilo testování systému AI. Souhlas subjektů údajů s účastí na takovém testování podle tohoto nařízení je odlišný od souhlasu subjektů údajů se zpracováním jejich osobních údajů podle příslušného práva v oblasti ochrany údajů, který jím není dotčen. Je rovněž důležité minimalizovat rizika a umožnit dohled ze strany příslušných orgánů, a proto požadovat, aby potenciální poskytovatelé předložili příslušnému orgánu dozoru nad trhem plán testování v reálných podmínkách, zaregistrovali testování ve specializovaných oddílech v databázi EU s výhradou určitých omezených výjimek, stanovili omezení doby, po kterou lze testování provádět, a vyžadovali další záruky pro osoby patřící do některé ze zranitelných skupin, jakož i písemnou dohodu vymezující úlohy a povinnosti potenciálních poskytovatelů a zavádějících subjektů a účinný dohled ze strany příslušných pracovníků zapojených do testování v reálném provozu. Dále je vhodné stanovit další záruky, které zajistí, aby predikce, doporučení nebo rozhodnutí systému AI mohly být účinně zrušeny a ignorovány a aby byly osobní údaje chráněny a vymazány, pokud subjekty odvolají svůj souhlas s účastí na testování, aniž by byla dotčena jejich práva jakožto subjektů údajů podle práva Unie o ochraně údajů. Pokud jde o předávání údajů, je rovněž vhodné předpokládat, že údaje shromážděné a zpracovávané pro účely testování v reálných podmínkách by měly být předávány do třetích zemí pouze v případě, že jsou zavedeny vhodné a použitelné záruky podle práva Unie, zejména v souladu se základy pro předávání osobních údajů podle práva Unie o ochraně údajů, zatímco pro neosobní údaje jsou zavedeny vhodné záruky v souladu s právem Unie, jako jsou nařízení Evropského parlamentu a Rady (EU) 2022/868 ([42]) a (EU) 2023/2854 ([43]).

(142) V zájmu zajištění sociálně a environmentálně prospěšných výsledků AI se členské státy vybízejí, aby podporovaly a prosazovaly výzkum a vývoj řešení v oblasti AI, která sociálně a environmentálně prospěšné výsledky podporují, jako jsou řešení založená na AI, jejichž cílem je zvýšit přístupnost pro osoby se zdravotním postižením, řešit socioekonomické nerovnosti nebo plnit environmentální cíle, a aby za tímto účelem přidělily dostatečné zdroje, včetně veřejných a unijních finančních prostředků, a případně aby se zaměřily zejména na projekty, které sledují uvedené cíle, jsou-li splněna kritéria způsobilosti a výběru. Tyto projekty by měly být založeny na zásadě interdisciplinární spolupráce mezi vývojáři AI, odborníky na nerovnost a nediskriminaci, přístupnost, spotřebitelská, environmentální a digitální práva, jakož i akademickými pracovníky.

(143) V zájmu podpory a ochrany inovací je důležité, aby byly obzvláště zohledněny zájmy malých a středních podniků, včetně podniků začínajících, které jsou poskytovateli nebo zavádějícími subjekty systémů AI. Za tímto účelem by členské státy měly vyvíjet iniciativy zaměřené na tyto provozovatele, a to včetně zvyšování povědomí a informační komunikace. Členské státy by měly poskytnout malým a středním podnikům, včetně podniků začínajících, které mají sídlo nebo pobočku v Unii, přednostní přístup k regulačním sandboxům pro AI za předpokladu, že splňují podmínky způsobilosti a kritéria výběru, a aniž by bránily jiným poskytovatelům a potenciálním poskytovatelům v přístupu k sandboxům za předpokladu, že jsou splněny stejné podmínky a kritéria. Členské státy by měly využít stávající kanály a případně vytvořit nové specializované kanály pro komunikaci s malými a středními podniky, včetně začínajících podniků, zavádějícími subjekty, dalšími inovátory a případně místními veřejnými orgány, aby podpořily malé a střední podniky v průběhu vývoje tím, že jim budou poskytovat pokyny a zodpovídat dotazy týkající se provádění tohoto nařízení. Tyto kanály by ve vhodných případech měly spolupracovat na vytváření synergií a zajištění jednotných pokynů pro malé a střední podniky, včetně podniků začínajících, a zavádějící subjekty. Členské státy by navíc měly usnadňovat účast malých a středních podniků a dalších příslušných zúčastněných stran na procesech rozvoje normalizace. Kromě toho by poskytovatelé měli při stanovování poplatků

([42]) Nařízení Evropského parlamentu a Rady (EU) 2022/868 ze dne 30. května 2022 o evropské správě dat a o změně nařízení (EU) 2018/1724 (akt o správě dat) (Úř. věst. L 152, 3.6.2022, s. 1).

([43]) Nařízení Evropského parlamentu a Rady (EU) 2023/2854 ze dne 13. prosince 2023 o harmonizovaných pravidlech pro spravedlivý přístup k datům a jejich využívání a o změně nařízení (EU) 2017/2394 a směrnice (EU) 2020/1828 (akt o datech) (Úř. věst. L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).

za posouzení shody oznámenými subjekty zohlednit zvláštní zájmy a potřeby poskytovatelů, kterými jsou malé a střední podniky včetně podniků začínajících. Komise by měla pravidelně posuzovat náklady malých a středních podniků, včetně podniků začínajících, na certifikaci a dodržování předpisů, mimo jiné na základě transparentních konzultací, a měla by spolupracovat s členskými státy na snižování těchto nákladů. Značné náklady pro poskytovatele a další provozovatele, zejména jedná-li se o poskytovatele a provozovatele menšího rozsahu, mohou představovat například 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 zavádějících subjektů. Za účelem řešení specifických potřeb malých a středních podniků, včetně podniků začínajících, by Komise měla na žádost rady poskytnout standardizované šablony pro oblasti, na něž se vztahuje toto nařízení. Kromě toho by Komise měla doplnit úsilí členských států tím, že všem poskytovatelům a zavádějícím subjektům poskytne jednotnou informační platformu se snadno použitelnými informacemi o tomto nařízení, uspořádá vhodné komunikační kampaně s cílem zvýšit povědomí o povinnostech vyplývajících z tohoto nařízení a vyhodnotí a podpoří sbližování osvědčených postupů při zadávání veřejných zakázek v souvislosti se systémy AI. K těmto podpůrným opatřením by měly mít přístup střední podniky, které donedávna splňovaly kritéria pro malé podniky ve smyslu přílohy doporučení Komise 2003/361/ES ([44]), neboť tyto nové střední podniky mohou někdy postrádat právní zdroje a odbornou přípravu nezbytnou k zajištění řádného porozumění tomuto nařízení a jeho dodržování.

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

(145) K provádění tohoto nařízení 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 včetně podniků začínajících, a oznámených subjektů podle tohoto nařízení, by mohly potenciálně přispět platformy pro AI na vyžádání, evropská centra pro digitální inovace a zkušební a experimentální zařízení zřízená Komisí a členskými státy na unijní nebo vnitrostátní úrovni. Platforma pro AI na vyžádání, evropská centra pro digitální inovace a zkušební a experimentální zařízení mohou v rámci svých úkolů a oblastí působnosti poskytovatelům a oznámeným subjektům poskytovat zejména technickou a vědeckou podporu.

(146) Kromě toho je s ohledem na velmi malou velikost některých provozovatelů a v zájmu zajištění proporcionality, pokud jde o náklady na inovace, vhodné umožnit mikropodnikům, aby jednu z nejnákladnějších povinností, konkrétně zavedení systému řízení kvality, splnily zjednodušeným způsobem, který by snížil jejich administrativní zátěž a náklady, aniž by to ovlivnilo úroveň ochrany a potřebu splňovat požadavky na vysoce rizikové systémy AI. Komise by měla vypracovat pokyny pro upřesnění prvků systému řízení kvality, které mohou mikropodniky realizovat tímto zjednodušeným způsobem.

(147) 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 (EU) 2017/746.

(148) Toto nařízení by mělo vytvořit rámec správy, který umožní koordinovat a podporovat uplatňování tohoto nařízení na vnitrostátní úrovni, jakož i budovat kapacity na úrovni Unie a integrovat zúčastněné strany v oblasti AI. Účinné provádění a prosazování tohoto nařízení vyžaduje rámec správy, který umožní koordinaci a budování ústředních odborných znalostí na úrovni Unie. Úřad pro AI byl zřízen rozhodnutím Komise ([45]) a jeho úkolem je rozvíjet odborné znalosti a schopnosti Unie v oblasti AI a přispívat k provádění práva Unie v oblasti AI. Členské státy by měly usnadnit úkoly úřadu pro AI s cílem podpořit rozvoj odborných znalostí a schopností Unie na úrovni Unie a posílit fungování jednotného digitálního trhu. Kromě toho by měla být zřízena rada složená ze zástupců členských států, vědecká komise pro integraci vědecké obce a poradní fórum, které bude přispívat prostřednictvím zúčastněných stran k provádění tohoto nařízení na unijní a vnitrostátní úrovni. Rozvoj odborných znalostí

([44]) Doporučení Komise ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků (Úř. věst. L 124, 20.5.2003, s. 36).

([45]) Rozhodnutí Komise ze dne 24.1.2024, kterým se zřizuje Evropský úřad pro umělou inteligenci C(2024) 390.

a schopností Unie by měl rovněž zahrnovat využití stávajících zdrojů a odborných znalostí, zejména prostřednictvím synergií se strukturami vytvořenými v souvislosti s vymáháním jiného práva na úrovni Unie a synergií se souvisejícími iniciativami na úrovni Unie, jako je společný podnik EuroHPC a zkušební a experimentální zařízení pro AI v rámci programu Digitální Evropa.

(149) V zájmu usnadnění hladkého, účinného a harmonizovaného provádění tohoto nařízení by měla být zřízena rada. Tato rada by měla odrážet různé zájmy ekosystému AI a měla by se skládat ze zástupců členských států. 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 AI. S cílem poskytnout členským státům určitou flexibilitu při jmenování svých zástupců do rady 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 článkem 33 uvedeného nařízení by Komise měla podporovat činnosti stálé podskupiny pro dozor nad trhem tím, že bude provádět hodnocení trhu nebo studie, 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 Unie, skupinami odborníků a sítěmi působícími v oblasti příslušného práva Unie, zejména s těmi, které působí v oblasti příslušného práva Unie upravujícího data, digitální produkty a služby.

(150) S cílem zajistit zapojení zúčastněných stran do provádění a uplatňování tohoto nařízení by mělo být zřízeno poradní fórum, které by poskytovalo poradenství a technické odborné znalosti radě a Komisi. Aby bylo zajištěno různorodé a vyvážené zastoupení zúčastněných stran mezi komerčními a nekomerčními zájmy, jakož i mezi středními a malými podniky a dalšími podniky v rámci kategorie komerčních zájmů, mělo by poradní fórum zahrnovat mimo jiné průmysl, začínající podniky, malé a střední podniky, akademickou obec, občanskou společnost, včetně sociálních partnerů, jakož i Agenturu pro základní práva, agenturu ENISA, Evropský výbor pro normalizaci (CEN), Evropský výbor pro normalizaci v elektrotechnice (CENELEC) a Evropský ústav pro telekomunikační normy (ETSI).

(151) Na podporu provádění a prosazování tohoto nařízení, zejména monitorovacích činností úřadu pro AI, pokud jde o obecné modely AI, by měla být zřízena vědecká komise složená z nezávislých odborníků. Nezávislí odborníci tvořící vědeckou komisi by měli být vybíráni na základě aktuálních vědeckých nebo technických odborných znalostí v oblasti AI a měli by plnit své úkoly nestranně, objektivně a zajišťovat důvěrnost informací a údajů získaných při plnění svých úkolů a činností. Aby bylo možné posílit vnitrostátní kapacity nezbytné pro účinné prosazování tohoto nařízení, měly by mít členské státy možnost požádat o podporu skupinu odborníků tvořících vědeckou komisi pro své činnosti v oblasti prosazování práva.

(152) S cílem podpořit odpovídající prosazování, pokud jde o systémy AI, a posílit kapacity členských států by měly být zřízeny podpůrné struktury Unie pro testování AI, které by měly být členským státům zpřístupněny.

(153) Při uplatňování a prosazování tohoto nařízení hrají klíčovou roli členské státy. V tomto ohledu by měl každý členský stát určit alespoň jeden oznamující orgán a alespoň jeden orgán dozoru nad trhem jako příslušné vnitrostátní orgány 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. V zájmu zvýšení efektivity organizace na straně členských států a stanovení jednotného kontaktního místa pro veřejnost a další protistrany na úrovni členských států a Unie by měl každý členský stát určit orgán dozoru nad trhem, který bude působit jako jednotné kontaktní místo.

(154) Příslušné vnitrostátní orgány by měly vykonávat své pravomoci nezávisle, nestranně a nezaujatě, aby chránily zásady objektivity svých činností a úkolů a zajistily uplatňování a provádění tohoto nařízení. Členové těchto orgánů by se měli zdržet jakéhokoli jednání neslučitelného s jejich povinnostmi a měli by podléhat pravidlům důvěrnosti podle tohoto nařízení.

(155) Všichni poskytovatelé vysoce rizikových systémů AI by měli mít zaveden systém monitorování po uvedení na trh s cílem zajistit, že budou schopni zohlednit zkušenosti s používáním vysoce rizikových systémů AI při zlepšování svých systémů a procesu návrhu a vývoje, případně že budou schopni včas přijmout veškerá případná nápravná opatření. Monitorování po uvedení na trh by mělo případně zahrnovat analýzu interakce s jinými systémy AI, včetně jiných zařízení a softwaru. Monitorování po uvedení na trh by se nemělo vztahovat na citlivé provozní údaje subjektů zavádějících systémy AI, které jsou donucovacími orgány. Tento systém je rovněž klíčovým předpokladem zajištění účinnějšího a včasnějšího řešení potenciálních rizik vyplývajících ze systémů AI, které se po uvedení na trh nebo do provozu dále „učí". Poskytovatelé by měli mít v této souvislosti rovněž povinnost zavést systém oznamování veškerých závažných incidentů, k nimž dojde v důsledku používání jejich systémů AI, příslušným orgánům, čímž se rozumí incident nebo porucha vedoucí k úmrtí nebo vážnému poškození zdraví, vážnému a nevratnému narušení řízení a provozu kritické infrastruktury, porušení povinností podle práva Unie, jejichž cílem je ochrana základních práv, nebo vážné škody na majetku nebo životním prostředí.

(156) 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 stanovené v tomto nařízení a v nařízení (EU) 2019/1020 a měly by vykonávat své pravomoci a plnit své povinnosti nezávisle, nestranně a nezaujatě. Ačkoli většina systémů AI nepodléhá zvláštním požadavkům a povinnostem podle tohoto nařízení, mohou orgány dozoru nad trhem přijmout opatření ve vztahu ke všem systémům AI, 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 dozor vykonáván, plnit své úkoly nezávisle, pokud tuto nezávislost vyžaduje právo Unie.

(157) 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 úřadů pro ochranu osobních 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 AI, které představují riziko pro zdraví, bezpečnost a základní práva. Postup pro tyto systémy AI představující riziko by se měl vztahovat na vysoce rizikové systémy AI 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 AI, které byly dodány na trh v rozporu s požadavky na transparentnost stanovenými v tomto nařízení a představují riziko.

(158) Právo 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 AI. 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 v rámci svých příslušných pravomocí jako příslušné orgány pro účely dohledu nad prováděním tohoto nařízení, včetně činností dozoru nad trhem ve vztahu k systémům AI poskytovaným nebo používaným finančními institucemi, které jsou předmětem regulace nebo dozoru, určeny příslušné orgány pro účely dohledu nad právními předpisy o finančních službách a jejich vymáhání, zejména příslušné orgány definované v nařízení Evropského parlamentu a Rady (EU) č. 575/2013 ([46]) a ve směrnicích Evropského parlamentu a Rady 2008/48/ES ([47]), 2009/138/ES ([48]), 2013/36/EU ([49]),

([46]) Nařízení Evropského parlamentu a Rady (EU) č. 575/2013 ze dne 26. června 2013 o obezřetnostních požadavcích na úvěrové instituce a investiční podniky a o změně nařízení (EU) č. 648/2012 (Úř. věst. L 176, 27.6.2013, s. 1).

([47]) Směrnice Evropského parlamentu a Rady 2008/48/ES ze dne 23. dubna 2008 o smlouvách o spotřebitelském úvěru a o zrušení směrnice Rady 87/102/EHS (Úř. věst. L 133, 22.5.2008, s. 66).

([48]) Směrnice Evropského parlamentu a Rady 2009/138/ES ze dne 25. listopadu 2009 o přístupu k pojišťovací a zajišťovací činnosti a jejím výkonu (Solventnost II) (Úř. věst. L 335, 17.12.2009, s. 1).

([49]) 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).

2014/17/EU ([50]) a (EU) 2016/97 ([51]), ledaže se členské státy rozhodnou ke splnění těchto úkolů dozoru nad trhem určit orgán jiný. Tyto příslušné orgány by měly mít veškeré pravomoci podle tohoto nařízení a nařízení (EU) 2019/1020, aby mohly prosazovat požadavky a povinnosti podle tohoto nařízení, včetně pravomoci provádět následné činnosti dozoru nad trhem, které mohou být případně začleněny do jejich stávajících mechanismů a postupů dohledu podle příslušného práva 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 (EU) č. 1024/2013 ([52]), měly neprodleně podat Evropské centrální bance zprávu o veškerých informacích zjištěných v průběhu své 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 2013/36/EU 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 zavádějícím subjektům vysoce rizikových systémů AI 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/ES a na zprostředkovatele pojištění podle směrnice (EU) 2016/97 a na další typy finančních institucí, na něž se vztahují požadavky týkající se vnitřní správy, opatření nebo postupů zavedených podle příslušného práva Unie v oblasti finančních služeb, aby byla zajištěna soudržnost a rovné zacházení ve finančním sektoru.

(159) Každý orgán dozoru nad trhem pro vysoce rizikové systémy AI v oblasti biometriky, který je uveden v příloze tohoto nařízení, pokud jsou tyto systémy používány pro účely vymáhání práva, řízení migrace, azylu a kontroly hranic nebo pro účely výkonu spravedlnosti a demokratických procesů, by měl mít účinné vyšetřovací a nápravné pravomoci, včetně přinejmenším pravomoci získat přístup ke všem zpracovávaným osobním údajům a ke všem informacím nezbytným pro plnění svých úkolů. Orgány dozoru nad trhem by měly mít možnost vykonávat své pravomoci zcela nezávisle. Jakýmkoli omezením jejich přístupu k citlivým provozním údajům podle tohoto nařízení by neměly být dotčeny pravomoci, které jim byly svěřeny směrnicí (EU) 2016/680. Žádnou výjimkou z poskytování údajů vnitrostátním úřadům pro ochranu osobních údajů podle tohoto nařízení by neměly být dotčeny stávající ani budoucí pravomoci těchto orgánů nad rámec tohoto nařízení.

(160) Orgány dozoru nad trhem a Komise by měly mít možnost navrhovat společné činnosti, včetně společných šetření, prováděné orgány dozoru nad trhem nebo orgány dozoru nad trhem společně s Komisí, jejichž cílem je podporovat dodržování předpisů, zjišťovat nesoulad, zvyšovat povědomí a poskytovat pokyny v souvislosti s tímto nařízením, pokud jde o konkrétní kategorie vysoce rizikových systémů AI, u nichž se zjistí, že představují vážné riziko ve dvou nebo více členských státech. Společné činnosti na podporu dodržování předpisů by měly být prováděny v souladu s článkem 9 nařízení (EU) 2019/1020. Úřad pro AI by měl pro společná šetření poskytovat koordinační podporu.

(161) Je nezbytné vyjasnit povinnosti a pravomoci na úrovni Unie a na vnitrostátní úrovni, pokud jde o systémy AI, které jsou založeny na obecných modelech AI. Aby se zabránilo překrývání pravomocí, pokud je systém AI založen na obecném modelu AI a daný model a systém poskytuje tentýž poskytovatel, měl by dohled probíhat na úrovni

([50]) Směrnice Evropského parlamentu a Rady 2014/17/EU ze dne 4. února 2014 o smlouvách o spotřebitelském úvěru na nemovitosti určené k bydlení a o změně směrnic 2008/48/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 (Úř. věst. L 60, 28.2.2014, s. 34).
([51]) Směrnice Evropského parlamentu a Rady (EU) 2016/97 ze dne 20. ledna 2016 o distribuci pojištění (Úř. věst. L 26, 2.2.2016, s. 19).
([52]) Nařízení Rady (EU) č. 1024/2013 ze dne 15. října 2013, kterým se Evropské centrální bance svěřují zvláštní úkoly týkající se politik, které se vztahují k obezřetnostnímu dohledu nad úvěrovými institucemi (Úř. věst. L 287, 29.10.2013, s. 63).

Unie prostřednictvím úřadu pro AI, který by za tímto účelem měl mít pravomoci orgánu dozoru nad trhem ve smyslu nařízení (EU) 2019/1020. Ve všech ostatních případech zůstávají za dohled nad systémy AI odpovědné vnitrostátní orgány dozoru nad trhem. V případě obecných systémů AI, které mohou zavádějící subjekty přímo používat alespoň k jednomu účelu, který je klasifikován jako vysoce rizikový, by však orgány dozoru nad trhem měly spolupracovat s úřadem pro AI na provádění hodnocení souladu a odpovídajícím způsobem informovat radu a další orgány dozoru nad trhem. Kromě toho by orgány dozoru nad trhem měly mít možnost požádat úřad pro AI o pomoc v případech, kdy určitý orgán dozoru nad trhem není schopen dokončit šetření týkající se konkrétního vysoce rizikového systému AI, protože nemá možnost získat přístup k určitým informacím týkajícím se obecného modelu AI, na němž je daný vysoce rizikový systém AI postaven. V takových případech by se měl obdobně použít postup týkající se vzájemné pomoci v přeshraničních případech podle kapitoly VI nařízení (EU) 2019/1020.

(162) V zájmu co nejlepšího využití centralizovaných odborných znalostí a synergií Unie na úrovni Unie by pravomoci dohledu nad povinnostmi poskytovatelů obecných modelů AI a jejich vymáhání měly být v pravomoci Komise. Úřad pro AI by měl mít možnost provádět veškerá nezbytná opatření ke sledování účinného provádění tohoto nařízení, pokud jde o obecné modely AI. Měl by mít možnost vyšetřovat případná porušení pravidel pro poskytovatele obecných modelů AI, a to jak z vlastního podnětu, tak na základě výsledků svých monitorovacích činností nebo na žádost orgánů dozoru nad trhem v souladu s podmínkami stanovenými v tomto nařízení. V zájmu podpory účinného sledování ze strany úřadu pro AI by měl tento úřad stanovit možnost, aby navazující poskytovatelé podávali stížnosti na možná porušení pravidel týkajících se poskytovatelů obecných modelů a systémů AI.

(163) S cílem doplnit systémy správy pro obecné modely AI by vědecká komise měla podporovat monitorovací činnosti úřadu pro AI a v některých případech může úřadu pro AI poskytovat kvalifikované výstrahy, které povedou k následným opatřením, jako jsou šetření. Tak by tomu mělo být v případě, kdy má vědecká komise důvod se domnívat, že obecný model AI představuje konkrétní a identifikovatelné riziko na úrovni Unie. Dále by tomu tak mělo být v případě, kdy má vědecká komise důvod se domnívat, že obecný model AI splňuje kritéria, která by vedla ke klasifikaci modelu AI jako obecného modelu AI se systémovým rizikem. Aby vědecká komise měla k dispozici informace nezbytné pro plnění těchto úkolů, měl by existovat mechanismus, na jehož základě může vědecká komise požádat Komisi, aby si vyžádala dokumentaci nebo informace od poskytovatele.

(164) Úřad pro AI by měl mít možnost přijímat nezbytná opatření ke sledování účinného provádění a dodržování povinností poskytovatelů obecných modelů AI stanovených v tomto nařízení. Úřad pro AI by měl mít možnost vyšetřovat případná porušení v souladu s pravomocemi stanovenými v tomto nařízení, mimo jiné si vyžádat dokumentaci a informace, provádět hodnocení a vyžádat si opatření od poskytovatelů obecných modelů AI. Při provádění hodnocení a za účelem využití nezávislých odborných znalostí by měl mít úřad pro AI možnost zapojit nezávislé odborníky, aby prováděli hodnocení jeho jménem. Dodržování povinností by mělo být vymahatelné mimo jiné prostřednictvím žádostí o přijetí vhodných opatření, včetně opatření ke zmírnění rizik v případě zjištěných systémových rizik, jakož i prostřednictvím omezení dodávání daného modelu na trh nebo jeho stažení z trhu či z oběhu. Měla by existovat záruka spočívající v tom, že by poskytovatelé obecných modelů AI disponovali, v případě potřeby nad rámec procesních práv stanovených v tomto nařízení, procesními právy stanovenými v článku 18 nařízení (EU) 2019/1020, která by se měla použít obdobně, aniž jsou dotčena konkrétnější procesní práva stanovená tímto nařízením.

(165) Vývoj systémů AI s výjimkou vysoce rizikových systémů AI v souladu s požadavky tohoto nařízení může vést k rozsáhlejšímu zavádění etické a důvěryhodné AI v Unii. Poskytovatelé systémů AI, které nejsou vysoce rizikové, by měli být vybízeni k vytváření kodexů chování, včetně souvisejících mechanismů správy, určených k podpoře dobrovolného uplatňování některých nebo veškerých povinných požadavků platných pro vysoce rizikové systémy AI, přizpůsobených zamýšlenému účelu systémů a nižšímu souvisejícímu riziku a s přihlédnutím k dostupným technickým řešením a osvědčeným postupům v odvětví, jako jsou modely a datové karty. Poskytovatelé a případně subjekty zavádějící veškeré vysoce rizikové či nerizikové systémy AI a modely AI by také měli být povzbuzováni k tomu, aby dobrovolně uplatňovali další požadavky týkající se například prvků etických pokynů Unie pro zajištění

důvěryhodnosti AI, udržitelnosti životního prostředí, opatření týkajících se gramotnosti v oblasti AI, inkluzivního a rozmanitého návrhu a vývoje systémů AI, včetně pozornosti věnované zranitelným osobám a přístupnosti pro osoby se zdravotním postižením, účasti zúčastněných stran, případně se zapojením příslušných zúčastněných stran, jako jsou podniky a organizace občanské společnosti, akademická obec, výzkumné organizace, odbory a organizace na ochranu spotřebitelů do návrhu a vývoje systémů AI a rozmanitosti vývojových týmů, včetně genderové vyváženosti. Aby se zajistila účinnost dobrovolných kodexů chování, měly by být založeny na jasných cílech a klíčových ukazatelích výkonnosti pro měření plnění těchto cílů. Měly by být rovněž vypracovány inkluzivním způsobem případně se zapojením příslušných zúčastněných stran, jako jsou podniky a organizace občanské společnosti, akademická obec, výzkumné organizace, odbory a organizace na ochranu spotřebitelů. Komise může vyvíjet iniciativy, včetně iniciativ odvětvové povahy, s cílem usnadnit snižování technických překážek bránících přeshraniční výměně dat pro účely rozvoje AI, a to i ohledně infrastruktury pro přístup k datům a sémantické a technické interoperability různých druhů dat.

