



V Bruseli 21. 4. 2021  
COM(2021) 206 final

2021/0106 (COD)

Návrh

**NARIADENIE EURÓPSKEHO PARLAMENTU A RADY,  
KTORÝM SA STANOVUJÚ HARMONIZOVANÉ PRAVIDLÁ V OBLASTI UMELEJ  
INTELIGENCIE (AKT O UMELEJ INTELIGENCII) A MENIA NIEKTORÉ  
LEGISLATÍVNE AKTY ÚNIE**

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

# DÔVODOVÁ SPRÁVA

## 1. KONTEXT NÁVRHU

### 1.1. Dôvody a ciele návrhu

Táto dôvodová správa je sprievodným dokumentom k návrhu nariadenia, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie (akt o umelej inteligencii). Umelá inteligencia je rýchlo sa rozvíjajúca skupina technológií, ktorá môže priniesť široké spektrum hospodárskych a spoločenských výhod vo všetkých priemyselných odvetviach a spoločenských činnostiach. Zlepšením predikcie, optimalizáciou operácií a pridelovania zdrojov, ako aj personalizáciou poskytovania služieb môže používanie umelej inteligencie podporiť sociálne a environmentálne priaznivé výsledky a poskytnúť spoločnostiam a európskemu hospodárstvu kľúčové konkurenčné výhody. Takéto opatrenia sú potrebné najmä v odvetviach s veľkým vplyvom, ktoré zahŕňajú zmenu klímy, životné prostredie a zdravie, verejný sektor, financie, mobilitu, vnútorné záležitosti a poľnohospodárstvo. Rovnaké prvky a techniky, ktoré poháňajú spoločenské a hospodárske prínosy umelej inteligencie však so sebou môžu priniesť aj nové riziká alebo negatívne dôsledky pre jednotlivcov či spoločnosť. EÚ sa vzhľadom na rýchlosť technologických zmien a možné výzvy zaväzuje, že sa bude usilovať o vyvážený prístup. Je v záujme Únie zachovať si vedúce postavenie EÚ v oblasti technológií a zabezpečiť, aby Európania mohli mať prospech z nových technológií vyvinutých a fungujúcich v súlade s hodnotami, základnými právami a zásadami Únie.

Týmto návrhom sa plní politický záväzok predsedníčky Ursuly von der Leyenovej, ktorá vo svojich politických usmerneniach pre Komisiu na roky 2019 – 2024 s názvom Ambicióznejšia Únia<sup>1</sup> oznámila, že Komisia predloží právne predpisy o koordinovanom európskom prístupe k ľudským a etickým dôsledkom umelej inteligencie. Na základe tohto oznámenia Komisia 19. februára 2020 zverejnila Bielu knihu o umelej inteligencii – európsky prístup k excelentnosti a dôvere<sup>2</sup>. V bielej knihe sa stanovujú politické možnosti, ako dosiahnuť dvojaký cieľ: nabádať k využívaniu umelej inteligencie a zároveň riešiť riziká spojené s niektorými použitiami tejto technológie. Cieľom tohto návrhu je vykonanie druhého cieľa v oblasti rozvoja ekosystému dôvery, a to navrhnutím právneho rámca pre dôveryhodnú umelú inteligenciu. Tento návrh je založený na hodnotách a základných právach EÚ a jeho cieľom je dodať ľuďom a ostatným používateľom odvahu prijať riešenia založené na umelej inteligencii a súčasne podporiť podniky, aby tieto riešenia rozvíjali. Umelá inteligencia by mala byť nástrojom pre ľudí a hybnou silou pre dobro v spoločnosti, pričom jej hlavným cieľom je zvýšenie blahobytu ľudí. Pravidlá pre umelú inteligenciu, ktorá je dostupná na trhu Únie alebo inak ovplyvňuje ľudí v Únii, by preto mali byť sústredené na človeka, aby sa ľudia mohli spoľahnúť, že táto technológia sa používa spôsobom, ktorý je bezpečný a v súlade s právnymi predpismi a že sú rešpektované základné práva. Komisia po zverejnení bielej knihy uskutočnila rozsiahlu konzultáciu so zainteresovanými stranami, o ktorú prejavilo veľký záujem množstvo zainteresovaných strán, ktoré vo veľkej miere vyjadrili podporu regulačným zásahom zameraným na riešenie výziev a obáv, ktoré prináša čoraz väčšie využívanie umelej inteligencie.

Návrh je reakciou aj na výslovné žiadosti Európskeho parlamentu a Európskej rady, ktoré opakovane vyzývajú na legislatívne opatrenia na zabezpečenie dobre fungujúceho vnútorného

<sup>1</sup> [https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission\\_sk.pdf](https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_sk.pdf).

<sup>2</sup> Európska komisia, Biela kniha o umelej inteligencii – európsky prístup k excelentnosti a dôvere, COM(2020) 65 final, 2020.

trhu so systémami umelej inteligencie, kde sa výhody aj riziká umelej inteligencie primerane riešia na úrovni Únie. Návrhom sa podporuje cieľ Únie stať sa svetovým lídrom v rozvoji bezpečnej, dôveryhodnej a etickej umelej inteligencie, ako ho vyjadrila Európska rada<sup>3</sup>, a zabezpečuje sa ochrana etických zásad, ako to osobitne požaduje Európsky parlament<sup>4</sup>.

Európska rada v roku 2017 vyzvala na „urýchlené zaobranie sa novými trendmi“ vrátane „otázok, ako je umelá inteligencia [...], pričom je zároveň potrebné zabezpečiť vysokú úroveň ochrany údajov, digitálnych práv a etických noriem“<sup>5</sup>. Rada vo svojich záveroch z roku 2019 o koordinovanom pláne vývoja a používania umelej inteligencie s pôvodom v Európe<sup>6</sup> ďalej zdôraznila význam zabezpečenia plného rešpektovania práv európskych občanov a vyzvala na to, aby sa preskúmali príslušné platné právne predpisy, aby spĺňali svoj účel vzhľadom na nové príležitosti a výzvy, ktoré prináša umelá inteligencia. Európska rada okrem toho požiadala o jasné určenie aplikácií umelej inteligencie, ktoré by sa mali považovať za vysokorizikové<sup>7</sup>.

V najnovších záveroch z 21. októbra 2020 ďalej vyzvala na riešenie nepriehľadnosti, zložitosti, zaujatosti, určitého stupňa nepredvídateľnosti a čiastočne autonómneho správania sa určitých systémov umelej inteligencie, aby sa zaistila ich kompatibilita so základnými právami a uľahčilo sa presadzovanie právnych predpisov<sup>8</sup>.

Európsky parlament takisto vykonáva značné množstvo práce v oblasti umelej inteligencie. V októbri 2020 prijal niekoľko uznesení týkajúcich sa umelej inteligencie, a to aj o etike<sup>9</sup>, zodpovednosti<sup>10</sup> a autorských právach<sup>11</sup>. V roku 2021 po nich nasledovali uznesenia o umelej inteligencii v trestných veciach<sup>12</sup> a vo vzdelávaní, v kultúre a audiovizuálnom odvetví<sup>13</sup>. V uznesení Európskeho parlamentu k rámcu etických aspektov umelej inteligencie, robotiky a súvisiacich technológií sa Komisii konkrétne odporúča, aby navrhla legislatívne opatrenia na využitie príležitostí a výhod umelej inteligencie, ale aj na zabezpečenie ochrany etických zásad. Uznesenie obsahuje text legislatívneho návrhu nariadenia o etických zásadách pre vývoj, nasadzovanie a používanie umelej inteligencie, robotiky a súvisiacich technológií. V súlade s politickým záväzkom predsedníčky Ursuly von der Leyenovej v jej politických

<sup>3</sup> Európska rada, [Mimoriadne zasadnutie Európskej rady \(1. a 2. októbra 2020\) – závery](#), EUCO 13/20, 2020, s. 6.

<sup>4</sup> Uznesenie Európskeho parlamentu z 20. októbra 2020 s odporúčaniami pre Komisiu k rámcu etických aspektov umelej inteligencie, robotiky a súvisiacich technológií, 2020/2012(INL).

<sup>5</sup> Európska rada, [Zasadnutie Európskej rady \(19. októbra 2017\) – závery](#), EUCO 14/17, 2017, s. 8.

<sup>6</sup> Rada Európskej únie, [Umelá inteligencia b\) Závery o koordinovanom pláne v oblasti umelej inteligencie – prijatie](#), 6177/19, 2019.

<sup>7</sup> Európska rada, [Mimoriadne zasadnutie Európskej rady \(1. a 2. októbra 2020\) – závery](#), EUCO 13/20, 2020.

<sup>8</sup> Rada Európskej únie, [Závery predsedníctva – Charta základných práv v kontexte umelej inteligencie a digitálnych zmien](#), 11481/20, 2020.

<sup>9</sup> Uznesenie Európskeho parlamentu z 20. októbra 2020 k rámcu etických aspektov umelej inteligencie, robotiky a súvisiacich technológií, [2020/2012\(INL\)](#).

<sup>10</sup> Uznesenie Európskeho parlamentu z 20. októbra 2020 k systému občianskoprávnej zodpovednosti za umelú inteligenciu, [2020/2014\(INL\)](#).

<sup>11</sup> Uznesenie Európskeho parlamentu z 20. októbra 2020 o právach duševného vlastníctva v súvislosti s rozvojom technológií umelej inteligencie, [2020/2015\(INI\)](#).

<sup>12</sup> Návrh správy Európskeho parlamentu, Umelá inteligencia v trestnom práve a jej využívanie policajnými a justičnými orgánmi v trestných veciach, [2020/2016\(INI\)](#).

<sup>13</sup> Návrh správy Európskeho parlamentu, Umelá inteligencia vo vzdelávaní, v kultúre a audiovizuálnom sektore, [2020/2017\(INI\)](#). [Komisia v tejto súvislosti prijala akčný plán digitálneho vzdelávania 2021 – 2027: Prispôsobenie vzdelávania a odbornej prípravy digitálnemu veku, v rámci ktorého sa predpokladá vypracovanie etických usmernení o umelej inteligencii a využívaní údajov vo vzdelávaní – oznámenie Komisie COM\(2020\) 624 final.](#)

usmerneniach, pokiaľ ide o uznesenia prijaté Európskym parlamentom podľa článku 225 ZFEÚ, sa v tomto návrhu zohľadňuje uvedené uznesenie Európskeho parlamentu pri plnom rešpektovaní zásad proporcionality, subsidiarity a lepšej tvorby práva.

Komisia vzhľadom na tento politický kontext predkladá navrhovaný regulačný rámec pre umelú inteligenciu s týmito **konkrétnymi cieľmi**:

- zabezpečiť, aby používané systémy umelej inteligencie uvedené na trh Únie boli bezpečné a v súlade s platnými právnymi predpismi týkajúcimi sa základných práv a hodnôt Únie,
- zabezpečiť právnu istotu na uľahčenie investícií a inovácií v oblasti umelej inteligencie,
- zlepšiť riadenie a účinné presadzovanie platných právnych predpisov týkajúcich sa základných práv a bezpečnostných požiadaviek uplatniteľných pre systémy umelej inteligencie,
- uľahčiť rozvoj jednotného trhu v záujme zákonných, bezpečných a dôveryhodných aplikácií umelej inteligencie a zabrániť fragmentácii trhu.

Na dosiahnutie týchto cieľov sa v tomto návrhu uvádza vyvážený a primeraný horizontálny regulačný prístup k umelej inteligencii, ktorý sa obmedzuje na minimálne nevyhnutné požiadavky na riešenie rizík a problémov spojených s umelou inteligenciou bez toho, aby zbytočne obmedzoval technologický vývoj alebo mu bránil alebo inak neúmerne zvyšoval náklady na uvádzanie riešení umelej inteligencie na trh. V návrhu sa stanovuje spoľahlivý a flexibilný rámec. Na jednej strane je komplexný a nadčasový vo svojich základných regulačných možnostiach vrátane požiadaviek založených na zásadách, ktoré by systémy umelej inteligencie mali spĺňať. Na druhej strane sa ním zavádza proporcionálny regulačný systém zameraný na presne definovaný regulačný prístup založený na riziku, ktorý nevytvára zbytočné obmedzenia obchodu, pričom právny zásah je prispôbený takým konkrétnym situáciám, v ktorých existuje oprávnený dôvod na obavy alebo v ktorých možno v blízkej budúcnosti takéto obavy odôvodnene očakávať. Právny rámec zároveň obsahuje flexibilné mechanizmy, ktoré umožňujú jeho dynamické prispôbovanie vývoju technológie a vzniku nových situácií vyvolávajúcich obavy.

V návrhu sa stanovujú harmonizované pravidlá pre vývoj, uvádzanie na trh a využívanie systémov umelej inteligencie v Únii na základe primeraného prístupu založeného na riziku. Navrhuje sa v ňom jednotná a nadčasová definícia umelej inteligencie. Určité osobitne škodlivé praktiky v oblasti umelej inteligencie sa zakazujú, pretože sú v rozpore s hodnotami Únie a súčasne sa navrhujú konkrétne obmedzenia a záruky v súvislosti s niektorými použitiami systémov diaľkovej biometrickej identifikácie na účely presadzovania práva. V návrhu sa stanovuje spoľahlivá metodika rizika na definovanie „vysokorizikových“ systémov umelej inteligencie, ktoré predstavujú významné riziká pre zdravie a bezpečnosť alebo základné práva osôb. Tieto systémy umelej inteligencie budú musieť spĺňať horizontálne záväzné požiadavky na dôveryhodnú umelú inteligenciu a dodržiavať postupy posudzovania zhody ešte pred ich uvedením na trh Únie. Poskytovateľom a používateľom týchto systémov sa ukladajú aj predvídateľné, primerané a jasné povinnosti s cieľom zaistiť bezpečnosť a dodržiavanie platných právnych predpisov, ktoré slúžia na ochranu základných práv počas celého životného cyklu systémov umelej inteligencie. V prípade niektorých konkrétnych systémov umelej inteligencie sa navrhujú iba minimálne povinnosti týkajúce sa transparentnosti, najmä ak sa používajú chatboty alebo tzv. deepfakes.

Navrhované pravidlá sa budú presadzovať prostredníctvom systému riadenia na úrovni členských štátov, a to na základe už existujúcich štruktúr, ako aj prostredníctvom

mechanizmu spolupráce na úrovni Únie, pričom sa zriadi Európska rada pre umelú inteligenciu. Okrem toho sa navrhujú aj ďalšie opatrenia na podporu inovácií, najmä prostredníctvom experimentálnych regulačných prostredí umelej inteligencie a ďalších opatrení na zníženie regulačnej záťaže, ako aj na podporu malých a stredných podnikov a startupov.

## **1.2. Súlad s existujúcimi ustanoveniami v tejto oblasti politiky**

Horizontálna povaha návrhu si vyžaduje úplný súlad s platnými právnymi predpismi Únie, ktoré sa vzťahujú na odvetvia, v ktorých sa vysokorizikové systémy umelej inteligencie už používajú alebo sa pravdepodobne budú používať v blízkej budúcnosti.

Návrh je takisto v súlade s Chartou základných práv EÚ a existujúcimi sekundárnymi právnymi predpismi Únie týkajúcimi sa ochrany údajov, ochrany spotrebiteľa, zákazu diskriminácie a rodovej rovnosti. Týmto návrhom nie je dotknuté všeobecné nariadenie o ochrane údajov [nariadenie (EÚ) 2016/679] ani smernica o presadzovaní práva [smernica (EÚ) 2016/680] a tento návrh ich dopĺňa súborom harmonizovaných pravidiel, ktoré sa vzťahujú na navrhovanie, vývoj a používanie určitých vysokorizikových systémov umelej inteligencie, ako aj obmedzeniami niektorých použití systémov diaľkovej biometrickej identifikácie. Týmto návrhom sa okrem toho dopĺňa platné právo Únie týkajúce sa zákazu diskriminácie konkrétnymi požiadavkami, ktorých cieľom je minimalizovať riziko algoritmickej diskriminácie, najmä v súvislosti s návrhom a kvalitou súborov údajov používaných na vývoj systémov umelej inteligencie, a ktoré obsahujú aj povinnosti testovania, riadenia rizík, dokumentácie a ľudského dohľadu počas celého životného cyklu systémov umelej inteligencie. Týmto návrhom nie je dotknuté uplatňovanie právnych predpisov Únie v oblasti hospodárskej súťaže.

Pokiaľ ide o vysokorizikové systémy umelej inteligencie, ktoré sú bezpečnostnými súčasťami výrobkov, tento návrh bude začlenený do odvetvových právnych predpisov v oblasti bezpečnosti s cieľom zabezpečiť súlad, zabrániť duplicitám a minimalizovať ďalšiu záťaž. Najmä pokiaľ ide o vysokorizikové systémy umelej inteligencie súvisiace s výrobkami, na ktoré sa vzťahujú právne predpisy nového legislatívneho rámca (napr. stroje, zdravotnícke pomôcky, hračky), požiadavky na systémy umelej inteligencie uvedené v tomto návrhu sa budú kontrolovať v rámci existujúcich postupov posudzovania zhody podľa príslušných právnych predpisov nového legislatívneho rámca. Pokiaľ ide o súhrn požiadaviek, zatiaľ čo na bezpečnostné riziká špecifické pre systémy umelej inteligencie sa majú vzťahovať požiadavky tohto návrhu, cieľom právnych predpisov nového legislatívneho rámca je zabezpečiť celkovú bezpečnosť konečného výrobku, a preto môžu obsahovať osobitné požiadavky týkajúce sa bezpečnej integrácie systému umelej inteligencie do konečného výrobku. Návrh nariadenia o strojových zariadeniach, ktorý je prijatý v rovnaký deň ako tento návrh, plne odráža tento prístup. Pokiaľ ide o vysokorizikové systémy umelej inteligencie súvisiace s výrobkami, na ktoré sa vzťahujú príslušné právne predpisy podľa starého prístupu (napr. letectvo, automobily), tento návrh by sa priamo neuplatňoval. Základné požiadavky *ex ante* na vysokorizikové systémy umelej inteligencie stanovené v tomto návrhu sa však budú musieť zohľadniť pri prijímaní príslušných vykonávacích alebo delegovaných právnych predpisov podľa týchto aktov.

Pokiaľ ide o systémy umelej inteligencie poskytované alebo používané regulovanými úverovými inštitúciami, orgány zodpovedné za dohľad nad právnymi predpismi Únie v oblasti finančných služieb by mali byť určené ako príslušné orgány pre dohľad nad požiadavkami tohto návrhu, aby sa zabezpečilo jednotné presadzovanie povinností podľa tohto návrhu a právnych predpisov Únie v oblasti finančných služieb, kde sú systémy umelej inteligencie do určitej miery nepriamo regulované vo vzťahu k internému systému riadenia úverových

inštitúcií. S cieľom ďalej posilniť súlad sa postup posudzovania zhody a niektoré procesné povinnosti poskytovateľov podľa tohto návrhu začleňujú do postupov podľa smernice 2013/36/EÚ o prístupe k činnosti úverových inštitúcií a prudenciálnom dohľade<sup>14</sup>.

Tento návrh je takisto v súlade s platnými právnymi predpismi Únie o službách, ako aj o sprostredkovateľských službách, ktoré upravuje smernica o elektronickom obchode 2000/31/ES<sup>15</sup> a nedávny návrh aktu o digitálnych službách, ktorý vypracovala Komisia<sup>16</sup>.

Pokiaľ ide o systémy umelej inteligencie, ktoré sú súčasťou rozsiahlych informačných systémov v priestore slobody, bezpečnosti a spravodlivosti spravovanom Agentúrou Európskej únie na prevádzkové riadenie rozsiahlych informačných systémov v priestore slobody, bezpečnosti a spravodlivosti (eu-LISA), tento návrh sa nebude vzťahovať na tie systémy umelej inteligencie, ktoré boli uvedené na trh alebo do prevádzky ešte pred uplynutím jedného roka od dátumu uplatňovania tohto nariadenia, pokiaľ náhrada alebo zmena týchto právnych aktov nevedie k významnej zmene návrhu alebo plánovaného účelu príslušného systému, resp. systémov umelej inteligencie.

### 1.3. Súlad s ostatnými politikami Únie

Návrh je súčasťou širšieho komplexného balíka opatrení zameraných na problémy súvisiace s vývojom a používaním umelej inteligencie, ako sa uvádza v bielej knihe o umelej inteligencii. Je teda zabezpečený súlad i komplementarita s inými prebiehajúcimi alebo plánovanými iniciatívami Komisie, ktorých cieľom je takisto riešenie týchto problémov vrátane revízie odvetvových právnych predpisov týkajúcich sa výrobkov (napr. smernica o strojových zariadeniach, smernica o všeobecnej bezpečnosti výrobkov), ako aj s iniciatívami, ktoré sa zameriavajú na otázky zodpovednosti týkajúce sa nových technológií vrátane systémov umelej inteligencie. Tieto iniciatívy budú vychádzať z tohto návrhu a budú ho dopĺňať, aby sa zabezpečila právna čistota a podporil rozvoj ekosystému dôvery v umelú inteligenciu v Európe.

Návrh je aj v súlade s celkovou digitálnou stratégiou Komisie v jej prínose k podpore technológie v službách človeka, čo je jeden z troch hlavných pilierov zamerania a cieľov politiky uvedených v oznámení Formovanie digitálnej budúcnosti Európy<sup>17</sup>. Stanovuje sa v ňom súdržný, účinný a primeraný rámec na zabezpečenie vývoja umelej inteligencie spôsobom, ktorý rešpektuje práva ľudí a získava si ich dôveru, vďaka čomu sa Európa pripraví na digitálny vek a ďalších desať rokov sa stane **digitálnym desaťročím**<sup>18</sup>.

Podpora inovácií založených na umelej inteligencii je navyše úzko spojená s **aktom o správe údajov**<sup>19</sup>, so **smernicou o otvorených dátach**<sup>20</sup> a s ďalšími iniciatívami v rámci **Európskej**

<sup>14</sup> Smernica Európskeho parlamentu a Rady 2013/36/EÚ z 26. júna 2013 o prístupe k činnosti úverových inštitúcií a prudenciálnom dohľade nad úverovými inštitúciami a investičnými spoločnosťami, o zmene smernice 2002/87/ES a o zrušení smerníc 2006/48/ES a 2006/49/ES (Text s významom pre EHP) (Ú. v. EÚ L 176, 27.6.2013, s. 338 – 436).

<sup>15</sup> Smernica Európskeho parlamentu a Rady 2000/31/ES z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode (ďalej len „smernica o elektronickom obchode“) (Ú. v. ES L 178, 17.7.2000, s. 1 – 16).

<sup>16</sup> Pozri návrh NARIADENIE EURÓPSKEHO PARLAMENTU A RADY o jednotnom trhu s digitálnymi službami (akt o digitálnych službách) a o zmene smernice 2000/31/ES, COM(2020) 825 final.

<sup>17</sup> Oznámenie Komisie, Formovanie digitálnej budúcnosti Európy, COM(2020) 67 final.

<sup>18</sup> [Digitálny kompas 2030: európska cesta k digitálnemu desaťročiu.](#)

<sup>19</sup> Návrh nariadenia o európskej správe údajov (akt o správe údajov) [COM\(2020\) 767](#).

<sup>20</sup> Smernica Európskeho parlamentu a Rady (EÚ) 2019/1024 z 20. júna 2019 o otvorených dátach a opakovanom použití informácií verejného sektora (PE/28/2019/REV/1, Ú. v. EÚ L 172, 26.6.2019, s. 56 – 83).



**dátovej stratégii**<sup>21</sup>, vďaka čomu sa vytvoria dôveryhodné mechanizmy a služby na opakované použitie, zdieľanie a zhromažďovanie údajov, ktoré sú nevyhnutné pre vývoj vysokokvalitných modelov umelej inteligencie založených na údajoch.

Návrhom sa okrem toho významne posilňuje úloha Únie v oblasti pomoci pri formovaní globálnych noriem a štandardov a podpore dôveryhodnej umelej inteligencie, ktorá je v súlade s hodnotami a záujmami Únie. Poskytuje Únii silný základ pre ďalšiu spoluprácu s externými partnermi vrátane tretích krajín a na medzinárodných fórach v otázkach týkajúcich sa umelej inteligencie.

## **2. PRÁVNY ZÁKLAD, SUBSIDIARITA A PROPORCIONALITA**

### **2.1. Právny základ**

Právnym základom tohto návrhu je predovšetkým článok 114 Zmluvy o fungovaní Európskej únie (ZFEÚ), v ktorom sa stanovuje prijímanie opatrení na zabezpečenie vytvorenia a fungovania vnútorného trhu.

Tento návrh predstavuje hlavnú súčasť stratégie EÚ pre jednotný digitálny trh. Hlavným cieľom tohto návrhu je zabezpečiť správne fungovanie vnútorného trhu stanovením harmonizovaných pravidiel, najmä v oblasti vývoja, uvedenia na trh Únie a používania výrobkov a služieb využívajúcich technológie umelej inteligencie alebo poskytovaných ako samostatné systémy umelej inteligencie. Niektoré členské štáty už zvažujú vnútroštátne pravidlá na zabezpečenie toho, aby bola umelá inteligencia bezpečná a aby sa vyvíjala a používala v súlade s povinnosťami týkajúcimi sa základných práv. To pravdepodobne povedie k dvom hlavným problémom: i) fragmentácii vnútorného trhu v oblasti základných prvkov týkajúcej sa najmä požiadaviek na výrobky a služby umelej inteligencie, ich uvádzania na trh, používania, zodpovednosti a dohľadu zo strany orgánov verejnej moci a ii) značnému poklesu právnej istoty tak pre poskytovateľov, ako aj používateľov systémov umelej inteligencie v tom, ako sa budú súčasné a nové pravidlá vzťahovať na tieto systémy v Únii. Vzhľadom na rozšírený cezhraničný pohyb výrobkov a služieb možno tieto dva problémy najlepšie vyriešiť prostredníctvom harmonizovaných právnych predpisov EÚ.

V návrhu sa v skutočnosti vymedzujú spoločné záväzné požiadavky týkajúce sa navrhovania a vývoja určitých systémov umelej inteligencie pred ich uvedením na trh, ktoré sa budú ďalej zavádzať prostredníctvom harmonizovaných technických noriem. V návrhu sa rieši aj situácia po uvedení systémov umelej inteligencie na trh, a to harmonizáciou spôsobu, akým sa vykonávajú kontroly *ex post*.

Navyše vzhľadom na to, že tento návrh obsahuje určité osobitné pravidlá ochrany jednotlivcov v súvislosti so spracúvaním osobných údajov, najmä obmedzenia používania systémov umelej inteligencie na diaľkovú biometrickú identifikáciu v reálnom čase vo verejne dostupných priestoroch na účely presadzovania práva, je vhodné, aby sa osobitné pravidlá uvedené v tomto nariadení zakladali na článku 16 ZFEÚ.

### **2.2. Subsidiarita (v prípade inej ako výlučnej právomoci)**

Povaha umelej inteligencie, ktorá sa často opiera o veľké a rozmanité súbory údajov a ktorá môže byť súčasťou akéhokoľvek výrobku alebo služby vo voľnom obehú na vnútornom trhu, má za následok, že ciele tohto návrhu nemožno účinne dosiahnuť len na úrovni členských štátov. Okrem toho vznikajúca zmes potenciálne odlišných vnútroštátnych pravidiel bude

<sup>21</sup> [Oznámenie Komisie, Európska dátová stratégia, COM\(2020\) 66 final.](#)

brániť plynulému obehu výrobkov a služieb súvisiacich so systémami umelej inteligencie v celej EÚ a bude neúčinná pri zaisťovaní bezpečnosti a ochrany základných práv a hodnôt Únie v jednotlivých členských štátoch. Vnútroštátne prístupy k riešeniu problémov vytvoria iba ďalšiu právnu neistotu a prekážky a spomalia uvádzanie umelej inteligencie na trh.