(166) Je důležité, aby systémy AI související s produkty, které podle tohoto nařízení nejsou vysoce rizikové, a proto nemusí splňovat požadavky, které jsou stanoveny pro vysoce rizikové systémy AI, byly při uvedení na trh nebo do provozu přesto bezpečné. Jako záchranná síť pro přispění k tomuto cíli by se uplatnila nařízení Evropského parlamentu a Rady (EU) 2023/988 ([53]).

(167) 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 unijním a vnitrostátním právem. Své úkoly a činnosti by měly vykonávat tak, aby chránily zejména práva duševního vlastnictví, důvěrné obchodní informace a obchodní tajemství, účinné provádění tohoto nařízení, veřejné a národní bezpečnostní zájmy, integritu trestního a správního řízení a integritu utajovaných informací.

(168) Dodržování tohoto nařízení by mělo být vymahatelné ukládáním sankcí a jiných donucovacích opatření. 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 dodržováním zásady ne bis in idem. Za účelem posílení a harmonizace správních sankcí za porušení tohoto nařízení by měly být stanoveny horní hranice pro stanovení správních pokut za určitá konkrétní porušení. Při posuzování výše pokut by členské státy měly v každém jednotlivém případě zohlednit všechny relevantní okolnosti konkrétní situace, s náležitým ohledem zejména na povahu, závažnost a dobu trvání protiprávního jednání a jeho důsledků a na velikost poskytovatele, zejména pokud je poskytovatelem malý nebo střední podnik nebo začínající podnik. Evropský inspektor ochrany údajů by měl být oprávněn ukládat pokuty orgánům, institucím a subjektům Unie spadajícím do oblasti působnosti tohoto nařízení.

(169) Dodržování povinností uložených poskytovatelům obecných modelů AI podle tohoto nařízení by mělo být vymahatelné mimo jiné prostřednictvím pokut. Za tímto účelem by měly být rovněž stanoveny přiměřené úrovně pokut za porušení těchto povinností, včetně nedodržení opatření požadovaných Komisí v souladu s tímto nařízením, s výhradou přiměřených promlčecích lhůt v souladu se zásadou proporcionality. Všechna rozhodnutí přijatá Komisí podle tohoto nařízení podléhají v souladu se Smlouvou o fungování EU přezkumu Soudním dvorem Evropské unie, včetně neomezené jurisdikce Soudního dvora Evropské unie ve vztahu k sankcím podle článku 261 Smlouvy o fungování EU.

(170) Unijní a vnitrostátní právo již poskytují účinné prostředky ochrany fyzickým a právnickým osobám, jejichž práva a svobody jsou používáním systémů AI nepříznivě ovlivněny. Aniž jsou tyto prostředky ochrany dotčeny, měla by být každá fyzická nebo právnická osoba, která má důvod se domnívat, že došlo k porušení tohoto nařízení, oprávněna podat stížnost příslušnému orgánu dozoru nad trhem.

(171) Dotčené osoby by měly mít právo obdržet vysvětlení, pokud je rozhodnutí zavádějícího subjektu založeno především na výstupech z určitých vysoce rizikových systémů AI, které spadají do oblasti působnosti tohoto nařízení, a pokud toto rozhodnutí má právní účinky nebo se jich podobně významně dotýká způsobem, který podle

([53]) Nařízení Evropského parlamentu a Rady (EU) 2023/988 ze dne 10. května 2023 o obecné bezpečnosti výrobků, o změně nařízení Evropského parlamentu a Rady (EU) č. 1025/2012 a směrnice Evropského parlamentu a Rady (EU) 2020/1828 a o zrušení směrnice Evropského parlamentu a Rady 2001/95/ES a směrnice Rady 87/357/EHS (Úř. věst. L 135, 23.5.2023, s. 1).

jejich názoru má nepříznivý dopad na jejich zdraví, bezpečnost nebo základní práva. Toto vysvětlení by mělo být jasné a smysluplné a mělo by poskytnout základ, na němž mohou dotčené osoby vykonávat svá práva. Právo na vysvětlení by se nemělo vztahovat na používání systémů AI, pro něž vyplývají výjimky nebo omezení z unijního nebo vnitrostátního práva, a mělo by se uplatňovat pouze v rozsahu, v jakém toto právo není již stanoveno právem Unie.

(172) Osoby jednající jako oznamovatelé porušení tohoto nařízení by měly být chráněny právem Unie. Oznamování porušení tohoto nařízení a ochrana osob oznamujících taková porušení by se proto mělo řídit směrnicí Evropského parlamentu a Rady (EU) 2019/1937 ([54]).

(173) Aby bylo zajištěno, 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 podmínek, za nichž systém AI nemá být nepovažován za vysoce rizikový, seznamu vysoce rizikových systémů AI, ustanovení týkajících se technické dokumentace, obsahu EU prohlášení o shodě, ustanovení týkajících se postupů posuzování shody a ustanovení zavádějících vysoce rizikové systémy AI, na které by se měl vztahovat postup posuzování shody založený na posouzení systému řízení kvality a posouzení technické dokumentace, prahových hodnot, referenčních hodnot a ukazatelů, mimo jiné doplněním těchto referenčních hodnot a ukazatelů, pravidel pro klasifikaci obecných modelů AI se systémovým rizikem, kritérií pro určení obecných modelů AI se systémovým rizikem, technické dokumentace pro poskytovatele obecných modelů AI a informací o transparentnosti pro poskytovatele obecných modelů AI. 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 ([55]). 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 přípravě aktů v přenesené pravomoci věnují.

(174) Vzhledem k rychlému technologickému vývoji a technickým odborným znalostem potřebným pro účinné uplatňování tohoto nařízení by Komise měla toto nařízení vyhodnotit a přezkoumat do 2. srpna 2029 a poté každé čtyři roky a podat zprávu Evropskému parlamentu a Radě. Dále by Komise měla s ohledem na důsledky pro oblast působnosti tohoto nařízení jednou ročně provést posouzení potřeby změnit seznam vysoce rizikových systémů AI a seznam zakázaných postupů. Kromě toho by Komise měla do 2. srpna 2028 a poté každé čtyři roky vyhodnotit potřebu změnit seznam nadpisů vysoce rizikových oblastí v příloze tohoto nařízení, systémy AI spadající do oblasti působnosti povinností v oblasti transparentnosti, účinnost systému dohledu a správy a pokrok ve vývoji produktů normalizace pro energeticky účinný vývoj obecných modelů AI, včetně potřeby dalších opatření nebo kroků, a podat o nich zprávu Evropskému parlamentu a Radě. Do 2. srpna 2028 a poté každé tři roky by Komise měla zhodnotit dopad a účinnost dobrovolných kodexů chování, které mají podpořit uplatňování požadavků stanovených pro vysoce rizikové systémy AI v případě jiných než vysoce rizikových systémů AI a případně dalších požadavků na takovéto systémy AI.

(175) 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 ([56]).

(176) Jelikož cíle tohoto nařízení, totiž zlepšit fungování vnitřního trhu a podpořit zavádění důvěryhodné AI zaměřené na člověka při současném zajištění vysoké úrovně ochrany zdraví, bezpečnosti a základních práv zakotvených v Listině, včetně demokracie, právního státu a ochrany životního prostředí před škodlivými účinky systémů AI v Unii

([54]) Směrnice Evropského parlamentu a Rady (EU) 2019/1937 ze dne 23. října 2019 o ochraně osob, které oznamují porušení práva Unie (Úř. věst. L 305, 26.11.2019, s. 17),

([55]) Úř. věst. L 123, 12.5.2016, s. 1.

([56]) 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).

a podpory inovací, nemůže být uspokojivě dosaženo na úrovni členských států, avšak z důvodu rozsahu nebo účinků jich 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.

(177) V zájmu zabezpečení právní jistoty, zajištění vhodného adaptačního období pro provozovatele a zabránění narušení trhu, mimo jiné zajištěním kontinuity používání systémů AI, je vhodné, aby se toto nařízení vztahovalo na vysoce rizikové systémy AI, 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 zamýšleného 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 AI podle tohoto tomto nařízení. Ve výjimečných případech a s ohledem na veřejnou odpovědnost by provozovatelé systémů AI, které jsou součástí rozsáhlých informačních systémů zřízených právními akty uvedenými v příloze tohoto nařízení, a provozovatelé vysoce rizikových systémů AI, které jsou určeny k použití orgány veřejné moci, měli přijmout nezbytná opatření ke splnění požadavků tohoto nařízení do konce roku 2030 a do 2. srpna 2030.

(178) Poskytovatelé vysoce rizikových systémů AI se vyzývají, aby začali dobrovolně plnit příslušné povinnosti vyplývající z tohoto nařízení již během přechodného období.

(179) Toto nařízení by se mělo použít ode dne 2. srpna 2026. S ohledem na nepřijatelné riziko spojené s používáním AI určitými způsoby by se však zákazy, stejně jako obecná ustanovení tohoto nařízení, měly použít již od 2. února 2025. Ačkoli plný účinek těchto zákazů následuje po zavedení správy a prosazování tohoto nařízení, je důležité předvídat uplatňování zákazů, aby se zohlednila nepřijatelná rizika a aby se ovlivnily další postupy, například v občanském právu. Infrastruktura související se správou a se systémem posuzování shody by navíc měla být funkční již před 2. srpnem 2026, a proto by se ustanovení o oznámených subjektech a o struktuře řízení měla použít ode dne 2. srpna 2025. Vzhledem k rychlému tempu technologického pokroku a přijímání obecných modelů AI by povinnosti poskytovatelů obecných modelů AI měly platit od 2. srpna 2025. Kodexy správné praxe by měly být připraveny do 2. května 2025, aby poskytovatelé mohli včas prokázat soulad. Úřad pro AI by měl zajistit, aby klasifikační pravidla a postupy byly aktuální s ohledem na technologický vývoj. 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 se proto použijí ode dne 2. srpna 2025.

(180) Evropský inspektor ochrany údajů a Evropský sbor pro ochranu údajů byli konzultováni v souladu s čl. 42 odst. 1 a 2 nařízení (EU) 2018/1725 a dne 18. června 2021 vydali své společné stanovisko,

PŘIJALY TOTO NAŘÍZENÍ:

KAPITOLA I

OBECNÁ USTANOVENÍ

Článek 1

Předmět

1. Účelem tohoto nařízení je zlepšit fungování vnitřního trhu, podporovat zavádění důvěryhodné umělé inteligence (AI) zaměřené na člověka a zároveň zajistit vysokou úroveň ochrany zdraví, bezpečnosti, základních práv zakotvených v Listině, včetně demokracie, právního státu a ochrany životního prostředí, před škodlivými účinky systémů AI v Unii, jakož i podporovat inovace.

2. Toto nařízení stanoví:

a) harmonizovaná pravidla pro uvádění systémů AI na trh a do provozu a pro jejich používání v Unii;

b) zákazy určitých postupů v oblasti AI;

c) zvláštní požadavky na vysoce rizikové systémy AI a povinnosti provozovatelů těchto systémů;

d) harmonizovaná pravidla transparentnosti pro některé systémy AI;

e) harmonizovaná pravidla pro uvádění obecných modelů AI na trh;

f) pravidla monitorování trhu, dozoru nad trhem a jeho správy a prosazování tohoto nařízení;

g) opatření na podporu inovací se zvláštním zaměřením na malé a střední podniky, včetně podniků začínajících.

Článek 2

Oblast působnosti

1. Toto nařízení se vztahuje na:

a) poskytovatele, kteří v Unii uvádějí na trh nebo do provozu systémy AI nebo uvádějí na trh obecné modely AI bez ohledu na to, zda jsou tito poskytovatelé usazeni nebo se nacházejí v Unii či ve třetí zemi;

b) subjekty, které zavádějí systémy AI a jsou usazeny nebo se nacházejí v Unii;

c) poskytovatele a subjekty, které zavádějí systémy AI, kteří jsou usazeni nebo se nacházejí ve třetí zemi, pokud se výstup systému AI používá v Unii;

d) dovozce a distributory systémů AI;

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

f) zplnomocněné zástupce poskytovatelů, kteří nejsou usazeni v Unii;

g) dotčené osoby, které se nacházejí v Unii.

2. Pro systémy AI klasifikované jako vysoce rizikové systémy AI v souladu s čl. 6 odst. 1, které souvisejí s produkty, na něž se vztahují harmonizační právní předpisy Unie uvedené v příloze I oddíle B, se použijí pouze čl. 6 odst. 1, články 102 až109 a článek 112tohoto nařízení. Článek 57 se použije pouze v případě, že požadavky na vysoce rizikové systémy AI podle tohoto nařízení byly začleněny do uvedených harmonizačních právních předpisů Unie.

3. Toto nařízení se nevztahuje na oblasti mimo oblast působnosti práva Unie a v žádném případě jím nejsou dotčeny pravomoci členských států v oblasti národní bezpečnosti, bez ohledu na typ subjektu, který členské státy pověřily plněním úkolů souvisejících s těmito pravomocemi.

Toto nařízení se nevztahuje na systémy AI pouze tehdy a do té míry, pokud jsou uváděny na trh nebo do provozu nebo jsou používány se změnami nebo bez nich výhradně pro vojenské či obranné účely nebo pro účely národní bezpečnosti, bez ohledu na typ subjektu, který tyto činnosti provádí.

Toto nařízení se nevztahuje na systémy AI, které nejsou uváděny na trh nebo do provozu v Unii, pokud se výstup používá v Unii výhradně pro vojenské či obranné účely nebo pro účely národní bezpečnosti, bez ohledu na typ subjektu, který tyto činnosti provádí.

4. Toto nařízení se nevztahuje ani 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 AI v rámci mezinárodní spolupráce či mezinárodních dohod o vymáhání práva a o justiční spolupráci s Unií nebo s jedním či více členskými státy, a to pod podmínkou, že daná třetí země nebo mezinárodní organizace poskytne přiměřené záruky, pokud jde o ochranu základních práv a svobod fyzických osob.

5. Tímto nařízením není dotčeno uplatňování ustanovení o odpovědnosti poskytovatelů zprostředkovatelských služeb uvedených v kapitole II nařízení (EU) 2022/2065.

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

7. Na osobní údaje zpracovávané v souvislosti s právy a povinnostmi stanovenými v tomto nařízení se vztahuje právo Unie o ochraně osobních údajů, soukromí a důvěrnosti sdělení. Tímto nařízením nejsou dotčena nařízení (EU) 2016/679 nebo (EU) 2018/1725 ani směrnice 2002/58/ES nebo (EU) 2016/680, aniž jsou dotčeny čl. 10 odst. 5 a článek 59 tohoto nařízení.

8. Toto nařízení se nevztahuje na žádné činnosti výzkumu, testování či vývoje v oblasti systémů AI nebo modelů AI před jejich uvedením na trh nebo do provozu. Tyto činnosti jsou prováděny v souladu s platným právem Unie. Uvedená výjimka nezahrnuje testování v reálných podmínkách.

9. Tímto nařízením nejsou dotčena pravidla stanovená jinými právními akty Unie, které se týkají ochrany spotřebitele a bezpečnosti výrobků.

10. Toto nařízení se nevztahuje na povinnosti zavádějících subjektů, které jsou fyzickými osobami a používají systémy AI v rámci čistě osobní neprofesionální činnosti.

11. Toto nařízení nebrání Unii ani členským státům v tom, aby zachovaly nebo zavedly právní a správní předpisy, které jsou příznivější pro pracovníky, pokud jde o ochranu jejich práv v souvislosti s používáním systémů AI zaměstnavateli, nebo které podporují či umožňují uplatňování kolektivních smluv příznivějších pro pracovníky.

12. Toto nařízení se nevztahuje na systémy AI zpřístupněné na základě svobodných licencí a licencí s otevřeným zdrojovým kódem, pokud nejsou uváděny na trh nebo do provozu jako vysoce rizikové systémy AI nebo jako systém AI, na který se vztahuje článek 5 nebo 50.

Článek 3

Definice

Pro účely tohoto nařízení se rozumí:

1) „systémem AI“ strojový systém navržený tak, aby po zavedení fungoval s různými úrovněmi autonomie a který po zavedení může vykazovat adaptabilitu a který za explicitními nebo implicitními účely z obdržených vstupů odvozuje, jak generovat výstupy, jako jsou predikce, obsah, doporučení nebo rozhodnutí, které mohou ovlivnit fyzická nebo virtuální prostředí;

2) „rizikem“ se rozumí kombinace pravděpodobnosti toho, že dojde k újmě, a závažnosti takové újmy;

3) „poskytovatelem“ fyzická nebo právnická osoba, veřejný orgán, agentura nebo jiný subjekt, který vyvíjí systém AI či obecný model AI nebo nechává vyvíjet systém AI či obecný model AI a uvádějí je na trh nebo které uvádějí systém AI do provozu pod svým vlastním jménem, názvem nebo ochrannou známkou, ať už za úplatu, nebo zdarma;

4) „zavádějícím subjektem“ nebo „subjektem, který zavádí“ fyzická nebo právnická osoba, veřejný orgán, agentura nebo jiný subjekt, které v rámci své pravomoci využívá systém AI, s výjimkou případů, kdy je systém AI využíván při osobní neprofesionální činnosti;

5) „zplnomocněným zástupcem“ i fyzická nebo právnická osoba nacházející se nebo usazená v Unii, která od poskytovatele systému AI nebo obecného modelu AI obdržela a přijala písemné pověření k tomu, aby jeho jménem plnila povinnosti a prováděla postupy stanovené tímto nařízením;

6) „dovozcem“ fyzická nebo právnická osoba nacházející se nebo usazená v Unii, která uvádí na trh systém AI označený jménem, názvem nebo ochrannou známkou fyzické nebo právnické osoby usazené ve třetí zemi;

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

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

9) „uvedením na trh“ první dodání systému AI nebo obecného modelu AI na trh Unie;

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

11) „uvedením do provozu“ dodání systému AI k prvnímu použití přímo zavádějícímu subjektu nebo pro vlastní použití v Unii se zamýšleným účelem;

12) „zamýšleným účelem“ použití systému AI zamýšlené 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) „rozumně předvídatelným nesprávným použitím“ použití systému AI způsobem, který není v souladu s jeho zamýšleným účelem, avšak může vyplývat z rozumně předvídatelného lidského chování nebo z interakce s jinými systémy, včetně jiných systémů AI;

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

15) „návodem k použití“ informace poskytnuté poskytovatelem, kterými zavádějící subjekt informuje zejména o zamýšleném účelu a řádném použití daného systému;

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

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

18) „výkonností systému AI“ schopnost systému AI dosáhnout svého zamýšleného účelu;

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

20) „posuzováním shody“ postup prokázání toho, zda byly splněny požadavky stanovené v kapitole III oddíle 2 tohoto nařízení týkající se vysoce rizikového systému AI;

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

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

23) „podstatnou změnou“ změna systému AI po jeho uvedení na trh nebo do provozu, kterou poskytovatel při počátečním posuzování shody nepředvídal ani neplánoval a v jejímž důsledku je ovlivněn soulad systému AI s požadavky stanovenými v kapitole III oddíle 2 tohoto nařízení nebo která vede ke změně zamýšleného účelu, pro který byl systém AI posuzován;

24) „označením CE“ označení, kterým poskytovatel vyjadřuje, že je systém AI ve shodě s požadavky stanovenými v kapitole III oddíle 2 a v dalších příslušných harmonizačních právních předpisech Unie, které upravují umísťování tohoto označení;

25) „systémem monitorování po uvedení na trh“ veškeré činnosti prováděné poskytovateli systémů AI s cílem shromažďovat a přezkoumávat zkušenosti získané v souvislosti s používáním systémů AI, 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“ harmonizovaná norma ve smyslu čl. 2 bodu 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) „trénovacími daty“ data používaná pro trénování systému AI přizpůsobováním jeho parametrů, které lze ovlivnit učením;

30) „validačními daty“ data používaná pro hodnocení trénovaného systému AI a pro vyladění jeho parametrů, které nelze ovlivnit učením, a procesu jeho učení, mimo jiné s cílem zabránit nedostatečnému přizpůsobování nebo nadměrnému přizpůsobování;

31) „souborem validačních dat“ samostatný soubor dat nebo součást souboru trénovacích dat, ať už s pevným, nebo proměnlivým rozdělením;

32) „testovacími daty“ data používaná k zajištění nezávislého zhodnocení systému AI za účelem potvrzení očekávané výkonnosti tohoto systému před jeho uvedením na trh nebo do provozu;

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

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

35) „biometrickou identifikací“ automatizované rozpoznávání fyzických, fyziologických, behaviorálních či psychických lidských znaků za účelem zjištění totožnosti fyzické osoby porovnáním biometrických údajů této osoby s biometrickými údaji jednotlivců, jež jsou uloženy v databázi;

36) „biometrickým ověřením“ automatizované „one-to-one“ ověření totožnosti fyzických osob, včetně autentizace, porovnáním jejich biometrických údajů s dříve poskytnutými biometrickými údaji;

37) „zvláštními kategoriemi osobních údajů“ kategorie osobních údajů uvedené v čl. 9 odst. 1 nařízení (EU) 2016/679, článku 10 směrnice (EU) 2016/680 a čl. 10 odst. 1 nařízení (EU) 2018/1725;

38) „citlivými operativními údaji“ operativní údaje týkající se činností v oblasti prevence, odhalování, vyšetřování nebo stíhání trestných činů, jejichž zpřístupnění by mohlo ohrozit integritu trestního řízení;

39) „systémem rozpoznávání emocí“ systém AI pro účely zjišťování nebo odvozování emocí nebo záměrů fyzických osob na základě jejich biometrických údajů;

40) „systémem biometrické kategorizace“ systém AI pro účely zařazení fyzických osob do určitých kategorií na základě jejich biometrických údajů, pokud není doplňkem k jiné komerční službě a není nezbytně nutný z objektivních technických důvodů;

41) „systémem biometrické identifikace na dálku“ systém AI pro účely identifikace fyzických osob bez jejich aktivního zapojení, obvykle na dálku, na základě porovnání biometrických údajů dané osoby s biometrickými údaji obsaženými v referenční databázi;

42) „systémem biometrické identifikace na dálku v reálném čase“ systém biometrické identifikace na dálku, kdy zachycení biometrických údajů, porovnání a identifikace probíhají bez zbytečného odkladu a zahrnují nejen okamžitou identifikaci, ale také omezená krátká zpoždění, jejichž cílem je zabránit obcházení pravidel;

43) „systémem následné biometrické identifikace na dálku“ systém biometrické identifikace na dálku jiný než systém biometrické identifikace na dálku v reálném čase;

44) „veřejně přístupným prostorem“ jakékoli fyzické místo ve veřejném nebo soukromém vlastnictví přístupné neurčenému počtu fyzických osob bez ohledu na to, zda se mohou uplatňovat určité podmínky přístupu, a bez ohledu na možná omezení kapacity;

45) „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;

46) „vymáháním 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;

47) „úřadem pro AI“ úloha Komise přispívat k zavádění a monitorování systémů AI a obecných modelů AI a k dohledu nad nimi, a správy AI jak je stanoveno v rozhodnutí Komise ze dne 24. ledna. 2024; odkazy na úřad pro AI v tomto nařízení se považují za odkazy na Komisi;

48) „příslušným vnitrostátním orgánem“ oznamující orgán nebo orgán dozoru nad trhem; pokud jde o systémy AI uváděné do provozu nebo používané orgány, institucemi a jinými subjekty Unie, odkazy na příslušné vnitrostátní orgány nebo orgány dozoru nad trhem v tomto nařízení se považují za odkazy na Evropského inspektora ochrany údajů;

49) „závažným incidentem“ incident nebo chybné fungování systému AI, 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 nebo provozu kritické infrastruktury;

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

d) závažné poškození majetku nebo životního prostředí;

50) „osobními údaji“ osobní údaje ve smyslu čl. 4 bodu 1 nařízení (EU) 2016/679;

51) „neosobními údaji“ jiné než osobní údaje ve smyslu čl. 4 bodu 1 nařízení (EU) 2016/679;

52) „profilováním“ profilování ve smyslu čl. 4 bodu 4 nařízení (EU) 2016/679;

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

54) „plánem testování v sandboxu“ dokument dohodnutý mezi zúčastněným poskytovatelem a příslušným orgánem obsahující popis cílů, podmínky, časový rámec, metodiku a požadavky na činnosti prováděné v rámci sandboxu;

55) „regulačním sandboxem pro AI“ kontrolovaný rámec zřízený příslušným orgánem, který poskytovatelům nebo potenciálním poskytovatelům systémů AI nabízí možnost vyvíjet, trénovat, ověřovat a testovat inovativní systém AI, případně v reálných podmínkách, podle plánu testování v sandboxu po omezenou dobu pod regulačním dohledem;

56) „gramotností v oblasti AI“ dovednosti, znalosti a chápání, které poskytovatelům, zavádějícím subjektům a dotčeným osobám umožňují, aby s přihlédnutím k jejich příslušným právům a povinnostem v souvislosti s tímto nařízením zaváděli systémy AI informovaným způsobem a aby si byli vědomi možností a rizik spojených s AI i možných škod, které může způsobit;

57) „testováním v reálných podmínkách“ dočasné testování systému AI pro jeho zamýšlený účel v reálných podmínkách mimo laboratoř nebo jinak simulované prostředí za účelem shromažďování spolehlivých a hodnověrných údajů a posuzování a ověřování shody systému AI s požadavky tohoto nařízení, u něhož nejsou naplněny podmínky spojené s uváděním systému AI na trh nebo do provozu ve smyslu tohoto nařízení, jsou-li splněny všechny podmínky stanovené v článcích 57 nebo 60;

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

59) „informovaným souhlasem“ svobodný, konkrétní, jednoznačný 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;

60) „deep fake“ obrazový, zvukový nebo video obsah vytvořený nebo manipulovaný umělou inteligencí, který se podobá existujícím osobám, objektům, místům subjektům či událostem a který by se dané osobě mohl nepravdivě jevit jako autentický nebo pravdivý;

61) „rozsáhlým porušením práva“ jakékoli jednání nebo opomenutí, které je v rozporu s právem Unie na ochranu zájmů jednotlivců a které:

a) poškodilo nebo by mohlo poškodit společné zájmy jednotlivců s bydlištěm v nejméně dvou jiných členských státech, než je členský stát, v němž:

i) má předmětné jednání nebo opomenutí původ nebo v němž k němu došlo;

ii) je usazen dotčený poskytovatel nebo případně jeho zplnomocněný zástupce, nebo

iii) je usazen zavádějící subjekt, pokud se protiprávního jednání dopustil takový subjekt;

b) poškodilo, poškozuje nebo může poškodit společné zájmy jednotlivců a které má společné rysy, včetně stejných protiprávních praktik nebo porušení téhož zájmu, a vyskytuje se souběžně nejméně ve třech členských státech, přičemž se jej dopouští stejný provozovatel;

62) „kritickou infrastrukturou“ kritická infrastruktura ve smyslu čl. 2 bodu 4 směrnice (EU) 2022/2557;

63) „obecným modelem AI“ model AI, včetně případů, kdy je tento model AI trénován velkým množstvím dat s využitím vlastního dohledu ve velkém měřítku, který vykazuje významnou obecnost a je schopen kompetentně plnit širokou škálu různých úkolů bez ohledu na způsob, jakým je daný model uveden na trh, a který lze začlenit do různých navazujících systémů nebo aplikací, s výjimkou modelů AI, které se používají pro činnosti výzkumu, vývoje nebo činnosti zaměřené na tvorbu prototypů před jejich uvedením na trh;

64) „schopnostmi s velkým dopadem“ schopnosti, které odpovídají schopnostem zaznamenaným v nejpokročilejších obecných modelech AI nebo je překračují;

65) „systémovým rizikem“ riziko, které je specifické pro schopnosti s velkým dopadem u obecných modelů AI, které má významný dopad na trh Unie v důsledku dosahu takových modelů nebo v důsledku skutečných či rozumně předvídatelných negativních dopadů na veřejné zdraví, bezpečnost, veřejnou bezpečnost, základní práva nebo společnost jako celek, které lze šířit ve velkém měřítku v celém hodnotovém řetězci;

66) „obecným systémem AI“ systém AI založený na obecném modelu AI, který je schopen sloužit různým účelům, a to jak pro přímé použití, tak pro integraci do jiných systémů AI;

67) „operací s pohyblivou řádovou čárkou“ jakákoli matematická operace nebo přiřazení zahrnující čísla s pohyblivou řádovou čárkou, což je podmnožina reálných čísel v počítači obvykle reprezentovaných celým číslem s pevně danou přesností, násobeným celočíselným exponentem pevného základu;

68) „navazujícím poskytovatelem“ poskytovatel systému AI, včetně obecného systému AI, který integruje model AI, bez ohledu na to, zda je model AI poskytován tímto samotným poskytovatelem a je vertikálně integrovaný, nebo zda je poskytován jiným subjektem na základě smluvních vztahů.

Článek 4

Gramotnost v oblasti AI

Poskytovatelé systémů AI a subjekty zavádějící AI přijímají opatření, aby v co největší možné míře zajistili dostatečnou úroveň gramotnosti v oblasti AI u svých zaměstnanců i u všech dalších osob, které se jejich jménem zabývají provozem a používáním systémů AI, s přihlédnutím k jejich technickým znalostem, zkušenostem, vzdělání a odborné přípravě a prostředí, v němž mají být systémy AI používány, a s ohledem na osoby nebo skupiny osob, na kterých mají být systémy AI používány.

KAPITOLA II

ZAKÁZANÉ POSTUPY V OBLASTI UMĚLÉ INTELIGENCE

Článek 5

Zakázané postupy v oblasti AI

1. Zakazují se následující postupy v oblasti AI:

a) uvádění na trh, uvádění do provozu nebo používání systémů AI, které využívají podprahových technik mimo vědomí osob nebo záměrně manipulativních či klamavých technik, jejichž cílem nebo důsledkem je podstatné narušení chování osoby nebo skupiny osob tím, že znatelně zhoršují jejich schopnost učinit informované rozhodnutí, což vede k tomu, že přijmou rozhodnutí, které by jinak neučinily, což dotčené osobě, jiné osobě nebo skupině osob způsobuje nebo by s přiměřenou pravděpodobností mohlo způsobit významnou újmu;

b) uvádění na trh, uvádění do provozu nebo používání systémů AI, které využívají zranitelnosti fyzické osoby nebo určité skupiny osob v důsledku jejich věku, zdravotního postižení nebo specifické sociální nebo ekonomické situace a jejichž cílem nebo důsledkem je podstatné narušení chování této osoby nebo osoby náležející k této skupině tak, že to dotčené osobě nebo jiné osobě způsobuje nebo by s přiměřenou pravděpodobností mohlo způsobit významnou újmu;

c) uvádění na trh, uvádění do provozu nebo používání systémů AI pro hodnocení nebo klasifikace fyzických osob nebo skupin osob v určitém časovém úseku na základě jejich sociálního chování nebo známých, odvozených 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 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) uvádění na trh, uvádění do provozu pro tento konkrétní účel nebo používání systémů AI pro posuzování rizik fyzických osob s cílem posoudit nebo předvídat riziko, že fyzická osoba spáchá trestný čin, a to výhradně na základě profilování fyzické osoby nebo posouzení jejích osobnostních znaků a vlastností; tento zákaz se nevztahuje na systémy AI používané na podporu lidského posouzení zaměřeného na zapojení osoby do trestné činnosti, které je již založeno na objektivních a ověřitelných skutečnostech přímo souvisejících s trestnou činností;

e) uvádění na trh, uvádění do provozu pro tento konkrétní účel nebo používání systémů AI, které vytvářejí nebo rozšiřují databáze rozpoznávání obličeje prostřednictvím necíleného získávání zobrazení obličeje z internetu nebo kamerových záznamů;

f) uvádění na trh, uvádění do provozu pro tento konkrétní účel nebo používání systémů AI s cílem odvodit emoce fyzické osoby na pracovišti a ve vzdělávacích institucích, s výjimkou případů, kdy je použití systému AI určeno k zavedení či k uvedení na trh z lékařských nebo bezpečnostních důvodů;

g) uvádění na trh, uvádění do provozu pro tento konkrétní účel nebo používání systémů biometrické kategorizace, které jednotlivě kategorizují fyzické osoby na základě jejich biometrických údajů za účelem dovození nebo odvození jejich rasy, politických názorů, členství v odborových organizacích, náboženského nebo filozofického přesvědčení, sexuálního života nebo sexuální orientace; tento zákaz se nevztahuje na označování nebo filtrování legálně získaných souborů biometrických údajů, jako jsou snímky, na základě biometrických údajů nebo kategorizace biometrických údajů v oblasti vymáhání práva;

h) používání systémů biometrické identifikace na dálku v reálném čase ve veřejně přístupných prostorech pro účely vymáhání práva, pokud to není nezbytně nutné pro jeden z následujících cílů, a jen v nezbytně nutné míře:

i) cílené vyhledávání určitých obětí únosů, obchodování s lidmi nebo sexuálního vykořisťování lidí, jakož i vyhledávání pohřešovaných osob;

ii) prevence konkrétního, závažného a bezprostředního ohrožení života nebo fyzické bezpečnosti fyzických osob nebo skutečného a bezprostředního či skutečného a předvídatelného teroristického útoku;

iii) lokalizace nebo identifikace osoby podezřelé ze spáchání trestného činu, za účelem trestního vyšetřování, stíhání nebo výkonu trestu za trestné činy uvedené v příloze II, za něž lze v dotčeném členském státě uložit trest odnětí svobody nebo ochranné opatření spojené s odnětím osobní svobody v maximální délce nejméně čtyři roky.

Prvním pododstavcem písm. h) není dotčen článek 9 nařízení (EU) 2016/679, pokud jde o zpracování biometrických údajů pro jiné účely, než je vymáhání práva.

2. Používání systémů biometrické identifikace na dálku v reálném čase ve veřejně přístupných prostorech pro účely vymáhání práva pro některý z cílů uvedených v odst. 1 prvním pododstavci písm. h) se zavede pro účely stanovené v daném ustanovení pouze k potvrzení totožnosti konkrétně cílené fyzické osoby a zohlední tyto prvky:

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

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 ve veřejně přístupných prostorech pro účely vymáhání práva pro dosažení kteréhokoli z cílů uvedených v odst. 1 prvním pododstavci písm. h) tohoto článku musí být navíc v souladu s nezbytnými a přiměřenými zárukami a podmínkami ve vztahu k použití podle vnitrostátního práva, jež použití takových systémů povoluje, zejména pokud jde o časová, zeměpisná a osobní omezení. Používání systému biometrické identifikace na dálku v reálném čase ve veřejně přístupných prostorech je povoleno pouze v případě, že donucovací orgán dokončil posouzení dopadů na základní práva podle článku 27 a zaregistroval systém v databázi EU podle článku 49. V řádně odůvodněných naléhavých případech však může být používání těchto systémů zahájeno bez registrace v databázi EU, pokud je tato registrace provedena bez zbytečného odkladu.

3. Pro účely odst. 1 prvního pododstavce písm. h) a odstavce 2 každé použití systému biometrické identifikace na dálku v reálném čase ve veřejně přístupných prostorech pro účely vymáhání práva podléhá předchozímu povolení ze strany justičního orgánu nebo nezávislého správního orgánu, jehož rozhodnutí je závazné a jenž se nachází v členském státě, ve kterém má k tomuto použití dojít, přičemž toto povolení je vydáno na základě odůvodněné žádosti a v souladu s podrobnými pravidly vnitrostátního práva uvedenými v odstavci 5. V řádně odůvodněné naléhavé situaci však může být používání systému zahájeno bez povolení za předpokladu, že se o takové povolení požádá bez zbytečného odkladu, nejpozději do 24 hodin. Je-li takové povolení zamítnuto, použití se s okamžitým účinkem zastaví a veškeré údaje, jakož i výsledky a výstupy tohoto použití se okamžitě vyřadí a vymažou.

Příslušný justiční orgán nebo nezávislý správní orgán, jehož rozhodnutí je závazné, 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 prvním pododstavci písm. h), který je uveden v žádosti, a zejména je omezeno na to, co je nezbytně nutné, pokud jde o dobu, jakož i zeměpisný a osobní rozsah. Při rozhodování o žádosti zohlední tento orgán

skutečnosti uvedené v odstavci 2. Výlučně na základě výstupu systému biometrické identifikace na dálku v reálném čase nelze přijmout žádné rozhodnutí, které má pro určitou osobu nepříznivé právní účinky.

4. Aniž je dotčen odstavec 3, každé použití systému biometrické identifikace na dálku v reálném čase na veřejně přístupných prostorech se pro účely vymáhání práva oznámí příslušnému orgánu dozoru nad trhem a vnitrostátnímu orgánu pro ochranu **osobních** údajů v souladu s vnitrostátními pravidly uvedenými v odstavci 5. Oznámení obsahuje přinejmenším informace uvedené v odstavci 6 a nezahrnuje citlivé operativní údaje.

5. Členský stát se může rozhodnout, že umožní plně nebo částečně povolit používání systémů biometrické identifikace na dálku v reálném čase na veřejně přístupných prostorech pro účely vymáhání práva v mezích a za podmínek uvedených v odst. 1 prvním pododstavci písm. h) a v odstavcích 2 a 3. Dotčené členské státy ve svém vnitrostátním právu stanoví nezbytná podrobná pravidla upravující žádosti o povolení uvedená v odstavci 3, vydávání a výkon těchto povolení, jakož i dohled nad nimi a podávání zpráv o nich. Tato pravidla rovněž stanoví, ve vztahu ke kterému cíli uvedenému v odst. 1 prvním pododstavci písm. h) a ke kterému trestnému činu uvedenému v písm. h) bodu iii) tohoto odstavce lze příslušným orgánům používání těchto systémů pro účely vymáhání práva povolit. Členské státy tato pravidla nejpozději 30 dnů po jejich přijetí oznámí Komisi. Členské státy mohou v souladu s právem Unie zavést přísnější právní předpisy týkající se používání systémů biometrické identifikace na dálku.

6. Vnitrostátní orgány dozoru nad trhem a vnitrostátní orgány pro ochranu osobních údajů členských států, které byly informovány o používání systémů biometrické identifikace na dálku v reálném čase ve veřejně přístupných prostorech pro účely vymáhání práva podle odstavce 4, předkládají Komisi ohledně tohoto používání výroční zprávy. Za tímto účelem poskytne Komise členským státům a vnitrostátním orgánům dozoru nad trhem a orgánům pro ochranu osobních údajů vzor, včetně informací o počtu rozhodnutí přijatých příslušnými justičními orgány nebo nezávislým správním orgánem, jejichž rozhodnutí je v případě žádostí o povolení v souladu s odstavcem 3 závazné, a o jejich výsledku.

7. Pro účely vymáhání práva Komise zveřejňuje výroční zprávy o používání systémů biometrické identifikace na dálku v reálném čase ve veřejně přístupných prostorech, a to na základě souhrnných údajů o členských státech vycházejících z výročních zpráv podle odstavce 6. Tyto výroční zprávy neobsahují citlivé operativní údaje o souvisejících činnostech v oblasti vymáhání práva.

8. Tímto článkem nejsou dotčeny zákazy, které se použijí v případě, že postupy AI porušují jiné právo Unie.

KAPITOLA III

POŽADAVKY NA VYSOCE RIZIKOVÉ SYSTÉMY AI

ODDÍL 1

Klasifikace systémů AI jako vysoce rizikových

Článek 6

Klasifikační pravidla pro vysoce rizikové systémy AI

1. Bez ohledu na to, zda je určitý systém AI uváděn na trh nebo do provozu nezávisle na produktech uvedených v písmenech a) a b), je tento systém AI považován za vysoce rizikový, jsou-li splněny obě následující podmínky:

a) daný systém AI je určen k použití jako bezpečnostní komponenta produktu nebo je samotný tento systém AI produktem, na který se vztahují harmonizační právní předpisy Unie uvedené v příloze I;

b) na produkt, jehož je daný systém AI bezpečnostní komponentou podle bodu a), případně na samotný tento systém AI jako produkt se vztahuje povinnost posouzení shody třetí stranou za účelem uvedení tohoto produktu na trh nebo do provozu podle harmonizačních právních předpisů Unie uvedených v příloze I.

2. Kromě vysoce rizikových systémů AI uvedených v odstavci 1 jsou za vysoce rizikové považovány systémy AI uvedené v příloze III.

3. Odchylně od odstavce 2 se systém AI uvedený v příloze III za vysoce rizikový nepovažuje, pokud nepředstavuje významné riziko újmy na zdraví, bezpečnosti nebo základních právech fyzických osob, a to ani tím, že by podstatně ovlivňoval výsledek rozhodování.

První pododstavec se použije, pokud je splněna některá z následujících podmínek:

a) systém AI je zamýšlen k plnění úzce zaměřeného procesního úkolu;

b) systém AI je zamýšlen ke zlepšení výsledku dříve dokončené lidské činnosti;

c) systém AI je zamýšlen k odhalování vzorců rozhodování nebo odchylek od předchozích vzorců rozhodování a nemá bez řádného lidského přezkumu nahradit nebo ovlivnit dříve dokončené lidské posouzení, nebo

d) systém AI je zamýšlen k provedení přípravného úkolu v rámci posouzení, jež je relevantní pro účely případů použití uvedených v příloze III.

Bez ohledu na první pododstavec se systém AI uvedený v příloze III za vysoce rizikový považuje vždy, pokud provádí profilování fyzických osob.

4. Poskytovatel, který se domnívá, že určitý systém AI uvedený v příloze III není vysoce rizikový, své posouzení zdokumentuje před uvedením tohoto systému na trh nebo do provozu. Na tohoto poskytovatele se vztahuje povinnost registrace stanovená v čl. 49 odst. 2. Na žádost příslušných vnitrostátních orgánů předloží poskytovatel dokumentaci o posouzení.

5. Komise po konzultaci s Evropskou radou pro umělou inteligenci (dále jen „rada“) a nejpozději do 2. února 2026 poskytne pokyny upřesňující praktické provádění tohoto článku v souladu s článkem 96 spolu s úplným seznamem praktických příkladů použití systémů AI, které jsou a které nejsou vysoce rizikové.

6. Komisi je svěřena pravomoc přijmout akty v přenesené pravomoci v souladu s článkem 97 ke změně odst. 3 druhého pododstavce tohoto článku doplněním nových podmínek k podmínkám tam uvedeným nebo změnou těchto podmínek, pokud existují konkrétní a spolehlivé důkazy o existenci systémů AI, které spadají do oblasti působnosti přílohy III, ale nepředstavují významné riziko poškození zdraví, bezpečnosti nebo základních práv fyzických osob.

7. Komise přijme akty v přenesené pravomoci v souladu s článkem 97 ke změně odst. 3 druhého pododstavce tohoto článku zrušením některé z podmínek tam uvedených, pokud existují konkrétní a spolehlivé důkazy o tom, že je to nezbytné pro zachování úrovně ochrany zdraví, bezpečnosti a základních práv v Unii stanovené tímto nařízením.

8. Změna podmínek stanovených v odst. 3 druhém pododstavci přijatá v souladu s odstavci 6 a 7 tohoto článku nesmí snížit celkovou úroveň ochrany zdraví, bezpečnosti a základních práv v Unii stanovenou tímto nařízením a musí zajistit soulad s akty v přenesené pravomoci přijatými podle čl. 7 odst. 1 a zohlednit vývoj trhu a technologií.

Článek 7

Změny přílohy III

1. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 97 za účelem úpravy přílohy III přidáním nebo změnou případů užívání vysoce rizikových systémů AI, pokud jsou splněny obě tyto podmínky:

a) systémy AI jsou určeny pro použití v kterékoli z oblastí uvedených v příloze III;

b) systémy AI představují riziko pro zdraví a bezpečnost nebo riziko nepříznivého dopadu na základní práva, přičemž takové riziko je stejné nebo větší než riziko újmy nebo nepříznivého dopadu, které představují vysoce rizikové systémy AI, jež jsou již uvedeny v příloze III.

2. Při posuzování podmínky podle odst. 1 písm. b) zohlední Komise tato kritéria:

a) zamýšlený účel daného systému AI;

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

c) povahu a množství údajů zpracovávaných a používaných systémem AI, zejména zda jsou zpracovávány zvláštní kategorie osobních údajů;

d) rozsah, v jakém systém AI jedná samostatně, a možnost, aby člověk zrušil rozhodnutí nebo doporučení, která mohou vést k potenciální újmě;

e) do jaké míry již používání systému AI způsobilo újmu na zdraví a bezpečnosti nebo mělo nepříznivý dopad na základní práva nebo vzbudilo významné obavy ohledně pravděpodobnosti takové újmy nebo nepříznivého dopadu, jak vyplývá například ze zpráv nebo zdokumentovaných tvrzení předložených příslušným vnitrostátním orgánům nebo případně z jiných zpráv;

f) potenciální rozsah takové újmy nebo nepříznivého dopadu, zejména pokud jde o jejich intenzitu a způsobilost ovlivnit více osob nebo nepřiměřeně ovlivnit určitou skupinu osob;

g) do jaké míry jsou osoby, které potenciálně utrpěly újmu nebo byly vystaveny nepříznivému dopadu, závislé na výsledku vytvořeném pomocí systému AI zejména proto, že z praktických nebo právních důvodů není rozumně možné účast na tomto výsledku odmítnout;

h) do jaké míry existuje nerovnováha moci či do jaké míry se osoby, které potenciálně utrpěly újmu nebo byly vystaveny nepříznivému dopadu, nacházejí ve zranitelném postavení ve vztahu k zavádějícímu subjektu daného systému AI, zejména v důsledku postavení, autority, znalostí, ekonomických nebo sociálních podmínek nebo věku;

i) do jaké míry je výsledek vytvořený s použitím systému AI snadno opravitelný či zvrátitelný, s přihlédnutí k dostupným technickým řešením pro jeho opravu či zvrácení, přičemž výsledky, které mají nepříznivý dopad na zdraví, bezpečnost nebo základní práva, se za snadno opravitelné či zvrátitelné nepovažují;

j) význam a pravděpodobnost přínosu zavedení systému AI pro jednotlivce, skupiny nebo společnost obecně, včetně možného zlepšení bezpečnosti produktů;

k) do jaké míry stávající právo Unie stanoví:

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

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

3. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 97 za účelem změny seznamu v příloze III spočívající v odstranění vysoce rizikových systémů AI, pokud jsou splněny obě tyto podmínky:

a) dotčený vysoce rizikový systém AI již nepředstavuje 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.

ODDÍL 2

Požadavky na vysoce rizikové systémy AI

Článek 8

Soulad s požadavky

1. Vysoce rizikové systémy AI musí splňovat požadavky stanovené v tomto oddíle, s přihlédnutím k jejich zamýšleným účelům, jakož i k obecně uznávanému stavu AI a technologií, které s AI souvisejí. Při zajišťování souladu s těmito požadavky se zohlední systém řízení rizik uvedený v článku 9.

2. Pokud produkt obsahuje systém AI, na nějž se vztahují požadavky tohoto nařízení i požadavky harmonizačních právních předpisů Unie uvedené v příloze I oddíle A, nesou poskytovatelé odpovědnost za zajištění toho, aby byl jejich produkt plně v souladu se všemi příslušnými požadavky podle platných harmonizačních právních předpisů Unie. Při zajišťování souladu vysoce rizikových systémů AI uvedených v odstavci 1 s požadavky stanovenými v tomto oddíle a v zájmu zajištění konzistentnosti, zamezení zdvojování a minimalizace další zátěže mají poskytovatelé možnost případně začlenit nezbytné procesy testování a podávání zpráv, informace a dokumentaci, které v souvislosti se svým produktem poskytují, do dokumentace a postupů, které již existují a jsou vyžadovány podle harmonizačních právních předpisů Unie uvedených v příloze I oddíle A.

Článek 9

Systém řízení rizik

1. Ve vztahu k vysoce rizikovým systémům AI je 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 AI, který vyžaduje pravidelný systematický přezkum a aktualizaci. Zahrnuje následující kroky:

a) identifikaci a analýzu známých a rozumně předvídatelných rizik, která může vysoce rizikový systém AI používaný v souladu se zamýšleným účelem představovat pro zdraví, bezpečnost nebo základní práva;

b) odhad a vyhodnocení rizik, která mohou vzniknout, když je vysoce rizikový systém AI používán v souladu se zamýšleným účelem a za podmínek rozumně předvídatelného nesprávného použití;

c) hodnocení dalších rizik, která mohou potenciálně vzniknout, na základě analýzy shromážděných údajů ze systému monitorování po uvedení na trh ve smyslu článku 72;

d) přijetí vhodných a cílených opatření k řízení rizik, jež jsou navržena tak, aby řešila rizika zjištěná podle písmene a).

3. Rizika uvedená v tomto článku zahrnují pouze rizika, která lze přiměřeně zmírnit nebo vyloučit vývojem nebo návrhem vysoce rizikového systému AI nebo poskytnutím odpovídajících technických informací.

4. Opatření k řízení rizik uvedená v odst. 2 písm. d) náležitě zohledňují účinky a možnou interakci vyplývající z kombinovaného uplatňování požadavků stanovených v tomto oddíle s cílem účinněji minimalizovat rizika a současně dosáhnout vhodné rovnováhy při provádění opatření ke splnění těchto požadavků.

5. Opatření k řízení rizik uvedená v odst. 2 písm. d) musí být taková, aby bylo příslušné zbytkové riziko spojené s každým nebezpečím a rovněž celkové zbytkové riziko vysoce rizikových systémů AI 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 technicky proveditelného návrhu a vývoje vysoce rizikového systému AI;

b) ve vhodných případech zavedení odpovídajících zmírňujících a kontrolních opatření, jež řeší rizika, která nelze vyloučit;

c) poskytování informací požadovaných podle článku 13 a v případě potřeby školení pro zavádějící subjekty.

Za účelem vyloučení nebo snížení rizik souvisejících s používáním daného vysoce rizikového systému AI by měly být náležitě zváženy technické znalosti, zkušenosti, vzdělání, odborná příprava, které se od zavádějícího subjektu očekává, a předpokládaný kontext, ve kterém má být systém používán.

6. Vysoce rizikové systémy AI jsou testovány za účelem identifikace nejvhodnějších a cílených opatření k řízení rizik. Testování zajistí, aby vysoce rizikové systémy AI podávaly výkony konzistentní s jejich zamýšleným účelem a aby byly v souladu s požadavky stanovenými v tomto oddíle.

7. Testovací postupy mohou zahrnovat testování v reálných podmínkách v souladu s článkem 60.

8. Testování vysoce rizikových systémů AI se provádí podle potřeby kdykoli v průběhu celého procesu vývoje a v každém případě před uvedením na trh nebo do provozu. Testování probíhá na základě předem definovaných metrik a pravděpodobnostních prahových hodnot, které jsou pro zamýšlený účel vysoce rizikového systému AI vhodné.

9. Při zavádění systému řízení rizik popsaného v odstavcích 1 až 7 poskytovatelé zváží, zda je s ohledem na jeho zamýšlený účel pravděpodobné, že vysoce rizikový systém AI bude mít nepříznivý dopad na osoby mladší 18 let a případně na jiné zranitelné skupiny.

10. V případě poskytovatelů vysoce rizikových systémů AI, na něž se vztahují požadavky týkající se vnitřních procesů řízení rizik podle jiných příslušných ustanovení práva Unie, mohou být aspekty popsané v odstavcích 1 až 9 součástí postupů řízení rizik stanovených podle uvedeného práva nebo kombinovány s těmito postupy.

Článek 10

Data a správa dat

1. Vysoce rizikové systémy AI, které využívají techniky zahrnující trénování modelů AI obsahujících data, jsou vyvíjeny na základě souborů trénovacích, validačních a testovacích dat, které splňují kritéria kvality uvedená v odstavcích 2 až 5, a to kdykoli se tyto datové soubory používají.

2. Soubory trénovacích, validačních a testovacích dat podléhají příslušným postupům v oblasti správy a řízení dat, jež jsou pro zamýšlený účel vysoce rizikového systému AI vhodné. Tyto postupy se týkají zejména:

a) příslušných možností návrhu;

b) postupů při sběru dat a původu dat a v případě osobních údajů původního účelu jejich sběru;

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

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

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

f) přezkoumání s ohledem na potenciální zkreslení, která by mohla ovlivnit zdraví a bezpečnost osob, mít nepříznivý dopad na základní práva nebo vést k diskriminaci, která je podle práva Unie zakázána, zejména pokud výstupy dat ovlivňují vstupy pro budoucí operace;

g) vhodná opatření k odhalení, prevenci a zmírnění případných zkreslení zjištěných podle písmene f);

h) identifikace relevantních nedostatků nebo chyb v datech, které brání dodržování tohoto nařízení, a způsobu, jak tyto nedostatky a chyby vyřešit.

3. Soubory trénovacích, validačních a testovacích dat jsou s ohledem na svůj zamýšlený účel relevantní, dostatečně reprezentativní a v maximální možné míře bez chyb a úplné. Mají náležité statistické vlastnosti, a to i případně rovněž s ohledem na osoby nebo skupiny osob, v souvislosti s nimiž má být daný vysoce rizikový systém AI používán. Tyto vlastnosti souborů dat lze splnit na úrovni jednotlivých souborů dat nebo na úrovni jejich kombinací.

4. Soubory trénovacích, validačních a testovacích dat zohledňují v rozsahu nezbytném pro jejich zamýšlený účel vlastnosti nebo prvky, které jsou specifické pro konkrétní zeměpisné, kontextuální, behaviorální nebo funkční prostředí, ve kterém má být daný vysoce rizikový systém AI používán.