Ciele tohto návrhu možno lepšie dosiahnuť na úrovni Únie, aby sa zabránilo ďalšej fragmentácii jednotného trhu na potenciálne protichodné vnútroštátne rámce brániace voľnému pohybu tovaru a služieb, ktoré obsahujú umelú inteligenciu. Spoľahlivý európsky regulačný rámec pre dôveryhodnú umelú inteligenciu okrem toho zabezpečí rovnaké podmienky a ochranu všetkých ľudí a súčasne posilní európsku konkurencieschopnosť a priemyselnú základňu v oblasti umelej inteligencie. Jedine spoločnými opatreniami na úrovni Únie možno takisto chrániť digitálnu suverenitu Únie a využiť jej nástroje a regulačné právomoci na formovanie globálnych pravidiel a noriem.

### **2.3. Proporcionalita**

Návrh vychádza z existujúcich právnych rámcov a je primeraný a potrebný na dosiahnutie svojich cieľov, pretože sa riadi prístupom založeným na riziku a prináša so sebou regulačnú záťaž iba vtedy, keď je pravdepodobné, že systém umelej inteligencie bude predstavovať vysoké riziko pre základné práva a bezpečnosť. V prípade iných systémov umelej inteligencie, ktoré nepredstavujú vysoké riziko, sa ukladajú iba veľmi obmedzené povinnosti týkajúce sa transparentnosti, napríklad pokiaľ ide o poskytovanie informácií umožňujúcich označiť použitie systému umelej inteligencie pri interakcii s ľuďmi. V prípade vysokorizikových systémov umelej inteligencie sú požiadavky na vysokokvalitné údaje, dokumentáciu a vysledovateľnosť, transparentnosť, ľudský dohľad, presnosť a spoľahlivosť nevyhnutne potrebné na zmiernenie rizík pre základné práva a bezpečnosť, ktoré so sebou prináša umelá inteligencia a na ktoré sa nevzťahujú iné existujúce právne rámce. Harmonizované normy a podporné usmerňujúce nástroje a nástroje na zabezpečenie dodržiavania predpisov pomôžu poskytovateľom a používateľom pri dodržiavaní požiadaviek stanovených v návrhu a minimalizujú ich náklady. Náklady, ktoré vzniknú prevádzkovateľom, sú primerané dosiahnutým cieľom, hospodárskym prínosom a zlepšeniu reputácie, ktoré môžu prevádzkovatelia od tohto návrhu očakávať.

### **2.4. Výber nástroja**

Výber nariadenia ako právneho nástroja je odôvodnený potrebou jednotného uplatňovania nových pravidiel, ako je definícia umelej inteligencie, zákaz určitých škodlivých praktík založených na umelej inteligencii a klasifikácia určitých systémov umelej inteligencie. Priama uplatniteľnosť nariadenia v súlade s článkom 288 ZFEÚ zníži právnu fragmentáciu a uľahčí rozvoj jednotného trhu pre zákonné, bezpečné a dôveryhodné systémy umelej inteligencie. Dosiahne sa to najmä zavedením harmonizovaného súboru základných požiadaviek týkajúcich sa systémov umelej inteligencie klasifikovaných ako vysokorizikové a povinností pre poskytovateľov a používateľov týchto systémov, čím salepší ochrana základných práv a poskytne právna istota tak prevádzkovateľom, ako aj spotrebiteľom.

Ustanovenia nariadenia súčasne nie sú príliš normatívne a ponechávajú priestor pre opatrenia členských štátov na rôznych úrovniach, pokiaľ ide o prvky, ktoré neohrozujú ciele iniciatívy, najmä vnútornú organizáciu systému dohľadu nad trhom a zavádzanie opatrení na podporu inovácií.



### 3. VÝSLEDKY HODNOTENÍ *EX POST*, KONZULTÁCIÍ SO ZAJINTERESOVANÝMI STRANAMI A POSÚDENÍ VPLYVU

#### 3.1. Konzultácia so zainteresovanými stranami

Tento návrh je výsledkom rozsiahlej konzultácie so všetkými hlavnými zainteresovanými stranami, pri ktorej Komisia uplatnila všeobecné zásady a minimálne normy pre konzultácie so zainteresovanými stranami.

**Verejná online konzultácia** sa začala 19. februára 2020 spolu s uverejnením bielej knihy o umelej inteligencii a trvala do 14. júna 2020. Cieľom uvedenej konzultácie bolo zhromaždiť názory a stanoviská k bielej knihe. Bola zameraná na všetky zainteresované strany z verejného i súkromného sektora vrátane verejnej správy, miestnych orgánov, obchodných i neobchodných organizácií, sociálnych partnerov, odborníkov, akademických pracovníkov a občanov. Komisia po analýze všetkých prijatých odpovedí zverejnila na svojom webovom sídle zhrnutie výsledkov a jednotlivé odpovede<sup>22</sup>.

Celkovo bolo prijatých 1 215 príspevkov, z ktorých 352 bolo od spoločností alebo obchodných organizácií/združení, 406 od jednotlivcov (92 % jednotlivcov bolo z EÚ), 152 v mene akademických/výskumných inštitúcií a 73 od orgánov verejnej moci. Názory občianskej spoločnosti zastupovalo 160 respondentov (z nich bolo deväť spotrebiteľských organizácií, 129 mimovládnych organizácií a 22 odborových zväzov), 72 respondentov prispelo ako „iní“. Z 352 obchodných a priemyselných zástupcov bolo 222 obchodných spoločností a obchodných zástupcov, z toho 41,5 % tvorili mikropodniky a malé a stredné podniky. Zvyšok predstavovali záujmové združenia. Celkovo 84 % odpovedí podnikov a priemyslu pochádzalo z EÚ<sup>27</sup>. V závislosti od otázky 81 až 598 respondentov využilo na vkladanie komentárov možnosť voľného textu. Prostredníctvom webového sídla EU Survey bolo predložených viac ako 450 pozičných dokumentov, a to buď popri odpovediach na dotazník (viac ako 400) alebo ako samostatné príspevky (viac ako 50).

Zainteresované strany sa celkovo zhodujú v tom, že je potrebné konať. Veľká väčšina zainteresovaných strán súhlasí s tým, že existujú legislatívne medzery alebo že sú potrebné nové právne predpisy. Niekoľko zainteresovaných strán však varuje Komisiu, aby sa vyhla duplicite, konfliktu povinností a nadmernej regulácii. V množstve pripomienok sa zdôrazňoval význam technologicky neutrálneho a primeraného regulačného rámca.

Zainteresované strany prevažne požadovali úzku, jasnú a presnú definíciu umelej inteligencie. Zainteresované strany navyše zdôraznili, že okrem objasnenia pojmu umelá inteligencia je dôležité definovať pojmy „riziko“, „vysokorizikový“, „nízkorizikový“, „diaľková biometrická identifikácia“ a „ujma“.

Väčšina respondentov je výslovne za prístup založený na riziku. Použitie rámca založeného na riziku sa považovalo za lepšiu možnosť ako všeobecná regulácia všetkých systémov umelej inteligencie. Typy rizík a hrozieb by mali byť založené na prístupe podľa jednotlivých odvetví a podľa jednotlivých prípadov. Pri výpočte rizík by sa mal zohľadniť aj vplyv na práva a bezpečnosť.

Na podporu umelej inteligencie by mohli byť veľmi užitočné experimentálne regulačné prostredia, ktoré vítajú určité zainteresované strany, najmä obchodné združenia.

Spomedzi tých, ktorí vyjadrili svoje stanovisko k modelom presadzovania, viac ako 50 % respondentov, najmä z obchodných združení, podporilo kombináciu hodnotenia rizík *ex ante* a presadzovania *ex post* v prípade vysokorizikových systémov umelej inteligencie.

<sup>22</sup> [Všetky výsledky konzultácie sa nachádzajú tu.](#)

### 3.2. Získavanie a využívanie expertízy

Návrh vychádza z dvojročnej analýzy a úzkeho zapojenia zainteresovaných strán vrátane akademických pracovníkov, podnikov, sociálnych partnerov, mimovládnych organizácií, členských štátov a občanov. Prípravné práce sa začali v roku 2018 zriadením inkluzívnej a širokej **expertnej skupiny na vysokej úrovni pre umelú inteligenciu (HLEG)** zloženej z 52 známych odborníkov, ktorých úlohou bolo radiť Komisii pri vykonávaní stratégie Komisie pre umelú inteligenciu. Komisia v apríli 2019 podporila<sup>23</sup> kľúčové požiadavky stanovené v etických usmerneniach pre dôveryhodnú umelú inteligenciu, ktoré vydala expertná skupina na vysokej úrovni pre umelú inteligenciu<sup>24</sup> a ktoré boli prepracované tak, aby zohľadňovali viac ako 500 príspevkov od zainteresovaných strán. Kľúčové požiadavky odrážajú rozšírený a spoločný prístup, že vývoj a používanie umelej inteligencie by sa mali riadiť určitými základnými hodnotovými zásadami, o čom svedčí množstvo etických kódexov a zásad vypracovaných mnohými súkromnými a verejnými organizáciami v Európe i mimo nej. Vďaka zoznamu bodov na posudzovanie dôveryhodnej umelej inteligencie<sup>25</sup> boli tieto požiadavky zavedené v skúšobnom procese, do ktorého sa zapojilo viac ako 350 organizácií.

Okrem toho bola vytvorená **Aliancia pre umelú inteligenciu**<sup>26</sup> ako platforma pre približne 4 000 zainteresovaných strán na účely diskusie o technologických a spoločenských dopadoch umelej inteligencie, ktoré vrcholia na každoročnom zhromaždení pre umelú inteligenciu.

**Bielou knihou** o umelej inteligencii sa ďalej rozvinul tento inkluzívny prístup a podnietili sa pripomienky viac ako 1 250 zainteresovaných strán vrátane viac ako 450 dodatočných pozičných dokumentov. V dôsledku toho Komisia zverejnila úvodné posúdenie vplyvu, ku ktorému bolo predložených viac ako 130 pripomienok<sup>27</sup>. Zorganizovali sa aj **ďalšie semináre a podujatia pre zainteresované strany**, pričom ich výsledky potvrdzujú analýzu v posúdení vplyvu, ako aj politické rozhodnutia uskutočnené v tomto návrhu<sup>28</sup>. Na účely posúdenia vplyvu bola obstaraná aj **externá štúdia**.

### 3.3. Posúdenie vplyvu

V súlade so svojou politikou „lepšej právnej regulácie“ Komisia vykonala posúdenie vplyvu tohto návrhu, ktoré preskúmal výbor Komisie pre kontrolu regulácie. Stretnutie s výborom pre kontrolu regulácie sa uskutočnilo 16. decembra 2020 a po ňom nasledovalo negatívne stanovisko. Po podstatnej revízii posúdenia vplyvu s cieľom reagovať na pripomienky a po opätovnom predložení posúdenia vplyvu výbor pre kontrolu regulácie vydal 21. marca 2021 pozitívne stanovisko. Stanoviská výboru pre kontrolu regulácie, odporúčania a objasnenie toho, ako sa zohľadnili, sú uvedené v prílohe 1 k posúdeniu vplyvu.

Komisia preskúmala rôzne politické možnosti na dosiahnutie všeobecného cieľa návrhu, ktorým je **zabezpečiť správne fungovanie jednotného trhu** vytvorením podmienok pre vývoj a používanie dôveryhodnej umelej inteligencie v Únii.

<sup>23</sup> Európska komisia, *Budovanie dôvery v umelú inteligenciu sústredenú na človeka*, COM(2019) 168.

<sup>24</sup> Expertná skupina na vysokej úrovni pre umelú inteligenciu, *Etické usmernenia pre dôveryhodnú umelú inteligenciu*, 2019.

<sup>25</sup> Expertná skupina na vysokej úrovni pre umelú inteligenciu, *Zoznam bodov na posudzovanie dôveryhodnej umelej inteligencie na vlastné hodnotenie*, 2020.

<sup>26</sup> Aliancia pre umelú inteligenciu je fórum viacerých zainteresovaných strán, ktoré bolo spustené v júni 2018, Aliancia pre umelú inteligenciu <https://ec.europa.eu/digital-single-market/en/european-ai-alliance>.

<sup>27</sup> Európska komisia, *Úvodné posúdenie vplyvu návrhu právneho aktu Európskeho parlamentu a Rady, ktorým sa stanovujú požiadavky na umelú inteligenciu*.

<sup>28</sup> Podrobnosti o všetkých konzultáciách, ktoré sa uskutočnili, sú uvedené v prílohe 2 k posúdeniu vplyvu.

Posudzovali sa štyri politické možnosti rôzneho stupňa regulačných zásahov:

- **možnosť 1:** legislatívny nástroj EÚ, ktorým sa stanovuje dobrovoľný systém označovania,
- **možnosť 2:** odvetvový prístup *ad hoc*,
- **možnosť 3:** horizontálny legislatívny nástroj EÚ na základe primeraného prístupu založeného na riziku,
- **možnosť 3+:** horizontálny legislatívny nástroj EÚ na základe primeraného prístupu založeného na riziku + kódexy správania pre systémy umelej inteligencie, ktoré nepredstavujú vysoké riziko,
- **možnosť 4:** horizontálny legislatívny nástroj EÚ, ktorým sa stanovujú záväzné požiadavky pre všetky systémy umelej inteligencie bez ohľadu na riziko, ktoré predstavujú.

Všetky možnosti politiky boli posúdené v súlade so stanovenou metodikou Komisie z hľadiska hospodárskych a spoločenských vplyvov s osobitným zameraním na vplyvy na základné práva. Uprednostňovanou možnosťou je možnosť 3+, regulačný rámec len pre vysokorizikové systémy umelej inteligencie, pričom kódexom správania sa môžu riadiť všetci poskytovatelia systémov umelej inteligencie, ktoré nepredstavujú vysoké riziko. Požiadavky sa budú týkať údajov, dokumentácie a výsledovateľnosti, poskytovania informácií a transparentnosti, ľudského dohľadu a spoľahlivosti a presnosti, a budú záväzné pre vysokorizikové systémy umelej inteligencie. Spoločnosti, ktoré zaviedli kódexy správania pre iné systémy umelej inteligencie, tak urobia dobrovoľne.

Uprednostňovaná možnosť sa považovala za vhodnú na čo najúčinnšie riešenie cieľov tohto návrhu. Keďže sa od vývojárov a používateľov umelej inteligencie vyžaduje obmedzený, ale účinný súbor opatrení, uprednostňovaná možnosť obmedzuje riziká porušovania základných práv a bezpečnosti ľudí a podporuje účinný dohľad a presadzovanie, a to tak, že požiadavky sa zameriavajú iba na systémy, kde existuje vysoké riziko, že by k takýmto porušeniam mohlo dôjsť. Výsledkom je, že vďaka tejto možnosti sú náklady na dosiahnutie súladu minimálne, a tak sa zabráni zbytočnému spomaleniu zavádzania v dôsledku vyšších cien a nákladov na dosiahnutie súladu. S cieľom riešiť prípadné nevýhody pre malé a stredné podniky táto možnosť obsahuje niekoľko ustanovení na podporu ich súladu a znižovania ich nákladov vrátane vytvorenia experimentálnych regulačných prostredí a povinnosti zohľadňovať záujmy malých a stredných podnikov pri stanovovaní poplatkov súvisiacich s posudzovaním zhody.

Uprednostňovaná možnosť zvýši dôveru ľudí v umelú inteligenciu, spoločnosti získajú právnu istotu a členské štáty nebudú mať dôvod na prijatie jednostranných opatrení, ktoré by mohli viesť k fragmentácii jednotného trhu. V dôsledku vyššieho dopytu vďaka väčšej dôvere, dostupnejších ponúk vďaka právnej istote a absencie prekážok cezhraničného pohybu systémov umelej inteligencie sa bude jednotný trh umelej inteligencie pravdepodobne úspešne rozvíjať. Európska únia bude naďalej rozvíjať rýchlo rastúci ekosystém umelej inteligencie pozostávajúci z inovatívnych služieb a výrobkov obsahujúcich technológiu umelej inteligencie alebo samostatné systémy umelej inteligencie, čo povedie k zvýšeniu digitálnej autonómie.

Podniky alebo orgány verejnej moci, ktoré vyvíjajú alebo používajú aplikácie umelej inteligencie predstavujúce vysoké riziko pre bezpečnosť alebo základné práva občanov, budú musieť dodržiavať konkrétne požiadavky a povinnosti. Súlad s týmito požiadavkami by predstavoval náklady vo výške približne 6 000 až 7 000 EUR za dodanie priemerného vysokorizikového systému umelej inteligencie v hodnote približne 170 000 EUR do roku

2025. Používateľom umelej inteligencie by podľa prípadu využitia okrem toho prípadne vznikali ročné náklady na čas strávený zabezpečovaním ľudského dohľadu. Tieto náklady sa odhadujú približne na 5 000 až 8 000 EUR ročne. Náklady na overovanie pre dodávateľov vysokorizikovej umelej inteligencie by mohli predstavovať ďalších 3 000 až 7 500 EUR. Podniky alebo orgány verejnej moci, ktoré vyvíjajú alebo používajú akékoľvek aplikácie umelej inteligencie, ktoré nie sú klasifikované ako vysokorizikové, by mali iba minimálne povinnosti poskytovať informácie. Mohli by sa však rozhodnúť pridať sa k ostatným a spoločne prijať kódex správania na dodržiavanie príslušných požiadaviek a zabezpečiť, že ich systémy umelej inteligencie budú dôveryhodné. V takom prípade by boli náklady nanajvyš také vysoké ako v prípade vysokorizikových systémov umelej inteligencie, pravdepodobne by však boli nižšie.

Vplyvy politických možností na rôzne kategórie zainteresovaných strán (hospodárske subjekty/podniky, orgány posudzovania zhody, normalizačné orgány a iné orgány verejnej moci, jednotlivci/občania, výskumníci) sú podrobne vysvetlené v prílohe 3 k posúdeniu vplyvu, ktoré podporuje tento návrh.

### **3.4. Regulačná vhodnosť a zjednodušenie**

V tomto návrhu sa stanovuje povinnosť, ktorá sa bude vzťahovať na poskytovateľov a používateľov vysokorizikových systémov umelej inteligencie. Pre poskytovateľov, ktorí vyvíjajú a uvádzajú takéto systémy na trh Únie, sa ním vytvorí právna istota a zabezpečí sa, aby nevznikla prekážka pre cezhraničné poskytovanie služieb a výrobkov súvisiacich s umelou inteligenciou. Pre spoločnosti, ktoré využívajú umelú inteligenciu, sa ním podporí dôvera medzi ich zákazníkmi. Pre vnútroštátne orgány verejnej moci sa ním podporí dôvera verejnosti v používanie umelej inteligencie a posilnia sa mechanizmy presadzovania (zavedením európskeho koordinačného mechanizmu, zabezpečením vhodných kapacít a uľahčením auditov systémov umelej inteligencie s novými požiadavkami na dokumentáciu, vysledovateľnosť a transparentnosť). V rámci sa navyše stanovujú konkrétne opatrenia na podporu inovácií vrátane experimentálnych regulačných prostredí a konkrétnych opatrení na podporu drobných používateľov a poskytovateľov vysokorizikových systémov umelej inteligencie, aby dodržiavali súlad s novými pravidlami.

Osobitným cieľom návrhu je aj posilnenie európskej konkurencieschopnosti a priemyselnej základne v oblasti umelej inteligencie. Zabezpečuje sa aj úplný súlad s existujúcimi odvetvovými právnymi predpismi Únie, ktoré sa vzťahujú na systémy umelej inteligencie (napr. týkajúcich sa výrobkov a služieb) a ktoré ďalej objasnia a zjednodušia presadzovanie nových pravidiel.

### **3.5. Základné práva**

Používanie umelej inteligencie s jej špecifickými vlastnosťami (napr. nepriehľadnosť, zložitosť, závislosť od údajov, autonómne správanie sa) môže nepriaznivo ovplyvniť množstvo základných práv zakotvených v Charte základných práv EÚ (ďalej len „charta“). Cieľom návrhu je zabezpečiť vysokú úroveň ochrany týchto základných práv a zameriava sa na rôzne zdroje rizík prostredníctvom jasne definovaného prístupu založeného na riziku. So súborom požiadaviek pre dôveryhodnú umelú inteligenciu a s primeranými povinnosťami pre všetkých účastníkov hodnotového reťazca sa návrhom posilní a podporí ochrana práv chránených v charte: právo na ľudskú dôstojnosť (článok 1), rešpektovanie súkromného života a ochrana osobných údajov (články 7 a 8), nediskriminácia (článok 21) a rovnosť medzi ženami a mužmi (článok 23). Jeho cieľom je zabrániť odrádzajúcemu účinku na práva na slobodu prejavu (článok 11) a slobodu zhromažďovania (článok 12), zabezpečiť ochranu práva na účinný prostriedok nápravy a na spravodlivý proces, práva na obhajobu a prezumpciu nevinu (články 47 a 48), ako aj všeobecnú zásadu dobrej správy vecí verejných.

Návrh okrem toho v príslušných oblastiach pozitívne ovplyvní práva niekoľkých osobitných skupín, ako sú práva pracovníkov na spravodlivé a primerané pracovné podmienky (článok 31), vysoká úroveň ochrany spotrebiteľa (článok 28), práva dieťaťa (článok 24) a integrácia osôb so zdravotným postihnutím (článok 26). Dôležité je aj právo na vysokú úroveň ochrany životného prostredia a zlepšenie kvality životného prostredia (článok 37), a to aj v súvislosti so zdravím a s bezpečnosťou ľudí. Povinnosti týkajúce sa testovania *ex ante*, riadenia rizík a ľudského dohľadu takisto uľahčia rešpektovanie iných základných práv tým, že minimalizujú riziko chybných alebo zaujatých rozhodnutí dosiahnutých pomocou umelej inteligencie v kritických oblastiach, ako vzdelávanie a odborná príprava, zamestnanosť, dôležité služby, presadzovanie práva a súdnictvo. V prípade, že naďalej bude dochádzať k porušovaniu základných práv, dotknutým osobám sa umožní účinná náprava zabezpečením transparentnosti a vysledovateľnosti systémov umelej inteligencie v kombinácii s prísnyimi následnými kontrolami.

Týmto návrhom sa ukladajú určité obmedzenia slobody podnikania (článok 16) a slobody umenia a vedeckého bádania (článok 13) s cieľom zabezpečiť súlad so závažnými dôvodmi verejného záujmu, ako sú zdravie, bezpečnosť, ochrana spotrebiteľa a ochrana ďalších základných práv (zodpovedná inovácia) pri vyvíjaní a používaní vysokorizikovej technológie umelej inteligencie. Tieto obmedzenia sú primerané a obmedzené na nevyhnutné minimum a ich cieľom je prevencia a zmiernenie závažných bezpečnostných rizík a pravdepodobného porušovania základných práv.

Povinnosti týkajúce sa vyššej transparentnosti takisto neprimerane neovplyvnia právo na ochranu duševného vlastníctva (článok 17 ods. 2), pretože budú obmedzené len na minimálne nevyhnutné informácie potrebné pre jednotlivcov na uplatnenie ich práva na účinný prostriedok nápravy a na nevyhnutnú transparentnosť voči orgánom dohľadu a orgánom presadzovania práva, a to v súlade s ich mandátmi. Každé zverejnenie informácií sa uskutoční v súlade s príslušnými právnymi predpismi v danej oblasti vrátane smernice 2016/943 o ochrane nesprístupneného know-how a obchodných informácií (obchodného tajomstva) pred ich neoprávneným získaním, využitím a sprístupnením. Ak orgány verejnej moci a notifikované osoby potrebujú prístup k dôverným informáciám alebo zdrojovému kódu na účely preskúmania dodržiavania podstatných povinností, vzťahujú sa na ne záväzné povinnosti dôvernosti.

#### **4. VPLYV NA ROZPOČET**

Členské štáty budú musieť určiť orgány dohľadu zodpovedné za vykonávanie legislatívnych požiadaviek. Ich funkcia dohľadu by mohla vychádzať z existujúcich systémov, napríklad pokiaľ ide o orgány posudzovania zhody alebo dohľadu nad trhom, vyžadovalo by si to však dostatočné technologické znalosti a ľudské a finančné zdroje. V závislosti od už existujúcej štruktúry v každom členskom štáte by to mohlo predstavovať 1 až 25 ekvivalentov plného pracovného času na členský štát.

Podrobný prehľad súvisiacich nákladov je uvedený vo finančnom výkaze, ktorý je pripojený k tomuto návrhu.

#### **5. ĎALŠIE PRVKY**

##### **5.1. Plány vykonávania, spôsob monitorovania, hodnotenia a podávania správ**

Zabezpečenie spoľahlivého mechanizmu monitorovania a hodnotenia je zásadné pre zaistenie účinnosti návrhu pri dosahovaní jeho konkrétnych cieľov. Za monitorovanie účinkov bude zodpovedať Komisia. Zavedie systém registrácie samostatných vysokorizikových aplikácií

umelej inteligencie v celoúnijnej verejnej databáze. Táto registrácia okrem toho umožní príslušným orgánom, používateľom a iným zúčastneným overiť si, či vysokorizikový systém umelej inteligencie spĺňa požiadavky stanovené v návrhu, a vykonávať zvýšený dohľad nad systémami umelej inteligencie, ktoré predstavujú vysoké riziko pre základné práva. Pri vkladaní údajov do tejto databázy budú poskytovatelia umelej inteligencie povinní poskytovať zmysluplné informácie o svojich systémoch, ako aj o posudzovaní zhody vykonanom na týchto systémoch.

Poskytovatelia umelej inteligencie budú navyše povinní informovať príslušné vnútroštátne orgány o závažných incidentoch alebo poruchách, ktoré predstavujú porušenie povinností v oblasti základných práv, a to hneď ako sa o nich dozvedia, ako aj o každom stiahnutí systémov umelej inteligencie od používateľa alebo z trhu. Príslušné vnútroštátne orgány potom vyšetrojú incidenty alebo poruchy, zhromažďujú všetky potrebné informácie a pravidelne ich zasielajú Komisii s primeranými metaúdajmi. Komisia tieto informácie o incidentoch doplní komplexnou analýzou celkového trhu s umelou inteligenciou.

Komisia uverejní správu, v ktorej zhodnotí a preskúma navrhovaný rámec pre umelú inteligenciu päť rokov od jeho dátumu nadobudnutia účinnosti.

## **5.2. Podrobné vysvetlenie konkrétnych ustanovení návrhu**

### **5.2.1. ROZSAH PÔSOBNOSTI A VYMEDZENIE POJMOV (HLAVA I)**

V **hlave I** sa vymedzuje predmet úpravy návrhu a rozsah pôsobnosti nových pravidiel, ktoré sa týkajú uvádzania na trh, uvádzania do prevádzky a používania systémov umelej inteligencie. V tejto hlave sa vymedzujú aj pojmy, ktoré sa používajú v celom nástroji. Definícia systému umelej inteligencie v právnom rámci má byť čo najviac technologicky neutrálna a nadčasová a má zohľadňovať rýchly technologický a trhový vývoj v oblasti umelej inteligencie. S cieľom zabezpečiť potrebnú právnu istotu sa hlava I dopĺňa prílohou I, ktorá obsahuje podrobný zoznam prístupov a techník pre vývoj umelej inteligencie, ktoré má Komisia prispôbiť v súlade s novým technologickým vývojom. S cieľom zabezpečiť rovnaké podmienky pre všetkých sa jasne definujú aj kľúčoví účastníci v rámci hodnotového reťazca umelej inteligencie, ako sú poskytovatelia a používatelia systémov umelej inteligencie, ktorými sú verejní i súkromní prevádzkovatelia.