5. Pokud je to nezbytně nutné pro zajištění detekce a oprav zkreslení ve vztahu k vysoce rizikovým systémům AI v souladu s odst. 2 písm. f) a g) tohoto článku, mohou poskytovatelé těchto systémů výjimečně zpracovávat zvláštní kategorie osobních údajů s výhradou vhodných záruk týkajících se základních práv a svobod fyzických osob. Kromě ustanovení nařízení (EU) 2016/679 a (EU) 2018/1725 a směrnice (EU) 2016/680musí být ve vztahu k takovému zpracování naplněny všechny tyto podmínky:

a) detekce a opravy zkreslení nelze účinně provést zpracováním jiných údajů, včetně syntetických nebo anonymizovaných údajů;

b) zvláštní kategorie osobních údajů podléhají technickým omezením opakovaného použití osobních údajů, jakož i nejmodernějším bezpečnostním opatřením a opatřením v oblasti ochrany soukromí, včetně pseudonymizace;

c) zvláštní kategorie osobních údajů podléhají opatřením, která zajistí, aby zpracovávané osobní údaje byly zabezpečeny a chráněny a aby se na ně vztahovaly vhodné záruky, včetně přísných kontrol a dokumentace přístupu, s cílem zabránit zneužití a zajistit, aby k těmto osobním údajům měly přístup pouze oprávněné osoby s odpovídajícími povinnostmi zachování důvěrnosti;

d) zvláštních kategorie osobních údajů nejsou přenášeny, převáděny nebo jinak zpřístupněny jiným stranám;

e) zvláštních kategorie osobních údajů se vymažou, jakmile je zkreslení opraveno nebo jakmile u těchto údajů uplyne doba uchovávání, podle toho, co nastane dříve;

f) záznamy o činnostech zpracování podle nařízení (EU) 2016/679 a (EU) 2018/1725 a směrnice (EU) 2016/680 obsahují důvody vedoucí k tomu, že bylo zpracování zvláštních kategorií osobních údajů nezbytně nutné k odhalení a nápravě zkreslení a že tohoto cíle nemohlo být dosaženo zpracováním jiných údajů.

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

Článek 11

Technická dokumentace

1. Před uvedením vysoce rizikového systému AI na trh je vypracována jeho technická dokumentace, jež je pak průběžně aktualizována.

Technická dokumentace je vypracována tak, aby prokazovala, že daný vysoce rizikový systém AI splňuje požadavky stanovené v tomto oddíle, a aby příslušným vnitrostátním orgánům a oznámeným subjektům poskytovala jasné a komplexní informace nezbytné k posouzení souladu systému AI s těmito požadavky. Obsahuje přinejmenším prvky uvedené v příloze IV. Malé a střední podniky, včetně podniků začínajících, mohou poskytnout jednotlivé položky technické dokumentace uvedené v příloze IV zjednodušeným způsobem. Za tímto účelem vytvoří Komise zjednodušený formulář technické dokumentace zaměřený na potřeby malých podniků a mikropodniků. V případě, že se malý nebo střední podnik, včetně podniků začínajících, rozhodne poskytnout informace požadované v příloze IV ve zjednodušeném formátu, použije formulář uvedený v tomto odstavci. Oznámené subjekty tento formulář akceptují pro účely posouzení shody.

2. Pokud je uváděn na trh nebo do provozu vysoce rizikový systém AI související s produktem, na který se vztahují harmonizační právní předpisy Unie uvedené v příloze I oddíle A, vypracuje se jediná technická dokumentace obsahující všechny informace uvedené v odstavci 1, jakož i informace požadované podle těchto právních aktů.

3. Komisi je svěřena pravomoc přijmout akty v přenesené pravomoci v souladu s článkem 97 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 tomto oddíle.

Článek 12

Vedení záznamů

1. Vysoce rizikové systémy AI po dobu svého životního cyklu technicky umožňují automatické zaznamenávání událostí (dále jen „protokoly“).

2. Aby byla zajištěna úroveň sledovatelnosti fungování vysoce rizikového systému AI, která je přiměřená zamýšlenému účelu systému, funkce protokolování umožní zaznamenávání událostí, které jsou relevantní pro:

a) identifikaci situací, které mohou vést k tomu, že daný vysoce rizikový systém AI bude představovat riziko ve smyslu čl. 79 odst. 1 nebo že dojde k podstatné změně;

b) usnadnění monitorování po uvedení na trh uvedené v článku 72, a

c) sledování fungování vysoce rizikových systémů AI podle čl. 26 odst. 5.

3. U vysoce rizikových systémů AI uvedených v bodu 1 písm. a) přílohy III funkce protokolování zajišťuje 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 zavádějícím subjektům

1. Vysoce rizikové systémy AI jsou navrženy a vyvinuty tak, aby bylo jejich fungování dostatečně transparentní a zavádějícím subjektům umožňovalo interpretovat výstup systému a vhodně jej používat. Je zajištěn vhodný typ a stupeň transparentnosti s cílem dosáhnout souladu s příslušnými povinnostmi poskytovatele a zavádějícího subjektu stanovenými v oddíle 3.

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

3. Návod k použití obsahuje alespoň tyto informace:

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

b) vlastnosti, schopnosti a omezení výkonnosti vysoce rizikového systému AI, mezi něž patří:

i) jeho zamýšlený účel;

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

iii) jakékoli známé nebo předvídatelné okolnosti související s používáním daného vysoce rizikového systému AI v souladu s jeho zamýšleným účelem nebo za podmínek rozumně předvídatelného nesprávného použití, které mohou vést k rizikům pro zdraví a bezpečnost nebo pro základní práva uvedeným v čl. 9 odst. 2;

iv) v příslušných případech technické schopnosti a vlastnosti vysoce rizikového systému AI, pokud jde o poskytování informací, které jsou relevantní pro vysvětlení jeho výstupů;

v) v příslušných případech jeho chování ve vztahu ke konkrétním osobám nebo skupinám osob, na něž má být systém používán;

vi) v příslušných případech specifikace vstupních údajů nebo jakýchkoli dalších informací relevantních z hlediska použitých souborů trénovacích, validačních a testovacích dat při zohlednění zamýšleného účelu vysoce rizikového systému AI;

vii) v příslušných případech informace, které zavádějícím subjektům umožní interpretovat výstup vysoce rizikového systému AI a odpovídajícím způsobem jej používat;

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

d) opatření v oblasti lidského dohledu uvedená v článku 14, včetně technických opatření zavedených za účelem usnadnění interpretace výstupů vysoce rizikových systémů AI ze strany zavádějících subjektů;

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

f) v relevantních případech popis mechanismů zahrnutých do vysoce rizikového systému AI, který zavádějícím subjektům umožní řádně shromažďovat, uchovávat a interpretovat protokoly v souladu s článkem 12.

Článek 14

Lidský dohled

1. Vysoce rizikové systémy AI jsou navrženy a vyvinuty takovým způsobem, a to i pomocí vhodných nástrojů rozhraní člověk-stroj, aby na ně mohly během období, kdy jsou používány, 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 AI v souladu s jeho zamýšleným účelem nebo za podmínek rozumně předvídatelného nesprávného použití, zejména pokud tato rizika přetrvávají navzdory uplatňování dalších požadavků stanovených v tomto oddíle.

3. Opatření dohledu jsou úměrná rizikům, úrovni autonomie a kontextu používání vysoce rizikového systému AI a jsou zajištěna jedním nebo oběma z těchto druhů opatření:

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

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

4. Pro účely provádění odstavců 1, 2 a 3 je vysoce rizikový systém AI poskytován zavádějícímu subjektu způsobem, jenž fyzickým osobám pověřeným lidským dohledem umožňuje, pokud je to vhodné a přiměřené, aby:

a) řádně porozuměly příslušným kapacitám a omezením daného vysoce rizikového systému AI a byly schopny náležitě monitorovat jeho fungování, a to i s ohledem na odhalování a řešení anomálií, dysfunkcí a neočekávaného výkonu;

b) si nadále uvědomovaly možnou tendenci automatického nebo nadměrného spoléhání na výstup vysoce rizikového systému AI (dále jen „zkreslení způsobené automatizací“, v angličtině „automation bias“), zejména u vysoce rizikových systémů AI užívaných pro poskytování informací nebo doporučení pro rozhodování fyzických osob;

c) správně interpretovaly výstup vysoce rizikového systému AI, například dostupné interpretační nástroje a metody;

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

e) zasáhly do fungování vysoce rizikového systému AI nebo jej přerušily tlačítkem „stop“ nebo podobným postupem, který umožní systém zastavit v bezpečném módu.

5. U vysoce rizikových systémů AI uvedených v bodě 1 písm. a) přílohy III jsou opatření uvedená v odstavci 3 tohoto článku taková, aby navíc zajišťovala, že na základě identifikace vyplývající z tohoto systému neprovede zavádějící subjekt žádné kroky ani rozhodnutí, pokud tato identifikace nebude samostatně ověřena a potvrzena alespoň dvěma fyzickými osobami, které disponují nezbytnou odbornou způsobilostí, odbornou přípravou a pravomocí.

Požadavek na samostatné ověření nejméně dvěma fyzickými osobami se nevztahuje na vysoce rizikové systémy AI používané pro účely vymáhání práva, migrace, ochrany hranic nebo azylu, pokud unijní nebo vnitrostátní právo považuje uplatňování tohoto požadavku za nepřiměřené.

Článek 15

Přesnost, spolehlivost a kybernetická bezpečnost

1. Vysoce rizikové systémy AI jsou navrženy a vyvinuty tak, aby dosahovaly náležité úrovně přesnosti, spolehlivosti a kybernetické bezpečnosti a aby v tomto ohledu dosahovaly konzistentních výsledků během celého svého životního cyklu.

2. S cílem řešit technické aspekty způsobů měření náležitých úrovní přesnosti a spolehlivosti stanovených v odstavci 1 a jakékoli další relevantní metriky výkonnosti Komise ve spolupráci s příslušnými zúčastněnými stranami a organizacemi, jako jsou metrologické a srovnávací orgány, případně podpoří vypracování referenčních hodnot a metodik měření.

3. Úrovně přesnosti a příslušné metriky přesnosti vysoce rizikových systémů AI jsou oznámeny v přiloženém návodu k použití.

4. Vysoce rizikové systémy AI musí být v nejvyšší možné míře 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. Za tímto účelem se přijmou technická a organizační opatření.

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

Vysoce rizikové systémy AI, které se po uvedení na trh nebo do provozu dále učí, jsou vyvíjeny tak, aby se vyloučilo nebo minimalizovalo riziko případně zkreslených výstupů ovlivňujících vstup pro budoucí operace (dále jen „smyčky zpětné vazby“, v angličtině. „feedback loops“) a aby se zajistilo, že tyto smyčky zpětné vazby budou řádně řešeny formou vhodných zmírňujících opatření.

5. Vysoce rizikové systémy AI jsou odolné proti pokusům neoprávněných třetích stran změnit jejich použití, vstupy nebo výkonnost zneužitím zranitelných míst těchto systémů.

Technická řešení zaměřená na zajištění kybernetické bezpečnosti vysoce rizikových systémů AI odpovídají příslušným okolnostem a rizikům.

Technická řešení umožňující řešení zranitelných míst specifických pro AI v příslušných případech zahrnují opatření pro prevenci, detekci, řešení a kontrolu útoků, které se pokoušejí manipulovat soubory trénovacích dat (tzv. „data poisoning“), případně předtrénovaných komponent používaných při trénování (tzv. „model poisoning“), vstupů, jejichž cílem je přimět daný model AI k tomu, aby udělal chybu (tzv. „matoucí vzory“ nebo „vyhýbání se modelu“), útoků na důvěrnost nebo chyb modelů a také opatření týkající se reakcí na uvedené útoky.

ODDÍL 3

Povinnosti poskytovatelů vysoce rizikových systémů AI, subjektů zavádějících vysoce rizikové systémy AI a dalších stran

Článek 16

Povinnosti poskytovatelů vysoce rizikových systémů AI

Poskytovatelé vysoce rizikových systémů AI:

a) zajišťují, aby jejich vysoce rizikové systémy AI splňovaly požadavky stanovené v oddíle 2;

b) uvedou na vysoce rizikovém systému AI, nebo není-li to možné, na obalu nebo v dokumentaci, která je k vysoce rizikovému systému AI přiložena, své jméno, zapsaný název společnosti nebo zapsanou ochrannou známku a adresu, na které je lze kontaktovat;

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

d) vedou dokumentaci uvedenou v článku 18;

e) pokud jsou vysoce rizikové systémy AI pod jejich kontrolou, zajišťují automatické generování protokolů těmito systémy, jak je uvedeno v článku 19;

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

g) vypracovávají EU prohlášení o shodě v souladu s článkem 47;

h) umístí na vysoce rizikový systém AI, nebo není-li to možné, na jeho obal nebo dokumentaci, která je k němu přiložena, označení CE, aby vyjádřili soulad s tímto nařízením podle článku 48;

i) dodržují povinnosti registrace uvedené v čl. 49 odst. 1;

j) přijímají nezbytná nápravná opatření a poskytují informace, jak je požadováno v článku 20;

k) na odůvodněnou žádost příslušného vnitrostátního orgánu prokáží soulad daného vysoce rizikového systému AI s požadavky stanovenými v oddíle 2;

l) zajistí, aby vysoce rizikový systém AI splňoval požadavky na přístupnost v souladu se směrnicemi (EU) 2016/2102 a (EU) 2019/882.

Článek 17

Systém řízení kvality

1. Poskytovatelé vysoce rizikových systémů AI zavedou 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 AI;

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

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

d) postupy přezkoumání, testování a validace prováděné před vývojem vysoce rizikového systému AI, 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 nebo nepokrývají všechny příslušné požadavky stanovené v oddíle 2, prostředky, které mají být použity k zajištění toho, aby vysoce rizikový systém AI tyto požadavky splňoval;

f) systémy a postupy pro správu dat, včetně získávání, 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 AI 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 72;

i) postupy týkající se ohlašování závažného incidentu v souladu s článkem 73;

j) řešení komunikace s příslušnými vnitrostátními orgány, dalšími příslušnými orgány včetně těch, které zajišťují nebo podporují přístupu k datům, s oznámenými subjekty, s jinými provozovateli, se zákazníky nebo s jinými zúčastněnými stranami;

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 je přiměřené velikosti organizace poskytovatele. Poskytovatelé za všech okolností dodržují míru přísnosti a úroveň ochrany, jež jsou nezbytné k tomu, aby jejich vysoce rizikové systémy AI byly v souladu s tímto nařízením.

3. Poskytovatelé vysoce rizikových systémů AI, na něž se vztahují povinnosti v souvislosti se systémy řízení kvality nebo rovnocennou funkcí podle příslušného odvětvového práva Unie, mohou zahrnout aspekty uvedené v odstavci 1 do systémů řízení kvality stanovených podle uvedeného práva.

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

Článek 18

Uchovávání dokumentace

1. Poskytovatel uchovává po dobu deseti let od uvedení vysoce rizikového systému AI 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) v relevantních případech dokumentaci týkající se změn schválených oznámenými subjekty;

d) v relevantních případech rozhodnutí a další dokumenty vydané oznámenými subjekty;

e) EU prohlášení o shodě podle článku 47.

2. 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.

3. Poskytovatelé, kteří jsou finančními institucemi, na něž se vztahují požadavky týkající se jejich vnitřní správy, systémů nebo postupů podle práva Unie v oblasti finančních služeb, uchovávají technickou dokumentaci jako součást dokumentace vedené podle příslušného práva Unie v oblasti finančních služeb.

Článek 19

Automaticky generované protokoly

1. Uživatelé vysoce rizikových systémů AI, uvedených v čl. 12 odst. 1, uchovávají protokoly automaticky generované jejich vysoce rizikovým systémem AI v rozsahu, v jakém jsou tyto protokoly pod jejich kontrolou. Aniž je dotčeno platné právo Unie nebo vnitrostátní právo, protokoly se uchovávají po dobu odpovídající zamýšlenému účelu vysoce rizikového systému AI, která činí nejméně šest měsíců, nestanoví-li jinak platné právo Unie nebo vnitrostátní právo, zejména právo 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 práva Unie v oblasti finančních služeb, uchovávají protokoly automaticky generované jejich vysoce rizikovými systémy AI jako součást dokumentace vedené podle příslušného práva v oblasti finančních služeb.

Článek 20

Nápravná opatření a informační povinnost

1. Poskytovatelé vysoce rizikových systémů AI, kteří se domnívají nebo mají důvod se domnívat, že vysoce rizikový systém AI, který uvedli na trh nebo do provozu, není s tímto nařízením ve shodě, přijmou okamžitě nezbytná nápravná opatření k uvedení daného systému ve shodu nebo k jeho případnému stažení z trhu či z oběhu nebo k jeho vyřazení z provozu. Náležitě informují distributory dotčeného vysoce rizikového systému AI a v relevantních případech zavádějící subjekty, zplnomocněného zástupce a dovozce.

2. Pokud určitý vysoce rizikový systém AI představuje riziko ve smyslu čl. 79 odst. 1 a poskytovatel se o tomto riziku dozví, neprodleně a případně ve spolupráci s nahlašujícím zavádějícím subjektem prošetří příčiny a informuje orgány dozoru nad trhem příslušné pro daný vysoce rizikový systém AI, a případně oznámený subjekt, který vydal pro daný vysoce rizikový systém AI certifikát podle článku 44, a uvede při tom zejména informace o povaze nesouladu a o všech příslušných nápravných opatřeních, která byla přijata.

Článek 21

Spolupráce s příslušnými orgány

1. Poskytovatelé vysoce rizikových systémů AI předloží příslušnému orgánu na základě odůvodněné žádosti všechny informace a dokumenty nezbytné k prokázání shody vysoce rizikového systému AI s požadavky stanovenými v oddíle 2, a to v jednom z úředních jazyků orgánů Unie stanovených příslušným členským státem, který je danému orgánu snadno srozumitelný.

2. Na základě odůvodněné žádosti příslušného orgánu poskytovatelé rovněž poskytnou žádajícímu příslušnému orgánu přístup k automaticky generovaným protokolům vysoce rizikového systému AI ve smyslu čl. 12 odst. 1 v rozsahu, v jakém jsou tyto protokoly pod jejich kontrolou.

3. S veškerými informacemi obdrženým příslušným orgánem podle tohoto článku se nakládá v souladu s povinnostmi zachování důvěrnosti stanovenými v článku 78.

Článek 22

Zplnomocněný zástupci poskytovatelů vysoce rizikových systémů AI

1. Nežli poskytovatelé usazení ve třetích zemích dodají na trh Unie vysoce rizikové systémy AI, jmenují formou písemného pověření zplnomocněného zástupce usazeného v Unii.

2. Poskytovatel umožní svému zplnomocněnému zástupci provádět úkoly vymezené v pověření, které od poskytovatele obdržel.

3. Zplnomocněný zástupce provádí úkoly vymezené v pověření, které od poskytovatele obdržel. Kopii pověření poskytne na požádání orgánům dozoru nad trhem v jednom z úředních jazyků orgánů Unie určeném příslušným orgánem. Pro účely tohoto nařízení zmocňuje pověření zplnomocněného zástupce k provádění těchto úkolů:

a) ověřit, zda bylo vypracováno EU prohlášení o shodě uvedené v článku 47 a technická dokumentace uvedená v článku 11 a zda poskytovatel provedl příslušný postup posuzování shody;

b) uchovávat pro potřebu příslušných orgánů a vnitrostátních orgánů či subjektů uvedených v čl. 74 odst. 10 po dobu deseti let od uvedení vysoce rizikového systému AI na trh nebo do provozu kontaktní údaje poskytovatele, který zplnomocněného zástupce jmenoval, kopii EU prohlášení o shodě uvedeného v článku 47, technickou dokumentaci a případně certifikát vydaný oznámeným subjektem;

c) poskytnout příslušnému orgánu na odůvodněnou žádost veškeré informace a dokumentaci, včetně informací a dokumentů uvedených v písmenu b) tohoto pododstavce, jež jsou nezbytné k prokázání shody vysoce rizikového systému AI s požadavky stanovenými v oddíle 2, včetně přístupu k protokolům, uvedeným v čl. 12 odst. 1, které daný vysoce rizikový systém AI automaticky generuje, a to v rozsahu, v jakém jsou tyto protokoly pod kontrolou poskytovatele;

d) spolupracovat s příslušnými orgány, na základě odůvodněné žádosti, na veškerých opatřeních, která takový orgán v souvislosti s daným vysoce rizikovým systémem AI přijme, zejména za účelem snížení a zmírnění rizik, která vysoce rizikový systém AI představuje;

e) případně splnit povinnosti registrace uvedené v čl. 49 odst. 1, nebo pokud registraci provádí sám poskytovatel, zajistit, aby informace uvedené v příloze VIII oddíle A bodu 3 byly správné.

Toto pověření zmocňuje zplnomocněného zástupce k tomu, aby se na něj vedle poskytovatele nebo namísto něj obracely příslušné orgány ve všech otázkách týkajících se zajištění souladu s tímto nařízením.

4. Pokud se zplnomocněný zástupce domnívá nebo má důvod se domnívat, že poskytovatel jedná v rozporu se svými povinnostmi podle tohoto nařízení, předmětné pověření ukončí. V takovém případě rovněž neprodleně informuje relevantní orgán dozoru nad trhem, a případně příslušný oznámený subjekt o ukončení pověření a jeho důvodech.

Článek 23

Povinnosti dovozců

1. Před uvedením vysoce rizikového systému AI na trh dovozci zajistí, aby byl systém v souladu s tímto nařízením, a v tomto ohledu ověří, že:

a) poskytovatel daného vysoce rizikového systému AI provedl příslušný postup posuzování shody uvedený v článku 43;

b) poskytovatel vypracoval technickou dokumentaci v souladu s článkem 11 a přílohou IV;

c) systém nese požadované označení CE a je k němu přiloženo EU prohlášení o shodě uvedené v článku 47 a návod k použití;

d) poskytovatel jmenoval zplnomocněného zástupce v souladu s čl. 22 odst. 1.

2. Má-li dovozce dostatečný důvod se domnívat, že určitý vysoce rizikový systém AI není ve shodě s tímto nařízením nebo že je zfalšovaný či je k němu připojena zfalšovaná dokumentace, neuvede tento systém na trh, dokud nebude uveden ve shodu. Pokud daný vysoce rizikový systém AI představuje riziko ve smyslu čl. 79 odst. 1, dovozce o této skutečnosti informuje poskytovatele systému, zplnomocněné zástupce a orgány dozoru nad trhem.

3. Dovozci případně uvedou na obalu nebo v dokumentaci, která je k vysoce rizikovému systému AI 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 AI odpovědnost, skladovací nebo přepravní podmínky případně neohrožovaly jeho soulad s požadavky stanovenými v oddíle 2.

5. Dovozci uchovávají po dobu deseti let od uvedení vysoce rizikového systému AI na trh nebo do provozu kopii případného certifikátu vydaného oznámeným subjektem o návodu k použití a EU prohlášení o shodě uvedeného v článku 47.

6. Dovozci poskytnou relevantním příslušným orgánům na odůvodněnou žádost veškeré informace a dokumentaci, včetně informací a dokumentů podle odstavce 5, jež jsou nezbytné k prokázání shody vysoce rizikového systému AI s požadavky stanovenými v oddíle 2 v jazyce, který je takovým orgánům snadno srozumitelný. Za tímto účelem rovněž zajistí, aby těmto orgánům mohla být zpřístupněna technická dokumentace.

7. Dovozci spolupracují s relevantními příslušnými orgány na veškerých opatřeních, která tyto orgány přijmou v souvislosti s vysoce rizikovým systémem AI, jejž dovozci uvedli na trh, zejména za účelem snížení a zmírnění rizik, která tento systém představuje.

Článek 24

Povinnosti distributorů

1. Před dodáním vysoce rizikového systému AI na trh distributoři ověří, zda je na daném systému umístěno požadované označení CE, zda je k němu přiloženo EU prohlášení o shodě uvedené v článku 47 a návod k použití a zda poskytovatel a případně dovozce systému splnili své příslušné povinnosti stanovené v čl. 16. písm. b) a c) a v čl. 23 odst. 3.

2. Domnívá-li se distributor nebo má-li důvod se domnívat, na základě informací, které má k dispozici, že vysoce rizikový systém AI není ve shodě s požadavky stanovenými v oddíle 2, nedodá tento vysoce rizikový systém AI na trh, dokud nebude uveden s těmito požadavky ve shodu. Pokud navíc tento vysoce rizikový systém AI představuje riziko ve smyslu čl. 79 odst. 1, distributor o této skutečnosti informuje poskytovatele, případně dovozce tohoto systému.

3. Distributoři zajistí, aby v době, kdy nesou za vysoce rizikový systém AI odpovědnost, skladovací nebo přepravní podmínky v příslušných případech neohrožovaly jeho soulad s požadavky stanovenými v oddíle 2.

4. Distributor, který se na základě informací, které má k dispozici, domnívá nebo má důvod se domnívat, že vysoce rizikový systém AI, který dodal na trh, není ve shodě s požadavky stanovenými v oddíle 2, 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 AI riziko ve smyslu čl. 79 odst. 1, distributor okamžitě informuje poskytovatele nebo dovozce systému a orgány příslušné pro dotčený vysoce rizikový systém AI, přičemž uvede podrobnosti, zejména o nesouladu a o veškerých přijatých nápravných opatřeních.

5. Na odůvodněnou žádost relevantního příslušného orgánu poskytnou distributoři vysoce rizikového systému AI tomuto orgánu všechny informace a dokumentaci týkající se jimi přijatých opatření podle odstavců 1 až 4, které jsou nezbytné k prokázání shody tohoto systému s požadavky stanovenými v oddíle 2.

6. Distributoři spolupracují s relevantními příslušnými orgány na veškerých opatřeních, která tyto orgány přijmou v souvislosti s vysoce rizikovým systémem AI, jejž distributoři dodali na trh, zejména za účelem snížení či zmírnění rizik, která tento systém představuje.

Článek 25

Povinnosti v celém hodnotovém řetězci AI

1. Jakýkoli distributor, dovozce, zavádějící subjekt nebo jiná třetí strana se pro účely tohoto nařízení považují za poskytovatele vysoce rizikového systému AI a vztahují se na ně povinnosti poskytovatele podle článku 16, pokud nastane kterákoli z následujících okolností:

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

b) provádějí podstatnou změnu vysoce rizikového systému AI, který je již uveden na trh nebo je již uveden do provozu, a to tak, že zůstává vysoce rizikovým systémem AI v souladu s článkem 6;

c) mění zamýšlený účel systému AI, včetně obecného systému AI, který nebyl klasifikován jako vysoce rizikový a je již uveden na trh nebo do provozu takovým způsobem, že se dotčený systém AI stane vysoce rizikovým systémem AI v souladu s článkem 6.

2. Pokud nastanou okolnosti uvedené v odstavci 1, poskytovatel, který původně uvedl systém AI na trh nebo do provozu, není pro účely tohoto nařízení již nadále považován za poskytovatele tohoto konkrétního systému AI. Tento původní poskytovatel úzce spolupracuje s novými poskytovateli a zpřístupní nezbytné informace a poskytne přiměřeně očekávaný technický přístup a další pomoc, které jsou nezbytné pro plnění povinností stanovených v tomto nařízení, zejména pokud jde o soulad s posuzováním shody vysoce rizikových systémů AI. Tento odstavec se nepoužije v případech, kdy původní poskytovatel jasně stanovil, že jeho systém AI nemá být změněn na vysoce rizikový systém AI, a proto se na něj nevztahuje povinnost předložit dokumentaci.

3. V případě vysoce rizikových systémů AI, které jsou bezpečnostními komponentami produktů, na něž se vztahují harmonizační právní předpisy Unie uvedené v příloze I oddíle A, se za poskytovatele vysoce rizikového systému AI považuje výrobce produktů, na nějž se pak vztahují povinnosti stanovené v článku 16 v případě, že nastane jedna z těchto situací:

a) vysoce rizikový systém AI je uváděn na trh společně s výrobkem pod jménem, názvem nebo ochrannou známkou výrobce produktu;

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

4. Poskytovatel vysoce rizikového systému AI a třetí strana, která dodává systém AI, nástroje, služby, komponenty nebo procesy, které jsou v tomto vysoce rizikovém systému AI používány nebo jsou do něj zabudovány, upřesní prostřednictvím písemné dohody nezbytné informace, schopnosti, technický přístup a jinou pomoc na základě obecně uznávaného stavu techniky, aby poskytovatel vysoce rizikového systému AI mohl v plném rozsahu plnit povinnosti stanovené v tomto nařízení. Tento odstavec se nevztahuje na třetí strany, které na základě svobodné a otevřené licence zpřístupňují veřejnosti jiné nástroje, služby, procesy nebo komponenty, než jsou obecné modely AI.

Úřad pro AI může vypracovat a doporučit dobrovolné vzorové podmínky smluv uzavíraných mezi poskytovateli vysoce rizikových systémů AI a třetími stranami, které dodávají nástroje, služby, komponenty nebo procesy, které jsou používány nebo integrovány do vysoce rizikových systémů AI. Při vypracovávání těchto dobrovolných vzorových podmínek zohlední úřad pro AI možné smluvní požadavky uplatňované v konkrétních odvětvích nebo obchodních případech. Tyto dobrovolné vzorové podmínky se zveřejní a bezplatně zpřístupní ve snadno použitelném elektronickém formátu.

5. Odstavci 2 a 3 není dotčena potřeba dodržovat a chránit práva duševního vlastnictví, důvěrné obchodní informace a obchodní tajemství v souladu s právem Unie a vnitrostátním právem.

Článek 26

Povinnosti zavádějících subjektů vysoce rizikových systémů AI

1. Subjekty zavádějící vysoce rizikové systémy AI přijmou vhodná technická a organizační opatření s cílem zajistit, že tyto systémy budou používány v souladu s návodem k použití přiloženým k těmto systémům na základě odstavců 3 a 6.

2. Zavádějící subjekty pověří lidským dohledem fyzické osoby, které k tomu mají nezbytnou způsobilost, odbornou přípravu a pravomoc, jakož i potřebnou podporu.

3. Povinnostmi uvedenými v odstavcích 1 a 2 nejsou dotčeny ostatní povinnosti zavádějících subjektů podle práva Unie nebo vnitrostátního práva ani volnost zavádějících subjektů při organizaci vlastních zdrojů a činností za účelem provádění opatření v oblasti lidského dohledu uvedených poskytovatelem.

4. Aniž jsou dotčeny odstavce 1 a 2, zavádějící subjekt zajistí v rozsahu, v jakém vykonává kontrolu nad vstupními údaji, aby s ohledem na zamýšlený účel vysoce rizikového systému AI byla vstupní data relevantní a dostatečně reprezentativní.

5. Zavádějící subjekty monitorují provoz vysoce rizikového systému AI na základě návodu k použití a v příslušných případech informují poskytovatele v souladu s článkem 72. Mají-li zavádějící subjekty důvod se domnívat, že používání vysoce rizikového systému AI v souladu s návodem k použití může založit riziko spojené se systémem AI ve smyslu čl. 79 odst. 1, bez zbytečného odkladu o této skutečnosti uvědomí poskytovatele nebo distributora a příslušné orgány dozoru nad trhem a používání systému pozastaví. Zjistí-li zavádějící subjekty závažný incident, neprodleně o tomto incidentu informují nejprve poskytovatele a poté dovozce nebo distributora a příslušné orgány dozoru nad trhem. V případě, že se zavádějícímu subjektu nepodaří poskytovatele kontaktovat, použije se obdobně článek 73. Tato povinnost se nevztahuje na citlivé operativní údaje subjektů zavádějících systémy AI, kteří jsou donucovacími orgány.

V případě zavádějících subjektů, které jsou finančními institucemi, na něž se vztahují požadavky týkající se jejich vnitřní správy, systémů nebo postupů podle práva 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 příslušného práva Unie v oblasti finančních služeb.

6. Subjekty zavádějící vysoce rizikové systémy AI uchovávají protokoly automaticky generované tímto vysoce rizikovým systémem AI v rozsahu, v jakém jsou tyto protokoly pod jejich kontrolou, po dobu odpovídající zamýšlenému účelu vysoce rizikového systému AI, jež není kratší než šest měsíců, pokud platné unijní nebo vnitrostátní právo, zejména právo Unie o ochraně osobních údajů, nestanoví jinak.

Zavádějící subjekty, které jsou finančními institucemi, na něž se vztahují požadavky týkající se jejich vnitřní správy, systémů nebo postupů podle práva Unie v oblasti finančních služeb, uchovávají protokoly jako součást dokumentace vedené podle příslušného práva Unie v oblasti finančních služeb.

7. Zavádějící subjekty, jež jsou zaměstnavateli, před uvedením do provozu nebo používáním vysoce rizikového systému AI na pracovišti informují zástupce zaměstnanců a dotčené pracovníky, že budou používání vysoce rizikového systému AI vystaveni. Tyto informace se případně poskytují jednak v souladu s pravidly a postupy stanovenými v právu Unie a vnitrostátním právu, a jednak v souladu se zvyklostmi pro informování pracovníků a jejich zástupců.

8. Subjekty zavádějící vysoce rizikové systémy AI, jež jsou veřejnými orgány nebo orgány, institucemi nebo jinými subjekty Unie, plní povinnosti registrace uvedené v článku 49. Pokud tyto zavádějící subjekty zjistí, že vysoce rizikový systém AI, který hodlají používat, nebyl zaregistrován v databázi EU uvedené v článku 71, pak tento systém nepoužijí a informují o této skutečnosti poskytovatele nebo distributora.

9. Subjekty zavádějící vysoce rizikové systémy AI v příslušných případech 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 podle článku 27 směrnice (EU) 2016/680.

10. Aniž je dotčena směrnice (EU) 2016/680, subjekt zavádějící vysoce rizikový systém AI pro následnou biometrickou identifikaci na dálku v rámci pátrání za účelem cíleného vyhledávání osoby podezřelé ze spáchání trestného činu nebo odsouzené za trestný čin požádá, buď předem, nebo bez zbytečného odkladu a nejpozději do 48 hodin, justiční orgán nebo správní orgán, jehož rozhodnutí je závazné a podléhá soudnímu přezkumu, o povolení použít daný systém, s výjimkou případů, kdy se tento systém používá k prvotní identifikaci potenciálního podezřelého na základě objektivních a ověřitelných skutečností přímo souvisejících s trestným činem. Každé použití je omezeno na to, co je nezbytně nutné pro vyšetřování konkrétního trestného činu.

Je-li povolení, o něž je požádáno podle prvního pododstavce, zamítnuto, používání systému pro následnou biometrickou identifikaci na dálku spojeného s tímto požadovaným povolením se s okamžitým účinkem ukončí a osobní údaje spojené s používáním daného vysoce rizikového systému AI, pro který bylo o povolení požádáno, se vymažou.

V žádném případě nesmí být tento vysoce rizikový systém AI pro následnou biometrickou identifikaci na dálku používán pro účely vymáhání práva necíleným způsobem, bez jakékoli souvislosti s určitým trestným činem, trestním řízením, skutečnou a aktuální nebo skutečnou a předvídatelnou hrozbou trestného činu nebo pátráním po konkrétní pohřešované osobě. Zajistí se, aby donucovací orgány nemohly výlučně na základě výstupu těchto systémů pro následnou biometrickou identifikaci na dálku přijmout žádné rozhodnutí, které má pro danou osobu nepříznivé právní účinky.

Tímto odstavcem není dotčen článek 9 nařízení (EU) 2016/679 a článek 10 směrnice (EU) 2016/680, pokud jde o zpracování biometrických údajů.

Bez ohledu na účel nebo zavádějící subjekt je každé použití těchto vysoce rizikových systémů AI zdokumentováno v příslušném policejním spisu a na požádání zpřístupněno příslušnému orgánu dozoru nad trhem a vnitrostátnímu orgánu pro ochranu osobních údajů, s výjimkou uvedení citlivých operativních údajů týkajících se vymáhání práva. Tímto pododstavcem nejsou dotčeny pravomoci, které směrnice (EU) 2016/680 svěřuje dozorovým orgánům.

Zavádějící subjekty předkládají příslušným orgánům dozoru nad trhem a vnitrostátním orgánům pro ochranu osobních údajů výroční zprávy, v níž je uvedeno, jak systémy pro následnou biometrickou identifikaci na dálku používají, s výjimkou uvedení citlivých operativních údajů týkajících se vymáhání práva. Zprávy je možné vypracovat souhrnně tak, aby se vztahovali k více než jednomu zavedení systému.

Členské státy mohou v souladu s právem Unie zavést přísnější právní předpisy týkající se používání systémů pro následnou biometrickou identifikaci na dálku.

11. Aniž je dotčen článek 50 tohoto nařízení, subjekty zavádějící vysoce rizikové systémy AI uvedené v příloze III, které přijímají rozhodnutí nebo pomáhají při přijímání rozhodnutí týkajících se fyzických osob, tyto fyzické osoby informují, že jsou použití vysoce rizikového systému AI vystaveny. Na vysoce rizikové systémy AI používané pro účely vymáhání práva se použije článek 13 směrnice (EU) 2016/680.

12. Zavádějící subjekty spolupracují s příslušnými orgány na veškerých opatřeních, která tyto orgány v souvislosti s vysoce rizikovým systémem AI přijmou za účelem provádění tohoto nařízení.

Článek 27

Posouzení dopadu vysoce rizikových systémů AI na základní práva

1. Před zavedením vysoce rizikového systému AI podle čl. 6 odst. 2, s výjimkou vysoce rizikových systémů AI určených k použití v oblasti uvedené v příloze III bodě 2, zavádějící subjekty, které jsou veřejnoprávními nebo soukromými subjekty poskytujícími veřejné služby, a zavádějící subjekty provozující vysoce rizikové systémy AI uvedené v příloze III bodě 5 písm. b) a c) provedou posouzení dopadu na základní práva, který může použití takového systému mít. Za tímto účelem provedou zavádějící subjekty posouzení, které zahrnuje:

a) popis procesů zavádějícího subjektu, v nichž bude vysoce rizikový systém AI používán v souladu s jeho zamýšleným účelem;

b) popis časového období a frekvence plánovaného použití každého z vysoce rizikových systémů AI;

c) kategorie fyzických osob a skupin, které by mohly být jeho používáním v konkrétním kontextu dotčeny;

d) specifická rizika újmy, která by mohla mít dopad na kategorie fyzických osob nebo skupiny osob určených podle písmene c) tohoto odstavce, a to při zohlednění informací dodaných poskytovatelem podle článku 13;

e) popis provádění opatření lidského dohledu, v souladu s návodem k použití;

f) opatření, která mají být přijata v případě naplnění těchto rizik, včetně opatření pro vnitřní správu a mechanismy vyřizování stížností.

2. Povinnost stanovená v odstavci 1 platí pro první použití vysoce rizikového systému AI. Zavádějící subjekt může v podobných případech vycházet z dříve provedeného posouzení dopadů na základní práva nebo ze stávajících posouzení, které provedl poskytovatel. Pokud během použití vysoce rizikového systému AI zavádějící subjekt posoudí, že se některý z prvků uvedených v odstavci 1 změnil nebo již není aktuální, přijme nezbytné kroky k aktualizaci těchto informací.

3. Po provedení posouzení uvedeném v odstavci 1 tohoto článku zavádějící subjekt informuje o jeho výsledcích orgán dozoru na trhem prostřednictvím vyplněného dotazníku uvedeného v odstavci 5 tohoto článku. V případě uvedeném v čl. 46 odst. 1 mohou být zavádějící subjekty od této povinnosti oznámení osvobozeny.

4. Je-li některá z povinností stanovených v tomto článku splněna již na základě posouzení dopadu na ochranu osobních údajů provedeného podle článku 35 nařízení (EU) 2016/679 nebo článku 27 směrnice (EU) 2016/680, potom může posouzení dopadu na základní práva uvedené v odstavci 1 tohoto článku doplnit posouzení dopadu na ochranu osobních údajů.

5. Úřad pro AI vypracuje vzor pro dotazník, a to i prostřednictvím automatizovaného nástroje, aby zavádějícím subjektům usnadnil plnění povinností podle tohoto článku.

ODDÍL 4

Oznamující orgány a oznámené subjekty

Článek 28

Oznamující orgány

1. Každý členský stát určí nebo zřídí alespoň jeden oznamující orgán odpovědný za vytvoření a provádění nezbytných postupů pro posuzování, jmenování a oznamování subjektů posuzování shody a za jejich kontrolu. Tyto postupy se vypracují ve spolupráci mezi oznamujícími orgány všech členských států.

2. Členské státy mohou rozhodnout, že posuzování a monitorování uvedené v odstavci 1 má provést 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 nedošlo ke střetu zájmu se subjekty posuzování shody a aby zabezpečily objektivitu a nestrannost svých činností.

4. Oznamující orgány musí být organizovány takovým způsobem, aby rozhodnutí týkající se oznámení subjektů posuzování shody přijímaly způsobilé osoby odlišné od těch, které provedly posouzení těchto subjektů.

5. Oznamující orgány nesmí nabízet ani poskytovat žádné činnosti, které provádějí subjekty posuzování shody, a nesmí poskytovat poradenské služby na komerčním nebo konkurenčním základě.

6. Oznamující orgány musí chránit důvěrnost informací získaných v souladu s článkem 78.

7. Oznamující orgány musí mít k dispozici přiměřený počet odborně způsobilých pracovníků, aby mohly řádně plnit své úkoly. Odborně způsobilí pracovníci mají podle potřeby nezbytné odborné znalosti pro svou činnost v oblastech, jako jsou informační technologie, AI a právo, včetně dohledu nad základními právy.

Článek 29

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 typů systémů AI, 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 31.

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 31.

4. 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 tohoto článku, a to kdykoli dojde k významným změnám, aby umožnil orgánu odpovědnému za oznámené subjekty kontrolovat a ověřovat nepřetržitý soulad se všemi požadavky stanovenými v článku 31.

Článek 30

Postup oznamování

1. Oznamující orgány mohou oznámit pouze subjekty posuzování shody, které splňují požadavky stanovené v článku 31.

2. K oznámení každého subjektu posuzování shody uvedeného v odstavci 1 Komisi a ostatním členským státům využijí oznamující orgány elektronický nástroj pro oznamování vyvinutý a spravovaný Komisí.

3. Oznámení uvedené v odstavci 2 tohoto článku obsahuje veškeré podrobnosti o dotčených činnostech posuzování shody, modulu nebo modulech posuzování shody a typech systémů AI a příslušné potvrzení o způsobilosti. Pokud se oznámení nezakládá na osvědčení o akreditaci uvedeném v čl. 29 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 31.

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. 29 odst. 2, nebo do dvou měsíců od oznámení, obsahuje-li doklady podle čl. 29 odst. 3.

5. Jsou-li námitky vzneseny, Komise s příslušnými členskými státy a subjektem posuzování shody neprodleně zahájí konzultace. S ohledem na to Komise rozhodne, zda je povolení oprávněné, či nikoli. Rozhodnutí Komise je určeno dotčenému členskému státu a příslušnému subjektu posuzování shody.

Článek 31

Požadavky na oznámené subjekty

1. Oznámený subjekt musí být zřízen podle vnitrostátního práva členského státu a mít právní subjektivitu.

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

3. Organizační struktura, rozdělení odpovědností, způsob podávání zpráv a fungování oznámených subjektů musí být takové, aby byla zajištěna důvěra v provádění a výsledky činností posuzování shody, které oznámené subjekty provádějí.

4. Oznámené subjekty jsou nezávislé na poskytovateli vysoce rizikového systému AI, u něhož provádějí činnosti posuzování shody. Oznámené subjekty jsou rovněž nezávislé na jakémkoliv jiném provozovateli, který má na posuzovaných vysoce rizikových systémech AI zájem, i na jakýchkoliv konkurentech poskytovatele. To nevylučuje používání posuzovaných vysoce rizikových systémů AI, které jsou nezbytné pro činnost subjektu posuzování shody, ani používání takových vysoce rizikových systémů AI pro osobní účely.

5. Subjekt posuzování shody, jeho nejvyšší vedení a pracovníci odpovědní za plnění úkolů posuzování shody se nesmějí přímo podílet na navrhování, vývoji, uvádění na trh nebo používání vysoce rizikových systémů AI ani nesmějí zastupovat strany, které se těmito činnostmi zabývají. Nesmějí vykonávat žádnou činnost, která by mohla ohrozit jejich nezávislý úsudek nebo důvěryhodnost ve vztahu k činnostem posuzování shody, k jejichž vykonávání jsou oznámeni. To platí zejména pro poradenské služby.

6. Oznámené subjekty jsou organizovány a provozovány tak, aby byla zaručena nezávislost, objektivita a nestrannost jejich činností. Oznámené subjekty zdokumentují a zavedou 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.

7. Oznámené subjekty mají zavedeny zdokumentované postupy zajišťující, aby jejich pracovníci, výbory, pobočky, subdodavatelé a jakýkoliv přidružený subjekt nebo pracovníci externích subjektů zachovávali v souladu s článkem 78 důvěrnost informací získaných při provádění činností posuzování shody, s výjimkou případů, kdy je zveřejnění těchto informací vyžadováno dle práva. 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.

8. Oznámené subjekty mají zavedeny postupy pro provádění činností, jež řádně zohledňují velikost poskytovatele, odvětví, v němž působí, jejich strukturu a míru složitosti dotčeného systému AI.

9. 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 jsou usazeny, v souladu s vnitrostátním právem nebo pokud není tento členský stát za posuzování shody sám přímo odpovědný.

10. Oznámené subjekty jsou schopny provádět všechny své úkoly podle tohoto nařízení, na nejvyšší úrovni profesní důvěryhodnosti 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.

11. 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 typů systémů AI, dat a datových výpočtů, jakož i požadavků uvedených v oddíle 2.

12. 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.

Článek 32

Předpoklad shody s požadavky na oznámené subjekty

Pokud subjekt posuzování shody prokáže, že vyhovuje kritériím stanoveným 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 31 v rozsahu, v němž se harmonizované normy na tyto požadavky vztahují.

Článek 33

Dceřiné společnosti oznámených subjektů a zadávání subdodávek

1. Pokud oznámený subjekt zadá konkrétní úkoly týkající se posuzování shody subdodavateli nebo dceřiné společnosti, zajistí, aby subdodavatel nebo dceřiná společnost splňovali požadavky stanovené v článku 31, a informuje o této skutečnosti oznamující orgán.

2. Oznámené subjekty nesou plnou odpovědnost za své úkoly provedené subdodavateli nebo dceřinými společnostmi.

3. Činnosti lze zadat subdodavateli nebo dceřiné společnosti pouze se souhlasem poskytovatele. Oznámené subjekty zveřejní seznam svých dceřiných společností.

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 subdodávky.

Článek 34

Povinnosti týkající se činnosti oznámených subjektů

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

2. Oznámené subjekty se při výkonu svých činností vyvarují zbytečné zátěže pro poskytovatele a náležitě zohlední velikost poskytovatele, odvětví, v němž působí, jeho strukturu a míru složitosti dotčeného vysoce rizikového systému AI, zejména v zájmu na minimalizace administrativní zátěže a nákladů na dodržování předpisů pro mikropodniky a malé podniky ve smyslu doporučení 2003/361/ES. Oznámený subjekt však dodržuje míru přísnosti a úroveň ochrany, jež jsou vyžadovány, aby byl vysoce rizikový systém AI 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 28, aby tento orgán mohl provádět činnosti související s posuzováním, jmenováním, oznamováním a monitorováním a usnadnit posuzování uvedené v tomto oddíle.

Článek 35

Identifikační čísla a seznamy oznámených subjektů

1. Komise přidělí každému oznámenému subjektu jedinečné identifikační číslo, a to i v případě, že je subjekt oznámen na základě více než jednoho aktu Unie.

2. Komise zveřejní seznam subjektů oznámených podle tohoto nařízení, včetně jejich identifikačních čísel 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 relevantní změny oznámení učiněné oznámeným subjektem prostřednictvím elektronického nástroje pro oznamování uvedeného v čl. 30 odst. 2.

2. V případě rozšíření rozsahu oznámení se použijí postupy stanovené v článcích 29 a 30.

V případě jiných změn oznámení, než jsou rozšíření jeho rozsahu, se použijí postupy stanovené v odstavcích 3 až 9.

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

4. Pokud má oznamující orgán dostatečný důvod se domnívat, že oznámený subjekt již nesplňuje požadavky stanovené v článku 31 nebo neplní své povinnosti, prošetří tuto záležitost s maximální péčí. V této souvislosti informuje dotčený oznámený subjekt o vznesených námitkách a poskytne mu možnost, aby se k záležitosti vyjádřil. Pokud oznamující orgán dospěje k závěru, že oznámený subjekt již nesplňuje požadavky stanovené v článku 31 nebo že tento subjekt neplní své povinnosti, omezí, pozastaví nebo případně zruší jmenování, podle toho, jak je neplnění dotyčných požadavků nebo povinností závažné. Neprodleně o této skutečnosti informuje Komisi a ostatní členské státy.

5. Pokud bylo jeho jmenování pozastaveno, omezeno nebo zcela či částečně zrušeno, daný oznámený subjekt o této skutečnosti do 10 dnů uvědomí dotčené výrobce.

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

7. 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 změny jmenování oznámil;

c) požádá oznámený subjekt, aby v přiměřeném časovém období stanoveném tímto orgánem pozastavil nebo zrušil veškeré certifikáty, které byly vydány neoprávněně, s cílem zajistit pokračující shodu vysoce rizikových systémů AI, 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 požádal o pozastavení nebo zrušení; tento orgán přijme v případě potřeby vhodná opatření s cílem zabránit možnému ohrožení zdraví, bezpečnosti nebo základních práv.

8. 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 pro opatření za účelem nápravy nedostatků, jež byly příčinou pozastavení nebo omezení, nebo

b) oznamující orgán 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 stávající certifikáty vydané na období pozastavení nebo omezení a být za ně odpovědný; v případě, že oznamující orgán rozhodne, že oznámený subjekt není způsobilý plnit své funkce ve vztahu ke stávajícím vydaným certifikátům, poskytovatel systému, na nějž se certifikát vztahuje, písemně potvrdí vnitrostátním příslušným orgánům členského státu, ve kterém má poskytovatel systému své registrované místo podnikání, do tří měsíců od pozastavení nebo omezení, že funkce oznámeného subjektu, totiž monitorovat a být nadále odpovědný za certifikáty, převezme dočasně, v době pozastavení nebo omezení, jiný kvalifikovaný oznámený subjekt.

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

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

b) jiný oznámený subjekt písemně potvrdí, že převezme za tyto systémy AI 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 jmenování, o této skutečnosti 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 kvalifikaci oznámeného subjektu nebo o tom, zda oznámený subjekt nadále splňuje požadavky stanovené v článku 31 a své příslušné povinnosti.

2. Oznamující orgán předloží Komisi na vyžádání všechny příslušné informace týkající se oznámení nebo zachování odborné způsobilosti dotčeného oznámeného subjektu.

3. Komise zajistí, aby se se všemi citlivými informacemi získanými v průběhu jejího šetření podle tohoto článku nakládalo jako s důvěrnými v souladu s článkem 78.

4. Pokud Komise zjistí, že oznámený subjekt nesplňuje nebo přestal splňovat požadavky pro své oznámení, informuje o této skutečnosti oznamující členský stát a vyzve ho, aby přijal nezbytná nápravná opatření, včetně případného pozastavení nebo zrušení oznámení. Pokud členský stát nezbytná nápravná opatření nepřijme, může Komise prostřednictvím prováděcího aktu jmenování pozastavit, omezit nebo zrušit. Tento prováděcí akt se přijme přezkumným postupem uvedeným v čl. 98 odst. 2.

Článek 38

Koordinace oznámených subjektů

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

2. Každý oznamující orgán zajistí, aby se jím oznámené subjekty účastnily práce skupiny uvedené v odstavci 1, a to přímo nebo prostřednictvím určených zástupců.

3. Komise zajistí výměnu poznatků a osvědčených postupů mezi oznamujícími orgány.

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 31 nebo zajistí rovnocennou úroveň souladu.

ODDÍL 5

Normy, posuzování shody, osvědčení, registrace

Článek 40

Harmonizované normy a produkty normalizace

1. Předpokládá se, že vysoce rizikové systémy AI nebo obecné modely AI, které jsou ve shodě s harmonizovanými normami nebo jejich částmi, na něž byly zveřejněny odkazy v *Úředním věstníku Evropské unie* v souladu s nařízením (EU) 1025/2012, jsou ve shodě s požadavky stanovenými v oddíle 2 této kapitoly nebo případně s povinnostmi stanovenými v kapitole V oddíle 2 a 3 tohoto nařízení v rozsahu, v jakém se dotyčné normy vztahují na tyto požadavky nebo povinnosti.

2. V souladu s článkem 10 nařízení (EU) č. 1025/2012 Komise bez zbytečného odkladu vydá žádosti o normalizaci týkající se všech požadavků stanovených v oddíle 2 této kapitoly a případně povinností stanovených v kapitole V oddíle 2 a 3 tohoto nařízení. V žádosti o normalizaci se rovněž požadují produkty týkající se postupů podávání zpráv a dokumentace s cílem zlepšit výkonnost systémů AI, pokud jde o zdroje, jako je snížení spotřeby energie a dalších zdrojů u vysoce rizikového systému AI během jeho životního cyklu, a o energeticky účinný vývoj obecných modelů AI. Při přípravě žádosti o normalizaci Komise konzultuje radu a příslušné zúčastněné strany, včetně poradního fóra.

Při vydávání žádosti o normalizaci evropským normalizačním organizacím Komise upřesní, že normy musí být jasné, konzistentní, a to i s normami vypracovanými v různých odvětvích pro produkty, na něž se vztahují stávající právní předpisy Unie v oblasti harmonizace uvedené v příloze I, a zaměřené na zajištění toho, aby vysoce rizikové systémy AI nebo obecné modely AI uváděné na trh nebo do provozu v Unii splňovaly příslušné požadavky nebo povinnosti stanovené v tomto nařízení.

Komise požádá evropské normalizační organizace, aby doložily, že ke splnění cílů uvedených v prvním a druhém pododstavci tohoto odstavce vynakládají v souladu s článkem 24 nařízení EU 1025/2012 maximální úsilí.

3. Účastníci procesu normalizace vynakládají úsilí na podporu investic a inovací v oblasti AI, mimo jiné prostřednictvím zvyšování právní jistoty, jakož i na podporu konkurenceschopnosti a růstu trhu Unie a k podpoře posílení globální spolupráce v oblasti normalizace, přičemž zohledňují stávající mezinárodní normy v oblasti AI, které jsou v souladu s hodnotami, základními právy a zájmy Unie, a zlepšují správu, na níž se podílí více stran, čímž se zajistí vyvážené zastoupení zájmů a účinná účast všech příslušných zúčastněných stran v souladu s články 5, 6 a 7 nařízení (EU) č. 1025/2012.