### **5.2.2. ZAKÁZANÉ PRAKTIKY V OBLASTI UMELEJ INTELIGENCIE (HLAVA II)**

V **hlave II** sa stanovuje zoznam zakázanej umelej inteligencie. Nariadenie sa riadi prístupom založeným na riziku, pričom sa rozlišuje medzi použitím umelej inteligencie, ktorá vytvára i) neprijateľné riziko; ii) vysoké riziko a iii) nízke alebo minimálne riziko. Zoznam zakázaných praktík v hlave II obsahuje všetky systémy umelej inteligencie, ktorých používanie sa považuje za neprijateľné, pretože je v rozpore s hodnotami Únie, napríklad porušovaním základných práv. Zákazy sa vzťahujú na praktiky, ktoré majú značný potenciál manipulovať s osobami prostredníctvom podprahových techník mimo ich vedomia alebo využívať zraniteľné miesta určitých zraniteľných skupín, ako sú deti alebo osoby so zdravotným postihnutím, s cieľom podstatne narušiť ich správanie spôsobom, ktorý im môže spôsobiť psychickú alebo fyzickú ujmu. Na ďalšie manipulatívne alebo zneužívajúce praktiky ovplyvňujúce dospelých ľudí, ktoré by mohli uľahčovať systémy umelej inteligencie, by sa mohli vzťahovať existujúce právne predpisy v oblasti ochrany údajov, ochrany spotrebiteľa a digitálnych služieb, ktoré zaručujú, že fyzické osoby sú riadne informované a môžu sa slobodne rozhodnúť nepodrobiť sa profilovaniu alebo iným praktikám, ktoré by mohli ovplyvniť ich správanie. V tomto návrhu sa zakazuje aj sociálne hodnotenie založené na umelej inteligencii na všeobecné účely vykonávané orgánmi verejnej moci. Napokon sa zakazuje aj používanie systémov diaľkovej biometrickej identifikácie v „reálnom čase“ na

verejne prístupných miestach na účely presadzovania práva, pokiaľ neplatia určité obmedzené výnimky.

### 5.2.3. VYSOKORIZIKOVÉ SYSTÉMY UMELEJ INTELIGENCIE (HLAVA III)

**Hlava III** obsahuje osobitné pravidlá pre systémy umelej inteligencie, ktoré vytvárajú vysoké riziko pre zdravie a bezpečnosť alebo základné práva fyzických osôb. V súlade s prístupom založeným na riziku sú tieto vysokorizikové systémy umelej inteligencie povolené na európskom trhu za predpokladu, že spĺňajú určité záväzné požiadavky a sú v súlade s posudzovaním zhody *ex ante*. Klasifikácia systému umelej inteligencie ako vysokorizikového je založená na plánovanom účele systému umelej inteligencie v súlade s existujúcimi právnymi predpismi o bezpečnosti výrobkov. Označenie za vysokorizikové preto nezávisí iba od funkcie vykonávanej systémom umelej inteligencie, ale aj od konkrétneho účelu a spôsobov, ktorými sa tento systém používa.

V kapitole 1 hlavy III sa stanovujú pravidlá klasifikácie a identifikujú sa dve hlavné kategórie vysokorizikových systémov umelej inteligencie:

- systémy umelej inteligencie určené na použitie ako bezpečnostná súčasť výrobkov, ktoré podliehajú posudzovaniu zhody *ex ante* treťou stranou,
- iné samostatné systémy umelej inteligencie s vplyvmi najmä na základné práva, ktoré sú výslovne uvedené v prílohe III.

Tento zoznam vysokorizikových systémov umelej inteligencie v prílohe III obsahuje obmedzený počet systémov umelej inteligencie, ktorých riziká sa už vyskytli alebo sa pravdepodobne v blízkej budúcnosti vyskytnú. Aby sa zabezpečilo, že nariadenie bude možné prispôbiť vznikajúcim použitiam a aplikáciám umelej inteligencie, Komisia môže rozšíriť zoznam vysokorizikových systémov umelej inteligencie používaných v rámci konkrétnych vopred určených oblastí uplatnením súboru kritérií a metodiky posudzovania rizika.

V kapitole 2 sa stanovujú právne požiadavky na vysokorizikové systémy umelej inteligencie v súvislosti s údajmi a so správou údajov, s uchovávaním dokumentácie a záznamov, transparentnosťou a poskytovaním informácií používateľom, s ľudským dohľadom, so spoľahlivosťou, s presnosťou a bezpečnosťou. Navrhované minimálne požiadavky patria už dnes medzi najmodernejšie pre mnohých obozretných prevádzkovateľov a sú výsledkom dvojročných prípravných prác, ktoré vychádzajú z etických usmernení expertnej skupiny na vysokej úrovni pre umelú inteligenciu<sup>29</sup> a ktoré skúšobne vykonávalo viac ako 350 organizácií<sup>30</sup>. Okrem toho sú vo veľkej miere v súlade s inými medzinárodnými odporúčaniami a zásadami, čo zabezpečuje, že navrhovaný rámec pre umelú inteligenciu je zlučiteľný s odporúčaniami a zásadami, ktoré prijali medzinárodní obchodní partneri EÚ. Presné technické riešenia na dosiahnutie súladu s týmito požiadavkami môžu poskytovať normy alebo iné technické špecifikácie alebo sa inak vypracujú v súlade so všeobecnými technickými alebo s vedeckými poznatkami podľa uváženia poskytovateľa systému umelej inteligencie. Táto flexibilita je mimoriadne dôležitá, pretože umožňuje poskytovateľom systémov umelej inteligencie vybrať si spôsob, ako splniť svoje požiadavky pri zohľadnení najmodernejšieho a technologického a vedeckého pokroku v tejto oblasti.

V kapitole 3 sa poskytovateľom vysokorizikových systémov umelej inteligencie ukladá jasný súbor horizontálnych povinností. Primerané povinnosti sa ukladajú aj používateľom a iným

<sup>29</sup> Expertná skupina na vysokej úrovni pre umelú inteligenciu, [Etické usmernenia pre dôveryhodnú umelú inteligenciu](#), 2019.

<sup>30</sup> Podporila ich aj Komisia vo svojom oznámení z roku 2019 o prístupe k umelej inteligencii sústredenom na človeka.



účastníkom v rámci hodnotového reťazca umelej inteligencie (napr. dovozcom, distribútorom, splnomocneným zástupcom).

V kapitole 4 sa stanovuje rámec pre zapojenie notifikovaných osôb ako nezávislých tretích strán do postupov posudzovania zhody, zatiaľ čo v kapitole 5 sa podrobne vysvetľujú postupy posudzovania zhody, ktoré sa majú dodržiavať pri každom type vysokorizikového systému umelej inteligencie. Cieľom postupu posudzovania zhody je minimalizovať záťaž pre hospodárske subjekty, ako aj pre notifikované osoby, ktorých kapacita sa musí v priebehu času postupne zvyšovať. Na systémy umelej inteligencie, ktoré sa majú používať ako bezpečnostné súčasti výrobkov, na ktoré sa vzťahujú právne predpisy nového legislatívneho rámca (napr. stroje, hračky, zdravotnícke pomôcky atď.), sa budú vzťahovať rovnaké mechanizmy súladu *ex-ante* a *ex post* a mechanizmy presadzovania ako na výrobky, ktorých sú súčasťou. Kľúčový rozdiel je v tom, že mechanizmy *ex-ante* a *ex post* zabezpečia nielen dodržiavanie požiadaviek stanovených v odvetvových právnych predpisoch, ale aj požiadaviek stanovených v tomto nariadení.

Pokiaľ ide o samostatné vysokorizikové systémy umelej inteligencie, ktoré sú uvedené v prílohe III, vytvorí sa nový systém dodržiavania a presadzovania právnych predpisov. Vyplýva to z modelu právnych predpisov nového legislatívneho rámca, ktorý sa vykonáva prostredníctvom vnútorných kontrol poskytovateľov, s výnimkou systémov diaľkovej biometrickej identifikácie, ktoré by podliehali posudzovaniu zhody treťou stranou. Komplexné posudzovanie zhody *ex ante* prostredníctvom vnútorných kontrol v kombinácii s prísnyim presadzovaním *ex post* by mohlo byť účinným a primeraným riešením pre tieto systémy vzhľadom na počiatočnú fázu regulačných zásahov a skutočnosť, že odvetvie umelej inteligencie je veľmi inovatívne a odborné znalosti v oblasti auditu sa teraz ešte len zhromažďujú. Posudzovanie prostredníctvom vnútorných kontrol, pokiaľ ide o samostatné vysokorizikové systémy umelej inteligencie, by si vyžadovalo úplný, účinný a riadne zdokumentovaný súlad *ex ante* so všetkými požiadavkami nariadenia a súlad so spoľahlivými systémami riadenia kvality a rizík a s monitorovaním po uvedení na trh. Keď poskytovateľ vykoná príslušné posúdenie zhody, mal by zaregistrovať tieto samostatné vysokorizikové systémy umelej inteligencie v databáze EÚ, ktorú bude spravovať Komisia, s cieľom zvýšiť verejnú transparentnosť a dohľad a posilniť dohľad *ex post* zo strany príslušných orgánov. Naopak z dôvodu súladu s existujúcimi právnymi predpismi o bezpečnosti výrobkov sa bude posudzovanie zhody systémov umelej inteligencie, ktoré sú bezpečnostnými súčasťami výrobkov, riadiť systémom s postupmi posudzovania zhody treťou stranou, ktoré sú už stanovené v príslušných odvetvových právnych predpisoch v oblasti bezpečnosti výrobkov. Nové opätovné posudzovanie zhody *ex ante* bude potrebné v prípade podstatných úprav systémov umelej inteligencie (a najmä zmien, ktoré presahujú rámec toho, čo poskytovateľ vopred stanovuje vo svojej technickej dokumentácii a čo je skontrolované v čase posudzovania zhody *ex ante*).

#### 5.2.4. POVINNOSTI TÝKAJÚCE SA TRANSPARENTNOSTI PRE URČITÉ SYSTÉMY UMELEJ INTELIGENCIE (HLAVA IV)

**Hlava IV** sa týka určitých systémov umelej inteligencie s cieľom zohľadniť osobitné riziká manipulácie, ktoré predstavujú. Povinnosti týkajúce sa transparentnosti sa budú vzťahovať na systémy, ktoré i) komunikujú s ľuďmi; ii) sa používajú na zisťovanie emócií alebo určovanie asociácie so (sociálnymi) kategóriami na základe biometrických údajov, alebo iii) vytvárajú obsah alebo s ním manipulujú (tzv. deepfakes). Ak osoby komunikujú so systémom umelej inteligencie alebo ich emócie alebo vlastnosti sú rozpoznávané automatizovanými prostriedkami, ľudia musia byť o tejto skutočnosti informovaní. Ak sa systém umelej inteligencie používa na vytváranie obrazového, zvukového alebo video obsahu alebo na manipuláciu s ním a tento obsah očividne pôsobí ako autentický obsah, mala by existovať

povinnosť zverejniť informáciu, že obsah sa vytvára automatizovanými prostriedkami, s výhradou výnimiek na legitímne účely (presadzovanie práva, sloboda prejavu). To umožňuje osobám robiť informované rozhodnutia alebo sa vyhnúť danej situácii.

#### 5.2.5. OPATRENIA NA PODPORU INOVÁCIÍ (HLAVA V)

**Hlava V** prispieva k cieľu vytvoriť právny rámec, ktorý je priaznivý pre inovácie, je nadčasový a odolný voči narušeniam. S týmto cieľom sa v rámci nej podporujú príslušné vnútroštátne orgány v tom, aby vytvorili experimentálne regulačné prostredia, a stanovuje sa základný rámec, pokiaľ ide o riadenie, dohľad a zodpovednosť. Experimentálne regulačné prostredia umelej inteligencie vytvárajú kontrolované prostredie na testovanie technológií na obmedzený čas na základe plánu testovania dohodnutého s príslušnými orgánmi. Hlava V obsahuje aj opatrenia na zníženie regulačnej záťaže pre malé a stredné podniky a startupy.

#### 5.2.6. RIADENIE A VYKONÁVANIE (HLAVY VI, VII A VIII)

V **hlave VI** sa zriaďujú systémy riadenia na úrovni Únie a na vnútroštátnej úrovni. Na úrovni Únie sa týmto návrhom zriaďuje Európska rada pre umelú inteligenciu (ďalej len „rada“) zložená zo zástupcov členských štátov a z Komisie. Rada umožní plynulé, účinné a harmonizované vykonávanie tohto nariadenia tým, že bude prispievať k účinnej spolupráci vnútroštátnych dozorných orgánov a Komisie a poskytovať Komisii poradenstvo a odborné znalosti. Okrem toho bude zhromažďovať najlepšie postupy a vymieňať si ich s členskými štátmi.

Na vnútroštátnej úrovni budú mať členské štáty povinnosť určiť jeden alebo viac príslušných vnútroštátnych orgánov a spomedzi nich vnútroštátny dozorný orgán na účely dohľadu nad uplatňovaním a vykonávaním nariadenia. Európsky dozorný úradník pre ochranu údajov bude pôsobiť ako príslušný orgán pre dohľad nad inštitúciami, agentúrami a orgánmi Únie, ak patria do rozsahu pôsobnosti tohto nariadenia.

Cieľom **hlavy VII** je uľahčiť monitorovacie práce Komisie a vnútroštátnych orgánov zriadením celoúnijnej databázy samostatných vysokorizikových systémov umelej inteligencie s vplyvom predovšetkým na základné práva. Databázu bude prevádzkovať Komisia a údaje jej budú poskytovať poskytovatelia systémov umelej inteligencie, od ktorých sa bude vyžadovať, aby svoje systémy zaregistrovali pred ich uvedením na trh alebo iným uvedením do prevádzky.

V **hlave VIII** sa poskytovateľom systémov umelej inteligencie ukladá monitorovacia povinnosť a povinnosť podávania správ, pokiaľ ide o monitorovanie po uvedení na trh a podávanie správ a vyšetrovanie incidentov a porúch súvisiacich s umelou inteligenciou. Orgány pre dohľad nad trhom by okrem toho kontrolovali trh a skúmali dodržiavanie povinností a požiadaviek týkajúcich sa všetkých vysokorizikových systémov umelej inteligencie, ktoré sú už uvedené na trh. Orgány pre dohľad nad trhom by mali všetky právomoci podľa nariadenia (EÚ) 2019/1020 o dohľade nad trhom. Presadzovaním *ex post* by sa malo zabezpečiť, aby orgány verejnej moci po uvedení systému umelej inteligencie na trh mali právomoci a zdroje na zásah v prípade, že systémy umelej inteligencie prinesú neočakávané riziká, ktoré si vyžadujú rýchle konanie. Okrem toho budú monitorovať, či prevádzkovatelia dodržiavajú príslušné povinnosti podľa tohto nariadenia. V návrhu sa nestanovuje automatické vytvorenie žiadnych ďalších subjektov ani orgánov na úrovni členských štátov. Členské štáty preto môžu menovať existujúce odvetvové orgány (a čerpať z ich odborných znalostí), ktorým by boli zverené aj právomoci na monitorovanie a presadzovanie ustanovení nariadenia.

Týmto nie je dotknutý existujúci systém a rozdelenie právomocí presadzovania povinností *ex post* týkajúcich sa základných práv v členských štátoch. Ak je to potrebné pre ich mandát,

existujúce orgány dohľadu a presadzovania práva budú mať aj právomoc požadovať akúkoľvek dokumentáciu vedenú podľa tohto nariadenia a pristupovať k nej, a v prípade potreby požiadať orgány dohľadu nad trhom, aby zorganizovali testovanie vysokorizikového systému umelej inteligencie technickými prostriedkami.

#### 5.2.7. *KÓDEXY SPRÁVANIA (HLAVA IX)*

V **hlave IX** sa stanovuje rámec pre vytváranie kódexov správania, ktorých cieľom je povzbudiť poskytovateľov systémov umelej inteligencie, ktoré nepredstavujú vysoké riziko, aby dobrovoľne uplatňovali záväzné požiadavky pre vysokorizikové systémy umelej inteligencie (ako sa stanovuje v hlave III). Poskytovatelia systémov umelej inteligencie, ktoré nepredstavujú vysoké riziko, si môžu sami vytvoriť a vykonávať kódexy správania. Tieto kódexy môžu obsahovať aj dobrovoľné záväzky týkajúce sa napríklad environmentálnej udržateľnosti, prístupnosti pre osoby so zdravotným postihnutím, účasti zainteresovaných strán na navrhovaní a vývoji systémov umelej inteligencie a rozmanitosti vývojových tímov.

#### 5.2.8. *ZÁVEREČNÉ USTANOVENIA (HLAVY X, XI A XII)*

V **hlave X** sa zdôrazňuje povinnosť všetkých strán rešpektovať dôvernosť informácií a údajov a stanovujú sa pravidlá výmeny informácií získaných v rámci vykonávania tohto nariadenia. Hlava X okrem toho obsahuje opatrenia na zabezpečenie účinného vykonávania nariadenia prostredníctvom účinných, primeraných a odradzujúcich sankcií za porušenie ustanovení.

V **hlave XI** sa stanovujú pravidlá delegovania právomoci a vykonávania právomoci. Na základe návrhu je Komisia splnomocnená v prípade potreby prijímať vykonávacie akty na zabezpečenie jednotného uplatňovania nariadenia alebo delegované akty na aktualizáciu alebo doplnenie zoznamov v prílohách I až VII.

**Hlava XII** obsahuje povinnosť Komisie pravidelne hodnotiť potrebu aktualizácie prílohy III a pripravovať pravidelné správy o hodnotení a preskúmaní nariadenia. Stanovujú sa v nej aj záverečné ustanovenia vrátane diferencovaného prechodného obdobia pre počiatočný dátum uplatňovania nariadenia s cieľom uľahčiť bezproblémové vykonávanie pre všetky dotknuté strany.

Návrh

**NARIADENIE EURÓPSKEHO PARLAMENTU A RADY,  
KTORÝM SA STANOVUJÚ HARMONIZOVANÉ PRAVIDLÁ V OBLASTI UMELEJ  
INTELIGENCIE (AKT O UMELEJ INTELIGENCII) A MENIA NIEKTORÉ  
LEGISLATÍVNE AKTY ÚNIE**

EURÓPSKY PARLAMENT A RADA EURÓPSKEJ ÚNIE,

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

so zreteľom na návrh Európskej komisie,

po postúpení návrhu legislatívneho aktu národným parlamentom,

so zreteľom na stanovisko Európskeho hospodárskeho a sociálneho výboru<sup>31</sup>,

so zreteľom na stanovisko Výboru regiónov<sup>32</sup>,

konajúc v súlade s riadnym legislatívnym postupom,

keďže:

- (1) Účelom tohto nariadenia je zlepšiť fungovanie vnútorného trhu stanovením jednotného právneho rámca, najmä pokiaľ ide o vývoj, uvádzanie na trh a používanie umelej inteligencie v súlade s hodnotami Únie. Toto nariadenie prihliada na viacero naliehavých dôvodov verejného záujmu, ako napr. vysoká úroveň ochrany zdravia, bezpečnosti a základných práv, a zabezpečuje voľný pohyb tovaru a služieb založených na umelej inteligencii cez hranice, čím bráni členským štátom ukladať obmedzenia na vývoj, uvádzanie na trh a používanie systémov umelej inteligencie, pokiaľ sa to týmto nariadením výslovne nepovolí.
- (2) Systémy umelej inteligencie (systémy UI) možno ľahko zaviesť vo viacerých odvetviach hospodárstva a spoločnosti, a to aj cezhranične, a môžu sa pohybovať po celej Únii. Niektoré členské štáty už zvažujú prijatie vnútroštátnych pravidiel na zabezpečenie toho, aby bola umelá inteligencia bezpečná a aby sa vyvíjala a používala v súlade s povinnosťami týkajúcimi sa základných práv. Rozdielne vnútroštátne pravidlá môžu viesť k fragmentácii vnútorného trhu a znížiť právnu istotu pre prevádzkovateľov, ktorí vyvíjajú alebo používajú systémy umelej inteligencie. Mala by sa preto zabezpečiť konzistentná a vysoká úroveň ochrany v celej Únii, pričom by sa malo zabrániť rozdielom, ktoré bránia voľnému pohybu systémov umelej inteligencie a súvisiacich výrobkov a služieb v rámci vnútorného trhu, a to stanovením jednotných povinností pre prevádzkovateľov a zaručením jednotnej ochrany naliehavých dôvodov verejného záujmu a práv osôb na celom vnútornom trhu na základe článku 114 Zmluvy o fungovaní Európskej únie (ZFEÚ). Keďže toto nariadenie obsahuje osobitné pravidlá ochrany jednotlivcov v súvislosti so spracúvaním osobných údajov, pokiaľ ide o obmedzenia používania systémov umelej

<sup>31</sup> Ú. v. EÚ C [...], [...], s. [...].

<sup>32</sup> Ú. v. EÚ C [...], [...], s. [...].

inteligencie na diaľkovú biometrickú identifikáciu v reálnom čase vo verejne dostupných priestoroch na účely presadzovania práva, je vhodné, aby sa tieto osobitné pravidlá uvedené v tomto nariadení zakladali na článku 16 ZFEÚ. Pokiaľ ide o tieto osobitné pravidlá a použitie článku 16 ZFEÚ, je vhodné poradiť sa s Európskym výborom pre ochranu údajov.

- (3) Umeľá inteligencia je rýchlo sa rozvíjajúca skupina technológií, ktorá môže prispieť k širokému spektru hospodárskych a spoločenských výhod vo všetkých priemyselných odvetviach a spoločenských činnostiach. Zlepšením predpovedí, optimalizáciou operácií a pridelovania zdrojov a personalizáciou digitálnych riešení, ktoré sú k dispozícii jednotlivcom a organizáciám, môže využívanie umelej inteligencie poskytnúť podnikom kľúčové konkurenčné výhody a podporiť sociálne a environmentálne priaznivé výsledky, napríklad v oblasti zdravotnej starostlivosti, poľnohospodárstva, vzdelávania a odbornej prípravy, riadenia infraštruktúry, energetiky, dopravy a logistiky, verejných služieb, bezpečnostnej ochrany, spravodlivosti, efektívneho využívania zdrojov a energie a zmierňovania zmeny klímy a adaptácie na ňu.
- (4) Umeľá inteligencia môže zároveň v závislosti od okolností týkajúcich sa jej konkrétneho uplatňovania a používania vytvárať riziká a poškodzovať verejné záujmy a práva, ktoré sú chránené právom Únie. Toto poškodenie môže byť hmotné aj nehmotné.
- (5) Na podporu rozvoja, využívania a zavádzania umelej inteligencie na vnútornom trhu je preto potrebný právny rámec Únie, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorý zároveň spĺňa vysokú úroveň ochrany verejných záujmov, ako sú zdravie a bezpečnosť, a ochrany základných práv, ako sú uznané a chránené právom Únie. Na dosiahnutie tohto cieľa by sa mali stanoviť pravidlá upravujúce uvádzanie určitých systémov umelej inteligencie na trh a do prevádzky, čím sa zabezpečí hladké fungovanie vnútorného trhu a umožní sa, aby tieto systémy využívali zásadu voľného pohybu tovaru a služieb. Stanovením uvedených pravidiel v tomto nariadení sa podporí cieľ Únie stať sa svetovým lídrom v rozvoji bezpečnej, dôveryhodnej a etickej umelej inteligencie, ako ho vyjadřila Európska rada<sup>33</sup>, a zabezpečí ochrana etických zásad, ako to osobitne požaduje Európsky parlament<sup>34</sup>.
- (6) Pojem systém umelej inteligencie by sa mal jasne vymedziť s cieľom zabezpečiť právnu istotu a zároveň poskytnúť flexibilitu na prispôbenie sa budúcemu technologickému vývoju. Vymedzenie pojmu by malo vychádzať z kľúčových funkčných charakteristík softvéru, najmä zo schopnosti generovať pre daný súbor človekom stanovených cieľov výstupy, ako je obsah, predpovede, odporúčania alebo rozhodnutia, ktoré ovplyvňujú prostredie, s ktorým systém komunikuje, či už vo fyzickom alebo digitálnom rozmere. Systémy umelej inteligencie môžu byť navrhnuté tak, aby fungovali s rôznymi úrovňami samostatnosti a mohli sa používať samostatne alebo ako komponent určitého výrobku bez ohľadu na to, či je systém do tohto výrobku fyzicky integrovaný (vstavaný) alebo či napomáha funkčnosti tohto výrobku bez toho, aby doň bol integrovaný (nevstavaný). Vymedzenie pojmu systém umelej inteligencie by sa malo doplniť o zoznam osobitných techník a prístupov používaných

---

<sup>33</sup> Európska rada, mimoriadne zasadnutie Európskej rady (1. a 2. októbra 2020) – závery, EUCO 13/20, 2020, s. 6.

<sup>34</sup> Uznesenie Európskeho parlamentu z 20. októbra 2020 s odporúčaniami pre Komisiu k rámci etických aspektov umelej inteligencie, robotiky a súvisiacich technológií, 2020/2012(INL).

na jeho vývoj, ktorý by sa mal vzhľadom na vývoj na trhu a technologický vývoj aktualizovať prostredníctvom delegovaných aktov, ktoré by prijala Komisia na účely zmeny uvedeného zoznamu.

- (7) Pojem „biometrické údaje“ použitý v tomto nariadení je v súlade s pojmom biometrické údaje vymedzeným v článku 4 bode 14 nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679<sup>35</sup>, v článku 3 bode 18 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1725<sup>36</sup> a v článku 3 bode 13 smernice Európskeho parlamentu a Rady (EÚ) 2016/680<sup>37</sup> a mal by sa vykladať v súlade s nimi.
- (8) Pojem „systém diaľkovej biometrickej identifikácie“, ako sa používa v tomto nariadení, by sa mal vymedziť funkčne ako systém umelej inteligencie určený na identifikáciu fyzických osôb na diaľku porovnávaním biometrických údajov osoby s biometrickými údajmi obsiahnutými v referenčnej databáze a bez toho, aby sa vopred vedelo, či bude cieľová osoba prítomná a či ju bude možné identifikovať, a to bez ohľadu na konkrétnu technológiu, procesy alebo typy použitých biometrických údajov. Vzhľadom na ich odlišné charakteristiky a spôsoby, akými sa používajú, ako aj na rôzne súvisiace riziká, by sa malo rozlišovať medzi systémom diaľkovej biometrickej identifikácie „v reálnom čase“ a systémom „následnej“ diaľkovej biometrickej identifikácie. V prípade systémov „v reálnom čase“ prebieha zachytávanie biometrických údajov, ich porovnávanie a identifikácia okamžite, takmer okamžite alebo v každom prípade bez výrazného oneskorenia. V tejto súvislosti by nemal existovať priestor na obchádzanie pravidiel tohto nariadenia o používaní predmetných systémov umelej inteligencie „v reálnom čase“ tým, že sa stanovujú menšie oneskorenia. Systémy v reálnom čase zahŕňajú používanie materiálu „naživo“ alebo „s malým časovým posunom“, ako sú napríklad videozáznamy generované kamerou alebo iným zariadením s podobnými funkciami. Naopak, v prípade systémov „následnej“ identifikácie už boli biometrické údaje zachytené a porovnanie a identifikácia sa uskutočňujú až po značnom oneskorení. Ide o materiály, ako sú fotografie alebo videozáznamy generované kamerami s uzavretým televíznym okruhom alebo súkromnými zariadeniami, ktoré boli vytvorené pred použitím tohto systému vo vzťahu k dotknutým fyzickým osobám.
- (9) Na účely tohto nariadenia by sa pojem „verejne prístupný priestor“ mal chápať ako akékoľvek fyzické miesto prístupné verejnosti bez ohľadu na to, či je dané miesto v súkromnom alebo verejnom vlastníctve. Tento pojem sa preto nevzťahuje na miesta, ktoré sú súkromnej povahy a zvyčajne nie sú voľne prístupné tretím stranám vrátane orgánov presadzovania práva, pokiaľ tieto strany neboli osobitne pozvané alebo oprávnené, ako napr. domácnosti, súkromné kluby, kancelárie, sklady a továrne. Nevzťahuje sa ani na online priestory, pretože nejde o fyzické priestory. Samotná

<sup>35</sup> Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1).

<sup>36</sup> Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES (Ú. v. EÚ L 295, 21.11.2018, s. 39).

<sup>37</sup> Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stihania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV (smernica o presadzovaní práva) (Ú. v. EÚ L 119, 4.5.2016, s. 89).

skutočnosť, že sa na prístup do konkrétneho priestoru môžu uplatňovať určité podmienky, ako napr. vstupenky alebo vekové obmedzenia, však neznamená, že daný priestor nie je verejne prístupný v zmysle tohto nariadenia. Z toho vyplýva, že okrem verejných priestorov, ako sú napríklad ulice, príslušné časti vládnych budov a väčšina dopravnej infraštruktúry, sú zvyčajne verejne prístupné aj priestory ako kiná, divadlá, obchody a nákupné centrá. To, či je daný priestor prístupný verejnosti, by sa však malo určovať od prípadu k prípadu so zreteľom na osobitosti konkrétnej situácie.

- (10) S cieľom zabezpečiť rovnaké podmienky a účinnú ochranu práv a slobôd fyzických osôb v celej Únii by sa pravidlá stanovené v tomto nariadení mali uplatňovať na poskytovateľov systémov umelej inteligencie nediskriminačným spôsobom bez ohľadu na to, či sú usadení v Únii alebo v tretej krajine, a na používateľov systémov umelej inteligencie usadených v Únii.
- (11) Určité systémy umelej inteligencie by vzhľadom na svoju digitálnu povahu mali patriť do rozsahu pôsobnosti tohto nariadenia, aj keď sa v Únii neuvádzajú na trh ani do prevádzky, ani sa v nej nepoužívajú. Ide napríklad o prevádzkovateľa usadeného v Únii, ktorý zmluvne zadáva určité služby prevádzkovateľovi usadenému mimo Únie v súvislosti s činnosťou vykonávanou systémom umelej inteligencie, ktorý by mohol byť označený ako vysokorizikový a ktorého účinky majú vplyv na fyzické osoby nachádzajúce sa v Únii. Za týchto okolností by systém umelej inteligencie, ktorý používa prevádzkovateľ mimo Únie, mohol spracúvať údaje zákonne zozbierané v Únii a prenášané z Únie a poskytovať zadávajúcemu prevádzkovateľovi v Únii výstup z uvedeného systému umelej inteligencie vyplývajúci z tohto spracovania bez toho, aby sa uvedený systém umelej inteligencie uvádzal na trh, do prevádzky alebo sa používal v Únii. S cieľom zabrániť obchádzaniu tohto nariadenia a zabezpečiť účinnú ochranu fyzických osôb nachádzajúcich sa v Únii by sa toto nariadenie malo vzťahovať aj na poskytovateľov a používateľov systémov umelej inteligencie, ktorí sú usadení v tretej krajine, a to v rozsahu, v akom sa výstup generovaný týmito systémami používa v Únii. S cieľom zohľadniť existujúce dojednania a osobitné potreby spolupráce so zahraničnými partnermi, s ktorými sa vymieňajú informácie a dôkazy, by sa však toto nariadenie nemalo vzťahovať na orgány verejnej moci tretej krajiny a medzinárodné organizácie, ak konajú v rámci medzinárodných dohôd uzavretých na vnútroštátnej alebo európskej úrovni v oblasti presadzovania práva a justičnej spolupráce s Úniou alebo jej členskými štátmi. Takéto dohody boli uzavreté dvojstranne medzi členskými štátmi a tretími krajinami alebo medzi Európskou úniou, Európolom a inými agentúrami EÚ a tretími krajinami a medzinárodnými organizáciami.
- (12) Toto nariadenie by sa malo vzťahovať aj na inštitúcie, úrady, orgány a agentúry Únie, ak konajú ako poskytovateľ alebo používateľ systému umelej inteligencie. Systémy umelej inteligencie vyvinuté alebo používané výlučne na vojenské účely by mali byť vylúčené z rozsahu pôsobnosti tohto nariadenia, ak toto používanie patrí do výlučnej právomoci spoločnej zahraničnej a bezpečnostnej politiky upravenej v hlave V Zmluvy o Európskej únii (ZEU). Týmto nariadením by nemali byť dotknuté ustanovenia o zodpovednosti poskytovateľov sprostredkovateľských služieb stanovené v smernici Európskeho parlamentu a Rady 2000/31/ES [v znení aktu o digitálnych službách].
- (13) S cieľom zabezpečiť jednotnú a vysokú úroveň ochrany verejných záujmov, pokiaľ ide o zdravie, bezpečnosť a základné práva, by sa mali stanoviť spoločné normatívne štandardy pre všetky vysokorizikové systémy umelej inteligencie. Tieto štandardy by mali byť v súlade s Chartou základných práv Európskej únie (ďalej len „charta“)



a mali by byť nediskriminačné a v súlade so záväzkami Únie v oblasti medzinárodného obchodu.

- (14) Na účely zavedenia primeraného a účinného súboru záväzných pravidiel pre systémy umelej inteligencie by sa mal dodržiavať jasne vymedzený prístup založený na riziku. Týmto prístupom by sa mal prispôbiť typ a obsah takýchto pravidiel intenzite a rozsahu rizík, ktoré môžu systémy umelej inteligencie vytvárať. Preto je potrebné zakázať určité praktiky v oblasti umelej inteligencie, stanoviť požiadavky na vysokorizikové systémy umelej inteligencie a povinnosti príslušných prevádzkovateľov, ako aj stanoviť povinnosti transparentnosti pre určité systémy umelej inteligencie.
- (15) Využívanie umelej inteligencie má síce mnoho výhod, túto technológiu však možno zneužiť a môže sa stať zdrojom nových a výkonných nástrojov umožňujúcich manipulatívne a zneužívajúce praktiky a praktiky v oblasti sociálnej kontroly. Takéto praktiky sú mimoriadne škodlivé a mali by sa zakázať, pretože sú v rozpore s hodnotami Únie týkajúcimi sa rešpektovania ľudskej dôstojnosti, slobody, rovnosti, demokracie a právneho štátu a základných práv Únie vrátane práva na nediskrimináciu, ochranu údajov a súkromia a práv dieťaťa.
- (16) Malo by sa zakázať uvádzanie na trh, do prevádzky alebo používanie určitých systémov umelej inteligencie určených na ovplyvňovanie ľudského správania, pri ktorých je pravdepodobné, že spôsobia fyzickú alebo psychickú ujmu. Takéto systémy umelej inteligencie využívajú podprahové komponenty, ktoré jednotlivci nie sú schopní vnímať, prípadne zneužívajú zraniteľnosť detí a ľudí, ktorí sú zraniteľní vzhľadom na svoj vek, telesnú alebo duševnú nespôsobilosť. Robia tak s úmyslom podstatne ovplyvniť správanie osoby, a to spôsobom, ktorý spôsobuje alebo pravdepodobne spôsobí ujmu tejto osobe alebo inej osobe. Takýto úmysel nemožno predpokladať, ak ovplyvnenie ľudského správania vyplýva z faktorov nesúvisiacich so systémom umelej inteligencie, ktoré sú mimo kontroly poskytovateľa alebo používateľa. Zákaz by nemal brániť výskumu takýchto systémov umelej inteligencie na legítimne účely, pokiaľ takýto výskum nepredstavuje využívanie systému umelej inteligencie vo vzťahoch človek – stroj, ktoré vystavuje fyzické osoby ujme, a pokiaľ sa vykonáva v súlade s uznávanými etickými normami vedeckého výskumu.
- (17) Systémy umelej inteligencie, ktoré poskytujú sociálne hodnotenie fyzických osôb na všeobecné účely vykonávané orgánmi verejnej moci alebo v ich mene, môžu viesť k diskriminačným výsledkom a vylúčeniu určitých skupín. Môžu porušovať právo na dôstojnosť a nediskrimináciu a hodnoty rovnosti a spravodlivosti. Takéto systémy umelej inteligencie hodnotia alebo klasifikujú dôveryhodnosť fyzických osôb na základe ich spoločenského správania vo viacerých kontextoch alebo známych či predpokladaných osobných alebo osobnostných charakteristík. Sociálne skóre získané na základe takýchto systémov umelej inteligencie môže viesť k poškodzujúcemu alebo nepriaznivému zaobchádzaniu s fyzickými osobami alebo celými skupinami takýchto osôb v sociálnych kontextoch nesúvisiacich s kontextom, v ktorom boli údaje pôvodne vygenerované alebo zhromaždené, prípadne k poškodzujúcemu zaobchádzaniu, ktoré je neprimerané alebo neodôvodnené vzhľadom na závažnosť ich sociálneho správania. Takéto systémy umelej inteligencie by sa preto mali zakázať.
- (18) Používanie systémov umelej inteligencie na diaľkovú biometrickú identifikáciu fyzických osôb „v reálnom čase“ vo verejne prístupných priestoroch na účely presadzovania práva sa považuje za obzvlášť rušivý zásah do práv a slobôd dotknutých osôb, keďže môže ovplyvniť súkromný život veľkej časti obyvateľstva,

vyvoláva pocit neustáleho sledovania a nepriamo odrádza od využívania slobody zhromažďovania a iných základných práv. Okrem toho bezprostrednosť vplyvu a obmedzené možnosti ďalších kontrol alebo opráv v súvislosti s používaním takýchto systémov fungujúcich „v reálnom čase“ so sebou prinášajú zvýšené riziká z hľadiska práv a slobôd osôb, ktorých sa týkajú činnosti v oblasti presadzovania práva.

- (19) Používanie týchto systémov na účely presadzovania práva by sa preto malo zakázať s výnimkou troch podrobne opísaných a úzko vymedzených situácií, keď je toto použitie nevyhnutne potrebné na dosiahnutie podstatného verejného záujmu, ktorého význam prevažuje nad rizikami. Tieto situácie zahŕňajú pátranie po potenciálnych obetiach trestných činov vrátane nezvestných detí, niektoré prípady ohrozenia života alebo fyzickej bezpečnosti fyzických osôb alebo hrozby teroristického útoku a odhaľovanie, lokalizáciu, identifikáciu alebo stíhanie páchatel'ov trestných činov uvedených v rámcovom rozhodnutí Rady 2002/584/SVV<sup>38</sup>, ak za ne podľa právnych predpisov dotknutého členského štátu možno v danom členskom štáte uložiť trest odňatia slobody alebo ochranné opatrenie spojené s odňatím slobody s hornou hranicou trestnej sadzby najmenej tri roky, alebo podozrivých zo spáchania takýchto trestných činov. Takáto hranica trestu odňatia slobody alebo ochranného opatrenia spojeného s odňatím slobody v súlade s vnútroštátnym právom prispieva k zabezpečeniu toho, že daný trestný čin bude dostatočne závažný na to, aby sa ním dalo potenciálne odôvodniť použitie systémov diaľkovej biometrickej identifikácie „v reálnom čase“. Okrem toho je pravdepodobné, že niektoré z 32 trestných činov uvedených v rámcovom rozhodnutí Rady 2002/584/SVV sú v praxi relevantnejšie ako iné, keďže nevyhnutnosť a primeranosť použitia diaľkovej biometrickej identifikácie „v reálnom čase“ budú pravdepodobne veľmi rôznorodé jednak z hľadiska praktického vykonávania odhaľovania, lokalizácie, identifikácie alebo stíhania páchatel'a jednotlivých uvedených trestných činov alebo osôb podozrivých z ich spáchania a zároveň vzhľadom na pravdepodobné rozdiely v závažnosti, pravdepodobnosti a rozsahu spôsobenej ujmy alebo možných negatívnych dôsledkov.
- (20) S cieľom zabezpečiť, aby sa tieto systémy používali zodpovedným a primeraným spôsobom, je tiež dôležité stanoviť, že v každej z týchto troch podrobne opísaných a úzko vymedzených situácií by sa mali zohľadniť určité prvky, najmä pokiaľ ide o povahu situácie, ktorá viedla k predloženiu žiadosti, o dôsledky využívania týchto systémov na práva a slobody všetkých dotknutých osôb a o záruky a podmienky zabezpečené pri tomto používaní. Okrem toho používanie systému diaľkovej biometrickej identifikácie „v reálnom čase“ vo verejne prístupných priestoroch na účely presadzovania práva by malo podliehať primeraným časovým a priestorovým obmedzeniam, najmä so zreteľom na dôkazy alebo náznaky týkajúce sa daných hrozieb, obetí alebo páchatel'a. Referenčná databáza osôb by mala byť vhodná pre každý prípad použitia v každej z troch uvedených situácií.
- (21) Každé použitie systému diaľkovej biometrickej identifikácie „v reálnom čase“ vo verejne prístupných priestoroch na účely presadzovania práva by malo podliehať výslovnému a osobitnému povoleniu súdneho orgánu alebo nezávislého správneho orgánu členského štátu. Toto povolenie by bolo v zásade potrebné získať pred použitím systému, s výnimkou riadne odôvodnených naliehavých situácií, t. j. situácií, v ktorých je potreba použiť predmetné systémy tak naliehavá, že je naozaj objektívne nemožné získať povolenie pred začatím tohto použitia. V takýchto naliehavých

<sup>38</sup>

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

situáciách by sa používanie malo obmedziť na absolútne nevyhnutné minimum a malo by podliehať primeraným zárukám a podmienkam stanoveným vo vnútroštátnom práve a špecifikovaným v kontexte každého jednotlivého naliehavého prípadu použitia samotným orgánom presadzovania práva. Okrem toho by sa orgán presadzovania práva mal v takýchto situáciách snažiť získať povolenie čo najskôr, pričom uvedie dôvody, pre ktoré ho nemohol požadovať skôr.

- (22) Navyše je vhodné v rámci podrobne opísanom týmto nariadením stanoviť, že takéto použitie na území členského štátu v súlade s týmto nariadením by malo byť možné len vtedy a do takej miery, do akej sa daný členský štát rozhodol výslovne stanoviť možnosť povoliť toto použitie vo svojich podrobných pravidlách vnútroštátneho práva. V dôsledku toho sa členské štáty môžu podľa tohto nariadenia naďalej na základe vlastného uváženia rozhodnúť, že takúto možnosť vôbec nestanovia alebo ju stanovia len v súvislosti s niektorými z cieľov, ktorými možno odôvodniť povolené použitie určené v tomto nariadení.
- (23) Používanie systémov umelej inteligencie na diaľkovú biometrickú identifikáciu fyzických osôb „v reálnom čase“ vo verejne prístupných priestoroch na účely presadzovania práva nevyhnutne zahŕňa spracúvanie biometrických údajov. Pravidlá tohto nariadenia, ktorými sa s výhradou určitých výnimiek takéto používanie zakazuje a ktoré sú založené na článku 16 ZFEÚ, by sa mali uplatňovať ako *lex specialis*, pokiaľ ide o pravidlá spracúvania biometrických údajov uvedené v článku 10 smernice (EÚ) 2016/680, čím by sa takéto používanie a spracúvanie príslušných biometrických údajov upravovalo vyčerpávajúcim spôsobom. Takéto používanie a spracúvanie by preto malo byť možné, len pokiaľ je zlučiteľné s rámcom stanoveným v tomto nariadení, a mimo tohto rámca by nemal existovať priestor na to, aby príslušné orgány, ak konajú na účely presadzovania práva, používali takéto systémy a spracúvali takéto údaje v súvislosti s týmto použitím z dôvodov uvedených v článku 10 smernice (EÚ) 2016/680. V tejto súvislosti nie je cieľom tohto nariadenia poskytnúť právny základ pre spracúvanie osobných údajov podľa článku 8 smernice 2016/680. Na používanie systémov umelej inteligencie na diaľkovú biometrickú identifikáciu „v reálnom čase“ vo verejne prístupných priestoroch na iné účely ako na presadzovanie práva, a to aj príslušnými orgánmi, by sa však nemal vzťahovať osobitný rámec týkajúci sa takéhoto použitia na účely presadzovania práva stanovený v tomto nariadení. Takéto použitie na iné účely ako na presadzovanie práva by preto nemalo podliehať požiadavke povolenia podľa tohto nariadenia a uplatniteľných podrobných pravidiel vnútroštátneho práva, na základe ktorých sa môže vykonávať.
- (24) Každé spracovanie biometrických údajov a iných osobných údajov súvisiace s používaním systémov umelej inteligencie na biometrickú identifikáciu, okrem spracovania v súvislosti s používaním systémov umelej inteligencie na diaľkovú biometrickú identifikáciu fyzických osôb „v reálnom čase“ vo verejne prístupných priestoroch na účely presadzovania práva, ako sa stanovuje v tomto nariadení, vrátane prípadov, keď tieto systémy používajú príslušné orgány vo verejne prístupných priestoroch na iné účely ako na presadzovanie práva, by malo naďalej spĺňať všetky prípadné požiadavky vyplývajúce z článku 9 ods. 1 nariadenia (EÚ) 2016/679, článku 10 ods. 1 nariadenia (EÚ) 2018/1725 a článku 10 smernice (EÚ) 2016/680.
- (25) V súlade s článkom 6a Protokolu č. 21 o postavení Spojeného kráľovstva a Írska s ohľadom na priestor slobody, bezpečnosti a spravodlivosti, ktorý je pripojený k ZEÚ a ZFEÚ, nie je Írsko viazané pravidlami stanovenými v článku 5 ods. 1 písm. d) a článku 5 ods. 2 a 3 tohto nariadenia prijatého na základe článku 16 Zmluvy o fungovaní EÚ, ktoré sa týkajú spracúvania osobných údajov členskými štátmi pri

vykonávaní činností, ktoré patria do rozsahu pôsobnosti tretej časti hlavy V kapitoly 4 alebo kapitoly 5 ZFEÚ, ak Írsko nie je viazané pravidlami, ktorými sa spravujú formy justičnej spolupráce v trestných veciach alebo policajnej spolupráce, v rámci ktorých sa musia dodržiavať ustanovenia prijaté na základe článku 16 ZFEÚ.

- (26) V súlade s článkami 2 a 2a Protokolu č. 22 o postavení Dánska, ktorý je pripojený k ZEÚ a ZFEÚ, nie je Dánsko viazané pravidlami stanovenými v článku 5 ods. 1 písm. d) a článku 5 ods. 2 a 3 tohto nariadenia prijatého na základe článku 16 ZFEÚ, ktoré sa týkajú spracúvania osobných údajov členskými štátmi pri vykonávaní činností, ktoré patria do rozsahu pôsobnosti tretej časti hlavy V kapitoly 4 alebo kapitoly 5 ZFEÚ, ani nepodlieha ich uplatňovaniu.
- (27) Vysokorizikové systémy umelej inteligencie by sa mali uviesť na trh Únie alebo do prevádzky len vtedy, ak spĺňajú určité povinné požiadavky. Týmito požiadavkami by sa malo zabezpečiť, aby vysokorizikové systémy umelej inteligencie, ktoré sú dostupné v Únii alebo ktorých výstupy sú v Únii inak využívané, nepredstavovali neprijateľné riziká pre dôležité verejné záujmy Únie uznané a chránené právom Únie. Systémy umelej inteligencie označené ako vysokorizikové by sa mali obmedziť na tie, ktoré majú významný škodlivý vplyv na zdravie, bezpečnosť a základné práva osôb v Únii, a takéto obmedzenie minimalizuje akékoľvek prípadné obmedzenie medzinárodného obchodu.
- (28) Systémy umelej inteligencie by mohli mať nepriaznivé účinky na zdravie a bezpečnosť osôb, najmä ak takéto systémy fungujú ako komponenty výrobkov. V súlade s cieľmi harmonizačných právnych predpisov Únie uľahčiť voľný pohyb výrobkov na vnútornom trhu a zabezpečiť, aby sa na trh dostali len bezpečné a inak vyhovujúce výrobky, je dôležité, aby sa riadne predchádzalo bezpečnostným rizikám, ktoré môže výrobok ako celok vytvárať svojimi digitálnymi komponentmi vrátane systémov umelej inteligencie, a aby sa tieto riziká náležite zmierňovali. Napríklad čoraz autonómnejšie roboty, či už v kontexte výroby alebo osobnej asistencie a starostlivosti, by mali byť schopné bezpečne fungovať a vykonávať svoje funkcie v zložitých prostrediach. Podobne v sektore zdravotníctva, kde existuje obzvlášť vysoké riziko v oblasti života a zdravia, by mali byť čoraz sofistikovanejšie diagnostické systémy a systémy podporujúce ľudské rozhodnutia spoľahlivé a presné. Pri klasifikácii systému umelej inteligencie ako vysokorizikového je obzvlášť dôležitý rozsah nepriaznivého vplyvu systému umelej inteligencie na základné práva chránené chartou. Medzi tieto práva patrí právo na ľudskú dôstojnosť, rešpektovanie súkromného a rodinného života, ochrana osobných údajov, sloboda prejavu a právo na informácie, sloboda zhromažďovania a združovania, nediskriminácia, ochrana spotrebiteľa, základné pracovné práva, práva osôb so zdravotným postihnutím, právo na účinný prostriedok nápravy a na spravodlivý proces, právo na obhajobu a prezumpcia nevinoty, právo na dobrú správu vecí verejných. Okrem týchto práv je dôležité zdôrazniť, že deti majú osobitné práva zakotvené v článku 24 Charty EÚ a v Dohovore Organizácie Spojených národov o právach dieťaťa (ďalej rozpracované vo všeobecnej poznámke č. 25 Dohovoru OSN o právach dieťaťa, pokiaľ ide o digitálne prostredie), ktoré si v oboch prípadoch vyžadujú zváženie zraniteľnosti detí a poskytnutie takejto ochrany a starostlivosti nevyhnutných pre ich blaho. Pri posudzovaní závažnosti ujmy, ktorú môže systém umelej inteligencie spôsobiť, a to aj v súvislosti so zdravím a bezpečnosťou osôb, by sa malo zohľadniť aj základné právo na vysokú úroveň ochrany životného prostredia zakotvené v charte a vykonávané v politikách Únie.

- (29) Pokiaľ ide o vysokorizikové systémy umelej inteligencie, ktoré sú bezpečnostnými komponentmi výrobkov alebo systémov, alebo ktoré sú samy výrobkami alebo systémami patriacimi do rozsahu pôsobnosti nariadenia Európskeho parlamentu a Rady (ES) č. 300/2008<sup>39</sup>, nariadenia Európskeho parlamentu a Rady (EÚ) č. 167/2013<sup>40</sup>, nariadenia Európskeho parlamentu a Rady (EÚ) č. 168/2013<sup>41</sup>, smernice Európskeho parlamentu a Rady 2014/90/EÚ<sup>42</sup>, smernice Európskeho parlamentu a Rady (EÚ) 2016/797<sup>43</sup>, nariadenia Európskeho parlamentu a Rady (EÚ) 2018/858<sup>44</sup>, nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1139<sup>45</sup> a nariadenia Európskeho parlamentu a Rady (EÚ) 2019/2144<sup>46</sup>, je vhodné uvedené akty zmeniť s cieľom zaistiť, aby Komisia pri prijímaní akýchkoľvek budúcich relevantných delegovaných alebo vykonávacích aktov na základe uvedených aktov zohľadňovala povinné požiadavky na vysokorizikové systémy umelej inteligencie stanovené v tomto nariadení na základe technických a regulačných osobitostí jednotlivých odvetví bez toho, aby zasahovala do existujúcich mechanizmov správy, posudzovania zhody a presadzovania a do orgánov zriadených v rámci uvedených aktov.
- (30) Pokiaľ ide o systémy umelej inteligencie, ktoré sú bezpečnostnými komponentmi výrobkov alebo ktoré sú samy výrobkami, ktoré patria do rozsahu pôsobnosti určitých harmonizačných právnych predpisov Únie, je vhodné klasifikovať ich podľa tohto nariadenia ako vysokorizikové, pokiaľ v prípade daného výrobku vykonáva postup posudzovania zhody orgán posudzovania zhody tretej strany podľa príslušných harmonizačných právnych predpisov Únie. Medzi takéto výrobky patria najmä

<sup>39</sup> Nariadenie Európskeho parlamentu a Rady (ES) č. 300/2008 z 11. marca 2008 o spoločných pravidlách v oblasti bezpečnostnej ochrany civilného letectva a o zrušení nariadenia (ES) č. 2320/2002 (Ú. v. EÚ L 97, 9.4.2008, s. 72).

<sup>40</sup> Nariadenie Európskeho parlamentu a Rady (EÚ) č. 167/2013 z 5. februára 2013 o schvaľovaní poľnohospodárskych a lesných vozidiel a o dohľade nad trhom s týmito vozidlami (Ú. v. EÚ L 60, 2.3.2013, s. 1).

<sup>41</sup> Nariadenie Európskeho parlamentu a Rady (EÚ) č. 168/2013 z 15. januára 2013 o schvaľovaní a dohľade nad trhom dvoj- alebo trojkolesových vozidiel a štvorkoliek (Ú. v. EÚ L 60, 2.3.2013, s. 52).

<sup>42</sup> Smernica Európskeho parlamentu a Rady 2014/90/EÚ z 23. júla 2014 o vybavení námorných lodí a o zrušení smernice Rady 96/98/ES (Ú. v. EÚ L 257, 28.8.2014, s. 146).

<sup>43</sup> Smernica Európskeho parlamentu a Rady (EÚ) 2016/797 z 11. mája 2016 o interoperabilite železničného systému v Európskej únii (Ú. v. EÚ L 138, 26.5.2016, s. 44).

<sup>44</sup> Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/858 z 30. mája 2018 o schvaľovaní motorových vozidiel a ich prípojných vozidiel, ako aj systémov, komponentov a samostatných technických jednotiek určených pre takéto vozidlá a o dohľade nad trhom s nimi, ktorým sa menia nariadenia (ES) č. 715/2007 a (ES) č. 595/2009 a zrušuje smernica 2007/46/ES (Ú. v. EÚ L 151, 14.6.2018, s. 1).

<sup>45</sup> Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1139 zo 4. júla 2018 o spoločných pravidlách v oblasti civilného letectva, ktorým sa zriaďuje Agentúra Európskej únie pre bezpečnosť letectva a ktorým sa menia nariadenia Európskeho parlamentu a Rady (ES) č. 2111/2005, (ES) č. 1008/2008, (EÚ) č. 996/2010, (EÚ) č. 376/2014 a smernice Európskeho parlamentu a Rady 2014/30/EÚ a 2014/53/EÚ a zrušujú nariadenia Európskeho parlamentu a Rady (ES) č. 552/2004 a (ES) č. 216/2008 a nariadenie Rady (EHS) č. 3922/91 (Ú. v. EÚ L 212, 22.8.2018, s. 1).

<sup>46</sup> Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/2144 z 27. novembra 2019 o požiadavkách na typové schvaľovanie motorových vozidiel a ich prípojných vozidiel a systémov, komponentov a samostatných technických jednotiek určených pre tieto vozidlá, pokiaľ ide o ich všeobecnú bezpečnosť a ochranu cestujúcich vo vozidle a zraniteľných účastníkov cestnej premávky, ktorým sa mení nariadenie Európskeho parlamentu a Rady (EÚ) 2018/858 a ktorým sa zrušujú nariadenia Európskeho parlamentu a Rady (ES) č. 78/2009, (ES) č. 79/2009 a (ES) č. 661/2009 a nariadenia Komisie (ES) č. 631/2009, (EÚ) č. 406/2010, (EÚ) č. 672/2010, (EÚ) č. 1003/2010, (EÚ) č. 1005/2010, (EÚ) č. 1008/2010, (EÚ) č. 1009/2010, (EÚ) č. 19/2011, (EÚ) č. 109/2011, (EÚ) č. 458/2011, (EÚ) č. 65/2012, (EÚ) č. 130/2012, (EÚ) č. 347/2012, (EÚ) č. 351/2012, (EÚ) č. 1230/2012 a (EÚ) 2015/166 (Ú. v. EÚ L 325, 16.12.2019, s. 1).

strojové zariadenia, hračky, výtahy, zariadenia a ochranné systémy určené na použitie v prostredí s nebezpečím výbuchu, rádiové zariadenia, tlakové zariadenia, vybavenie rekreačných plavidiel, lanovkové zariadenia, spotrebiče spaľujúce plynné palivá, zdravotnícke pomôcky a diagnostické zdravotnícke pomôcky *in vitro*.