Článek 41

Společné specifikace

1. Komise může přijímat prováděcí akty, kterými stanoví společné specifikace pro požadavky stanovené v oddíle 2 této kapitoly nebo případně pro povinnosti stanovené v kapitole V oddíle 2 a 3, pokud jsou splněny tyto podmínky:

a) Komise požádala podle čl. 10 odst. 1 nařízení (EU) č. 1025/2012 jednu nebo více evropských normalizačních organizací, aby vypracovaly harmonizovanou normu pro požadavky stanovené v oddíle 2 této kapitoly nebo, v příslušných případech, pro povinnosti stanovené v oddílech 2 a 3 kapitoly V, a:

   i) žádost nebyla žádnou z evropských normalizačních organizací akceptována nebo

ii) harmonizované normy, které byly vypracovány na základě této žádostí, nebyly dodány ve lhůtě stanovené v souladu s čl. 10 odst. 1 nařízení (EU) č. 1025/2012 nebo

iii) příslušné harmonizované normy dostatečně neřeší problémy v oblasti základních práv nebo

iv) harmonizované normy nejsou v souladu s žádostí a

b) v *Úředním věstníku Evropské unie* není zveřejněn odkaz na harmonizované normy, které se vztahují na požadavky uvedené v oddíle 2 této kapitoly nebo, v příslušných případech, na povinnosti uvedené v kapitole V oddíle 2 a 3, v souladu s nařízením (EU) č. 1025/2012, ani se neočekává, že takový odkaz bude v přiměřené lhůtě zveřejněn.

Komise při vypracovávání společných specifikací konzultuje poradní fórum uvedené v článku 67.

Prováděcí akty uvedené v prvním pododstavci tohoto odstavce se přijímají přezkumným postupem podle čl. 98 odst. 2.

2. Komise před vypracováním návrhu prováděcího aktu informuje výbor uvedený v článku 22 nařízení (EU) č. 1025/2012, že považuje podmínky stanovené v odstavci 1 tohoto článku za splněné.

3. Předpokládá se, že vysoce rizikové systémy AI a obecné modely AI, které jsou ve shodě s obecnými specifikacemi uvedenými v odstavci 1, nebo s částmi těchto specifikací, jsou ve shodě s požadavky stanovenými v oddíle 2 této kapitoly nebo, v příslušných případech, v souladu s povinnosti uvedenými v kapitole V oddíle 2 a 3, v rozsahu, v jakém se tyto obecné specifikace vztahují na uvedené požadavky nebo povinnosti.

4. Pokud je harmonizovaná norma evropskou normalizační organizací přijata a Komisi je navrženo, aby odkaz na ni zveřejnila v *Úředním věstníku Evropské unie*, Komise harmonizovanou normu posoudí v souladu s nařízením (EU) č. 1025/2012. Je-li odkaz na harmonizovanou normu zveřejněn v *Úředním věstníku Evropské unie*, Komise zruší prováděcí akty uvedené v odstavci 1 nebo jejich části, které se týkají stejných požadavků stanovených v oddíle 2 této kapitoly nebo, v příslušných případech, stejných povinností stanovených v kapitole V oddíle 2 a 3..

5. Pokud poskytovatelé vysoce rizikových systémů AI nebo obecných modelů AI nejsou ve shodě se společnými specifikacemi uvedenými v odstavci 1, řádně zdůvodní, že přijali technická řešení, která splňují požadavky uvedené v oddíle 2 této kapitoly nebo, v příslušných případech, která jsou v souladu s povinnostmi stanovenými v kapitole V oddíle 2 a 3, v míře, která je s nimi přinejmenším rovnocenná.

6. Pokud se některý členský stát domnívá, že určitá společná specifikace nesplňuje plně základní požadavky uvedené v tomto oddíle nebo, v příslušných případech, není v souladu s povinnostmi stanovenými v kapitole V oddíle 2 a 3, uvědomí o této skutečnosti Komisi s podrobným vysvětlením. Komise tyto informace posoudí a případně změní prováděcí akt, který dotyčnou společnou specifikaci stanoví.

Článek 42

Předpoklad shody s určitými požadavky

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

2. Má se za to, že vysoce rizikové systémy AI, které byly certifikovány nebo pro které bylo vydáno prohlášení o shodě v rámci systému kybernetické bezpečnosti podle nařízení (EU) 2019/881 a na které byl zveřejněn odkaz v *Úředním věstníku Evropské unie*, jsou ve shodě 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 AI uvedených v bodě 1 přílohy III, u nichž poskytovatel při prokazování souladu vysoce rizikového systému AI s požadavky stanovenými v oddíle 2 použil harmonizované normy uvedené v článku 40 nebo v relevantních případech společné specifikace uvedené v článku 41, si poskytovatel zvolí jeden z následujících postupů posuzování shody na základě:

a) interní kontroly uvedené v příloze VI nebo

b) posouzení systému řízení kvality a posouzení technické dokumentace za účasti oznámeného subjektu podle přílohy VII.

Při prokazování souladu vysoce rizikového systému AI s požadavky stanovenými v oddíle 2 se poskytovatel řídí postupem posuzování shody stanoveným v příloze VII, pokud:

a) neexistují harmonizované normy uvedené v článku 40 a nejsou k dispozici společné specifikace uvedené v článku 41;

b) poskytovatel nepoužil harmonizovanou normu nebo použil jen její část;

c) společné specifikace uvedené v písmenu a) existují, ale poskytovatel je nepoužil;

d) jedna nebo více harmonizovaných norem uvedených v písmenu a) byla zveřejněna s omezením a pouze pro tu část normy, která byla omezena.

Pro účely postupu posuzování shody uvedeného v příloze VII si poskytovatel může zvolit kterýkoli z oznámených subjektů. Je-li však vysoce rizikový systém AI určen k uvedení do provozu donucovacími, imigračními nebo azylovými orgány nebo orgány, institucemi a jinými subjekty EU, jedná jako oznámený subjekt orgán dozoru nad trhem uvedený v čl. 74 odst. 8, případně 9.

2. U vysoce rizikových systémů AI uvedených v bodech 2 až 8 přílohy III uplatňují poskytovatelé postup posuzování shody založený na interní kontrole uvedené v příloze VI, který nestanoví zapojení oznámeného subjektu.

3. U vysoce rizikových systémů AI, na které se vztahují právní předpisy Unie v oblasti harmonizace uvedené v oddíle A přílohy I, uplatňuje poskytovatel příslušné postupy posouzení shody, které stanoví uvedené právní akty. Na tyto vysoce rizikové systémy AI se vztahují požadavky stanovené v oddíle 2 této kapitoly, 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 AI s požadavky stanovenými v oddíle 2, pokud byl posouzen soulad těchto oznámených subjektů s požadavky stanovenými v čl. 31 odst. 4, 5, 10 a 11 v rámci postupu pro oznamování podle těchto právních aktů.

Pokud právní akt uvedený v oddíle A přílohy I umožňuje 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 v relevantních případech společné specifikace uvedené v článku 41, které pokrývají všechny požadavky stanovené v oddíle 2 této kapitoly.

4. U vysoce rizikových systémů AI, u kterých již byl postup posuzování shody proveden, musí být proveden nový postup posuzování shody v případě podstatné změny, bez ohledu na to, zda má být změněný systém dále distribuován, nebo zda jej i nadále používá jeho současný zavádějící subjekt.

U vysoce rizikových systémů AI, které se po uvedení na trh nebo do provozu dále učí, nepředstavují změny takového vysoce rizikového systému AI a jeho výkonnosti podstatnou změnu, pokud byly poskytovatelem před stanoveny v okamžiku počátečního posouzení shody a jsou součástí informací obsažených v technické dokumentaci uvedené v bodě 2 písm. f) přílohy IV.

5. Komisi je svěřena pravomoc přijmout akty v přenesené pravomoci v souladu s článkem 97 s cílem změnit přílohy VI a VII jejich aktualizací s ohledem na technický pokrok.

6. Komisi je svěřena pravomoc přijmout akty v přenesené pravomoci v souladu s článkem 97, kterými se mění odstavce 1 a 2 tohoto článku, s cílem podrobit vysoce rizikové systémy AI 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 interní 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, kterou uvádějí a která nepřesáhne pět let pro systémy AI, na něž se vztahuje příloha I, a čtyři roky pro systémy AI, na něž se vztahuje příloha III. Na žádost poskytovatele může být platnost certifikátu prodlužována o další období, z nichž žádné nepřekročí délku pěti let pro systémy AI, na něž se vztahuje příloha I, a čtyři roky pro systémy AI, na něž se vztahuje příloha III, 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 AI již nesplňuje požadavky uvedené v oddíle 2, 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.

Proti rozhodnutím oznámených subjektů, včetně rozhodnutí o vydaných certifikátech shody, je možné se odvolat.

Článek 45

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 veškerých schváleních systému řízení kvality vydaných v souladu s požadavky přílohy VII;

b) o veškerých zamítnutích, omezeních, pozastaveních či 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 unijních certifikátech posouzení technické dokumentace nebo jakýchkoli jejich dodatcích, které zamítl, zrušil, pozastavil či jinak omezil, a na požádání o certifikátech nebo dodatcích k nim, které vydal.

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

4. Oznámené subjekty zajistí v souladu s čl. 78 důvěrnost informací, které obdrží.

Článek 46

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 AI 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 se provádí bez zbytečného odkladu.

2. 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 AI bez povolení uvedeného v odstavci 1, pokud je o takové povolení požádáno bez zbytečného odkladu v průběhu používání nebo po něm. Pokud je povolení uvedené v odstavci 1 zamítnuto, používání vysoce rizikového systému AI se s okamžitým účinkem zastaví a všechny výsledky a výstupy tohoto použití se okamžitě vyřadí.

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

4. Pokud do patnácti kalendářních dnů od obdržení informací uvedených v odstavci 3 proti povolení vydanému orgánem dozoru nad trhem členského státu v souladu s odstavcem 1 žádný členský stát ani Komise nevznesou námitku, považuje se povolení za oprávněné.

5. Pokud některý členský stát do patnácti kalendářních dnů od přijetí oznámení uvedeného v odstavci 3 námitky proti povolení vydanému orgánem dozoru nad trhem jiného členského státu vznese nebo pokud se Komise domnívá, že toto povolení je v rozporu s právem Unie nebo se závěrem členských států ohledně souladu systému podle odstavce 3 neopodstatněné, zahájí Komise s příslušným členským státem neprodleně konzultace. Dotčení provozovatelé jsou konzultováni a mají možnost předložit svá stanoviska. S ohledem na to Komise rozhodne, zda je povolení oprávněné či nikoli. Rozhodnutí Komise je určeno dotčenému členskému státu a příslušným provozovatelům.

6. Pokud Komise považuje povolení za neodůvodněné, orgán dozoru nad trhem dotčeného členského státu jej zruší.

7. U vysoce rizikových systémů AI souvisejících s produkty, na něž se vztahují harmonizační právní předpisy Unie uvedené v oddíle A přílohy I, se použijí pouze odchylky od posuzování shody stanovené v uvedených harmonizačních právních předpisech Unie.

Článek 47

EU prohlášení o shodě

1. Poskytovatel vypracuje pro každý vysoce rizikový systém AI písemné strojově čitelné, fyzické nebo elektronicky podepsané EU prohlášení o shodě a po dobu deseti let od uvedení vysoce rizikového systému AI na trh nebo do provozu je uchovává pro potřebu příslušných vnitrostátních orgánů. V EU prohlášení o shodě je uveden vysoce rizikový systém AI, 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 AI splňuje požadavky stanovené v oddíle 2. EU prohlášení o shodě obsahuje informace stanovené v příloze V a je přeloženo do jazyka, který je snadno srozumitelný příslušným vnitrostátním orgánům v členských státech, v nichž je vysoce rizikový systém AI dodáván na trh nebo uveden 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 veškeré právo Unie, které se vztahuje na daný vysoce rizikový systém AI. 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 oddíle 2. Poskytovatel toto EU prohlášení o shodě podle potřeby průběžně aktualizuje.

5. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 97 za účelem změny přílohy V aktualizací obsahu EU prohlášení o shodě uvedeného v uvedené příloze s cílem zavést prvky, které mohou být nutné s ohledem na technický pokrok.

Článek 48

Označení CE

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

2. U vysoce rizikových systémů AI poskytovaných digitálně se digitální označení CE použije pouze v případě, že je snadno přístupné prostřednictvím rozhraní, z něhož je systém přístupný, nebo prostřednictvím snadno přístupného strojově čitelného kódu nebo jiných elektronických prostředků.

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

4. V relevantních případech následuje za označením CE identifikační číslo oznámeného subjektu odpovědného za postupy posuzování shody stanovené v článku 43. Identifikační číslo oznámeného subjektu umístí sám subjekt, nebo jej umístí podle jeho pokynů poskytovatel nebo jeho zplnomocněný zástupce. Identifikační číslo je rovněž uvedeno ve všech propagačních materiálech, které uvádí, že daný vysoce rizikový systém AI splňuje požadavky na označení CE.

5. Pokud se na vysoce rizikové systémy AI vztahuje jiné právo Unie, které rovněž stanoví připojení označení CE, pak se v tomto označení uvádí, že vysoce rizikové systémy AI splňují také požadavky daného jiného práva.

Článek 49

Registrace

1. Před uvedením vysoce rizikového systému AI uvedeného v příloze III, s výjimkou vysoce rizikových systémů AI podle bodu 2 přílohy III, na trh nebo do provozu poskytovatel nebo případně zplnomocněný zástupce zaregistruje sebe a svůj systém do databáze EU uvedené v článku 71.

2. Před uvedením systému AI, u něhož poskytovatel došel k závěru, že nepředstavuje vysoké riziko podle čl. 6 odst. 3, na trh nebo do provozu tento poskytovatel nebo případně zplnomocněný zástupce zaregistruje sebe a tento systém do databáze EU uvedené v článku 71.

3. Před uvedením do provozu nebo použitím vysoce rizikového systému AI uvedeného v příloze III, s výjimkou vysoce rizikových systémů AI uvedených v bodě 2 přílohy III, zavádějící subjekty, které jsou veřejnými orgány, orgány, institucemi nebo jinými subjekty Unie nebo osobami jednajícími jejich jménem, se zaregistrují, vyberou systém a zaregistrují jeho používání v databázi EU uvedené v článku 71.

4. V případě vysoce rizikových systémů AI uvedených v bodech 1, 6 a 7 přílohy III v oblastech vymáhání práva, migrace, azylu a správy ochrany hranic se registrace uvedená v odstavcích 1, 2 a 3 tohoto článku provádí v zabezpečené neveřejné části databáze EU uvedené v článku 71 a obsahuje v příslušných případech pouze tyto informace uvedené v těchto částech:

a) oddíl A body 1 až 10 přílohy VIII, s výjimkou bodů 6, 8 a 9;

b) oddíl B, body 1 až 5 a body 8 a 9 přílohy VIII;

c) oddíl C body 1 až 3 přílohy VIII;

d) body 1. 2,3 a 5 přílohy IX.

Do těchto konkrétních omezených částí databáze EU uvedených v prvním pododstavci tohoto odstavce mají přístup pouze Komise a vnitrostátní orgány uvedené v čl. 74 odst. 8.

5. Vysoce rizikové systémy AI uvedené v příloze III bodě 2 se registrují na vnitrostátní úrovni.

KAPITOLA IV

POVINNOSTI POSKYTOVATELŮ URČITÝCH SYSTÉMŮ AI A SUBJEKTŮ, JEŽ TYTO SYSTÉMY ZAVÁDĚJÍ, POKUD JDE O TRANSPARENTNOST

Článek 50

Povinnosti poskytovatelů zavádějící subjektů určitých systémů AI, pokud jde o transparentnost

1. Poskytovatelé zajistí, aby systémy AI určené k přímé interakci s fyzickými osobami byly navrhovány a vyvíjeny tak, že dotčené fyzické osoby budou vyrozuměny o tom, že komunikují se systémem AI, není-li tato skutečnost zřejmá 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 AI, které jsou ze zákona oprávněny odhalovat trestné činy, předcházet jim, vyšetřovat je nebo stíhat, s výjimkou případů, kdy jsou tyto systémy k dispozici veřejnosti za účelem hlášení trestných činů.

2. Poskytovatelé systémů AI, včetně obecných systémů AI, vytvářejících syntetický zvukový, obrazový, video nebo textový obsah, zajistí, aby výstupy systému AI byly označeny ve strojově čitelném formátu a zjistitelné jako uměle vytvořené nebo manipulované. Poskytovatelé zajistí, aby jejich technická řešení byla účinná, interoperabilní, robustní a spolehlivá, pokud je to technicky proveditelné, s přihlédnutím ke zvláštnostem a omezením různých druhů obsahu, nákladům na provádění a obecně uznávanému nejmodernějšímu stavu technologií, tak jak mohou být zachyceny v příslušných technických normách. Tato povinnost se neuplatní v rozsahu, v jakém systémy AI plní asistenční funkci pro standardní editaci nebo podstatně nemění vstupní údaje poskytnuté zavádějícím subjektem nebo jejich sémantiku, nebo pokud je to zákonem povoleno k odhalování, prevenci, vyšetřování nebo stíhání trestných činů.

3. Subjekty zavádějící systém rozpoznávání emocí nebo systém biometrické kategorizace informují o provozu systému fyzické osoby, které jsou mu vystaveny, a zpracovávají osobní údaje podle potřeby v souladu s nařízeními (EU) 2016/679 a (EU) 2018/1725 a směrnicí (EU) 2016/680. Tato povinnost se nevztahuje na systémy AI používané pro biometrickou kategorizaci a rozpoznávání emocí, kterým zákon umožňuje odhalovat trestné činy, předcházet jim nebo je vyšetřovat, s výhradou příslušných záruk týkajících se práv a svobod třetích stran a v souladu s právem Unie.

4. Subjekty zavádějící systém AI, který vytváří obrazový, zvukový nebo video obsah představující tzv. „deep fake“ nebo s ním manipuluje, musí zveřejnit, že obsah byl uměle vytvořen nebo s ním bylo manipulováno. Tato povinnost se nevztahuje na případy, kdy je použití povoleno zákonem k odhalování trestných činů, předcházení jim, jejich vyšetřování nebo jejich stíhání. Pokud je obsah součástí zjevně uměleckého, tvůrčího, satirického, fiktivního či obdobného díla nebo programu, povinnosti týkající se transparentnosti stanovené v tomto odstavci jsou omezeny na zveřejnění existence takového vytvořeného nebo zmanipulovaného obsahu vhodným způsobem, který nebrání zobrazení nebo užívání díla.

Subjekty zavádějící systém AI, který vytváří text, jenž je zveřejněn za účelem informování veřejnosti o záležitostech veřejného zájmu, nebo který s takovým textem manipuluje, uvedou, že text byl vytvořen uměle nebo s ním bylo manipulováno. Tato povinnost se nevztahuje na případy, kdy je použití povoleno zákonem k odhalování, prevenci, vyšetřování nebo stíhání trestných činů nebo kdy byl obsah vytvořený umělou inteligencí podroben procesu přezkumu člověkem nebo redakční kontroly a pokud za zveřejnění obsahu nese redakční odpovědnost fyzická nebo právnická osoba.

5. Informace uvedené v odstavcích 1 až 4 se dotčeným fyzickým osobám poskytují jasným a rozlišitelným způsobem nejpozději v době první interakce nebo expozice. Informace musí být v souladu s použitelnými požadavky na přístupnost.

6. Odstavci 1 až 4 nejsou dotčeny požadavky a povinnosti stanovené v kapitole III a nejsou jimi dotčeny další povinnosti týkající se transparentnosti stanovené v unijním nebo vnitrostátním právu pro subjekty zavádějící systémy AI.

7. Úřad pro AI podporuje a usnadňuje vypracování kodexů správné praxe na úrovni Unie s cílem usnadnit účinné provádění povinností týkajících se odhalování a označování uměle vytvořeného nebo manipulovaného obsahu. Komise může přijímat prováděcí akty za účelem schválení těchto kodexů správné praxe v souladu s postupem stanoveným v čl. 56 odst. 6. Pokud se Komise domnívá, že kodex není přiměřený, může přijmout prováděcí akt, kterým se stanoví společná pravidla pro plnění těchto povinností v souladu s přezkumným postupem stanoveným v čl. 98 odst. 2.

KAPITOLA V

OBECNÉ MODELY AI

ODDÍL 1

Klasifikační pravidla

Článek 51

Klasifikace obecných modelů AI jako obecných modelů AI se systémovým rizikem

1. Obecný model AI se klasifikuje jako obecný model AI se systémovým rizikem, pokud splňuje některé z těchto podmínek:

a) má schopnosti s vysokým dopadem vyhodnocené na základě vhodných technických nástrojů a metodik, včetně ukazatelů a referenčních hodnot;

b) na základě rozhodnutí Komise, z moci úřední nebo na základě kvalifikované výstrahy vědecké komise má s ohledem na kritéria stanovená v příloze XIII kapacity nebo dopady rovnocenné těm, které jsou stanoveny v písmenu a).

2. Má se za to, že obecný model AI má schopnosti s velkým dopadem podle odst. 1 písm. a), pokud je kumulativní hodnota výpočtu použitého pro jeho výcvik měřená jako množství výpočetních operací s pohyblivou řádovou čárkou vyšší než 10^{25}.

3. Komise přijme akty v přenesené pravomoci v souladu s článkem 97 za účelem změny prahových hodnot uvedených v odstavcích 1 a 2 tohoto článku, jakož i za účelem doplnění referenčních hodnot a ukazatelů s ohledem na vývoj technologií, jako jsou algoritmická zlepšení nebo zvýšená účinnost hardwaru, aby tyto prahové hodnoty odrážely současný stav techniky.

Článek 52

Postup

1. Pokud všeobecný model AI splňuje podmínku uvedenou v čl. 51 odst. 1 písm. a), oznámí to příslušný poskytovatel neprodleně a v každém případě do dvou týdnů po splnění tohoto požadavku, nebo jakmile bude známo, že bude splněn. Toto oznámení obsahuje informace nezbytné k prokázání toho, že byl splněn příslušný požadavek. Pokud se Komise dozví o obecném modelu AI, který představuje systémová rizika, o němž nebyla informována, může se rozhodnout, že jej označí za model se systémovým rizikem.

2. Poskytovatel obecného modelu AI, který splňuje podmínku uvedenou v čl. 51 odst. 1 písm. a), může spolu se svým oznámením předložit dostatečně podložené argumenty prokazující, že ačkoli obecný model AI výjimečně splňuje tento požadavek, nepředstavuje vzhledem ke svým specifickým vlastnostem systémová rizika, a proto by neměl být klasifikován jako obecný model AI se systémovým rizikem.

3. Pokud Komise dospěje k závěru, že argumenty předložené podle odstavce 2 nejsou dostatečně podložené a příslušný poskytovatel nebyl schopen prokázat, že obecný model AI nepředstavuje vzhledem ke svým specifickým vlastnostem systémová rizika, zamítne tyto argumenty a obecný model AI se považuje za obecný model AI se systémovým rizikem.

4. Komise může určit obecný model AI jako model představující systémová rizika z moci úřední nebo na základě kvalifikované výstrahy vědecké komise podle čl. 90 odst. 1 písm. a) na základě kritérií stanovených v příloze XIII.

Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 97 za účelem změny přílohy XIII prostřednictvím specifikace a aktualizace kritérií uvedených v uvedené příloze.

5. Komise zohlední odůvodněnou žádost poskytovatele, jehož model byl určen jako obecný model AI se systémovým rizikem podle odstavce 4, a může rozhodnout o přehodnocení toho, zda lze na základě kritérií stanovených v příloze XIII mít nadále za to, že představuje systémová rizika. Tato žádost musí obsahovat objektivní, podrobné a nové důvody, které se objevily od rozhodnutí o určení. Poskytovatelé mohou požádat o nové posouzení nejdříve šest měsíců po rozhodnutí o určení. Pokud se Komise po novém posouzení rozhodne zachovat označení jako obecný model AI se systémovým rizikem, mohou poskytovatelé požádat o nové posouzení nejdříve šest měsíců po tomto rozhodnutí.

6. Komise zajistí, aby byl zveřejněn seznam obecných modelů AI se systémovým rizikem, a tento seznam průběžně aktualizuje, aniž je dotčena potřeba dodržovat a chránit práva duševního vlastnictví a důvěrné obchodní informace nebo obchodní tajemství v souladu s právem Unie a vnitrostátním právem.

ODDÍL 2

Povinnosti poskytovatelů obecných modelů AI

Článek 53

Povinnosti poskytovatelů obecných modelů AI

1. Poskytovatelé obecných modelů AI:

a) vypracují a aktualizují technickou dokumentaci modelu, včetně souvisejícího procesu trénování a testování a výsledků jeho hodnocení, která obsahuje alespoň informace stanovené v příloze XI za účelem jejího poskytnutí na požádání úřadu pro AI a příslušným vnitrostátním orgánům;

b) vypracují, aktualizují a zpřístupňují informace a dokumentaci poskytovatelům systémů AI, kteří hodlají obecný model AI začlenit do svých systémů AI. Aniž je dotčena potřeba dodržovat a chránit práva duševního vlastnictví a důvěrné obchodní informace nebo obchodní tajemství v souladu s právem Unie a vnitrostátním právem, informace a dokumentace:

   i) umožní poskytovatelům systémů AI, aby dobře porozuměli schopnostem a omezením všeobecného modelu AI a plnili své povinnosti podle tohoto nařízení; a

   ii) zahrnují přinejmenším prvky uvedené v příloze XII;

c) zavedou politiku pro dodržování práva Unie v oblasti autorského práva a práv souvisejících, a zejména pro určení a dodržování výhrady práv vyjádřené podle čl. 4 odst. 3 směrnice (EU) 2019/790, a to i prostřednictvím nejmodernějších technologií;

d) vypracují a zveřejní dostatečně podrobné shrnutí obsahu používaného pro odbornou přípravu obecného modelu AI podle vzoru poskytnutého úřadem pro AI.

2. Povinnosti stanovené v odst. 1 písm. a) a b) se nevztahují na poskytovatele modelů AI, jež jsou zpřístupňovány na základě svobodné a otevřené licence, která umožňuje přístup k modelu, jeho používání, úpravu a distribuci, a jejichž parametry, včetně vah, informací o architektuře modelu a informací o používání modelu, jsou veřejně dostupné. Tato výjimka se nevztahuje na obecné modely AI se systémovými riziky.

3. Poskytovatelé obecných modelů AI podle potřeby spolupracují při výkonu svých kompetencí a pravomocí podle tohoto nařízení s Komisí a příslušnými vnitrostátními orgány.

4. Poskytovatelé obecných modelů AI mohou při prokazování souladu s povinnostmi stanovenými v odstavci 1 tohoto článku vycházet z kodexů správné praxe ve smyslu článku 56, dokud nebude zveřejněna harmonizovaná norma. Soulad s evropskými harmonizovanými normami zakládá domněnku souladu ze strany poskytovatelů v rozsahu, v jakém tyto normy zahrnují tyto povinnostmi. Poskytovatelé obecných modelů AI, kteří nedodržují schválený kodex správné praxe nebo nesplňuji evropskou harmonizovanou normu, prokáží za účelem posouzení Komisí alternativní vhodné způsoby prokazování shody.

5. Za účelem usnadnění souladu s přílohou XI, zejména s bodem 2 písm. d) a e) uvedené přílohy, je Komisi svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 97, v nichž podrobně popíše metodiky měření a výpočtu s cílem umožnit srovnatelnost a ověřitelnost dokumentace.

6. Komisi je svěřena pravomoc přijmout akty v přenesené pravomoci v souladu s čl. 97 odst. 2 s cílem aktualizovat s ohledem na technický pokrok přílohy XI a XII.

7. S veškerými informacemi nebo dokumentací získanými orgány dozoru nad trhem podle tohoto článku, včetně obchodních tajemství, se nakládá v souladu s povinnostmi zachování důvěrnosti stanovenými v článku 78.

Článek 54

Zplnomocnění zástupci poskytovatelů obecných modelů AI

1. Před uvedením obecného modelu AI na trh poskytovatelé usazení ve třetích zemích jmenují formou písemného pověření zplnomocněného zástupce usazeného v Unii.

2. Poskytovatel umožní svému zplnomocněnému zástupci provádět úkoly vymezené v pověření, které obdržel od poskytovatele.

3. Zplnomocněný zástupce provádí úkoly vymezené v pověření, které obdržel od poskytovatele. Kopii pověření poskytne na požádání úřadu pro AI v jednom z úředních jazyků orgánů Unie. Pro účely tohoto nařízení zmocňuje pověření zplnomocněného zástupce k provádění těchto úkolů:

a) ověřit, že byla vypracována technická dokumentace uvedená v příloze XI a že poskytovatel splnil všechny povinnosti uvedené v článku 53 a případně v článku 55;

b) uchovávat kopii technické dokumentace uvedené v příloze XI pro potřeby úřadu pro AI a příslušných vnitrostátních orgánů po dobu deseti let od uvedení obecného modelu AI na trh a kontaktní údaje poskytovatele, který zplnomocněného zástupce jmenoval;

c) poskytnout úřadu pro AI na odůvodněnou žádost všechny informace a dokumentaci, které jsou nezbytné k prokázání souladu s povinnostmi uvedenými v této kapitole, včetně informací a dokumentace uvedených v písmenu b);

d) spolupracovat na základě odůvodněné žádosti s úřadem pro AI a příslušnými orgány při veškerých opatřeních, která tyto orgány přijmou v souvislosti s obecným modelem AI, včetně případů, kdy je daný model začleněn do systémů AI uváděných na trh nebo do provozu v Unii.

4. Toto pověření zmocňuje zplnomocněného zástupce k tomu, aby se na něj vedle poskytovatele nebo namísto něj obracel úřad pro AI nebo příslušné orgány ve všech otázkách týkajících se zajištění souladu s tímto nařízením.

5. Zplnomocněný zástupce pověření ukončí, pokud se domnívá nebo má důvod se domnívat, že poskytovatel jedná v rozporu se svými povinnostmi podle tohoto nařízení. V takovém případě rovněž neprodleně informuje úřad pro AI o ukončení pověření a jeho důvodech.

6. Povinnost stanovená v tomto článku se nevztahuje na poskytovatele obecných modelů AI, jež jsou zpřístupňovány na základě svobodné a otevřené licence, která umožňuje přístup k modelu, jeho používání, úpravu a distribuci, a jejichž parametry, včetně vah, informací o architektuře modelu a informací o používání modelu, jsou veřejně dostupné, pokud však obecné modely AI nepředstavují systémová rizika.

ODDÍL 3

Povinnosti poskytovatelů obecných modelů AI se systémovým rizikem

Článek 55

Povinnosti poskytovatelů obecných modelů AI se systémovým rizikem

1. Kromě povinností uvedených v článcích 53 a 54 poskytovatelé obecných modelů AI se systémovým rizikem:

a) provádějí hodnocení modelu v souladu se standardizovanými protokoly a nástroji odrážejícími nejmodernější stav technologií, včetně provádění a dokumentace kontradiktorního testování modelu s cílem určit a zmírnit systémové riziko;

b) posuzují a zmírňují možná systémová rizika na úrovni Unie, včetně jejich zdrojů, která mohou vyplývat z vývoje, uvádění na trh nebo používání obecných modelů AI se systémovým rizikem;

c) sledují, dokumentují a bez zbytečného odkladu hlásí úřadu pro AI a případně příslušným vnitrostátním orgánům relevantní informace o závažných incidentech a možná nápravná opatření k jejich řešení;

d) zajišťují odpovídající úroveň ochrany kybernetické bezpečnosti pro obecný model AI se systémovým rizikem a fyzickou infrastrukturu modelu.

2. Poskytovatelé obecných modelů AI se systémovým rizikem mohou při prokazování souladu s povinnostmi stanovenými v odstavci 1 tohoto článku vycházet z kodexů správné praxe ve smyslu článku 56, dokud nebude zveřejněna harmonizovaná norma. Soulad s evropskými harmonizovanými normami zakládá domněnku souladu ze strany poskytovatelů v rozsahu, v jakém tyto normy zahrnují dané povinnosti. Poskytovatelé obecných modelů AI, kteří nedodržují schválený kodex správné praxe nebo nesplňují evropskou harmonizovanou normu, prokáží za účelem posouzení Komisí alternativní vhodné způsoby prokazování shody.

3. S veškerými informacemi nebo dokumentací získanými orgány dozoru nad trhem podle tohoto článku, včetně obchodních tajemství, se nakládá v souladu s povinnostmi zachování důvěrnosti stanovenými v článku 78.

ODDÍL 4

Kodexy správné praxe

Článek 56

Kodexy správné praxe

1. Úřad pro AI s přihlédnutím k mezinárodním přístupům podporuje a usnadňuje vypracování kodexů správné praxe na úrovni Unie s cílem přispět k řádnému uplatňování tohoto nařízení.

2. Úřad pro AI a rada usilují o zajištění toho, aby kodexy správné praxe zahrnovaly alespoň povinnosti stanovené v článcích 53 a 55, včetně těchto záležitostí:

a) prostředky k zajištění toho, aby informace uvedené v čl. 53 odst. 1 písm. a) a b) byly aktualizovány s ohledem na vývoj trhu a technologií;

b) adekvátní úroveň podrobnosti pro shrnutí obsahu použitého pro trénování;

c) určení druhu a povahy systémových rizik na úrovni Unie, včetně jejich případných zdrojů;

d) opatření, postupy a způsoby posuzování a řízení systémových rizik na úrovni Unie, včetně jejich dokumentace, které jsou úměrné rizikům, zohledňují jejich závažnost a pravděpodobnost a berou zřetel na konkrétní výzvy spojené s řešením těchto rizik s přihlédnutím k možným způsobům, jak tato rizika mohou vzniknout a projevit se v celém hodnotovém řetězci AI.

3. Úřad pro AI může vyzvat všechny poskytovatele obecných modelů AI, jakož i příslušné vnitrostátní orgány, aby se na vypracovávání kodexů správné praxe podíleli. Tento proces mohou podpořit organizace občanské společnosti, průmysl, akademická obec a další příslušné zúčastněné strany, jako jsou navazující poskytovatelé a nezávislí odborníci.

4. Úřad pro AI a rada usilují o zajištění toho, aby v kodexech správné praxe byly jasně stanoveny jejich specifické cíle, aby tyto kodexy obsahovaly závazky nebo opatření včetně případných klíčových ukazatelů výkonnosti, jimiž bude dosažení těchto cílů zajištěno, a aby náležitě zohledňovaly potřeby a zájmy všech zúčastněných stran, včetně dotčených osob, na úrovni Unie.

5. Úřad pro AI usiluje o zajištění toho, aby účastníci kodexů správné praxe pravidelně podávali úřadu pro AI zprávy o provádění závazků a přijatých opatřeních a jejich výsledcích, a to případně i na základě klíčových ukazatelů výkonnosti. Klíčové ukazatele výkonnosti a závazky v oblasti podávání zpráv zohledňují rozdíly mezi různými účastníky, pokud jde o jejich velikost a kapacitu.

6. Úřad pro AI a rada pravidelně sledují a vyhodnocují dosahování cílů kodexů správné praxe ze strany účastníků a jejich přínos k řádnému uplatňování tohoto nařízení. Úřad pro AI a rada posoudí, zda kodexy správné praxe zahrnují povinnosti stanovené v článcích 53 a 55, a pravidelně sledují a vyhodnocují dosahování jejich cílů. Své posouzení přiměřenosti kodexů správné praxe zveřejní.

Komise může prostřednictvím prováděcího aktu určitý kodex správné praxe schválit a udělit mu obecnou platnost v rámci Unie. Tento prováděcí akt se přijme přezkumným postupem uvedeným v čl. 98 odst. 2.

7. Úřad pro AI může vyzvat všechny poskytovatele obecných modelů AI, aby se kodexy správné praxe dodržovali. V případě poskytovatelů obecných modelů AI, které nepředstavují systémová rizika, může být toto dodržování omezeno na povinnosti stanovené v článku 53, pokud tito poskytovatelé výslovně neprohlásí, že mají zájem kodex dodržovat v plném rozsahu.

8. Úřad pro AI rovněž podle potřeby podporuje a usnadňuje přezkum a úpravu kodexů správné praxe, zejména s ohledem na vznikající normy. Úřad pro AI je nápomocen při posuzování dostupných norem.

9. Kodex správné praxe je k dispozici nejpozději do 2. května 2025. Úřad pro AI podnikne nezbytné kroky včetně výzvy adresované poskytovatelům podle odstavce 7.

Nebude-li do 2. srpna 2025 možno kodex správné praxe dokončit nebo pokud se úřad pro AI po posouzení podle odstavce 6 tohoto článku bude domnívat, že kodex není přiměřený, může Komise prostřednictvím prováděcích aktů stanovit společná pravidla pro plnění povinností stanovených v článcích 53 a 55, včetně záležitostí uvedených v odstavci 2 tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 98 odst. 2.

KAPITOLA VI

OPATŘENÍ NA PODPORU INOVACÍ

Článek 57

Regulační sandboxy pro AI

1. Členské státy zajistí, aby jejich příslušné orgány zřídily alespoň jeden regulační sandbox pro AI na vnitrostátní úrovni, který bude funkční do 2. srpna 2026. Tento sandbox mohou rovněž zřídit společně s příslušnými orgány jiných členských států. Komise může pro účely zřízení a provozu regulačních sandboxů pro AI poskytovat technickou podporu, poradenství a nástroje.

Povinnost podle prvního pododstavce může být rovněž splněna účastí ve stávajícím sandboxu, pokud tato účast poskytuje zúčastněným členským státům rovnocennou úroveň vnitrostátního pokrytí.

2. Další regulační sandboxy pro AI mohou být rovněž zřízeny na regionální nebo místní úrovni nebo společně s příslušnými orgány jiných členských států.

3. Evropský inspektor ochrany údajů může rovněž zřídit regulační sandbox pro AI pro orgány, instituce nebo jiné subjekty Unie a může vykonávat úlohy a úkoly příslušných vnitrostátních orgánů v souladu s touto kapitolou.

4. Členské státy zajistí, aby příslušné orgány uvedené v odstavcích 1 a 2 přidělily dostatečné zdroje pro účinné a urychlené dosažení souladu s tímto článkem. Příslušné vnitrostátní orgány případně spolupracují s dalšími relevantními orgány a mohou umožnit zapojení dalších subjektů v rámci ekosystému AI. Tímto článkem nejsou dotčeny jiné regulační sandboxy zřízené podle práva Unie nebo vnitrostátního práva. Členské státy zajistí náležitou úroveň spolupráce mezi orgány vykonávajícími dohled nad těmito jinými sandboxy a příslušnými vnitrostátními orgány.

5. Regulační sandboxy pro AI zřízené podle odstavce 1 poskytují kontrolované prostředí, které podporuje inovace a usnadňuje vývoj, trénování, testování a validaci inovativních systémů AI po omezenou dobu před jejich uvedením na trh nebo do provozu podle konkrétního plánu testování v sandboxu, na kterém se dohodli poskytovatelé nebo potenciální poskytovatelé a příslušný orgán. Tyto sandboxy mohou zahrnovat testování v reálných podmínkách pod dohledem v nich..

6. Příslušné orgány případně poskytnou v rámci regulačního sandboxu pro AI pokyny, dohled a podporu s cílem určit rizika, zejména pro základní práva, zdraví a bezpečnost, testování, zmírňující opatření a jejich účinnost ve vztahu k povinnostem a požadavkům, jež jsou vymezeny tímto nařízením a případně jiným unijním a vnitrostátním právem a nad nimiž je v rámci daného sandboxu vykonáván dohled.

7. Příslušné orgány poskytnou poskytovatelům a potenciálním poskytovatelům účastnícím se na regulačním sandboxu pro AI pokyny týkající se regulačních očekávání a toho, jak plnit požadavky a povinnosti stanovené v tomto nařízení.

Na žádost poskytovatele nebo potenciálního poskytovatele systému AI poskytne příslušný orgán písemný doklad o činnostech, které byly v rámci sandboxu úspěšně provedeny. Příslušný orgán rovněž předloží výstupní zprávu s podrobným popisem činností prováděných v rámci sandboxu, souvisejících výsledků a výsledků učení. Poskytovatelé mohou tuto dokumentaci použít k prokázání souladu s tímto nařízením v rámci postupu posuzování shody nebo příslušných činností dozoru nad trhem. V tomto ohledu orgány dozoru nad trhem a oznámené subjekty výstupní zprávy a písemný doklad poskytnutý příslušným vnitrostátním orgánem kladně zohlední, aby bylo možno postupy posuzování shody v přiměřeném rozsahu urychlit.

8. S výhradou ustanovení o důvěrnosti v článku 78 a se souhlasem poskytovatele nebo potenciálního poskytovatele jsou Komise a rada oprávněny do výstupních zpráv nahlížet a podle potřeby je zohlední při plnění svých úkolů podle tohoto nařízení. Pokud poskytovatel nebo potenciální poskytovatel a příslušný vnitrostátní orgán výslovně souhlasí, může být výstupní zpráva zpřístupněna veřejnosti prostřednictvím jednotné informační platformy uvedené v tomto článku.

9. Cílem vytvoření regulačních sandboxů pro AI je přispět k těmto cílům:

a) větší právní jistota v zájmu dosažení souladu s tímto nařízením nebo relevantních případech s jiným platným unijním a vnitrostátním právem;

b) podpora sdílení osvědčených postupů prostřednictvím spolupráce s orgány zapojenými do regulačního sandboxu pro AI;

c) podpora inovací a konkurenceschopnosti a usnadňování vývoje ekosystému AI;

d) přispění k fakticky podloženému regulačnímu učení;

e) snazší a rychlejší přístup systémů AI na trh Unie, zejména pokud jsou poskytovány malými a středními podniky, včetně podniků začínajících.

10. Příslušné vnitrostátní orgány zajistí, aby v rozsahu, v němž dané inovativní systémy AI zahrnují zpracování osobních údajů nebo jinak spadají do oblasti dohledu jiných vnitrostátních orgánů nebo příslušných orgánů poskytujících nebo podporujících přístup k údajům, byly vnitrostátní orgány pro ochranu osobních údajů a tyto jiné vnitrostátní nebo příslušné orgány přidruženy k provozu daného regulačního sandboxu pro AI a aby byly zapojeny do dohledu nad těmito aspekty v rozsahu svých příslušných úkolů a pravomocí.

11. Regulační sandboxy pro AI nemají vliv na pravomoci příslušných orgánů dohlížejících na sandboxy v oblasti dohledu a nápravy, a to ani na regionální či místní úrovni. Veškerá významná rizika pro zdraví, bezpečnost a základní práva zjištěná během vývoje a testování těchto systémů AI jsou následně přiměřeně zmírněna. Není-li účinné zmírnění možné, příslušné vnitrostátní orgány mají pravomoc zkušební proces nebo účast v sandboxu dočasně či trvale pozastavit a o tomto rozhodnutí informují úřad pro AI. Příslušné vnitrostátní orgány plní své pravomoci dohledu v mezích příslušného práva, přičemž při uplatňování právních ustanovení ohledně konkrétního projektu regulačního sandboxu pro AI využijí své diskreční pravomoci s cílem podpořit v Unii inovace v oblasti AI.

12. Poskytovatelé a potenciální poskytovatelé účastnící se regulačního sandboxu pro AI nesou podle platného práva Unie a vnitrostátního práva v oblasti upravujícího odpovědnost i nadále odpovědnost za jakoukoli škodu způsobenou třetím stranám v důsledku experimentů, jež jsou v daném sandboxu prováděny. Nicméně v případě, že potenciální poskytovatelé dodržují konkrétní plán a podmínky účasti a řídí se v dobré víře pokyny vydanými příslušnými vnitrostátními orgány, orgány v případě porušení tohoto nařízení neuloží žádné správní pokuty. Pokud byly do dohledu nad systémem AI v sandboxu aktivně zapojeny další příslušné orgány, odpovědné za jiné unijní a vnitrostátní právo, a poskytly pro dodržování tohoto práva pokyny, neukládají se v souvislosti s předmětnými předpisy žádné správní pokuty.

13. Regulační sandboxy pro AI jsou navrženy a zavedeny tak, aby v relevantních případech usnadňovaly přeshraniční spolupráci mezi příslušnými vnitrostátními orgány.

14. Příslušné vnitrostátní orgány koordinují své činnosti a spolupracují v rámci rady.

15. Příslušné vnitrostátní orgány informují úřad pro AI a radu o zřízení sandboxu a mohou je požádat o podporu a pokyny. Úřad pro AI zveřejní seznam stávajících i plánovaných sandboxů a aktualizuje jej s cílem podpořit v regulačních sandboxech pro AI větší interakci a podnítit přeshraniční spolupráci.

16. Příslušné vnitrostátní orgány předkládají úřadu pro AI a radě výroční zprávy, a to od jednoho roku po zřízení regulačního sandboxu pro AI a poté každý rok až do jeho ukončení, a závěrečnou zprávu. Tyto zprávy obsahují informace o pokroku při zavádění uvedených sandboxů a jejich výsledcích, včetně osvědčených postupů, incidentů, získaných zkušeností a doporučení ohledně jejich uspořádání a případně ohledně uplatňování a revize tohoto nařízení, včetně souvisejících aktů v přenesení pravomoci a prováděcích aktů, a ohledně uplatňování jiného práva Unie, nad nimiž příslušné orgány v rámci daného sandboxu provádí dohled. Příslušné vnitrostátní orgány tyto výroční zprávy nebo jejich shrnutí zpřístupní veřejnosti online. Komise tyto výroční zprávy v případě potřeby zohlední při plnění svých úkolů podle tohoto nařízení.

17. Komise vytvoří jednotné a vyhrazené rozhraní obsahující veškeré relevantní informace týkající se regulačních sandboxů pro AI s cílem umožnit zúčastněným stranám interakci s regulačními sandboxy pro AI a pokládat příslušným orgánům dotazy a žádat o nezávazné pokyny týkající se souladu inovativních produktů, služeb a obchodních modelů zahrnujících technologie AI s tímto nařízením, v souladu s čl. 62 odst. 1 písm. c). Komise svou činnost případně aktivně koordinuje s příslušnými vnitrostátními orgány.

Článek 58

Podrobná ustanovení pro regulační sandboxy pro AI a jejich fungování

1. Aby se zabránilo roztříštěnosti v celé Unii, přijme Komise prováděcí akty, kterými stanoví podrobná ustanovení pro zřízení, vývoj, provádění a provoz regulačních sandboxů pro AI a pro dohled nad nimi. Prováděcí akty obsahují společné hlavní zásady týkající se těchto otázek:

a) kritéria způsobilosti a výběru pro účast na regulačním sandboxu pro AI;

b) postupy pro podávání žádostí, účast, monitorování, ukončení účasti, jakož i ukončení samotného regulačního sandboxu pro AI, včetně plánu testování v sandboxu a výstupní zprávy;

c) podmínky vztahující se na účastníky.

Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 98 odst. 2.

2. Prováděcí akty uvedené v odstavci 1 zajistí následující:

a) regulační sandboxy pro AI jsou otevřeny jakémukoli žádajícímu poskytovateli či potenciálnímu poskytovateli systému AI, který splňuje kritéria způsobilosti a výběru, která jsou transparentní a spravedlivá, a příslušné vnitrostátní orgány informují žadatele o svém rozhodnutí do tří měsíců od podání žádosti;

b) regulační sandboxy pro AI umožňují široký a rovný přístup a drží krok s poptávkou po účasti v nich; poskytovatelé či potenciální poskytovatelé mohou rovněž podávat žádosti společně se subjekty zavádějícími systémy AI a jinými příslušnými třetími stranami;

c) podrobná ustanovení pro regulační sandboxy pro AI a podmínky pro ně v co největší míře podporují flexibilitu pro příslušné vnitrostátní orgány při zřizování a provozování jejich regulačních sandboxů pro AI;

d) přístup k regulačním sandboxům pro AI je bezplatný pro malé a střední podniky, včetně podniků začínajících, aniž jsou dotčeny mimořádné náklady, které mohou příslušné vnitrostátní orgány vymáhat spravedlivým a přiměřeným způsobem;

e) prostřednictvím výsledků učení v regulačních sandboxech pro AI usnadňují poskytovatelům či potenciálním poskytovatelům plnění povinností posuzování shody podle tohoto nařízení a dobrovolné uplatňování kodexů chování uvedených v článku 95;

f) regulační sandboxy pro AI usnadňují zapojení dalších příslušných subjektů v rámci ekosystému AI, jako jsou oznámené subjekty a normalizační organizace, malé a střední podniky, včetně začínajících podniků, podniky, inovátoři, testovací a experimentální zařízení, výzkumné a experimentální laboratoře a evropská centra pro digitální inovace, centra excelence a jednotliví výzkumní pracovníci, s cílem umožnit a usnadnit spolupráci s veřejným a soukromým sektorem;

g) postupy, procesy a správní požadavky týkající se podávání žádostí, výběru, účasti v regulačním sandboxu pro AI a jeho opuštění jsou jednoduché, snadno srozumitelné a jasně sdělené s cílem usnadnit účast malých a středních podniků s omezenými právními a správními kapacitami, včetně podniků začínajících, a jsou dostupné v celé Unii, aby se zabránilo roztříštěnosti a aby účast v regulačním sandboxu pro AI zřízeném členským státem nebo evropským inspektorem ochrany údajů byla vzájemně a jednotně uznávána a měla v celé Unii stejné právní účinky;

h) účast v regulačním sandboxu pro AI je omezena na dobu, která je přiměřená složitosti a rozsahu projektu, a která může být prodloužena příslušným vnitrostátním orgánem;

i) regulační sandboxy pro AI usnadňují vývoj nástrojů a infrastruktury pro testování, srovnávání, posuzování a vysvětlování aspektů systémů AI relevantních pro regulační učení, jako je přesnost, spolehlivost a kybernetická bezpečnost a rovněž opatření k omezení rizik pro lidská práva a společnost obecně.

3. Potenciální poskytovatelé v regulačních sandboxech pro AI, zejména malé a střední podniky a podniky začínající, jsou podle potřeby nasměrováni na služby před zaváděním, jako jsou pokyny k provádění tohoto nařízení, na další služby vytvářející přidanou hodnotu, jako je pomoc s normalizačními dokumenty a certifikací, testovací a experimentální zařízení, evropská centra pro digitální inovace a centra excelence.

4. Pokud příslušné vnitrostátní orgány zvažují, že povolí testování v reálných podmínkách, nad nímž je vykonáván dohled v rámci regulačního sandboxu pro AI 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 59

Další zpracování osobních údajů pro účely vývoje určitých systémů AI ve veřejném zájmu v rámci regulačního sandboxu pro AI

1. Osobní údaje zákonně shromážděné pro jiné účely mohou být v regulačním sandboxu pro AI zpracovávány výhradně pro účely vývoje, trénování a testování určitých systémů AI v sandboxu, pokud jsou splněny všechny tyto podmínky:

a) systémy AI jsou vyvinuty veřejným orgánem nebo jinou fyzickou nebo právnickou osobou za účelem ochrany podstatného veřejného zájmu v jedné nebo více z následujících oblastí:

   i) veřejná bezpečnost a veřejné zdraví, včetně zjišťování, diagnostiky prevence, kontroly a léčby nemocí a zlepšování systémů zdravotní péče;

   ii) vysoká úroveň ochrany a zlepšování kvality životního prostředí, ochrana biologické rozmanitosti, ochrana proti znečištění, opatření zelené transformace, opatření na zmírňování změny klimatu a přizpůsobování se této změně;

   iii) energetická udržitelnost;

   iv) bezpečnost a odolnost dopravních systémů a mobility, kritické infrastruktury a sítí;

   v) účinnost a kvalita veřejné správy a veřejných služeb;

b) zpracovávané údaje jsou nezbytné pro splnění jednoho nebo více požadavků uvedených v kapitole III oddíle 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 sandboxu 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, a existují mechanismy reakce umožňující okamžité zmírnění těchto rizik a v případě potřeby i zastavení zpracování;

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

e) poskytovatelé mohou dále sdílet původně shromážděné údaje pouze v souladu s právem Unie v oblasti ochrany údajů; žádné osobní údaje vytvořené v rámci sandboxu nelze sdílet mimo sandbox;

f) žádné zpracování osobních údajů v rámci sandboxu nevede k opatřením nebo rozhodnutím ovlivňujícím subjekty údajů ani nemá vliv na uplatňování jejich práv stanovených v právu Unie v oblasti osobních údajů;

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

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

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

j) stručného shrnutí projektu AI vyvinutého v sandboxu, jeho cílů a očekávaných výsledků je zveřejněno na internetových stránkách příslušných orgánů; tato povinnost se nevztahuje na citlivé operativní údaje týkající se činností donucovacích orgánů, orgánů ochrany hranic, imigračních nebo azylových orgánů.

2. Pro účely prevence, vyšetřování, odhalování či stíhání trestných činů nebo pro účely výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení pod dozorem a v pravomoci donucovacích orgánů, vychází zpracování osobních údajů v regulačních sandboxech pro AI ze zvláštního unijního nebo vnitrostátního práva a podléhá stejným kumulativním podmínkám, jež jsou uvedeny v odstavci 1.

3. Odstavcem 1 není dotčeno právo Unie ani vnitrostátní právo, které vylučuje zpracování osobních údajů pro jiné účely než pro účely, které toto právo výslovně uvádí, ani právo Unie a vnitrostátní právo, které stanoví základ pro zpracování osobních údajů, jež je nezbytný pro účely vývoje, testování nebo trénování inovativních systémů AI, nebo jakýkoli jiný právní základ v souladu s právem Unie o ochraně osobních údajů.