- (31) Klasifikácia systému umelej inteligencie ako vysokorizikového podľa tohto nariadenia by nemala nevyhnutne znamenať, že výrobok, ktorého bezpečnostným komponentom je systém umelej inteligencie, alebo samotný systém umelej inteligencie ako výrobok sa považuje za „vysokorizikový“ podľa kritérií stanovených v príslušných harmonizačných právnych predpisoch Únie, ktoré sa vzťahujú na daný výrobok. Platí to najmä pre nariadenie Európskeho parlamentu a Rady (EÚ) 2017/745<sup>47</sup> a nariadenie Európskeho parlamentu a Rady (EÚ) 2017/746<sup>48</sup>, kde sa pre výrobky so stredným a vysokým rizikom vyžaduje posudzovanie zhody tret'ou stranou.
- (32) Pokiaľ ide o samostatné systémy umelej inteligencie, t. j. vysokorizikové systémy umelej inteligencie iné ako tie, ktoré sú bezpečnostnými komponentmi výrobkov, alebo ktoré sú samy výrobkami, je vhodné klasifikovať ich ako vysokorizikové, ak vzhľadom na svoj zamýšľaný účel predstavujú vysoké riziko poškodenia zdravia a bezpečnosti alebo základných práv osôb, pričom sa berie do úvahy závažnosť možnej ujmy a pravdepodobnosť jej výskytu, a ak sa využívajú vo viacerých oblastiach uvedených v nariadení, ktoré sú jasne vopred vymedzené. Identifikácia týchto systémov je založená na rovnakej metodike a kritériách, aké sa predpokladajú aj v prípade akýchkoľvek budúcich zmien zoznamu vysokorizikových systémov umelej inteligencie.
- (33) Technické nepresnosti systémov umelej inteligencie určených na diaľkovú biometrickú identifikáciu fyzických osôb môžu viesť k skresleným výsledkom a mať diskriminačné účinky. Platí to najmä v prípade veku, etnického pôvodu, pohlavia alebo zdravotných postihnutí. Preto by sa systémy diaľkovej biometrickej identifikácie „v reálnom čase“ a „následnej“ diaľkovej biometrickej identifikácie mali klasifikovať ako vysokorizikové. Vzhľadom na riziká, ktoré predstavujú, by oba typy systémov diaľkovej biometrickej identifikácie mali podliehať osobitným požiadavkám týkajúcim sa schopností logovania a ľudského dohľadu.
- (34) Pokiaľ ide o riadenie a prevádzku kritickej infraštruktúry, je vhodné klasifikovať ako vysokorizikové také systémy umelej inteligencie, ktoré sú určené na používanie ako bezpečnostné komponenty pri riadení a prevádzke cestnej premávky a pri dodávkach vody, plynu, tepla a elektrickej energie, keďže ich zlyhanie alebo porucha môže ohroziť život a zdravie osôb vo veľkom rozsahu a viesť k značným narušeniam bežného vykonávania sociálnych a hospodárskych činností.
- (35) Za vysokorizikové by sa mali považovať systémy umelej inteligencie používané vo vzdelávaní alebo odbornej príprave, najmä na určovanie prístupu osôb do inštitúcií vzdelávania a odbornej prípravy alebo na ich priradenie k týmto inštitúciám, alebo na hodnotenie osôb na základe testov ako súčasť ich vzdelávania alebo ako predpoklad pre ich vzdelávanie, pretože môžu určovať vzdelávací a profesionálny priebeh života

---

<sup>47</sup> Nariadenie Európskeho parlamentu a Rady (EÚ) 2017/745 z 5. apríla 2017 o zdravotníckych pomôckach, zmene smernice 2001/83/ES, nariadenia (ES) č. 178/2002 a nariadenia (ES) č. 1223/2009 a o zrušení smerníc Rady 90/385/EHS a 93/42/EHS (Ú. v. EÚ L 117, 5.5.2017, s. 1).

<sup>48</sup> Nariadenie Európskeho parlamentu a Rady (EÚ) 2017/746 z 5. apríla 2017 o diagnostických zdravotníckych pomôckach *in vitro* a o zrušení smernice 98/79/ES a rozhodnutia Komisie 2010/227/EÚ (Ú. v. EÚ L 117, 5.5.2017, s. 176).

osoby, a tým ovplyvňovať jej schopnosť zabezpečiť si živobytie. Ak sú takéto systémy navrhnuté a používané nesprávne, môžu porušovať právo na vzdelanie a odbornú prípravu, ako aj právo nebyť diskriminovaný a tým zachovávať zaužívané formy diskriminácie.

- (36) Ako vysokorizikové by sa mali klasifikovať aj systémy umelej inteligencie používané pri zamestnávaní, riadení pracovníkov a prístupe k samostatnej zárobkovej činnosti, najmä pri náboře a výbere osôb, pri rozhodovaní o povýšení a ukončení pracovného pomeru a pri pridelovaní úloh, monitorovaní alebo hodnotení osôb v zmluvných pracovnoprávných vzťahoch, pretože tieto systémy môžu významne ovplyvniť budúce kariérne vyhliadky a živobytie týchto osôb. Príslušné zmluvné pracovnoprávne vzťahy by mali zahŕňať zamestnancov a osoby, ktorí poskytujú služby prostredníctvom platforiem, ako sa uvádza v pracovnom programe Komisie na rok 2021. Takéto osoby by sa v zásade nemali považovať za používateľov v zmysle tohto nariadenia. Takéto systémy môžu počas celého procesu prijímania do zamestnania a počas hodnotenia, povyšovania alebo udržiavania osôb v zmluvných pracovnoprávných vzťahoch zachovávať zaužívané formy diskriminácie, napríklad žien, určitých vekových skupín, osôb so zdravotným postihnutím alebo osôb určitého rasového alebo etnického pôvodu alebo sexuálnej orientácie. Systémy umelej inteligencie používané na monitorovanie výkonnosti a správania týchto osôb môžu mať vplyv aj na ich práva na ochranu údajov a súkromia.
- (37) Ďalšou oblasťou, v ktorej si využívanie systémov umelej inteligencie zaslúži osobitnú pozornosť, je prístup k určitým základným súkromným a verejným službám a dávkam, ktoré sú potrebné na to, aby sa ľudia mohli plne zapojiť do spoločnosti alebo si mohli zlepšiť životnú úroveň, a ich využívanie. Ako vysokorizikové by sa mali klasifikovať najmä systémy umelej inteligencie používané na bodové hodnotenie kreditného rizika alebo hodnotenie úverovej bonity fyzických osôb, pretože určujú prístup týchto osôb k finančným zdrojom alebo základným službám, ako sú bývanie, elektrická energia a telekomunikačné služby. Systémy umelej inteligencie používané na tento účel môžu viesť k diskriminácii osôb alebo skupín a zachovávať zaužívané formy diskriminácie, napríklad na základe rasového alebo etnického pôvodu, zdravotných postihnutí, veku, sexuálnej orientácie, alebo môžu vytvárať nové formy diskriminačných vplyvov. Vzhľadom na veľmi obmedzený rozsah vplyvu a dostupné alternatívy na trhu je vhodné stanoviť výnimku pre systémy umelej inteligencie na účely posudzovania úverovej bonity a bodového hodnotenia kreditného rizika, pokiaľ ich uvedú do prevádzky malí poskytovatelia pre svoju vlastnú potrebu. Fyzické osoby, ktoré žiadajú o dávky a služby verejnej pomoci alebo ktoré od orgánov verejnej moci prijímajú tieto dávky a služby, sú zvyčajne od týchto dávok a služieb závislé a nachádzajú sa v zraniteľnom postavení vo vzťahu k zodpovedným orgánom. Ak sa systémy umelej inteligencie používajú na určenie toho, či by orgány mali takéto dávky a služby zamietnuť, znížiť, zrušiť alebo žiadať o ich vrátenie, môžu mať významný vplyv na živobytie osôb a môžu porušovať ich základné práva, ako je právo na sociálnu ochranu, nediskrimináciu, ľudskú dôstojnosť alebo účinný prostriedok nápravy. Preto by sa tieto systémy mali klasifikovať ako vysokorizikové. Toto nariadenie by však nemalo brániť rozvoju a využívaniu inováčných prístupov vo verejnej správe, pre ktorú by mohlo byť širšie využívanie vyhovujúcich a bezpečných systémov umelej inteligencie prospešné, za predpokladu, že tieto systémy nepredstavujú vysoké riziko pre právnické a fyzické osoby. V konečnom dôsledku by sa ako vysokorizikové mali klasifikovať aj systémy umelej inteligencie používané na vysielanie záchranných služieb prvej reakcie alebo na stanovovanie priority ich vysielania, pretože prijímajú



rozhodnutia v situáciách, ktoré sú veľmi kritické z hľadiska života a zdravia osôb a ich majetku.

(38) Opatrenia orgánov presadzovania práva zahŕňajúce určité použitia systémov umelej inteligencie sa vyznačujú značným stupňom nerovnováhy právomocí a môžu viesť k sledovaniu, zatknutiu alebo pozbaveniu slobody fyzickej osoby, ako aj k iným nepriaznivým vplyvom na základné práva zaručené chartou. Najmä ak systém umelej inteligencie nie je trénovaný na vysokokvalitných údajoch, nespĺňa primerané požiadavky, pokiaľ ide o jeho presnosť alebo spoľahlivosť, alebo nie je pred uvedením na trh alebo do prevádzky riadne koncipovaný a otestovaný, môže ľudí vylúčiť diskriminačným alebo inak nesprávnym či nespravodlivým spôsobom. Okrem toho by mohlo byť obmedzené uplatňovanie dôležitých procesných základných práv, ako je právo na účinný prostriedok nápravy a na spravodlivý proces, ako aj právo na obhajobu a prezumpcia nevinu, najmä ak takéto systémy umelej inteligencie nie sú dostatočne transparentné, vysvetliteľné a zdokumentované. Preto je vhodné klasifikovať ako vysokorizikové viaceré systémy umelej inteligencie určené na používanie v kontexte presadzovania práva, kde je presnosť, spoľahlivosť a transparentnosť obzvlášť dôležitá, aby sa zabránilo nepriaznivým vplyvom, zachovala dôvera verejnosti a zabezpečila zodpovednosť a účinná náprava. Vzhľadom na povahu predmetných činností a súvisiace riziká by tieto vysokorizikové systémy umelej inteligencie mali zahŕňať najmä systémy umelej inteligencie, ktoré majú orgány presadzovania práva používať na individuálne posúdenia rizika, ako detektory lži a podobné nástroje alebo na zisťovanie emocionálneho stavu fyzickej osoby, odhaľovanie vykonštruovaných správ, ktoré manipulujú s obsahom (tzv. deepfakes), na hodnotenie spoľahlivosti dôkazov v trestnom konaní, na predpovedanie výskytu alebo opätovného výskytu skutočného alebo potenciálneho trestného činu na základe profilovania fyzických osôb alebo posudzovania osobnostných a povahových rysov alebo trestnej činnosti fyzických osôb alebo skupín v minulosti, na profilovanie v priebehu odhaľovania, vyšetrovania alebo stíhania trestných činov, ako aj na analýzu trestnej činnosti vo vzťahu k fyzickým osobám. Systémy umelej inteligencie, ktoré sú osobitne určené na používanie daňovými a colnými orgánmi v správnych konaniach, by sa nemali považovať za vysokorizikové systémy umelej inteligencie používané orgánmi presadzovania práva na účely predchádzania trestným činom, ich odhaľovania, vyšetrovania a stíhania.

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

toto nariadenie, by mali spĺňať príslušné procedurálne požiadavky stanovené v smernici Európskeho parlamentu a Rady 2013/32/EÚ<sup>49</sup>, nariadení Európskeho parlamentu a Rady (ES) č. 810/2009<sup>50</sup> a iných príslušných právnych predpisoch.

- (40) Niektoré systémy umelej inteligencie určené na výkon spravodlivosti a demokratických procesov by sa mali klasifikovať ako vysokorizikové vzhľadom na ich potenciálne významný vplyv na demokraciu, právny štát, osobné slobody, ako aj právo na účinný prostriedok nápravy a na spravodlivý proces. Ako vysokorizikové je vhodné kvalifikovať systémy umelej inteligencie určené na pomoc justičným orgánom pri skúmaní a výklade skutočností a práva a pri uplatňovaní práva na konkrétny súbor skutočností, najmä z dôvodu riešenia rizík možných skreslení, chýb a nepriehľadnosti. Takáto kvalifikácia by sa však nemala vzťahovať na systémy umelej inteligencie určené na čisto pomocné administratívne činnosti, ktoré nemajú vplyv na skutočný výkon spravodlivosti v jednotlivých prípadoch, ako napr. anonymizácia alebo pseudonymizácia súdnych rozhodnutí, dokumentov alebo údajov, komunikácia medzi zamestnancami, administratívne úlohy alebo pridelovanie zdrojov.
- (41) Skutočnosť, že systém umelej inteligencie sa podľa tohto nariadenia klasifikuje ako vysokorizikový, by sa nemala vykladať tak, že používanie tohto systému je nevyhnutne zákonné podľa iných aktov práva Únie alebo vnútroštátneho práva zlučiteľného s právom Únie, ako napr. v oblasti ochrany osobných údajov, používania detektorov lži a podobných nástrojov alebo iných systémov na zisťovanie emocionálneho stavu fyzických osôb. Akékoľvek takéto použitie by sa malo naďalej vykonávať výlučne v súlade s uplatniteľnými požiadavkami vyplývajúcimi z charty a z uplatniteľných aktov sekundárneho práva Únie a vnútroštátneho práva. Toto nariadenie by sa nemalo chápať tak, že poskytuje právny základ pre spracúvanie osobných údajov, prípadne vrátane osobitných kategórií osobných údajov.
- (42) S cieľom zmierniť riziká, ktoré vyplývajú používateľom a dotknutým osobám z vysokorizikových systémov umelej inteligencie uvedených na trh Únie alebo inak uvedených do prevádzky na trhu Únie, by sa mali uplatňovať určité povinné požiadavky, pričom by sa mal zohľadniť zamýšľaný účel používania tohto systému a systém riadenia rizík, ktorý zavedie poskytovateľ.
- (43) Požiadavky by sa mali vzťahovať na vysokorizikové systémy umelej inteligencie, pokiaľ ide o kvalitu použitých súborov údajov, technickú dokumentáciu a uchovávanie záznamov, transparentnosť a poskytovanie informácií používateľom, ľudský dohľad a spoľahlivosť, presnosť a kybernetickú bezpečnosť. Tieto požiadavky sú potrebné na účinné zmiernenie rizík pre zdravie, bezpečnosť a základné práva, ktoré sa uplatňujú vzhľadom na zamýšľaný účel systému, a nie sú primerane dostupné žiadne iné opatrenia menej obmedzujúce obchod, takže nedochádza k neodôvodneným obmedzeniam obchodu.
- (44) Pre výkonnosť mnohých systémov umelej inteligencie je kľúčová vysoká kvalita údajov, najmä ak sa využívajú techniky zahŕňajúce tréning modelov, aby vysokorizikový systém umelej inteligencie fungoval podľa zamýšľaného účelu a bezpečne a aby sa nestal zdrojom diskriminácie zakázanej právom Únie. Súbor

<sup>49</sup> Smernica Európskeho parlamentu a Rady 2013/32/EÚ z 26. júna 2013 o spoločných konaniach o poskytovaní a odnímaní medzinárodnej ochrany (Ú. v. EÚ L 180, 29.6.2013, s. 60).

<sup>50</sup> Nariadenie európskeho parlamentu a Rady (ES) č. 810/2009 z 13. júla 2009, ktorým sa ustanovuje vízový kódex Spoločenstva (vízový kódex) (Ú. v. EÚ L 243, 15.9.2009, s. 1).

vysokokvalitných tréningových, validačných a testovacích údajov si vyžadujú vykonávanie primeraných postupov správy a riadenia údajov. Súbor tréningových, validačných a testovacích údajov by mali byť dostatočne relevantné, reprezentatívne a bez chýb a mali by byť úplné vzhľadom na zamýšľaný účel systému. Mali by mať aj primerané štatistické vlastnosti, a to aj pokiaľ ide o osoby alebo skupiny osôb, v prípade ktorých sa má vysokorizikový systém umelej inteligencie používať. Súbor tréningových, validačných a testovacích údajov by mali v rozsahu, v akom si to vyžaduje zamýšľaný účel, zohľadňovať najmä vlastnosti, charakteristiky alebo prvky, ktoré sú špecifické pre konkrétne geografické, behaviorálne alebo funkčné podmienky alebo súvislosti, v ktorých sa má systém umelej inteligencie používať. Na ochranu práva iných osôb pred diskrimináciou, ktorá by mohla vyplývať zo skreslenia systémom umelej inteligencie, by poskytovatelia mali mať vzhľadom na významný verejný záujem možnosť spracúvať aj osobitné kategórie osobných údajov s cieľom zabezpečiť monitorovanie, odhaľovanie a nápravu tohto skreslenia vo vzťahu k vysokorizikovým systémom umelej inteligencie.

- (45) Pokiaľ ide o vývoj vysokorizikových systémov umelej inteligencie, niektorí aktéri, ako sú poskytovatelia, notifikované osoby a iné príslušné subjekty, ako napr. centrá digitálnych inovácií, testovacie experimentačné zariadenia a výskumní pracovníci, by mali mať prístup k súborom vysokokvalitných údajov a využívať ich v rámci svojich príslušných oblastí činnosti, ktoré súvisia s týmto nariadením. Pri poskytovaní dôveryhodného, zodpovedného a nediskriminačného prístupu k vysokokvalitným údajom na účely tréningovania, validácie a testovania systémov umelej inteligencie budú mať zásadný význam európske spoločné dátové priestory zriadené Komisiou a uľahčenie výmeny údajov medzi podnikmi a s verejnou správou vo verejnom záujme. Napríklad v oblasti zdravia uľahčí európsky priestor pre údaje týkajúce sa zdravia nediskriminačný prístup k údajom týkajúcim sa zdravia a tréningovanie algoritmov umelej inteligencie na týchto súboroch údajov, a to bezpečným, včasným, transparentným a dôveryhodným spôsobom chrániacim súkromie, pričom sa zabezpečí primerané inštitucionálne riadenie. Relevantné príslušné orgány vrátane sektorových orgánov, ktoré poskytujú alebo podporujú prístup k údajom, môžu takisto podporovať poskytovanie vysokokvalitných údajov na tréningovanie, validáciu a testovanie systémov umelej inteligencie.
- (46) Na overenie súladu s požiadavkami podľa tohto nariadenia je nevyhnutné mať informácie o tom, ako boli vyvinuté vysokorizikové systémy umelej inteligencie a ako fungujú počas celého svojho životného cyklu. Preto sa vyžaduje uchovávanie záznamov a dostupnosť technickej dokumentácie obsahujúcej informácie, ktoré sú potrebné na posúdenie súladu systému umelej inteligencie s príslušnými požiadavkami. Takéto informácie by mali zahŕňať všeobecné charakteristiky, schopnosti a obmedzenia systému, použité algoritmy, údaje, postupy tréningovania, testovania a validácie, ako aj dokumentáciu o príslušnom systéme riadenia rizík. Technická dokumentácia by sa mala priebežne aktualizovať.
- (47) Pre vysokorizikové systémy umelej inteligencie by sa mal vyžadovať určitý stupeň transparentnosti, aby sa vyriešila nepriehľadnosť, ktorá môže spôsobiť, že niektoré systémy umelej inteligencie budú pre fyzické osoby nezrozumiteľné alebo príliš zložité. Používatelia by mali byť schopní interpretovať výstup systému a vhodne ho používať. K vysokorizikovým systémom umelej inteligencie by preto mala byť pripojená príslušná dokumentácia a návod na použitie, ktoré by mali obsahovať stručné a jasné informácie, a to prípadne aj v súvislosti s možnými rizikami pre základné práva a diskrimináciu.

- (48) Vysokorizikové systémy umelej inteligencie by mali byť koncipované a vyvinuté tak, aby fyzické osoby mohli dohliadať na ich fungovanie. Na tento účel by mal poskytovateľ systému určiť pred jeho uvedením na trh alebo do prevádzky vhodné opatrenia ľudského dohľadu. Takýmito opatreniami by sa malo prípadne zaručiť najmä to, že do systému budú zabudované prevádzkové obmedzenia, ktoré samotný systém nedokáže potlačiť, a že systém bude reagovať na ľudského operátora a fyzické osoby, ktorým bol zverený ľudský dohľad, budú mať potrebnú spôsobilosť, odbornú prípravu a právomoc vykonávať túto úlohu.
- (49) Vysokorizikové systémy umelej inteligencie by mali fungovať konzistentne počas celého svojho životného cyklu a mali by spĺňať primeranú úroveň presnosti, spoľahlivosti a kybernetickej bezpečnosti v súlade so všeobecne uznávaným stavom techniky. Používatelia by mali byť informovaní o úrovni a metrikách na meranie presnosti.
- (50) Technická spoľahlivosť je kľúčovou požiadavkou pre vysokorizikové systémy umelej inteligencie. Tie by mali byť odolné voči rizikám súvisiacim s obmedzeniami systému (napr. chyby, poruchy, nezrovnalosti, neočakávané situácie), ako aj voči zlomyseľným konaniam, ktoré môžu ohroziť bezpečnosť systému umelej inteligencie a viesť k škodlivému alebo inému nežiaducemu správaniu. Neschopnosť chrániť pred týmito rizikami by mohla mať vplyv na bezpečnosť alebo negatívne ovplyvniť základné práva, napríklad v dôsledku chybných rozhodnutí alebo nesprávnych alebo skreslených výstupov vygenerovaných systémom umelej inteligencie.
- (51) Kybernetická bezpečnosť zohráva kľúčovú úlohu pri zabezpečovaní odolnosti systémov umelej inteligencie voči pokusom o zmenu ich použitia, správania, výkonnosti alebo o ohrozenie ich bezpečnostných vlastností tretími stranami, ktoré so škodlivým úmyslom zneužívajú zraniteľné miesta systému. Kybernetické útoky na systémy umelej inteligencie môžu využívať aktíva špecifické pre umelú inteligenciu, ako sú súbory trénovacích údajov (napr. otrávenie údajov) alebo trénované modely (napr. nepriateľské útoky), alebo zneužívať zraniteľné miesta digitálnych aktív systému umelej inteligencie alebo základnej infraštruktúry IKT. Na zabezpečenie úrovne kybernetickej bezpečnosti primeranej rizikám by preto poskytovatelia vysokorizikových systémov umelej inteligencie mali prijať vhodné opatrenia a náležite pritom zohľadniť základnú infraštruktúru IKT.
- (52) Ako súčasť harmonizačných právnych predpisov Únie by sa pravidlá uplatniteľné na uvádzanie vysokorizikových systémov umelej inteligencie na trh, do prevádzky a na ich používanie mali stanoviť v súlade s nariadením Európskeho parlamentu a Rady (ES) č. 765/2008<sup>51</sup>, ktorým sa stanovujú požiadavky akreditácie výrobkov a dohľadu nad trhom s nimi, rozhodnutím Európskeho parlamentu a Rady č. 768/2008/ES<sup>52</sup> o spoločnom rámci na uvádzanie výrobkov na trh a s nariadením Európskeho parlamentu a Rady (EÚ) 2019/1020<sup>53</sup> o dohľade nad trhom a súlade výrobkov („nový legislatívny rámec pre uvádzanie výrobkov na trh“).

---

<sup>51</sup> Nariadenie Európskeho parlamentu a Rady (ES) č. 765/2008 z 9. júla 2008, ktorým sa stanovujú požiadavky akreditácie a dohľadu nad trhom v súvislosti s uvádzaním výrobkov na trh a ktorým sa zrušuje nariadenie (EHS) č. 339/93 (Ú. v. EÚ L 218, 13.8.2008, s. 30).

<sup>52</sup> Rozhodnutie Európskeho parlamentu a Rady č. 768/2008/ES z 9. júla 2008 o spoločnom rámci na uvádzanie výrobkov na trh a o zrušení rozhodnutia 93/465/EHS (Ú. v. EÚ L 218, 13.8.2008, s. 82).

<sup>53</sup> Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/1020 z 20. júna 2019 o dohľade nad trhom a súlade výrobkov a o zmene smernice 2004/42/ES a nariadení (ES) č. 765/2008 a (EÚ) č. 305/2011 (Text s významom pre EHP) (Ú. v. EÚ L 169, 25.6.2019, s. 1 – 44).

- (53) Je vhodné, aby konkrétna fyzická alebo právnická osoba vymedzená ako poskytovateľ prevzala zodpovednosť za uvedenie vysokorizikového systému umelej inteligencie na trh alebo do prevádzky bez ohľadu na to, či je táto fyzická alebo právnická osoba osobou, ktorá systém skoncipovala alebo vyvinula.
- (54) Poskytovateľ by mal zaviesť spoľahlivý systém riadenia kvality, zabezpečiť dokončenie požadovaného postupu posudzovania zhody, vypracovať príslušnú dokumentáciu a vytvoriť spoľahlivý systém monitorovania po uvedení na trh. Orgány verejnej moci, ktoré uvádzajú do prevádzky vysokorizikové systémy umelej inteligencie pre vlastnú potrebu, môžu prijať a vykonávať pravidlá systému riadenia kvality ako súčasť systému riadenia kvality prijatého na vnútroštátnej prípadne regionálnej úrovni, pričom zohľadnia osobitosti odvetvia a právomoci a organizáciu príslušného orgánu verejnej moci.
- (55) Ak sa vysokorizikový systém umelej inteligencie, ktorý je bezpečnostným komponentom výrobku, na ktorý sa vzťahujú príslušné odvetvové právne predpisy nového legislatívneho rámca, neuvádza na trh ani do prevádzky nezávisle od daného výrobku, výrobca konečného výrobku, ako sa vymedzuje v príslušných právnych predpisoch nového legislatívneho rámca, by mal dodržiavať povinnosti poskytovateľa stanovené v tomto nariadení, a najmä zabezpečiť, aby systém umelej inteligencie zabudovaný do konečného výrobku spĺňal požiadavky tohto nariadenia.
- (56) S cieľom umožniť presadzovanie tohto nariadenia a vytvoriť rovnaké podmienky pre prevádzkovateľov je pri zohľadnení rôznych foriem sprístupňovania digitálnych produktov dôležité zabezpečiť, aby osoba usadená v Únii mohla za každých okolností poskytnúť orgánom všetky potrebné informácie o súlade systému umelej inteligencie. Preto ak nie je možné identifikovať dovozcu, poskytovateľa usadení mimo Únie vymenujú písomným splnomocnením pred sprístupnením svojich systémov umelej inteligencie na trhu Únie splnomocneného zástupcu usadeného v Únii.
- (57) V súlade so zásadami nového legislatívneho rámca by sa mali stanoviť osobitné povinnosti pre príslušné hospodárske subjekty, ako sú dovozcovia a distribútori, s cieľom zabezpečiť právnu istotu a uľahčiť dodržiavanie regulačných požiadaviek zo strany týchto príslušných hospodárskych subjektov.
- (58) Vzhľadom na povahu systémov umelej inteligencie a riziká pre bezpečnosť a základné práva, ktoré môžu súvisieť s ich používaním, a to aj pokiaľ ide o potrebu zabezpečiť riadne monitorovanie výkonnosti systému umelej inteligencie v reálnom prostredí, je vhodné stanoviť osobitné povinnosti používateľov. Používatelia by hlavne mali používať vysokorizikové systémy umelej inteligencie v súlade s návodom na použitie a mali by sa stanoviť určité ďalšie povinnosti, pokiaľ ide o monitorovanie fungovania systémov umelej inteligencie a prípadne aj uchovávanie záznamov.
- (59) Je vhodné predpokladať, že používateľom systému umelej inteligencie by mala byť fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, pod ktorého právomocou sa systém umelej inteligencie prevádzkuje, s výnimkou prípadov, keď sa používa v rámci osobnej neprofesionálnej činnosti.
- (60) Vzhľadom na zložitosť hodnotového reťazca umelej inteligencie by príslušné tretie strany, najmä tie, ktoré sú zapojené do predaja a dodávania softvéru, softvérových nástrojov a komponentov, vopred trénovaných modelov a údajov, alebo poskytovateľa sieťových služieb mali podľa potreby spolupracovať s poskytovateľmi a používateľmi s cieľom umožniť im dodržiavanie povinností podľa tohto nariadenia a s príslušnými orgánmi zriadenými podľa tohto nariadenia.

- (61) Kľúčovú úlohu pri poskytovaní technických riešení poskytovateľom na zabezpečenie súladu s týmto nariadením by mala zohrávať normalizácia. Dodržiavanie harmonizovaných noriem vymedzených v nariadení Európskeho parlamentu a Rady (EÚ) č. 1025/2012<sup>54</sup> by malo byť pre poskytovateľov prostriedkom na preukázanie zhody s požiadavkami tohto nariadenia. Komisia by však mohla prijať spoločné technické špecifikácie v oblastiach, v ktorých harmonizované normy neexistujú alebo nie sú dostatočné.
- (62) Na zabezpečenie vysokej úrovne dôveryhodnosti vysokorizikových systémov umelej inteligencie by tieto systémy mali pred svojím uvedením na trh alebo do prevádzky podliehať posudzovaniu zhody.
- (63) S cieľom minimalizovať zaťaženie prevádzkovateľov a predchádzať prípadnej duplicitě je vhodné, aby sa v prípade vysokorizikových systémov umelej inteligencie súvisiacich s výrobkami, na ktoré sa vzťahujú existujúce harmonizačné právne predpisy Únie na základe prístupu nového legislatívneho rámca, posudzoval súlad týchto systémov umelej inteligencie s požiadavkami tohto nariadenia v rámci posudzovania zhody, ktoré sa už upravuje na základe uvedených právnych predpisov. Uplatniteľnosť požiadaviek tohto nariadenia by preto nemala mať vplyv na konkrétnu logiku, metodiku ani všeobecnú štruktúru posudzovania zhody podľa príslušných osobitných právnych predpisov nového legislatívneho rámca. Tento prístup sa plne odráža v súhre tohto nariadenia s [nariadením o strojových zariadeniach]. Zatiaľ čo požiadavky tohto nariadenia sa zaoberajú bezpečnostnými rizikami systémov umelej inteligencie, ktoré zaisťujú bezpečnostné funkcie v strojových zariadeniach, [nariadenie o strojových zariadeniach] obsahuje určité osobitné požiadavky, ktorými sa zaručí bezpečné zakomponovanie systémov umelej inteligencie do celého strojového zariadenia tak, aby nebola ohrozená bezpečnosť strojového zariadenia ako celku. V [nariadení o strojových zariadeniach] sa uplatňuje rovnaké vymedzenie pojmu systému umelej inteligencie ako v tomto nariadení.
- (64) Vzhľadom na rozsiahlejšie skúsenosti profesionálnych certifikačných subjektov pred uvedením na trh v oblasti bezpečnosti výrobkov a na rozličnú povahu súvisiacich rizík je vhodné aspoň v počiatočnej fáze uplatňovania tohto nariadenia obmedziť rozsah uplatňovania posudzovania zhody treťou stranou v prípade vysokorizikových systémov umelej inteligencie iných ako tých, ktoré sa týkajú výrobkov. Posudzovanie zhody takýchto systémov by mal preto spravidla vykonávať poskytovateľ na vlastnú zodpovednosť s jedinou výnimkou, ktorú tvoria systémy umelej inteligencie určené na používanie na diaľkovú biometrickú identifikáciu osôb, v prípade ktorých by sa malo predpokladať zapojenie notifikovanej osoby do posudzovania zhody, pokiaľ tieto systémy nie sú zakázané.
- (65) S cieľom vykonávať posudzovanie zhody treťou stranou v prípade systémov umelej inteligencie, ktoré sa majú používať na diaľkovú biometrickú identifikáciu osôb, by podľa tohto nariadenia mali byť notifikované osoby určené príslušnými vnútroštátnymi orgánmi za predpokladu, že spĺňajú súbor požiadaviek, najmä pokiaľ ide o nezávislosť, spôsobilosť a neexistenciu konfliktu záujmov.

---

<sup>54</sup> Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1025/2012 z 25. októbra 2012 o európskej normalizácii, ktorým sa menia a dopĺňajú smernice Rady 89/686/EHS a 93/15/EHS a smernice Európskeho parlamentu a Rady 94/9/ES, 94/25/ES, 95/16/ES, 97/23/ES, 98/34/ES, 2004/22/ES, 2007/23/ES, 2009/23/ES a 2009/105/ES a ktorým sa zrušuje rozhodnutie Rady 87/95/EHS a rozhodnutie Európskeho parlamentu a Rady č. 1673/2006/ES (Ú. v. EÚ L 316, 14.11.2012, s. 12).

- (66) V súlade so všeobecne zaužívaným pojmom podstatnej zmeny pre výrobky regulované harmonizačnými právnymi predpismi Únie je vhodné, aby sa systém umelej inteligencie podrobil novému posudzovaniu zhody vždy, keď nastane zmena, ktorá môže ovplyvniť súlad systému s týmto nariadením, alebo keď sa zmení zamýšľaný účel systému. Okrem toho, pokiaľ ide o systémy umelej inteligencie, ktoré sa po uvedení na trh alebo do prevádzky ďalej učia (t. j. automaticky prispôbujú spôsob vykonávania funkcií), je potrebné vypracovať pravidlá, ktorými sa stanoví, že zmeny algoritmu a jeho výkonnosti, ktoré vopred stanovil poskytovateľ a ktoré boli posúdené v čase posudzovania zhody, by nemali predstavovať podstatnú zmenu.
- (67) Vysokorizikové systémy umelej inteligencie by mali niesť označenie CE, ktoré by preukazovalo ich súlad s týmto nariadením, aby im bol umožnený voľný pohyb v rámci vnútorného trhu. Členské štáty by nemali vytvárať neodôvodnené prekážky uvedeniu na trh ani do prevádzky v prípade vysokorizikových systémov umelej inteligencie, ktoré spĺňajú požiadavky stanovené v tomto nariadení a majú označenie CE.
- (68) Rýchla dostupnosť inovačných technológií môže mať za určitých podmienok zásadný význam pre zdravie a bezpečnosť osôb a pre spoločnosť ako celok. Je preto vhodné, aby členské štáty mohli z výnimočných dôvodov verejnej bezpečnosti alebo ochrany života a zdravia fyzických osôb a ochrany priemyselného a obchodného vlastníctva povoliť uvedenie na trh alebo do prevádzky v prípade systémov umelej inteligencie, ktoré neboli podrobené posudzovaniu zhody.
- (69) S cieľom uľahčiť prácu Komisie a členských štátov v oblasti umelej inteligencie, ako aj zvýšiť transparentnosť voči verejnosti by sa od poskytovateľov vysokorizikových systémov umelej inteligencie, ktoré nesúvisia s výrobkami patriacimi do rozsahu pôsobnosti príslušných existujúcich harmonizačných právnych predpisov Únie, malo vyžadovať, aby svoje vysokorizikové systémy umelej inteligencie zaregistrovali v databáze EÚ, ktorú má zriadiť a spravovať Komisia. Prevádzkovateľom uvedenej databázy by v súlade s nariadením Európskeho parlamentu a Rady (EÚ) 2018/1725<sup>55</sup> mala byť Komisia. Aby sa zaistila plná funkčnosť tejto databázy pri jej zavedení, by postup pri vytváraní databázy mal zahŕňať funkčné špecifikácie vypracované Komisiou a nezávislú audítorskú správu.
- (70) Určité systémy umelej inteligencie určené na interakciu s fyzickými osobami alebo generovanie obsahu môžu predstavovať osobitné riziko podvodu predstieraním identity alebo podvodného konania bez ohľadu na to, či sú klasifikované ako vysokorizikové alebo nie. Preto by používanie týchto systémov malo za určitých okolností podliehať osobitným povinnostiam transparentnosti bez toho, aby boli dotknuté požiadavky a povinnosti týkajúce sa vysokorizikových systémov umelej inteligencie. Predovšetkým by fyzické osoby mali byť informované o tom, že komunikujú so systémom umelej inteligencie, pokiaľ to nie je zrejmé z okolností a kontextu používania. Okrem toho by fyzické osoby mali byť informované, keď sú vystavené systému na rozpoznávanie emócií alebo systému biometrickej kategorizácie. Takéto informácie a oznámenia by sa mali poskytovať vo formátoch prístupných pre osoby so zdravotným postihnutím. Používatelia, ktorí používajú systém umelej inteligencie na vytváranie obrazového, zvukového alebo video obsahu alebo na

<sup>55</sup>

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

manipuláciu s ním a tento obsah sa očividne podobá existujúcim osobám, miestam alebo udalostiam a nepravdivo na človeka pôsobí ako autentický obsah, by mali zverejniť, že tento obsah bol umelo vytvorený alebo zmanipulovaný, tak, že výstup umelej inteligencie zodpovedajúcim spôsobom označia a zverejnia jeho umelý pôvod.

- (71) Umelá inteligencia je rýchlo sa rozvíjajúca skupina technológií, ktorá si vyžaduje nové formy regulačného dohľadu a bezpečný priestor na experimentovanie, pričom sa musí zabezpečiť, aby inovácia bola zodpovedná a aby boli integrované primerané záruky a opatrenia na zmiernenie rizika. Na zabezpečenie právneho rámca, ktorý bude priaznivý pre inovácie, nadčasový a odolný voči narušeniu, by bolo potrebné podporiť príslušné vnútroštátne orgány jedného alebo viacerých členských štátov, aby zriadili experimentálne regulačné prostredia pre umelú inteligenciu s cieľom uľahčiť vývoj a testovanie inovačných systémov umelej inteligencie pod prísny regulačným dohľadom skôr, než sa tieto systémy uvedú na trh alebo inak uvedú do prevádzky.
- (72) Cieľmi experimentálnych regulačných prostredí by mala byť podpora inovácií v oblasti umelej inteligencie vytvorením kontrolovaného experimentálneho a testovacieho prostredia vo fáze vývoja a pred uvedením na trh, aby sa zabezpečil súlad inovačných systémov umelej inteligencie s týmto nariadením a inými príslušnými právnymi predpismi Únie a členských štátov, posilnenie právnej istoty inovátorov, dohľadu príslušných orgánov a porozumenia príležitostiam, vznikajúcim rizikám a vplyvom používania umelej inteligencie, ako aj urýchlenie prístupu na trhy, a to aj odstránením prekážok pre malé a stredné podniky (MSP) a startupy. S cieľom zabezpečiť jednotné vykonávanie v celej Únii a úspory z rozsahu je vhodné stanoviť spoločné pravidlá pre zavádzanie experimentálnych regulačných prostredí a rámec pre spoluprácu medzi príslušnými orgánmi zapojenými do dohľadu nad experimentálnymi prostrediami. Toto nariadenie by malo poskytnúť právny základ pre používanie osobných údajov zozbieraných na iné účely na vývoj určitých systémov umelej inteligencie vo verejnom záujme v rámci experimentálneho regulačného prostredia pre umelú inteligenciu v súlade s článkom 6 ods. 4 nariadenia (EÚ) 2016/679 a článkom 6 nariadenia (EÚ) 2018/1725 a bez toho, aby bol dotknutý článok 4 ods. 2 smernice (EÚ) 2016/680. Účastníci experimentálneho prostredia by mali zabezpečiť primerané záruky a spolupracovať s príslušnými orgánmi, a to aj tým, že budú postupovať podľa ich usmernení a konať promptne a v dobrej viere s cieľom zmierniť akékoľvek vysoké riziko pre bezpečnosť a základné práva, ktoré môže vzniknúť počas vývoja a experimentovania v experimentálnom prostredí. Pri rozhodovaní o uložení správnej pokuty podľa článku 83 ods. 2 nariadenia 2016/679 a článku 57 smernice 2016/680 by sa malo zohľadniť správanie účastníkov v experimentálnom prostredí.
- (73) V záujme podpory a ochrany inovácií je dôležité, aby sa osobitne prihliadalo na záujmy malých poskytovateľov a používateľov systémov umelej inteligencie. Na tento účel by členské štáty mali vyvíjať iniciatívy zamerané na týchto prevádzkovateľov vrátane zvyšovania informovanosti a informačnej komunikácie. Aj notifikované osoby zohľadnia pri stanovovaní poplatkov za posudzovanie zhody osobitné záujmy a potreby malých poskytovateľov. Značné náklady pre poskytovateľov a iných, najmä menších prevádzkovateľov môžu predstavovať náklady na preklady súvisiace s povinnou dokumentáciou a komunikáciou s orgánmi. Členské štáty by mali podľa možnosti zabezpečiť, aby jedným z jazykov, ktoré určili a akceptovali na účely dokumentácie príslušných poskytovateľov a komunikácie s prevádzkovateľmi, bol jazyk, ktorému vo všeobecnosti rozumie čo najväčší počet cezhraničných používateľov.



- (74) S cieľom minimalizovať riziká spojené s vykonávaním vyplývajúce z nedostatku poznatkov a odborných znalostí na trhu, ako aj uľahčiť poskytovateľom a notifikovaným osobám plnenie ich povinností podľa tohto nariadenia by k vykonávaniu tohto nariadenia mali podľa možnosti prispievať platforma umelej inteligencie na požiadanie, európske centrá digitálnych inovácií a testovacie a experimentačné zariadenia zriadené Komisiou a členskými štátmi na vnútroštátnej úrovni alebo na úrovni EÚ. V rámci svojho príslušného poslania a oblastí pôsobnosti môžu poskytovať najmä technickú a vedeckú podporu poskytovateľom a notifikovaným osobám.
- (75) Je vhodné, aby Komisia v čo najväčšej možnej miere uľahčila prístup k testovacím a experimentačným zariadeniam orgánom, skupinám alebo laboratóriám zriadeným alebo akreditovaným podľa akýchkoľvek príslušných harmonizačných právnych predpisov Únie, ktoré plnia úlohy v súvislosti s posudzovaním zhody výrobkov alebo zariadení, na ktoré sa uvedené harmonizačné právne predpisy Únie vzťahujú. Týka sa to najmä panelov odborníkov, odborných laboratórií a referenčných laboratórií v oblasti zdravotníckych pomôcok podľa nariadenia (EÚ) 2017/745 a nariadenia (EÚ) 2017/746.
- (76) Na uľahčenie bezproblémového, účinného a harmonizovaného vykonávania tohto nariadenia by sa mala zriadiť Európska rada pre umelú inteligenciu. Táto rada by mala byť zodpovedná za niekoľko poradných úloh vrátane vydávania stanovísk, odporúčaní, poradenstva alebo usmernení v záležitostiach týkajúcich sa vykonávania tohto nariadenia vrátane technických špecifikácií alebo existujúcich noriem týkajúcich sa požiadaviek stanovených v tomto nariadení a poskytovania poradenstva a pomoci Komisii v konkrétnych otázkach súvisiacich s umelou inteligenciou.
- (77) Pri uplatňovaní a presadzovaní tohto nariadenia zohrávajú kľúčovú úlohu členské štáty. V tejto súvislosti by mal na účely dohľadu nad uplatňovaním a vykonávaním tohto nariadenia každý členský štát určiť jeden alebo viac príslušných vnútroštátnych orgánov. Aby sa zvýšila efektívnosť organizácie zo strany členských štátov a vytvorilo oficiálne kontaktné miesto vo vzťahu k verejnosti a iným partnerom na úrovni členských štátov a Únie, by sa mal v každom členskom štáte určiť jeden vnútroštátny orgán ako vnútroštátny dozorný orgán.
- (78) Všetci poskytovatelia vysokorizikových systémov umelej inteligencie by mali mať zavedený systém monitorovania po uvedení na trh, aby zabezpečili, že budú schopní zohľadniť skúsenosti s používaním vysokorizikových systémov umelej inteligencie na zlepšenie svojich systémov a procesu koncipovania a vývoja, alebo aby mohli včas prijať akékoľvek možné nápravné opatrenia. Tento systém je takisto kľúčový na zabezpečenie toho, aby sa možné riziká vyplývajúce zo systémov umelej inteligencie, ktoré sa po uvedení na trh alebo do prevádzky ďalej učia, mohli účinnejšie a včas riešiť. V tejto súvislosti by sa od poskytovateľov malo vyžadovať, aby mali zavedený systém, prostredníctvom ktorého by príslušným orgánom nahlasovali všetky závažné incidenty alebo porušenia vnútroštátnych právnych predpisov a právnych predpisov Únie na ochranu základných práv vyplývajúce z používania ich systémov umelej inteligencie.
- (79) S cieľom zabezpečiť primerané a účinné presadzovanie požiadaviek a povinností stanovených v tomto nariadení, ktoré predstavuje harmonizačné právne predpisy Únie, by sa mal v celom rozsahu uplatňovať systém dohľadu nad trhom a súladu výrobkov stanovený nariadením (EÚ) 2019/1020. Vnútroštátne orgány verejnej moci alebo subjekty, ktoré dohliadajú na uplatňovanie práva Únie na ochranu základných práv,

vrátane orgánov pre otázky rovnosti, by mali mať prístup, pokiaľ je to pre ich mandát nutné, aj k všetkej dokumentácii vytvorenej podľa tohto nariadenia.

- (80) Právne predpisy Únie o finančných službách zahŕňajú pravidlá a požiadavky vnútornej správy a riadenia rizík, ktoré sa vzťahujú na regulované finančné inštitúcie počas poskytovania týchto služieb vrátane prípadov, keď využívajú systémy umelej inteligencie. S cieľom zabezpečiť jednotné uplatňovanie a presadzovanie povinností podľa tohto nariadenia a príslušných pravidiel a požiadaviek právnych predpisov Únie v oblasti finančných služieb by mali byť orgány zodpovedné za dohľad nad právnymi predpismi v oblasti finančných služieb a za ich presadzovanie, prípadne vrátane Európskej centrálnej banky, určené za príslušné orgány na účely dohľadu nad vykonávaním tohto nariadenia vrátane činností dohľadu nad trhom, pokiaľ ide o systémy umelej inteligencie, ktoré poskytujú alebo používajú regulované finančné inštitúcie a finančné inštitúcie podliehajúce dohľadu. Na účely ďalšieho posilnenia súladu medzi týmto nariadením a pravidlami, ktoré sa vzťahujú na úverové inštitúcie regulované podľa smernice Európskeho parlamentu a Rady 2013/36/EÚ<sup>56</sup>, je takisto vhodné začleniť postup posudzovania zhody a niektoré procesné povinnosti poskytovateľov v súvislosti s riadením rizík, monitorovaním po uvedení na trh a dokumentáciou do existujúcich povinností a postupov na základe smernice 2013/36/EÚ. Na zabránenie prekryvaniu by sa mali zväžiť aj obmedzené výnimky v súvislosti so systémom riadenia kvality poskytovateľov a s povinnosťou monitorovania uloženou používateľom vysokorizikových systémov umelej inteligencie, pokiaľ sa vzťahujú na úverové inštitúcie regulované smernicou 2013/36/EÚ.
- (81) Vývoj systémov umelej inteligencie iných ako vysokorizikových systémov umelej inteligencie v súlade s požiadavkami tohto nariadenia môže viesť k rozsiahlejšiemu využívaniu dôveryhodnej umelej inteligencie v Únii. Poskytovatelia systémov umelej inteligencie, ktoré nepredstavujú vysoké riziko, by sa mali nabádať k tomu, aby vytvárali kódexy správania určené na podporu dobrovoľného uplatňovania povinných požiadaviek uplatniteľných na vysokorizikové systémy umelej inteligencie. Ďalej by mali byť poskytovatelia povzbudzovaní k tomu, aby dobrovoľne uplatňovali ďalšie požiadavky týkajúce sa napríklad environmentálnej udržateľnosti, prístupnosti pre osoby so zdravotným postihnutím, účasti zainteresovaných strán na koncipovaní a vývoji systémov umelej inteligencie a rozmanitosti vývojových tímov. Komisia môže vypracovať iniciatívy, a to aj odvetvovej povahy, na uľahčenie odstraňovania technických prekážok, ktoré bránia cezhraničnej výmene údajov na účely rozvoja umelej inteligencie, a to aj v oblasti infraštruktúry prístupu k údajom, sémantickej a technickej interoperability rôznych typov údajov.
- (82) Je dôležité, aby systémy umelej inteligencie týkajúce sa výrobkov, ktoré nie sú vysokorizikové v súlade s týmto nariadením, a preto sa od nich nevyžaduje, aby spĺňali požiadavky stanovené v tomto nariadení, však boli pri uvádzaní na trh alebo do prevádzky bezpečné. S cieľom prispieť k dosiahnutiu tohto cieľa by sa ako bezpečnostná sieť uplatňovala smernica Európskeho parlamentu a Rady 2001/95/ES<sup>57</sup>.

<sup>56</sup> Smernica Európskeho parlamentu a Rady 2013/36/EÚ z 26. júna 2013 o prístupe k činnosti úverových inštitúcií a prudenciálnom dohľade nad úverovými inštitúciami a investičnými spoločnosťami, o zmene smernice 2002/87/ES a o zrušení smerníc 2006/48/ES a 2006/49/ES (Ú. v. EÚ L 176, 27.6.2013, s. 338).

<sup>57</sup> Smernica Európskeho parlamentu a Rady 2001/95/ES z 3. decembra 2001 o všeobecnej bezpečnosti výrobkov (Ú. v. ES L 11, 15.1.2002, s. 4).

- (83) Na zabezpečenie dôveryhodnej a konštruktívnej spolupráce príslušných orgánov na úrovni Únie a na vnútroštátnej úrovni by mali všetky strany zapojené do uplatňovania tohto nariadenia rešpektovať dôvernosc informácií a údajov získaných pri plnení svojich úloh
- (84) Členské štáty by mali prijať všetky opatrenia potrebné na zabezpečenie vykonávania ustanovení tohto nariadenia vrátane stanovenia účinných, primeraných a odrádzajúcich sankcií za ich porušenie. V prípade určitých konkrétnych porušení by členské štáty mali zohľadniť rozpätia a kritériá stanovené v tomto nariadení. Európsky dozorný úradník pre ochranu údajov by mal mať právomoc ukladať správne pokuty inštitúciám, agentúram a orgánom Únie, ktoré patria do rozsahu pôsobnosti tohto nariadenia.
- (85) S cieľom zabezpečiť, aby sa regulačný rámec mohol v prípade potreby upraviť, by sa mala na Komisiu delegovať právomoc prijímať akty v súlade s článkom 290 ZFEÚ na účely zmeny techník a prístupov na vymedzenie systémov umelej inteligencie uvedených v prílohe I, harmonizačných právnych predpisov Únie uvedených v prílohe II, vysokorizikových systémov umelej inteligencie uvedených v prílohe III, ustanovení týkajúcich sa technickej dokumentácie uvedených v prílohe IV, obsahu EÚ vyhlásenia o zhode v prílohe V, ustanovení týkajúcich sa postupov posudzovania zhody v prílohách VI a VII a ustanovení, ktorými sa stanovujú systémy umelej inteligencie, na ktoré by sa mal vzťahovať postup posudzovania zhody založený na posúdení systému riadenia kvality a posúdení technickej dokumentácie. Je osobitne dôležité, aby Komisia počas prípravných prác uskutočnila príslušné konzultácie, a to aj na úrovni odborníkov, a aby tieto konzultácie vykonávala v súlade so zásadami stanovenými v Medziinštitucionálnej dohode z 13. apríla 2016 o lepšej tvorbe práva<sup>58</sup>. Predovšetkým, v záujme rovnakého zastúpenia pri príprave delegovaných aktov, sa všetky dokumenty doručujú Európskemu parlamentu a Rade v rovnakom čase ako odborníkom z členských štátov, a odborníci Európskeho parlamentu a Rady majú systematický prístup na zasadnutia skupín odborníkov Komisie, ktoré sa zaoberajú prípravou delegovaných aktov.
- (86) S cieľom zabezpečiť jednotné podmienky vykonávania tohto nariadenia by sa mali na Komisiu preniesť vykonávacie právomoci. Uvedené právomoci by sa mali vykonávať v súlade s nariadením Európskeho parlamentu a Rady (EÚ) č. 182/2011<sup>59</sup>.
- (87) Keďže cieľ tohto nariadenia nie je možné uspokojivo dosiahnuť na úrovni samotných členských štátov a z dôvodov rozsahu alebo dôsledkov činnosti ho možno lepšie dosiahnuť na úrovni Únie, môže Únia prijať opatrenia v súlade so zásadou subsidiarity podľa článku 5 ZEÚ. V súlade so zásadou proporcionality podľa uvedeného článku toto nariadenie neprekračuje rámec nevyhnutný na dosiahnutie tohto cieľa.
- (88) Toto nariadenie by sa malo uplatňovať od ... [*Úrad pre publikácie – vložiť dátum stanovený v článku 85*]. Infraštruktúra súvisiaca so správou a systémom posudzovania zhody by však mala byť funkčná pred uvedeným dátumom, preto by sa ustanovenia o notifikovaných osobách a riadiacej štruktúre mali uplatňovať od ... [*Úrad pre publikácie – vložiť dátum – tri mesiace po nadobudnutí účinnosti tohto nariadenia*]. Okrem toho by členské štáty mali stanoviť pravidlá týkajúce sa sankcií vrátane správnych pokút, oznámiť ich Komisii a zabezpečiť ich riadne a účinné vykonávanie

<sup>58</sup> Ú. v. EÚ L 123, 12.5.2016, s. 1.

<sup>59</sup> Nariadenie Európskeho parlamentu a Rady (EÚ) č. 182/2011 zo 16. februára 2011, ktorým sa ustanovujú pravidlá a všeobecné zásady mechanizmu, na základe ktorého členské štáty kontrolujú vykonávanie vykonávacích právomocí Komisie (Ú. v. EÚ L 55, 28.2.2011, s. 13).

do dátumu začatia uplatňovania tohto nariadenia. Ustanovenia o sankciách by sa preto mali uplatňovať od [Úrad pre publikácie – vložiť dátum – dvanásť mesiacov po nadobudnutí účinnosti tohto nariadenia].

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

PRIJALI TOTO NARIADENIE:

## HLAVA I

### VŠEOBECNÉ USTANOVENIA

#### Článok 1

##### *Predmet úpravy*

V tomto nariadení sa stanovujú:

- a) harmonizované pravidlá uvádzania na trh, uvádzania do prevádzky a používania systémov umelej inteligencie v Únii;
- b) zákaz určitých praktík v oblasti umelej inteligencie;
- c) osobitné požiadavky na vysokorizikové systémy umelej inteligencie a povinnosti prevádzkovateľov takýchto systémov;
- d) harmonizované pravidlá transparentnosti pre systémy umelej inteligencie určené na interakciu s fyzickými osobami, systémy na rozpoznávanie emócií a systémy biometrickej kategorizácie, ako aj pre systémy umelej inteligencie používané na vytváranie obrazového, zvukového obsahu alebo videoobsahu alebo na manipuláciu s takýmto obsahom;
- e) pravidlá monitorovania trhu a dohľadu nad ním.

#### Článok 2

##### *Rozsah pôsobnosti*

1. Toto nariadenie sa vzťahuje na:

- a) poskytovateľov uvádzajúcich v Únii na trh alebo do prevádzky systémy umelej inteligencie bez ohľadu na to, či sú títo poskytovatelia usadení v Únii alebo v tretej krajine;
- b) používateľov systémov umelej inteligencie, ktorí sa nachádzajú v Únii;
- c) poskytovateľov a používateľov systémov umelej inteligencie, ktorí sa nachádzajú v tretej krajine, ak sa výstup vytvorený systémom používa v Únii.