Článek 60

Testování vysoce rizikových systémů AI v reálných podmínkách mimo regulační sandboxy pro AI

1. Poskytovatelé nebo potenciální poskytovatelé vysoce rizikových systémů AI uvedených v příloze III mohou provádět testování vysoce rizikových systémů AI v reálných podmínkách mimo regulační sandboxy pro AI v souladu s tímto článkem a plánem testování v reálných podmínkách provozu uvedeným v tomto článku, aniž jsou dotčeny zákazy podle článku 5.

Komise v prováděcích aktech upřesní podrobné prvky plánu testování v reálných podmínkách. Tyti prováděcí akty budou přijaty přezkumným postupem podle čl. 98 odst. 2.

Tímto odstavcem není dotčeno právo Unie ani vnitrostátní právo týkající se testování vysoce rizikových systémů AI v reálných podmínkách v souvislosti s produkty, na něž se vztahují harmonizační právní předpisy uvedené v příloze I.

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

3. Testováním vysoce rizikových systémů AI v reálných podmínkách podle tohoto článku není dotčen žádný etický přezkum, který je vyžadován právem Unie nebo vnitrostátním právem.

4. Poskytovatelé nebo potenciální poskytovatelé mohou provádět testování v reálných podmínkách pouze v případě, že jsou 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, v němž má být testování v reálných podmínkách provedeno;

b) vnitrostátní orgán dozoru nad trhem v členském státě, v němž se testování v reálných podmínkách má provést, testování v reálných podmínkách a plán testování v reálných podmínkách schválil; pokud orgán dozoru nad trhem neposkytne odpověď do 30 dnů, testování v reálných podmínkách a plán zkoušek v reálných podmínkách se považují za schválené; nestanoví-li vnitrostátní právo implicitní schválení, testování v reálných podmínkách nadále podléhá povolení;

c) poskytovatel nebo potenciální poskytovatel, s výjimkou poskytovatelů nebo potenciálních poskytovatelů vysoce rizikových systémů AI uvedených v bodech 1, 6 a 7 přílohy III v oblasti vymáhání práva, migrace, azylu a řízení ochrany hranic a vysoce rizikových systémů AI uvedených v bodě 2 přílohy III, zaregistroval testování v reálných podmínkách v souladu s čl. 71 odst. 4 s uvedením celounijního jedinečného identifikačního čísla a informací stanovených v příloze IX; poskytovatel nebo potenciální poskytovatel vysoce rizikových systémů AI uvedených v bodech 1, 6 a 7 přílohy III v oblasti vymáhání práva, migrace, azylu a řízení ochrany hranic zaregistroval testování v reálných podmínkách v zabezpečené, neveřejné části databáze EU podle čl. 49 odst. 4 písm. d) s celounijním jedinečným identifikačním číslem a informacemi v tomto článku uvedenými; poskytovatel nebo potenciální poskytovatel vysoce rizikových systémů AI uvedený v bodě 2 přílohy III zaregistroval testování v reálných podmínkách v souladu s čl. 49 odst. 5;

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

e) údaje shromážděné a zpracované pro účely testování v reálných podmínkách se předávají třetím zemím pouze za předpokladu, že jsou uplatňovány vhodné a použitelné záruky podle práva Unie;

f) testování v reálných podmínkách netrvá déle, než je nezbytné k dosažení jeho cílů, a v žádném případě ne déle než šest měsíců, přičemž tato doba může být prodloužena o dalších šest měsíců, pokud poskytovatel nebo potenciální poskytovatel toto prodloužení předem oznámí orgánu dozoru nad trhem spolu s vysvětlením, proč je ho zapotřebí;

g) subjekty testování v reálných podmínkách, které vzhledem ke svému věku nebo postižení spadají do zranitelných skupin, jsou náležitě chráněny;

h) pokud poskytovatel nebo potenciální poskytovatel uspořádá testování v reálných podmínkách ve spolupráci s jedním nebo více zavádějícími subjekty či potenciálními zavádějícími subjekty, tyto subjekty byly informovány o všech aspektech testování, které jsou relevantní pro jejich rozhodnutí účastnit se, a obdrželi příslušné pokyny pro použití systému AI uvedeného v článku 13; poskytovatel nebo potenciální poskytovatel a zavádějící subjekt nebo potenciální zavádějící subjekt 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 jiným platným právem Unie a vnitrostátním právem;

i) subjekty testování v reálných podmínkách udělily informovaný souhlas v souladu s článkem 61, nebo pokud by v případě vymáhání práva získání informovaného souhlasu testování systému AI bránilo, samotné testování a výsledek testování v reálných podmínkách nemají na subjekty hodnocení žádný negativní dopad a osobní údaje těchto subjektů jsou po provedení testu vymazány;

j) na testování v reálných podmínkách účinně dohlíží poskytovatel nebo potenciální poskytovatel, jakož i zavádějící subjekty nebo potenciální zavádějící subjekty prostřednictvím osob, které mají jak odpovídající kvalifikaci v příslušné oblasti, tak nezbytnou kapacitu, odbornou přípravu a pravomoc k plnění svých úkolů;

k) predikce, doporučení nebo rozhodnutí systému AI lze účinně zvrátit a nezohlednit.

5. Kterékoli subjekty testování v reálných podmínkách nebo případně jejich 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, a může požádat o okamžité a trvalé vymazání svých osobních údajů. Odvoláním informovaného souhlasu nejsou dotčeny již provedené činnosti.

6. V souladu s článkem 75 svěří členské státy svým orgánům dozoru nad trhem pravomoci požadovat od poskytovatelů a potenciálních poskytovatelů informace, provádět neohlášené kontroly na dálku nebo kontroly na místě a provádět kontroly postupu testování v reálných podmínkách a souvisejících vysoce rizikových systémů AI. Orgány dozoru nad trhem využijí těchto pravomocí k zajištění bezpečného vývoje testování v reálných podmínkách.

7. Veškeré závažné incidenty zjištěné v průběhu testování v reálných podmínkách se oznámí vnitrostátnímu orgánu dozoru nad trhem v souladu s článkem 73. Poskytovatel nebo potenciální poskytovatel přijme okamžitá zmírňující opatření nebo, pokud to není možné, testování v reálných podmínkách pozastaví, dokud k tomuto zmírnění nedojde, nebo testování jiným způsobem ukončí. Po takovém ukončení testování v reálných podmínkách stanoví poskytovatel nebo potenciální poskytovatel postup pro okamžité stažení systému AI z oběhu.

8. Poskytovatelé nebo potenciální poskytovatelé oznámí vnitrostátnímu orgánu dozoru nad trhem v členském státě, v němž se testování v reálných podmínkách provádí, že testování v reálných podmínkách bylo pozastaveno nebo ukončeno, a jaké jsou konečné výsledky.

9. Podle platného práva Unie a vnitrostátního práva upravujícího odpovědnost nesou poskytovatel nebo potenciální poskytovatel odpovědnost za veškeré škody, jež byly v průběhu jejich testování v reálných podmínkách způsobeny.

Článek 61

Informovaný souhlas s účastí na testování v reálných podmínkách mimo regulační sandboxy pro AI

1. Pro účely testování v reálných podmínkách podle článku 60 musí být od subjektů testování získám dobrovolný informovaný souhlas udělený před jejich účastí na tomto testování, a poté, co řádně obdržely stručné, jasné, relevantní a srozumitelné informace týkající se:

a) povahy a cílů testování v reálných podmínkách a možných obtíží, které mohou být s jejich účastí spojeny;

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

c) jejich práv a záruk týkajících se jejich účasti, zejména jejich práva odmítnout účast a práva kdykoliv od testování v reálných podmínkách odstoupit, aniž by jim z toho plynula jakákoliv újma a aniž by byly povinny poskytnout jakékoliv odůvodnění;

d) opatření ohledně žádostí o zrušení nebo nezohlednění predikcí, doporučení nebo rozhodnutí systému AI;

e) celounijního jedinečného identifikačního čísla testování v reálných podmínkách v souladu s čl. 60 odst. 4 písm. c) a kontaktních údajů poskytovatele nebo jeho právního zástupce, od něhož lze získat další informace.

2. Informovaný souhlas je datován a zdokumentován a jeho kopie je poskytnuta subjektům testování nebo jejich právnímu zástupci.

Článek 62

Opatření pro poskytovatele a zavádějící subjekty, zejména malé a střední podniky, včetně podniků začínajících

1. Členské státy učiní tato opatření:

a) poskytují přednostní přístup k regulačním sandboxům pro AI malým a středním podnikům, které mají sídlo nebo pobočku v Unii, včetně podniků začínajících, a to v rozsahu, v jakém splňují kritéria a podmínky způsobilosti a výběru. Přednostní přístup nebrání jiným malým a středním podnikům, které nejsou uvedeny v tomto odstavci, včetně podniků začínajících, v přístupu k regulačnímu sandboxu pro AI, pokud rovněž splňují podmínky způsobilosti a kritéria výběru;

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

c) využívají stávající vyhrazené kanály a případně zřídí kanály nové pro komunikaci s malými a středními podniky, včetně podniků začínajících, se zavádějícími subjekty, dalšími inovátory a v případě potřeby s místními veřejnými orgány, a prostřednictvím těchto kanálů poskytují poradenství a reagují na dotazy týkající se provádění tohoto nařízení, a to i v souvislosti s účastí na regulačních sandboxech pro AI;

d) usnadňují účast malých a středních podniků a dalších příslušných zúčastněných stran na procesu rozvoje normalizace.

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

3. Úřad pro AI učiní tato opatření:

a) poskytuje standardizované šablony pro oblasti, na něž se vztahuje toto nařízení, jak stanoví výbor ve své žádosti;

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

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

d) vyhodnocuje a podporuje sbližování osvědčených postupů při zadávacím řízení v souvislosti se systémy AI.

Článek 63

Výjimky pro specifické provozovatele

1. Mikropodniky ve smyslu doporučení 2003/361/ES mohou některé prvky systému řízení kvality vyžadované článkem 17 tohoto nařízení dodržovat zjednodušeným způsobem, pokud nemají partnerské podniky nebo propojené podniky ve smyslu uvedeného doporučení. Za tímto účelem Komise vypracuje pokyny k prvkům systému řízení kvality, které lze splnit zjednodušeným způsobem s ohledem na potřeby mikropodniků, aniž by byla dotčena úroveň ochrany nebo potřeba souladu s požadavky týkajícími se vysoce rizikových systémů AI.

2. Odstavec 1 tohoto článku 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, 10, 11, 12, 13, 14, 15, 72 a 73.

KAPITOLA VII

SPRÁVA

ODDÍL 1

Správa na úrovni Unie

Článek 64

Úřad pro AI

1. Komise rozvíjí odborné znalosti a schopnosti Unie v oblasti umělé inteligence prostřednictvím úřadu pro AI.

2. Členské státy usnadní plnění úkolů svěřených úřadu pro AI, jak je uvedeno v tomto nařízení.

Článek 65

Zřízení a struktura Evropské rady pro umělou inteligenci

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

2. Členy rady jsou zástupci členských států, za každý členský stát vždy jeden. Jako pozorovatel je zapojen evropský inspektor ochrany údajů. Na zasedáních rady je rovněž přítomen úřad pro AI, který 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.

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

4. Členské státy zajistí, aby jejich zástupci v radě:

a) měli ve svém členském státě příslušné kompetence a pravomoci, a mohli se tak aktivně podílet na plnění úkolů rady uvedených v článku 66;

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

c) 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.

5. Určení zástupci členských států přijmou dvoutřetinovou většinou jednací řád rady. Jednací řád zejména stanoví postupy pro výběrové řízení, dobu trvání mandátu předsedy a jeho konkrétní úkoly, podrobná ustanovení pro hlasování a organizaci činností rady a jejích podskupin.

6. Rada zřídí dvě stálé podskupiny, které poskytují 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.

Rada může pro účely zkoumání konkrétních otázek podle potřeby zřizovat další stálé nebo dočasné podskupiny. K účasti na těchto podskupinách nebo na konkrétní zasedání těchto podskupin mohou být jako pozorovatelé případně přizváni zástupci poradního fóra uvedeného v článku 67.

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

8. Radě předsedá jeden ze zástupců členských států. Úřad pro AI poskytuje radě sekretariát, na žádost předsedy svolává zasedání a připravuje pořad jednání v souladu s úkoly rady podle tohoto nařízení a s jejím jednacím řádem.

Článek 66

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) přispívat ke koordinaci mezi příslušnými vnitrostátními orgány odpovědnými za uplatňování tohoto nařízení a ve spolupráci s dotčenými orgány dozoru nad trhem a s výhradou jejich souhlasu podporovat společné činnosti orgánů dozoru nad trhem uvedené v čl. 74 odst. 11;

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

c) poskytovat poradenství ohledně provádění tohoto nařízení, zejména pokud jde o prosazování pravidel týkajících se obecných modelů AI;

d) přispívat k harmonizaci správní praxe v členských státech, a to i v souvislosti s odchylkou od postupů posuzování shody podle článku 46, fungováním regulačních sandboxů pro AI a testováním v reálných podmínkách podle článků 57, 59 a 60;

e) 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 ohledně:

i) vypracování a uplatňování kodexů chování a kodexů správné praxe podle tohoto nařízení, jakož i pokynů Komise;

ii) hodnocení a přezkumu tohoto nařízení podle článku 112, a to i pokud jde o zprávy o závažných incidentech uvedené v článku 73, fungování databáze EU uvedené v článku 71 a přípravu aktů v přenesené pravomoci nebo prováděcích aktů a pokud jde o možné sladění tohoto nařízení s harmonizačními právními předpisy Unie uvedenými v příloze I;

iii) technických specifikací nebo stávajících norem týkajících se požadavků stanovených v kapitole III oddíle 2;

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

v) trendů, jako je evropská globální konkurenceschopnost v oblasti AI, zavádění AI v Unii a rozvoje digitálních dovedností;

vi) trendů týkajících se rozvíjející se typologie hodnotových řetězců AI, zejména pokud jde o konečné důsledky z hlediska odpovědnosti;

vii) možné potřeby změny přílohy III v souladu s článkem 7 a možné potřeby případné revize článku 5 podle článku 112 s přihlédnutím k relevantním dostupným důkazům a nejnovějšímu technologickému vývoji;

f) napomáhat Komisi při podpoře gramotnosti v oblasti AI a zvyšování povědomí a informovanosti veřejnosti o přínosech, rizicích, zárukách a právech a povinnostech v souvislosti s používáním systémů AI;

g) usnadňovat rozvoj společných kritérií a společný výklad příslušných pojmů stanovených v tomto nařízení ze strany hospodářských subjektů a příslušných orgánů, a mimo jiné v tomto ohledu přispět k vypracování referenčních hodnot;

h) podle potřeby spolupracovat s dalšími orgány, institucemi nebo jinými subjekty Unie, jakož i s příslušnými skupinami a sítěmi odborníků Unie, zejména v oblasti bezpečnosti produktů, kybernetické bezpečnosti, hospodářské soutěže, digitálních a mediálních služeb, finančních služeb, ochrany spotřebitele, dat a základních práv;

i) přispívat k účinné spolupráci s příslušnými orgány třetích zemí a s mezinárodními organizacemi;

j) pomáhat příslušným vnitrostátním orgánům a Komisi při rozvoji organizačních a technických odborných znalostí potřebných pro provádění tohoto nařízení, mimo jiné přispíváním k posuzování potřeb odborné přípravy pracovníků členských států zapojených do provádění tohoto nařízení;

k) pomáhat úřadu pro AI při podpoře příslušných vnitrostátních orgánů při zřizování a rozvoji regulačních sandboxů pro AI a usnadňovat spolupráci a sdílení informací mezi regulačními sandboxy pro AI;

l) přispívat k vypracování pokynů a poskytovat v této oblasti relevantní poradenství;

m) poskytovat Komisi poradenství ve vztahu k mezinárodním záležitostem týkajícím se AI;

n) poskytovat Komisi stanoviska ke kvalifikovaným výstrahám ohledně obecných modelů AI;

o) přijímat od členských států stanoviska ke kvalifikovaným výstrahám týkajícím se obecných modelů AI a k vnitrostátním zkušenostem a postupům v oblasti monitorování a prosazování systémů AI, zejména systémů, které integrují obecné modely AI.

Článek 67

Poradní fórum

1. Zřizuje se poradní fórum, jehož úkolem je poskytovat technické odborné znalosti a poskytovat poradenství radě a Komisi a přispívat k jejich úkolům vyplývajícím z tohoto nařízení.

2. Složení poradního fóra je vyváženým výběrem zúčastněných stran, včetně průmyslu, začínajících podniků, malých a středních podniků, občanské společnosti a akademické obce. Složení poradního fóra je vyvážené s ohledem na komerční i nekomerční zájmy a v rámci kategorie komerčních zájmů musí být vyvážený také poměr malých a středních podniků a jiných podniků.

3. Komise jmenuje členy poradního fóra v souladu s kritérii stanovenými v odstavci 2 z řad zúčastněných stran, kteří mají uznávané odborné znalosti v oblasti AI.

4. Funkční období členů poradního fóra je dvouleté a nelze je prodloužit více než dvakrát po sobě.

5. Stálými členy poradního fóra jsou Agentura pro základní práva, Agentura Evropské unie pro kybernetickou bezpečnost (ENISA), Evropský výbor pro normalizaci (CEN), Evropský výbor pro normalizaci v elektrotechnice (CENELEC) a Evropský ústav pro telekomunikační normy (ETSI).

6. Poradní fórum vypracuje svůj jednací řád. Ze svých členů volí dva spolupředsedy v souladu s kritérii stanovenými v odstavci 2. Funkční období spolupředsedů je dvouleté a lze je jednou prodloužit.

7. Zasedání poradního fóra se konají alespoň dvakrát ročně. Poradní fórum může na svá zasedání přizvat odborníky a další zúčastněné strany.

8. Poradní fórum může na žádost rady nebo Komise vypracovávat stanoviska, doporučení a písemné příspěvky.

9. Poradní fórum může podle potřeby zřídit stálé nebo dočasné podskupiny pro účely posuzování konkrétních otázek souvisejících s cíli tohoto nařízení.

10. Poradní fórum vypracuje výroční zprávu o své činnosti. Tato zpráva se zveřejní.

Článek 68

Vědecká komise nezávislých odborníků

1. Komise přijme prostřednictvím prováděcího aktu ustanovení o zřízení vědecké komise nezávislých odborníků (dále jen „vědecká komise“), jejímž úkolem je podporovat činnosti v oblasti prosazování práva podle tohoto nařízení. Tento prováděcí akt se přijme přezkumným postupem uvedeným v čl. 98 odst. 2.

2. Vědecká komise se skládá z odborníků vybraných Komisí na základě aktuálních vědeckých nebo technických odborných znalostí v oblasti AI nezbytných pro plnění úkolů stanovených v odstavci 3 a je schopna prokázat splnění všech těchto podmínek:

a) má v oblasti AI zvláštní odborné znalosti a schopnosti a odborné znalosti vědecké nebo technické povahy;

b) není závislá na žádném poskytovateli systémů AI nebo obecných modelů AI;

c) je schopna vykonávat činnosti s náležitou péčí, přesně a objektivně.

Komise za konzultace s radou určí počet odborníků v komisi v souladu s požadovanými potřebami a zajistí spravedlivé genderové a zeměpisné zastoupení.

3. Vědecká komise poskytuje poradenství a podporu úřadu pro AI, zejména pokud jde o tyto úkoly:

a) podpora provádění a prosazování tohoto nařízení, pokud jde o obecné modely a systémy AI, přičemž zejména:

   i) upozorňuje úřad pro AI na možná systémová rizika na úrovni Unie, pokud jde o obecné modely AI v souladu s článkem 90;

   ii) přispívá k vývoji nástrojů a metodik pro hodnocení schopností obecných modelů a systémů AI, mimo jiné prostřednictvím referenčních hodnot;

   iii) poskytuje poradenství ohledně klasifikace obecných modelů AI se systémovým rizikem;

   iv) poskytuje poradenství ohledně klasifikace různých obecných modelů a systémů AI;

v) přispívá k vývoji nástrojů a šablon;

b) podpora činnosti orgánů dozoru nad trhem, a to na jejich žádost;

c) podpora přeshraniční činnosti dozoru nad trhem podle čl. 74 odst. 11, aniž jsou dotčeny pravomoci orgánů dozoru nad trhem;

d) podpora úřadu pro AI při plnění jeho povinností v souvislosti s ochranným postupem Unie podle článku 81.

4. Odborníci v rámci vědecké komise plní své úkoly nestranně a objektivně a zajišťují důvěrnost informací a údajů získaných při plnění svých úkolů a činností. Při plnění svých úkolů podle odstavce 3 od nikoho nevyžadují ani nepřijímají pokyny. Každý odborník vypracuje prohlášení o zájmech, které je veřejně dostupné. Úřad o AI zavede systémy a postupy s cílem aktivně řídit případné střety zájmů a zabránit jim.

5. Prováděcí akt uvedený v odstavci 1 obsahuje ustanovení o podmínkách, postupech a podrobných opatřeních pro vědeckou komisi a její členy při vydávání výstrah a při žádosti o pomoc úřadu pro AI při plnění úkolů vědecké komise.

Článek 69

Přístup ke skupině odborníků ze strany členských států

1. Členské státy mohou požádat odborníky vědecké komise o podporu svých činností v oblasti prosazování práva podle tohoto nařízení.

2. Za poradenství a podporu poskytnuté odborníky mohou být od členských států žádány poplatky. Struktura a výše poplatků, jakož i rozsah a struktura nahraditelných nákladů, se stanoví prostřednictvím prováděcího aktu uvedeného v čl. 68 odst. 1, přičemž se zohlední cíle náležitého provádění tohoto nařízení, nákladová efektivnost a nutnost zajistit, aby všechny členské státy měly k odborníkům účinný přístup.

3. Komise podle potřeby usnadní členským státům včasný přístup k odborníkům a zajistí, aby kombinace podpůrných činností prováděných prostřednictvím podpůrných unijních struktur pro testování AI podle článku 84 a odborníky podle tohoto článku byla účinně organizována a přinášela maximální přidanou hodnotu.

ODDÍL 2

Příslušné vnitrostátní orgány

Článek 70

Určení příslušných vnitrostátních orgánů a jednotného kontaktního místa

1. Pro účely tohoto nařízení každý členský stát zřídí nebo určí jakožto příslušné vnitrostátní orgány alespoň jeden oznamující orgán a alespoň jeden orgán dozoru nad trhem. Tyto příslušné vnitrostátní orgány vykonávají své pravomoci nezávisle, nestranně a nezaujatě, aby chránily objektivitu svých činností a úkolů a zajistily uplatňování a provádění tohoto nařízení. Členové těchto orgánů se zdrží jakéhokoliv jednání neslučitelného s povahou svých povinností. Jsou-li uvedené zásady dodrženy, mohou být takové činnosti a úkoly prováděny jedním nebo několika určenými orgány v souladu s organizačními potřebami členského státu.

2. Členské státy sdělí Komisi totožnost oznamujících orgánů a orgánů dozoru nad trhem a úkoly těchto orgánů, jakož i veškeré jejich následné změny. Členské státy zveřejní informace o způsobu, jímž lze příslušné orgány a jednotná kontaktní místa kontaktovat prostřednictvím elektronických komunikačních prostředků, a to do 2. srpna 2025. Členské státy určí orgán dozoru nad trhem, který bude působit jako jednotné kontaktní místo pro toto nařízení, a Komisi totožnost tohoto jednotného kontaktního místa oznámí. Komise zveřejní seznam jednotných kontaktních míst.

3. Členské státy zajistí, aby jejich příslušným vnitrostátním orgánům byly poskytnuty odpovídající technické, finanční a lidské zdroje a infrastruktura, které jim umožní účinně plnit úkoly podle tohoto nařízení. Příslušné vnitrostátní orgány mají zejména trvale k dispozici dostatečný počet pracovníků, jejichž způsobilost a odborné znalosti zahrnují důkladné porozumění technologiím AI, údajům a výpočtu údajů, ochraně osobních údajů, kybernetické bezpečnosti, základním právům a zdravotním a bezpečnostním rizikům, jakož i znalost platných norem a právních předpisů. Členské státy požadavky na odbornost a zdroje uvedené v tomto odstavci každoročně posoudí a v případě potřeby aktualizují.

4. Příslušné vnitrostátní orgány přijmou vhodná opatření k zajištění kybernetické bezpečnosti na náležité úrovni.

5. Při plnění svých úkolů jedná příslušný vnitrostátní orgán v souladu s povinnostmi týkajícími se důvěrnosti stanovenými v článku 78.

6. Do 2. srpna 2025, a poté jednou za dva roky, předloží členské státy Komisi zprávu o stavu finančních a lidských zdrojů příslušných vnitrostátních orgánů a posoudí jejich přiměřenost. Komise předá tyto informace radě k projednání a případným doporučením.

7. Komise usnadňuje výměnu zkušeností mezi příslušnými vnitrostátními orgány.

8. Příslušné vnitrostátní orgány mohou poskytovat pokyny a poradenství ohledně provádění tohoto nařízení, zejména malým a středním podnikům, včetně podniků začínajících, přičemž případně zohlední pokyny a poradenství rady a Komise. Kdykoli mají příslušné vnitrostátní orgány v úmyslu poskytnout pokyny a rady týkající se systému AI v oblastech, na které se vztahuje jiné právo Unie, vedou podle potřeby konzultaci s vnitrostátními orgány příslušnými podle tohoto práva Unie.

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

KAPITOLA VIII

DATABÁZE EU OBSAHUJÍCÍ VYSOCE RIZIKOVÉ SYSTÉMY AI

Článek 71

Databáze EU obsahující vysoce rizikové systémy AI uvedené v příloze III

1. Komise ve spolupráci s členskými státy zřizuje a udržuje databázi EU obsahující informace uvedené v odstavcích 2 a 3 tohoto článku ohledně vysoce rizikových systémů AI podle čl. 6 odst. 2, které jsou registrovány v souladu s články 49 a 60 a systémy umělé inteligence, které nejsou považovány za vysoce rizikové podle čl. 6 odst. 3 a které jsou registrovány v souladu s čl. 6 odst. 4 a článkem 49. Při stanovování funkčních specifikací takové databáze Komise konzultuje příslušné odborníky a při aktualizaci funkčních specifikací této databáze Komise konzultuje radu.

2. Poskytovatel nebo případně zplnomocněný zástupce vloží do databáze EU údaje uvedené v oddíle A a B přílohy VIII.

3. Zavádějící subjekt, který je orgánem veřejné moci, agenturou nebo subjektem nebo jedná jejich jménem v souladu s čl. 49 odst. 3 a 4, vloží do databáze EU údaje uvedené v oddíle C přílohy VIII.

4. Informace v databázi EU registrované v souladu s článkem 49 jsou s výjimkou oddílu uvedeného v čl. 49 odst. 4 a čl. 60 odst. 4 písm. c) přístupné a veřejně dostupné uživatelsky vstřícným způsobem. Tyto informace by měly být snadno dohledatelné a strojově čitelné. Informace registrované v souladu s článkem 60 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.

5. Databáze EU obsahuje osobní údaje pouze v míře nezbytné pro shromažďování a zpracovávání informací v souladu s tímto nařízením. Tyto informace zahrnují jména a kontaktní údaje fyzických osob, které odpovídají za registraci systému a mají zákonnou pravomoc zastupovat poskytovatele nebo případně zavádějící subjekt.