2. Len článok 84 tohto nariadenia sa uplatňuje na vysokorizikové systémy umelej inteligencie, ktoré sú bezpečnostnými komponentmi výrobkov alebo systémov, alebo ktoré sú samy výrobkami alebo systémami a patria do rozsahu pôsobnosti týchto aktov:

- a) nariadenie (ES) č. 300/2008;
- b) nariadenie (EÚ) č. 167/2013;
- c) nariadenie (EÚ) č. 168/2013;

- d) smernica 2014/90/EÚ;
  - e) smernica (EÚ) 2016/797;
  - f) nariadenie (EÚ) 2018/858;
  - g) nariadenie (EÚ) 2018/1139;
  - h) nariadenie (EÚ) 2019/2144.
3. Toto nariadenie sa neuplatňuje na systémy umelej inteligencie vyvinuté alebo používané výlučne na vojenské účely.
  4. Toto nariadenie sa neuplatňuje na orgány verejnej moci v tretej krajine ani na medzinárodné organizácie, ktoré podľa odseku 1 patria do rozsahu pôsobnosti tohto nariadenia, ak tieto orgány alebo organizácie používajú systémy umelej inteligencie v rámci medzinárodných dohôd o presadzovaní práva a justičnej spolupráci s Úniou alebo s jedným alebo viacerými členskými štátmi.
  5. Týmto nariadením nie je dotknuté uplatňovanie ustanovení o zodpovednosti sprostredkovateľov poskytovateľov služieb uvedených v kapitole II oddiele IV smernice Európskeho parlamentu a Rady 2000/31/ES<sup>60</sup> [nahrádza sa zodpovedajúcimi ustanoveniami aktu o digitálnych službách].

### Článok 3 Vymedzenie pojmov

Na účely tohto nariadenia sa uplatňuje toto vymedzenie pojmov:

1. „systém umelej inteligencie“ je softvér vyvinutý s jednou alebo viacerými technikami a prístupmi uvedenými v prílohe I, ktorý môže pre daný súbor cieľov vymedzených človekom vytvárať výstupy, ako je obsah, predpovede, odporúčania alebo rozhodnutia ovplyvňujúce prostredie, s ktorým sú v interakcii;
2. „poskytovateľ“ je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý vyvíja systém umelej inteligencie alebo ktorý má systém umelej inteligencie vyvinutý s cieľom uviesť ho na trh alebo do prevádzky pod vlastným menom alebo ochrannou známkou, či už za odplatu alebo bezodplatne;
3. „malý poskytovateľ“ je poskytovateľ, ktorý je mikropodnikom alebo malým podnikom v zmysle odporúčania Komisie 2003/361/ES<sup>61</sup>;
4. „používateľ“ je každá fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý používa systém umelej inteligencie v rámci svojej právomoci, s výnimkou prípadov, keď sa systém umelej inteligencie používa v rámci osobnej neprofesionálnej činnosti;
5. „splnomocnený zástupca“ je každá fyzická alebo právnická osoba usadená v Únii, ktorá od poskytovateľa systému umelej inteligencie dostala písomné splnomocnenie v jeho mene plniť povinnosti a vykonávať postupy stanovené týmto nariadením;

---

<sup>60</sup> Smernica Európskeho parlamentu a Rady 2000/31/ES z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode (smernica o elektronickom obchode) (Ú. v. ES L 178, 17.7.2000, s. 1).

<sup>61</sup> Odporúčanie Komisie zo 6. mája 2003 o vymedzení mikropodnikov, malých a stredných podnikov (Ú. v. EÚ L 124, 20.5.2003, s. 36).

6. „dovozca“ je každá fyzická alebo právnická osoba usadená v Únii, ktorá uvádza na trh alebo do prevádzky systém umelej inteligencie, ktorý je označený menom alebo ochrannou známkou fyzickej alebo právnickej osoby usadenej mimo Únie;
7. „distribútor“ je každá fyzická alebo právnická osoba v dodávateľskom reťazci okrem poskytovateľa alebo dovozcu, ktorá na trhu Únie sprístupňuje systém umelej inteligencie bez toho, aby ovplyvňovala jeho vlastnosti;
8. „prevádzkovateľ“ je poskytovateľ, používateľ, splnomocnený zástupca, dovozca a distribútor;
9. „uviedenie na trh“ je prvé sprístupnenie systému umelej inteligencie na trhu Únie;
10. „sprístupnenie na trhu“ je každá dodávka systému umelej inteligencie na účely distribúcie alebo používania na trhu Únie v rámci obchodnej činnosti, či už za odplatu, alebo bezodplatne;
11. „uviedenie do prevádzky“ je dodanie systému umelej inteligencie na prvé použitie priamo používateľovi alebo na vlastné použitie na trhu Únie na zamýšľaný účel;
12. „zamýšľaný účel“ je použitie systému umelej inteligencie, ktoré určil poskytovateľ, vrátane osobitného kontextu a podmienok používania, ako sa uvádza v informáciách od poskytovateľa v návode na použitie, v propagačných alebo predajných materiáloch a vyhláseniach, ako aj v technickej dokumentácii;
13. „logicky predvídateľné nesprávne použitie“ je také použitie systému umelej inteligencie, ktoré nie je v súlade so zamýšľaným účelom, ale ktoré môže byť výsledkom logicky predvídateľného ľudského správania alebo interakcie s inými systémami;
14. „bezpečnostný komponent výrobku alebo systému“ je komponent výrobku alebo systému, ktorý pre daný výrobok alebo systém plní bezpečnostnú funkciu alebo ktorého zlyhanie alebo porucha ohrozuje zdravie a bezpečnosť osôb alebo majetku;
15. „návod na použitie“ sú informácie, ktoré poskytuje poskytovateľ s cieľom informovať používateľa najmä o zamýšľanom účele a správnom používaní systému umelej inteligencie vrátane konkrétnych geografických, behaviorálnych alebo funkčných podmienok, v ktorých sa má vysokorizikový systém umelej inteligencie používať;
16. „stiahnutie systému umelej inteligencie od používateľa“ je každé opatrenie zamerané na to, aby sa systém umelej inteligencie sprístupnený používateľovi vrátil poskytovateľovi;
17. „stiahnutie systému umelej inteligencie z trhu“ je každé opatrenie, ktorého cieľom je zabrániť distribúcii, predvádzaniu a ponúkaniu systému umelej inteligencie;
18. „výkonnosť systému umelej inteligencie“ je schopnosť systému umelej inteligencie dosiahnuť zamýšľaný účel;
19. „notifikujúci orgán“ je vnútroštátny orgán zodpovedný za stanovenie a vykonávanie nevyhnutných postupov na posudzovanie, určovanie a notifikáciu orgánov posudzovania zhody a za ich monitorovanie;
20. „posudzovanie zhody“ je postup overovania, či boli splnené požiadavky stanovené v hlave III kapitole 2 tohto nariadenia týkajúce sa systému umelej inteligencie;
21. „orgán posudzovania zhody“ je orgán, ktorý ako tretia strana vykonáva činnosti posudzovania zhody vrátane skúšania, certifikácie a kontroly;

22. „notifikovaná osoba“ je orgán posudzovania zhody určený v súlade s týmto nariadením a inými relevantnými harmonizačnými právnymi predpismi Únie;
23. „podstatná zmena“ je zmena systému umelej inteligencie po jeho uvedení na trh alebo do prevádzky, ktorá ovplyvňuje súlad systému umelej inteligencie s požiadavkami stanovenými v hlave III kapitole 2 tohto nariadenia alebo vedie k zmene zamýšľaného účelu, na aký bol systém umelej inteligencie posudzovaný;
24. „označenie zhody CE“ (označenie CE) je označenie, ktorým poskytovateľ vyjadruje, že systém umelej inteligencie je v zhode s požiadavkami stanovenými v hlave III kapitole 2 tohto nariadenia a v iných uplatniteľných právnych predpisoch Únie, ktorými sa harmonizujú podmienky uvádzania výrobkov na trh (ďalej len „harmonizačné právne predpisy Únie“) a v ktorých sa stanovuje umiestňovanie tohto označenia;
25. „monitorovanie po uvedení na trh“ sú všetky činnosti, ktoré vykonávajú poskytovatelia systémov umelej inteligencie na proaktívne zhromažďovanie a skúmanie skúseností získaných z používania systémov umelej inteligencie, ktoré uvádzajú na trh alebo do prevádzky, a to na účely zisťovania akejkoľvek potreby okamžite uplatniť všetky potrebné nápravné či preventívne opatrenia;
26. „orgán dohľadu nad trhom“ je vnútroštátny orgán, ktorý vykonáva činnosti a prijíma opatrenia podľa nariadenia (EÚ) 2019/1020;
27. „harmonizovaná norma“ je európska norma podľa vymedzenia v článku 2 ods. 1 písm. c) nariadenia (EÚ) č. 1025/2012;
28. „spoločné špecifikácie“ sú dokument, ktorý nie je normou a ktorý obsahuje technické riešenia poskytujúce prostriedky na dosiahnutie súladu s určitými požiadavkami a povinnosťami stanovenými podľa tohto nariadenia;
29. „trénovacie údaje“ sú údaje, ktoré sa používajú na tréning systému umelej inteligencie adaptáciou jeho parametrov, ktoré sa dajú naučiť, vrátane váh neurónovej siete;
30. „validačné údaje“ sú údaje, ktoré sa používajú na vyhodnotenie natrénovaného systému umelej inteligencie a na doladenie jeho parametrov, ktoré sa nedajú naučiť, a jeho procesu učenia, okrem iného s cieľom zabrániť pretrénovaniu, pričom súbor validačných údajov môže byť samostatný súbor údajov alebo časť súboru tréningových údajov, a to buď v pevnom alebo variabilnom rozdelení;
31. „testovacie údaje“ sú údaje, ktoré sa používajú na nezávislé hodnotenie natrénovaného a zvalidovaného systému umelej inteligencie s cieľom potvrdiť očakávanú výkonnosť tohto systému pred jeho uvedením na trh alebo do prevádzky;
32. „vstupné údaje“ sú údaje poskytnuté systému umelej inteligencie alebo priamo získané týmto systémom, na základe ktorých systém vytvára výstup;
33. „biometrické údaje“ sú osobné údaje, ktoré sú výsledkom osobitného technického spracovania týkajúceho sa fyzických, fyziologických alebo behaviorálnych charakteristických znakov fyzickej osoby a ktoré umožňujú alebo potvrdzujú jedinečnú identifikáciu tejto fyzickej osoby, ako sú vyobrazenia tváre alebo daktyloskopické údaje;
34. „systém na rozpoznávanie emócií“ je systém umelej inteligencie na účely identifikácie alebo odvodenia emócií alebo úmyslov fyzických osôb na základe ich biometrických údajov;

35. „systém biometrickej kategorizácie“ je systém umelej inteligencie na účely zaradenia fyzických osôb do konkrétnych kategórií, ako je pohlavie, vek, farba vlasov, farba očí, tetovanie, etnický pôvod alebo sexuálna či politická orientácia, a to na základe ich biometrických údajov;
36. „systém diaľkovej biometrickej identifikácie“ je systém umelej inteligencie na účely identifikácie fyzických osôb na diaľku porovnávaním biometrických údajov osoby s biometrickými údajmi obsiahnutými v referenčnej databáze, a to bez toho, aby používateľ systému umelej inteligencie vopred vedel, či bude daná osoba prítomná a či ju možno identifikovať;
37. „systém diaľkovej biometrickej identifikácie v reálnom čase“ je systém diaľkovej biometrickej identifikácie, v ktorom zachytávanie biometrických údajov, ich porovnávanie a identifikácia prebiehajú bez výrazného oneskorenia. Aby sa zabránilo obchádzaniu pravidiel, patrí sem nielen okamžitá identifikácia, ale aj identifikácia s určitými menšími oneskoreniami;
38. „systém následnej diaľkovej biometrickej identifikácie“ je systém diaľkovej biometrickej identifikácie, ktorý nie je systémom diaľkovej biometrickej identifikácie v reálnom čase;
39. „verejne prístupný priestor“ je akékoľvek fyzické miesto prístupné verejnosti bez ohľadu na to, či sa pre prístup môžu uplatniť určité podmienky;
40. „orgán presadzovania práva“ je:
- a) každý orgán verejnej moci príslušný v oblasti predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania, alebo v oblasti výkonu trestných sankcií vrátane ochrany pred ohrozením verejnej bezpečnosti a predchádzania takémuto ohrozeniu alebo
  - b) každý iný orgán alebo subjekt, ktorý bol právom členského štátu poverený vykonávať verejnú moc a verejné právomoci na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií vrátane ochrany pred ohrozením verejnej bezpečnosti a predchádzania takémuto ohrozeniu;
41. „presadzovanie práva“ sú činnosti vykonávané orgánmi presadzovania práva na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania, alebo na účely výkonu trestných sankcií vrátane ochrany pred ohrozením verejnej bezpečnosti a predchádzania takémuto ohrozeniu;
42. „vnútroštátny dozorný orgán“ je orgán, na ktorý členský štát deleguje zodpovednosť za vykonávanie a uplatňovanie tohto nariadenia, za koordináciu činností zverených danému členskému štátu, za pôsobenie ako jednotné kontaktné miesto pre Komisiu a za zastupovanie členského štátu v Európskej rade pre umelú inteligenciu;
43. „príslušný vnútroštátny orgán“ je vnútroštátny dozorný orgán, notifikujúci orgán a orgán dohľadu nad trhom;
44. „závažný incident“ je každý incident, ktorý priamo alebo nepriamo vyústi, mohol vyústiť alebo môže vyústiť do:
- a) smrti osoby alebo vážneho poškodenia zdravia osoby, majetku alebo životného prostredia;
  - b) vážneho a nezvratného narušenia riadenia a prevádzky kritickej infraštruktúry.



*Článok 4*  
*Zmeny prílohy I*

Komisia je splnomocnená prijímať delegované akty v súlade s článkom 73 s cieľom zmeniť zoznam techník a prístupov uvedených v prílohe I, a tak aktualizovať tento zoznam podľa trhového a technologického vývoja na základe charakteristických vlastností, ktoré sú podobné technikám a prístupom uvedeným v tejto prílohe.

**HLAVA II**

**ZAKÁZANÉ PRAKTIKY V OBLASTI UMELEJ INTELIGENCIE**

*Článok 5*

1. Zakazujú sa tieto praktiky v oblasti umelej inteligencie:
  - a) uvádzanie na trh, uvádzanie do prevádzky alebo používanie systému umelej inteligencie, ktorý s cieľom podstatne narušiť správanie osoby využíva podprahové techniky mimo vedomia osoby tak, že tejto alebo inej osobe spôsobí alebo by mohol spôsobiť fyzickú alebo psychickú ujmu;
  - b) uvádzanie na trh, uvádzanie do prevádzky alebo používanie systému umelej inteligencie, ktorý s cieľom podstatne narušiť správanie osoby patriacej do konkrétnej skupiny osôb využíva ktorúkoľvek zo zraniteľností tejto skupiny osôb vyplývajúcich z ich veku, fyzického alebo duševného postihnutia tak, že tejto alebo inej osobe spôsobí alebo by mohol spôsobiť fyzickú alebo psychickú ujmu;
  - c) uvádzanie na trh, uvádzanie do prevádzky alebo používanie systémov umelej inteligencie orgánmi verejnej moci alebo v ich mene na účely hodnotenia alebo klasifikácie dôveryhodnosti fyzických osôb počas určitého obdobia na základe ich spoločenského správania alebo známych či predpokladaných osobných alebo osobnostných charakteristík, pričom takto získané sociálne skóre vedie k jednému alebo obidvom z týchto výsledkov:
    - i) škodlivé alebo nepriaznivé zaobchádzanie s určitými fyzickými osobami alebo celými skupinami fyzických osôb v sociálnych kontextoch, ktoré nesúvisia s kontextmi, v ktorých boli údaje pôvodne generované alebo zhromaždené;
    - ii) škodlivé alebo nepriaznivé zaobchádzanie s určitými fyzickými osobami alebo celými skupinami fyzických osôb, ktoré je neodôvodnené alebo neprimerané ich spoločenskému správaniu alebo jeho závažnosti;
  - d) používanie systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva, pokiaľ takéto použitie nie je nevyhnutné a v nutnej miere potrebné na jeden z týchto cieľov:
    - i) cielené pátranie po konkrétnych potenciálnych obetiach trestných činov vrátane nezvestných detí;
    - ii) predchádzanie konkrétnemu, závažnému a bezprostrednému ohrozeniu života alebo fyzickej bezpečnosti fyzických osôb alebo teroristickému útoku;

- iii) odhaľovanie, lokalizácia, identifikácia alebo stíhanie páchatel'a trestného činu uvedeného v článku 2 ods. 2 rámcového rozhodnutia Rady 2002/584/SVV<sup>62</sup>, za ktorý možno podľa právnych predpisov dotknutého členského štátu v tomto členskom štáte uložiť trest odňatia slobody alebo ochranné opatrenie s hornou hranicou trestnej sadzby najmenej tri roky, alebo osoby podozrivej zo spáchania takéhoto trestného činu.
2. Pri používaní systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva na dosiahnutie ktoréhokoľvek z cieľov uvedených v odseku 1 písm. d) sa musia zohľadniť tieto prvky:
- a) povaha situácie, ktorá viedla k možnému použitiu, najmä závažnosť, pravdepodobnosť a rozsah poškodenia spôsobeného v prípade nepoužitia systému;
  - b) dôsledky použitia systému pre práva a slobody všetkých dotknutých osôb, najmä závažnosť, pravdepodobnosť a rozsah týchto dôsledkov.

Používanie systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva na dosiahnutie ktoréhokoľvek z cieľov uvedených v odseku 1 písm. d) musí okrem toho byť v súlade s nevyhnutnými a primeranými zárukami a podmienkami týkajúcimi sa tohto používania, najmä pokiaľ ide o časové, geografické a osobné obmedzenia.

3. Pokiaľ ide o odsek 1 písm. d) a odsek 2, podlieha každé jednotlivé použitie systému diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva predchádzajúcemu povoleniu udelenému súdnym orgánom alebo nezávislým správny orgánom členského štátu, v ktorom sa má použitie uskutočniť, vydanému na základe odôvodnenej žiadosti a v súlade s podrobnými pravidlami vnútroštátneho práva uvedenými v odseku 4. V riadne odôvodnenej naliehavej situácii sa však použitie systému môže začať bez povolenia a o povolenie možno požiadať až počas používania alebo po ňom.

Príslušný súdny alebo správny orgán udelí povolenie len vtedy, ak sa na základe objektívnych dôkazov alebo jasných indícií, ktoré mu boli predložené, presvedčí, že použitie predmetného systému diaľkovej biometrickej identifikácie v reálnom čase je potrebné a primerané na dosiahnutie jedného z cieľov uvedených v odseku 1 písm. d), ako sa uvádza v žiadosti. Pri rozhodovaní o žiadosti príslušný súdny alebo správny orgán zohľadní prvky uvedené v odseku 2.

4. Členský štát sa môže rozhodnúť, že na účely presadzovania práva v rámci obmedzení a za podmienok uvedených v odseku 1 písm. d) a odsekoch 2 a 3 stanoví možnosť úplne alebo čiastočne povoliť používanie systému diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch. Tento členský štát vo svojom vnútroštátnom práve stanoví potrebné podrobné pravidlá na podávanie žiadostí o povolenia uvedené v odseku 3, ich vydávanie a výkon, ako aj pre dohľad nad nimi. V týchto pravidlách sa takisto uvedie, v súvislosti s ktorým z cieľov uvedených v odseku 1 písm. d) a s ktorým z trestných činov uvedených v jeho bode

---

<sup>62</sup> Rámcové rozhodnutie Rady 2002/584/SVV z 13. júna 2002 o európskom zatykači a postupoch odovzdávania osôb medzi členskými štátmi (Ú. v. ES L 190, 18.7.2002, s. 1).

iii) môžu byť príslušné orgány oprávnené používať tieto systémy na účely presadzovania práva.

## HLAVA III

### VYSOKORIZIKOVÉ SYSTÉMY UMELEJ INTELIGENCIE

#### KAPITOLA 1

### KLASIFIKÁCIA SYSTÉMOV UMELEJ INTELIGENCIE AKO VYSOKORIZIKOVÝCH SYSTÉMOV

#### Článok 6

##### *Pravidlá klasifikácie vysokorizikových systémov umelej inteligencie*

1. Bez ohľadu na to, či sa systém umelej inteligencie nezávisle od výrobkov uvedených v písmenách a) a b) uvádza na trh alebo do prevádzky, považuje sa za vysokorizikový, ak sú splnené obe tieto podmienky:
  - a) systém umelej inteligencie je určený na používanie ako bezpečnostný komponent výrobku, na ktorý sa vzťahujú harmonizačné právne predpisy Únie uvedené v prílohe II, alebo je sám osebe takýmto výrobkom;
  - b) výrobok, ktorého bezpečnostným komponentom je systém umelej inteligencie, alebo samotný systém umelej inteligencie ako výrobok sa musí podrobiť posúdeniu zhody treťou stranou s cieľom uviesť daný výrobok na trh alebo do prevádzky podľa harmonizačných právnych predpisov Únie uvedených v prílohe II.
2. Okrem vysokorizikových systémov umelej inteligencie uvedených v odseku 1 sa za vysokorizikové považujú aj systémy umelej inteligencie uvedené v prílohe III.

#### Článok 7

##### *Zmeny prílohy III*

1. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 73 s cieľom aktualizovať zoznam v prílohe III doplnením vysokorizikových systémov umelej inteligencie, ak sú splnené obe tieto podmienky:
  - a) systémy umelej inteligencie sú určené na používanie v ktorejkoľvek z oblastí uvedených v bodoch 1 až 8 prílohy III;
  - b) systémy umelej inteligencie predstavujú riziko poškodenia zdravia a bezpečnosti alebo riziko nepriaznivého vplyvu na základné práva, ktoré je vzhľadom na svoju závažnosť a pravdepodobnosť výskytu prinajmenšom rovnocenné riziku poškodenia alebo nepriaznivého vplyvu, ktoré predstavujú vysokorizikové systémy umelej inteligencie už uvedené v prílohe III.
2. Pri posudzovaní toho, či systém umelej inteligencie predstavuje na účely odseku 1 riziko poškodenia zdravia a bezpečnosti alebo riziko nepriaznivého vplyvu na základné práva, ktoré je prinajmenšom rovnocenné riziku poškodenia, ktoré predstavujú vysokorizikové systémy umelej inteligencie už uvedené v prílohe III, zohľadní Komisia tieto kritériá:

- a) zamýšľaný účel systému umelej inteligencie;
- b) rozsah, v akom sa systém umelej inteligencie používa alebo sa pravdepodobne bude používať;
- c) rozsah, v akom používanie systému umelej inteligencie už spôsobilo poškodenie zdravia a bezpečnosti alebo nepriaznivý vplyv na základné práva, alebo vyvolalo vážne obavy v súvislosti s naplnením takéhoto poškodenia alebo nepriaznivého vplyvu, preukázaný správami alebo zdokumentovanými tvrdeniami predloženými príslušným vnútroštátnym orgánom;
- d) potenciálny rozsah takéhoto poškodenia alebo nepriaznivého vplyvu, najmä pokiaľ ide o jeho intenzitu a schopnosť zasiahnuť značný počet osôb;
- e) rozsah, v akom sú potenciálne poškodené alebo nepriaznivo ovplyvnené osoby závislé od výsledku vytvoreného systémom umelej inteligencie, najmä preto, že z praktických alebo právnych dôvodov nie je odôvodnene možné sa na tomto výsledku nepodieľať;
- f) rozsah, v akom sú potenciálne poškodené alebo nepriaznivo ovplyvnené osoby vo vzťahu k používateľovi systému umelej inteligencie v zraniteľnom postavení, najmä v dôsledku nerovnováhy moci, znalostí, hospodárskych alebo sociálnych okolností alebo veku;
- g) rozsah, v akom sa výsledok vytvorený systémom umelej inteligencie dá ľahko zvrátiť, pričom výsledky, ktoré majú vplyv na zdravie alebo bezpečnosť osôb, sa nepovažujú za také, ktoré sa dajú ľahko zvrátiť;
- h) rozsah, v akom sa v existujúcich právnych predpisoch Únie stanovujú:
  - i) účinné nápravné opatrenia v súvislosti s rizikami, ktoré systém umelej inteligencie predstavuje, s výnimkou nárokov na náhradu škody;
  - ii) účinné opatrenia na predchádzanie týmto rizikám alebo ich podstatnú minimalizáciu.

## KAPITOLA 2

### POŽIADAVKY NA VYSOKORIZIKOVÉ SYSTÉMY UMELEJ INTELIGENCIE

#### *Článok 8*

#### *Súlad s požiadavkami*

1. Vysokorizikové systémy umelej inteligencie musia spĺňať požiadavky stanovené v tejto kapitole.
2. Pri zabezpečovaní súladu s týmito požiadavkami sa zohľadňuje zamýšľaný účel vysokorizikového systému umelej inteligencie a systém riadenia rizík uvedený v článku 9.

#### *Článok 9*

#### *Systém riadenia rizík*

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

2. Systém riadenia rizík sa chápe ako nepretržitý opakovaný proces počas celého životného cyklu vysokorizikového systému umelej inteligencie, ktorý si vyžaduje pravidelné systematické aktualizovanie. Zahŕňa tieto kroky:
  - a) identifikácia a analýza známych a predvídateľných rizík spojených s každým vysokorizikovým systémom umelej inteligencie;
  - b) odhad a hodnotenie rizík, ktoré môžu vzniknúť pri používaní vysokorizikového systému umelej inteligencie v súlade so zamýšľaným účelom a za podmienok logicky predvídateľného nesprávneho použitia;
  - c) hodnotenie ďalších možných vznikajúcich rizík na základe analýzy údajov získaných zo systému monitorovania po uvedení na trh uvedeného v článku 61;
  - d) prijatie vhodných opatrení na riadenie rizík v súlade s ustanoveniami nasledujúcich odsekov.
3. V opatreniach na riadenie rizík uvedených v odseku 2 písm. d) sa náležite zohľadnia účinky a možné interakcie vyplývajúce z kombinovaného uplatňovania požiadaviek stanovených v tejto kapitole 2. Zohľadní sa v nich všeobecne uznávaný stav techniky, a to aj v súlade s príslušnými harmonizovanými normami alebo spoločnými špecifikáciami.
4. Opatrenia na riadenie rizík uvedené v odseku 2 písm. d) musia byť také, aby sa zvyškové riziká spojené s jednotlivými nebezpečenstvami, ako aj celkové zvyškové riziko vysokorizikových systémov umelej inteligencie považovali za prijateľné za predpokladu, že vysokorizikový systém umelej inteligencie sa používa v súlade so zamýšľaným účelom alebo za podmienok logicky predvídateľného nesprávneho použitia. Tieto zvyškové riziká sa oznámia používateľovi.

Pri určovaní najvhodnejších opatrení na riadenie rizík sa zabezpečí:

- a) čo najrozsiahlejšie odstránenie alebo obmedzenie rizík prostredníctvom primeranej koncepcie a primeraného vývoja;
- b) prípadné zavedenie primeraných zmierňujúcich a kontrolných opatrení v súvislosti s rizikami, ktoré nemožno odstrániť;
- c) poskytovanie primeraných informácií podľa článku 13, najmä pokiaľ ide o riziká uvedené v odseku 2 písm. b) tohto článku, a prípadne odborná príprava pre používateľov.

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

5. Na účely určenia najvhodnejších opatrení na riadenie rizík sa vysokorizikové systémy umelej inteligencie testujú. Testovaním sa zabezpečí, aby vysokorizikové systémy umelej inteligencie konzistentne fungovali v súlade so zamýšľaným účelom a spĺňali požiadavky stanovené v tejto kapitole.
6. Postupy testovania musia byť vhodné na dosiahnutie zamýšľaného účelu systému umelej inteligencie a nemusia ísť nad rámec toho, čo je nevyhnutné na jeho dosiahnutie.
7. Testovanie vysokorizikových systémov umelej inteligencie sa vykonáva podľa potreby kedykoľvek počas celého procesu vývoja a v každom prípade pred uvedením

na trh alebo do prevádzky. Testovanie sa vykonáva na základe vopred vymedzených metrick a pravdepodobnostných prahových hodnôt, ktoré sú primerané zamýšľanému účelu vysokorizikového systému umelej inteligencie.

8. Pri zavádzaní systému riadenia rizík opísaného v odsekoch 1 až 7 sa osobitne zohľadní to, či je pravdepodobné, že k vysokorizikovým systémom umelej inteligencie budú mať prístup deti alebo že tieto systémy budú mať na deti vplyv.
9. V prípade úverových inštitúcií regulovaných smernicou 2013/36/EÚ, musia byť aspekty opísané v odsekoch 1 až 8 súčasťou postupov riadenia rizík stanovených týmito inštitúciami podľa článku 74 uvedenej smernice.

#### *Článok 10* *Údaje a správa údajov*

1. Vysokorizikové systémy umelej inteligencie, ktoré využívajú techniky zahŕňajúce tréovanie modelov s údajmi, sa musia vyvíjať na základe súborov tréovacích, validačných a testovacích údajov, ktoré spĺňajú kritériá kvality uvedené v odsekoch 2 až 5.
2. Pre súbory tréovacích, validačných a testovacích údajov musia platiť primerané postupy správy a riadenia údajov. Tieto postupy sa týkajú najmä:
  - a) príslušných rozhodnutí o koncepčných riešeniach;
  - b) zberu údajov;
  - c) príslušných operácií prípravy údajov, ako je anotácia, označovanie, čistenie, obohacovanie a agregácia;
  - d) formulovania relevantných predpokladov, najmä pokiaľ ide o informácie, ktoré majú údaje merať a reprezentovať;
  - e) predchádzajúceho posúdenia dostupnosti, množstva a vhodnosti potrebných súborov údajov;
  - f) preskúmania z hľadiska možných skreslení;
  - g) identifikácie prípadných medzier alebo nedostatkov v údajoch a spôsobu, akým možno tieto medzery a nedostatky odstrániť.
3. Súbory tréovacích, validačných a testovacích údajov musia byť relevantné, reprezentatívne, bezchybné a úplné. Musia mať primerané štatistické vlastnosti, a to prípadne aj pokiaľ ide o osoby alebo skupiny osôb, v prípade ktorých sa má vysokorizikový systém umelej inteligencie používať. Tieto charakteristiky súborov údajov sa môžu splniť na úrovni jednotlivých súborov údajov alebo ich kombinácie.
4. Súbory tréovacích, validačných a testovacích údajov musia, pokiaľ si to vyžaduje zamýšľaný účel, zohľadňovať vlastnosti alebo prvky, ktoré sú špecifické pre konkrétne geografické, behaviorálne alebo funkčné podmienky, v ktorých sa má vysokorizikový systém umelej inteligencie používať.
5. Pokiaľ je to nevyhnutne potrebné na účely zabezpečenia monitorovania, odhaľovania a nápravy skreslenia v súvislosti s vysokorizikovými systémami umelej inteligencie, poskytovatelia takýchto systémov môžu spracúvať osobitné kategórie osobných údajov uvedené v článku 9 ods. 1 nariadenia (EÚ) 2016/679, článku 10 smernice (EÚ) 2016/680 a článku 10 ods. 1 nariadenia (EÚ) 2018/1725, a to pod podmienkou primeraných záruk pre základné práva a slobody fyzických osôb, ku ktorým patria aj

technické obmedzenia opätovného použitia a používanie najmodernejších opatrení v oblasti bezpečnosti a ochrany súkromia, ako je pseudonymizácia alebo šifrovanie v prípadoch, v ktorých anonymizácia môže významne ovplyvniť sledovaný účel.

6. Pri vývoji vysokorizikových systémov umelej inteligencie, pri ktorých sa nevyužívajú techniky zahŕňajúce trénovanie modelov, sa musia uplatňovať vhodné postupy správy a riadenia údajov s cieľom zabezpečiť, aby tieto vysokorizikové systémy umelej inteligencie boli v súlade s odsekom 2.

### *Článok 11*

#### *Technická dokumentácia*

1. Pred uvedením vysokorizikového systému umelej inteligencie na trh alebo do prevádzky sa vypracuje technická dokumentácia tohto systému, ktorá sa aktualizuje.  
Technická dokumentácia sa vypracuje tak, aby sa v nej preukazovalo, že vysokorizikový systém umelej inteligencie spĺňa požiadavky stanovené v tejto kapitole, a aby sa príslušným vnútroštátnym orgánom a notifikovaným osobám poskytli všetky informácie potrebné na posúdenie súladu systému umelej inteligencie s uvedenými požiadavkami. Musí obsahovať aspoň prvky stanovené v prílohe IV.
2. Ak sa na trh alebo do prevádzky uvádza vysokorizikový systém umelej inteligencie súvisiaci s výrobkom, na ktorý sa vzťahujú právne akty uvedené v oddiele A prílohy II, vypracuje sa jediná technická dokumentácia obsahujúca všetky informácie stanovené v prílohe IV, ako aj informácie požadované podľa uvedených právnych aktov.
3. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 73 s cieľom zmeniť prílohu IV, ak je to potrebné na zabezpečenie toho, aby technická dokumentácia vzhľadom na technický pokrok poskytovala všetky informácie potrebné na posúdenie súladu systému s požiadavkami stanovenými v tejto kapitole.

### *Článok 12*

#### *Vedenie záznamov*

1. Vysokorizikové systémy umelej inteligencie musia byť koncipované a vyvinuté tak, aby boli počas svojej prevádzky schopné automaticky zaznamenávať udalosti („logy“). Tieto schopnosti logovania musia byť v súlade s uznávanými normami alebo spoločnými špecifikáciami.
2. Schopnosťami logovania sa počas celého životného cyklu systému umelej inteligencie zabezpečí úroveň vysledovateľnosti jeho fungovania, ktorá je primeraná zamýšľanému účelu systému.
3. Schopnosti logovania musia predovšetkým umožňovať monitorovanie prevádzky vysokorizikového systému umelej inteligencie, pokiaľ ide o výskyt situácií, ktoré môžu viesť k tomu, že systém umelej inteligencie bude predstavovať riziko v zmysle článku 65 ods. 1, alebo môžu spôsobiť podstatnú zmenu, a uľahčovať monitorovanie po uvedení na trh podľa článku 61.
4. V prípade vysokorizikových systémov umelej inteligencie uvedených v odseku 1 písm. a) prílohy III sa v rámci logovania musí dať zabezpečiť aspoň:
  - a) záznam každého časového úseku používania systému (dátum a čas začiatku a dátum a čas ukončenia každého použitia);

- b) referenčná databáza, na základe ktorej systém skontroloval vstupné údaje;
- c) vstupné údaje, pri ktorých vyhľadávanie viedlo k zhode;
- d) identifikácia fyzických osôb zapojených podľa článku 14 ods. 5 do overovania výsledkov.

### Článok 13

#### *Transparentnosť a poskytovanie informácií používateľom*

1. Vysokorizikové systémy umelej inteligencie musia byť koncipované a vyvinuté tak, aby sa zabezpečilo, že ich prevádzka je dostatočne transparentná na to, aby používateľom umožnila interpretovať výstupy systému a vhodne ich používať. Musí sa zabezpečiť primeraný druh a stupeň transparentnosti, aby používatelia a poskytovatelia mohli dodržiavať príslušné povinnosti stanovené v kapitole 3 tejto hlavy.
2. K vysokorizikovým systémom umelej inteligencie musí byť vo vhodnom digitálnom formáte alebo inak priložený návod na použitie obsahujúci stručné, úplné, správne a jasné informácie, ktoré sú pre používateľov relevantné, prístupné a zrozumiteľné.
3. V informáciách podľa odseku 2 sa uvádzajú:
  - a) totožnosť a kontaktné údaje prevádzkovateľa a v príslušných prípadoch jeho splnomocneného zástupcu;
  - b) charakteristiky, schopnosti a obmedzenia výkonnosti vysokorizikového systému umelej inteligencie vrátane:
    - i) jeho zamýšľaného účelu;
    - ii) úrovne presnosti, spoľahlivosti a kybernetickej bezpečnosti podľa článku 15, na základe ktorej bol vysokorizikový systém umelej inteligencie testovaný a validovaný a ktorú možno očakávať, ako aj všetky známe a predvídateľné okolnosti, ktoré môžu mať vplyv na túto očakávanú úroveň presnosti, spoľahlivosti a kybernetickej bezpečnosti;
    - iii) všetkých známych alebo predvídateľných okolností súvisiacich s používaním vysokorizikového systému umelej inteligencie v súlade s jeho zamýšľaným účelom alebo za podmienok logicky predvídateľného nesprávneho použitia, ktoré môžu viesť k rizikám pre zdravie a bezpečnosť alebo pre základné práva;
    - iv) jeho výkonnosti, pokiaľ ide o osoby alebo skupiny osôb, v prípade ktorých sa má systém používať;
    - v) prípadne špecifikácií vstupných údajov alebo akýchkoľvek iných relevantných informácií z hľadiska použitých súborov tréningových, validačných a testovacích údajov, pričom sa zohľadní zamýšľaný účel systému umelej inteligencie;
  - c) prípadné zmeny vysokorizikového systému umelej inteligencie a jeho výkonnosti, ktoré v čase počiatočného posudzovania zhody vopred určil poskytovateľ;
  - d) opatrenia na zabezpečenie ľudského dohľadu uvedené v článku 14 vrátane technických opatrení zavedených na uľahčenie výkladu výstupov systémov umelej inteligencie používateľmi;



- e) očakávaná životnosť vysokorizikového systému umelej inteligencie a všetky potrebné opatrenia na údržbu a starostlivosť, ktorými sa má zabezpečiť riadne fungovanie tohto systému umelej inteligencie, a to aj pokiaľ ide o aktualizácie softvéru.

#### *Článok 14* *Ludský dohľad*

1. Vysokorizikové systémy umelej inteligencie musia byť koncipované a vyvinuté tak, aby nad nimi počas obdobia používania systému umelej inteligencie mohli fyzické osoby vykonávať účinný dohľad, a to aj pomocou vhodných nástrojov rozhrania človek – stroj.
2. Ludský dohľad sa zameriava na prevenciu alebo minimalizáciu rizík pre zdravie, bezpečnosť alebo základné práva, ktoré môžu vzniknúť pri používaní vysokorizikového systému umelej inteligencie v súlade so zamýšľaným účelom alebo za podmienok logicky predvídateľného nesprávneho použitia, najmä ak takéto riziká bez ohľadu na uplatňovanie iných požiadaviek stanovených v tejto kapitole pretrvávajú.
3. Ludský dohľad sa zabezpečuje jedným alebo všetkými týmito opatreniami:
  - a) opatrenia, ktoré identifikuje poskytovateľ, a ak je to technicky uskutočniteľné, začlení ich do vysokorizikového systému umelej inteligencie pred jeho uvedením na trh alebo do prevádzky;
  - b) opatrenia, ktoré identifikuje poskytovateľ pred uvedením vysokorizikového systému umelej inteligencie na trh alebo do prevádzky a ktoré môže zaviesť používateľ.
4. Opatrenia uvedené v odseku 3 musia osobám, ktorým je zverený ľudský dohľad, umožniť, aby podľa okolností:
  - a) plne pochopili kapacity a obmedzenia vysokorizikového systému umelej inteligencie a boli schopné riadne monitorovať jeho prevádzku tak, aby bolo možné čo najskôr odhaliť a odstrániť príznaky anomálií, porúch a neočakávaného správania systému;
  - b) si boli neustále vedomé novej tendencie automatického spoliehania sa alebo nadmerného spoliehania sa na výstupy vytvorené vysokorizikovým systémom umelej inteligencie („automatizačné skreslenie“), a to najmä v prípade vysokorizikových systémov umelej inteligencie používaných na poskytovanie informácií alebo odporúčaní pre rozhodnutia, ktoré majú prijať fyzické osoby;
  - c) boli schopné správne interpretovať výstupy vysokorizikového systému umelej inteligencie, najmä s prihliadnutím na charakteristiky systému a dostupné interpretačné nástroje a metódy;
  - d) boli schopné v akejkoľvek konkrétnej situácii rozhodnúť, že sa vysokorizikový systém umelej inteligencie nebude používať alebo sa výstup vysokorizikového systému umelej inteligencie inak nezohľadní, potlačí alebo zvráti;
  - e) boli schopné zasiahnuť do prevádzky vysokorizikového systému umelej inteligencie alebo ho prerušiť tlačidlom zastavenia alebo podobným postupom.
5. V prípade vysokorizikových systémov umelej inteligencie uvedených v bode 1 písm. a) prílohy III musia byť opatrenia podľa odseku 3 také, aby sa navyše zabezpečilo, že

používateľ na základe identifikácie vyplývajúcej zo systému neprijme žiadne kroky ani rozhodnutie, pokiaľ tento výsledok nebol overený a potvrdený aspoň dvoma fyzickými osobami.

### Článok 15

#### *Presnosť, spoľahlivosť a kybernetická bezpečnosť*

1. Vysokorizikové systémy umelej inteligencie musia byť koncipované a vyvinuté tak, aby vzhľadom na svoj zamýšľaný účel dosahovali primeranú úroveň presnosti, spoľahlivosti a kybernetickej bezpečnosti a aby v týchto ohľadoch konzistentne fungovali počas celého svojho životného cyklu.
2. Úrovně presnosti a príslušné metriky na meranie presnosti vysokorizikových systémov umelej inteligencie sa musia uvádzať v priloženom návode na použitie.
3. Vysokorizikové systémy umelej inteligencie musia byť odolné voči chybám, poruchám alebo nezrovnalostiam, ktoré sa môžu vyskytnúť v rámci systému alebo prostredia, v ktorom sa systém prevádzkuje, a to najmä z dôvodu ich interakcie s fyzickými osobami alebo inými systémami.

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

Vysokorizikové systémy umelej inteligencie, ktoré sa po uvedení na trh alebo do prevádzky ďalej učia, sa musia vyvíjať tak, aby sa zabezpečilo, že prípadné skreslené výstupy v dôsledku výstupov používaných ako vstup pre budúce operácie („slučky spätnej väzby“) budú náležite riešené vhodnými zmierňujúcimi opatreniami.

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

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

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

## KAPITOLA 3

### **POVINNOSTI POSKYTOVATEĽOV A POUŽÍVATEĽOV VYSOKORIZIKOVÝCH SYSTÉMOV UMELEJ INTELIGENCIE A INÝCH STRÁN**

#### Článok 16

##### *Povinnosti poskytovateľov vysokorizikových systémov umelej inteligencie*

Poskytovatelia vysokorizikových systémov umelej inteligencie musia:

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

- b) mať zavedený systém riadenia kvality, ktorý je v súlade s článkom 17;
- c) vypracovať technickú dokumentáciu vysokorizikového systému umelej inteligencie;
- d) uchovávať logy automaticky generované ich vysokorizikovými systémami umelej inteligencie, ak ich majú pod kontrolou;
- e) zabezpečiť, aby sa vysokorizikový systém umelej inteligencie pred uvedením na trh alebo do prevádzky podrobil príslušnému postupu posudzovania zhody;
- f) plniť povinnosti týkajúce sa registrácie uvedené v článku 51;
- g) prijať potrebné nápravné opatrenia, ak vysokorizikový systém umelej inteligencie nie je v súlade s požiadavkami stanovenými v kapitole 2 tejto hlavy;
- h) informovať o nesúlade a o všetkých prijatých nápravných opatreniach príslušné vnútroštátne orgány členských štátov, v ktorých systém umelej inteligencie sprístupnili alebo uviedli do prevádzky, a v relevantných prípadoch aj notifikovanú osobu;
- i) umiestniť označenie CE na svoje vysokorizikové systémy umelej inteligencie, a tak v súlade s článkom 49 vyjadriť zhodu s týmto nariadením;
- j) na žiadosť príslušného vnútroštátneho orgánu preukázať zhodu vysokorizikového systému umelej inteligencie s požiadavkami stanovenými v kapitole 2 tejto hlavy.

#### *Článok 17*

##### *Systém riadenia kvality*

1. Poskytovatelia vysokorizikových systémov umelej inteligencie zavedú systém riadenia kvality, ktorým sa zabezpečí súlad s týmto nariadením. Tento systém sa systematicky a usporiadane zdokumentuje vo forme písomných zásad, postupov a pokynov a musí zahŕňať aspoň tieto aspekty:
  - a) stratégiu dodržiavania regulačných požiadaviek vrátane dodržiavania postupov posudzovania zhody a postupov riadenia zmien vysokorizikového systému umelej inteligencie;
  - b) techniky, postupy a systematické opatrenia, ktoré sa majú použiť pri koncipovaní vysokorizikového systému umelej inteligencie, kontrole jeho koncepcie a jej overovaní;
  - c) techniky, postupy a systematické opatrenia, ktoré sa majú použiť pri vývoji vysokorizikového systému umelej inteligencie a pri kontrole a zabezpečení jeho kvality;
  - d) postupy preskúmania, testovania a validácie, ktoré sa majú vykonávať pred vývojom vysokorizikového systému umelej inteligencie, počas neho a po ňom, a častotou, s akou sa musia vykonávať;
  - e) technické špecifikácie vrátane noriem, ktoré sa majú uplatňovať, a v prípade, že sa príslušné harmonizované normy neuplatňujú v plnom rozsahu, prostriedky, ktoré sa majú použiť na zabezpečenie toho, aby vysokorizikový systém umelej inteligencie spĺňal požiadavky stanovené v kapitole 2 tejto hlavy;
  - f) systémy a postupy správy údajov vrátane zberu údajov, ich analýzy, označovania, ukladania, filtrovania, hĺbkovej analýzy, agregácie, uchovávania a všetkých ďalších operácií týkajúcich sa údajov, ktoré sa vykonávajú pred

uvedením vysokorizikových systémov umelej inteligencie na trh alebo do prevádzky a na účely ich uvedenia na trh alebo do prevádzky;

- g) systém riadenia rizík uvedený v článku 9;
  - h) vytvorenie, zavedenie a vedenie systému monitorovania po uvedení na trh v súlade s článkom 61;
  - i) postupy týkajúce sa podávania správ o závažných incidentoch a poruchách v súlade s článkom 62;
  - j) vybavovanie komunikácie s príslušnými vnútroštátnymi orgánmi, príslušnými orgánmi vrátane odvetvových orgánov, ktoré poskytujú alebo podporujú prístup k údajom, s notifikovanými osobami, inými prevádzkovateľmi, zákazníkmi alebo inými zainteresovanými stranami;
  - k) systémy a postupy vedenia záznamov o všetkých príslušných dokumentoch a informáciách;
  - l) riadenie zdrojov vrátane opatrení týkajúcich sa bezpečnosti dodávok;
  - m) rámec zodpovednosti, v ktorom sa stanovujú povinnosti manažmentu a ostatných zamestnancov, pokiaľ ide o všetky aspekty uvedené v tomto odseku.
2. Vykonávanie aspektov uvedených v odseku 1 musí byť primerané veľkosti organizácie poskytovateľa.
3. V prípade poskytovateľov, ktorí sú úverovými inštitúciami regulovanými smernicou 2013/36/EÚ, sa povinnosť zaviesť systém riadenia kvality považuje za splnenú, keď sa dodržiavajú pravidlá týkajúce sa opatrení, postupov a mechanizmov vnútorného riadenia podľa článku 74 uvedenej smernice. V tejto súvislosti sa zohľadnia všetky harmonizované normy uvedené v článku 40 tohto nariadenia.

#### *Článok 18*

##### *Povinnosť vypracovať technickú dokumentáciu*

1. Poskytovatelia vysokorizikových systémov umelej inteligencie vypracujú v súlade s prílohou IV technickú dokumentáciu uvedenú v článku 11.
2. Poskytovatelia, ktorí sú úverovými inštitúciami regulovanými smernicou 2013/36/EÚ, vedú technickú dokumentáciu ako súčasť dokumentácie týkajúcej sa opatrení, postupov a mechanizmov vnútorného riadenia podľa článku 74 uvedenej smernice.

#### *Článok 19*

##### *Posudzovanie zhody*

1. Poskytovatelia vysokorizikových systémov umelej inteligencie musia zabezpečiť, aby sa ich systémy pred uvedením na trh alebo do prevádzky podrobili príslušnému postupu posudzovania zhody v súlade s článkom 43. Ak sa po tomto posúdení zhody preukáže súlad systémov umelej inteligencie s požiadavkami stanovenými v kapitole 2 tejto hlavy, poskytovatelia vypracujú EÚ vyhlásenie o zhode v súlade s článkom 48 a umiestnia označenie zhody CE v súlade s článkom 49.
2. V prípade vysokorizikových systémov umelej inteligencie uvedených v bode 5 písm. b) prílohy III, ktoré uvádzajú na trh alebo do prevádzky poskytovatelia, ktorí sú

úverovými inštitúciami regulovanými smernicou 2013/36/EÚ, sa posudzovanie zhody vykonáva ako súčasť postupu uvedeného v článkoch 97 až 101 uvedenej smernice.

#### *Článok 20*

##### *Automaticky generované logy*

1. Poskytovatelia vysokorizikových systémov umelej inteligencie uchovávajú logy automaticky generované svojimi vysokorizikovými systémami umelej inteligencie, pokiaľ sú tieto logy na základe zmluvnej dohody s používateľom alebo zo zákona pod ich kontrolou. Logy sa uchovávajú počas obdobia, ktoré je primerané vzhľadom na zamýšľaný účel vysokorizikového systému umelej inteligencie a uplatniteľné právne povinnosti podľa právnych predpisov Únie alebo vnútroštátneho práva.
2. Poskytovatelia, ktorí sú úverovými inštitúciami regulovanými smernicou 2013/36/EÚ, uchovávajú logy automaticky generované svojimi vysokorizikovými systémami umelej inteligencie ako súčasť dokumentácie podľa článku 74 uvedenej smernice.

#### *Článok 21*

##### *Nápravné opatrenia*

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

#### *Článok 22*

##### *Povinnosť informovať*

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

#### *Článok 23*

##### *Spolupráca s príslušnými orgánmi*

Poskytovatelia vysokorizikových systémov umelej inteligencie na žiadosť príslušného vnútroštátneho orgánu poskytnú tomuto orgánu všetky informácie a dokumentáciu potrebnú na preukázanie zhody vysokorizikového systému umelej inteligencie s požiadavkami stanovenými v kapitole 2 tejto hlavy, a to v úradnom jazyku Únie, ktorý určí dotknutý členský štát. Na základe odôvodnenej žiadosti príslušného vnútroštátneho orgánu sprístupnia poskytovatelia tomuto orgánu aj logy automaticky generované vysokorizikovým systémom umelej inteligencie, pokiaľ sú tieto logy na základe zmluvnej dohody s používateľom alebo zo zákona pod ich kontrolou.

*Článok 24*  
*Povinnosti výrobcov výrobkov*

Ak sa vysokorizikový systém umelej inteligencie súvisiaci s výrobkami, na ktoré sa vzťahujú právne akty uvedené v oddiele A prílohy II, uvádza na trh alebo do prevádzky spolu s výrobkom vyrobeným v súlade s uvedenými právnymi aktmi a pod menom výrobcu výrobku, za súlad systému umelej inteligencie s týmto nariadením preberá zodpovednosť výrobca výrobku, a pokiaľ ide o systém umelej inteligencie, má rovnaké povinnosti, aké toto nariadenie ukladá poskytovateľovi.

*Článok 25*  
*Splnomocnení zástupcovia*

1. Ak nie je možné identifikovať dovozcu, poskytovateľa usadení mimo Únie pred sprístupnením svojich systémov na trhu Únie písomným splnomocnením vymenujú splnomocneného zástupcu usadeného v Únii.
2. Splnomocnený zástupca vykonáva úlohy uvedené v splnomocnení, ktoré mu udelil poskytovateľ. Splnomocnenie poveruje splnomocneného zástupcu vykonávaním týchto úloh:
  - a) uchovávať kópiu EÚ vyhlásenia o zhode a technickej dokumentácie, aby bola k dispozícii pre príslušné vnútroštátne orgány a vnútroštátne orgány uvedené v článku 63 ods. 7;
  - b) poskytnúť príslušnému vnútroštátnemu orgánu na základe odôvodnenej žiadosti všetky informácie a dokumentáciu potrebné na preukázanie súladu vysokorizikového systému umelej inteligencie s požiadavkami stanovenými v kapitole 2 tejto hlavy vrátane prístupu k logom automaticky generovaným vysokorizikovým systémom umelej inteligencie, pokiaľ sú tieto logy na základe zmluvnej dohody s používateľom alebo zo zákona pod kontrolou poskytovateľa;
  - c) na základe odôvodnenej žiadosti spolupracovať s príslušnými vnútroštátnymi orgánmi pri každom opatrení, ktoré tieto orgány v súvislosti s vysokorizikovým systémom umelej inteligencie prijímú.

*Článok 26*  
*Povinnosti dovozcov*

1. Pred uvedením vysokorizikového systému umelej inteligencie na trh dovozcovia takéhoto systému zabezpečia, aby:
  - a) poskytovateľ uvedeného systému umelej inteligencie vykonal vhodný postup posudzovania zhody;
  - b) poskytovateľ vypracoval technickú dokumentáciu v súlade s prílohou IV;
  - c) systém bol označený požadovaným označením zhody a aby k nemu bola priložená požadovaná dokumentácia a návod na použitie.
2. Ak sa dovozca domnieva alebo má dôvod domnievať sa, že vysokorizikový systém umelej inteligencie nie je v súlade s týmto nariadením, nesmie tento systém uviesť na trh, kým sa tento systém umelej inteligencie neuvedie do súladu. Ak vysokorizikový systém umelej inteligencie predstavuje riziko v zmysle článku 65 ods. 1, dovozca

o tom informuje poskytovateľa systému umelej inteligencie a orgány dohľadu nad trhom.

3. Dovozcovia na vysokorizikovom systéme umelej inteligencie, alebo ak to nie je možné, na jeho obale, prípadne v jeho sprievodnej dokumentácii uvedú svoje meno, registrované obchodné meno alebo registrovanú ochrannú známku a adresu, na ktorej ich možno kontaktovať.
4. Dovozcovia zabezpečia, aby v čase, keď nesú za vysokorizikový systém umelej inteligencie zodpovednosť, podmienky jeho uskladnenia alebo prepravy v relevantných prípadoch neohrozovali jeho súlad s požiadavkami stanovenými v kapitole 2 tejto hlavy.
5. Dovozcovia na základe odôvodnenej žiadosti poskytnú príslušnému vnútroštátnemu orgánu všetky informácie a dokumentáciu potrebné na preukázanie súladu vysokorizikového systému umelej inteligencie s požiadavkami stanovenými v kapitole 2 tejto hlavy, a to v jazyku, ktorý je pre tento príslušný vnútroštátny orgán ľahko zrozumiteľný, vrátane prístupu k logom automaticky generovaným vysokorizikovým systémom umelej inteligencie, pokiaľ sú tieto logy na základe zmluvnej dohody s používateľom alebo zo zákona pod kontrolou poskytovateľa. Spolupracujú s týmito orgánmi aj pri akomkoľvek opatrení, ktoré príslušný vnútroštátny orgán prijme v súvislosti s uvedeným systémom.

#### Článok 27

##### *Povinnosti distribútorov*

1. Pred sprístupnením vysokorizikového systému umelej inteligencie na trhu distribútori overia, či je tento vysokorizikový systém umelej inteligencie označený požadovaným označením zhody CE, či je k nemu pripojená požadovaná dokumentácia a návod na použitie a či si poskytovateľ, prípadne dovozca systému splnili povinnosti stanovené v tomto nariadení.
2. Ak sa distribútor domnieva alebo má dôvod domnievať sa, že vysokorizikový systém umelej inteligencie nie je v súlade s požiadavkami stanovenými v kapitole 2 tejto hlavy, nesmie tento systém sprístupniť na trhu, kým sa tento systém neuvedie do súladu s uvedenými požiadavkami. Ak systém navyše predstavuje riziko v zmysle článku 65 ods. 1, distribútor o tom informuje poskytovateľa, prípadne dovozcu systému.
3. Distribútori zabezpečia, aby v čase, keď nesú za vysokorizikový systém umelej inteligencie zodpovednosť, podmienky jeho uskladnenia alebo prepravy v relevantných prípadoch neohrozovali súlad systému s požiadavkami stanovenými v kapitole 2 tejto hlavy.
4. Distribútor, ktorý sa domnieva alebo má dôvod domnievať sa, že vysokorizikový systém umelej inteligencie, ktorý sprístupnil na trhu, nie je v súlade s požiadavkami stanovenými v kapitole 2 tejto hlavy, prijme nápravné opatrenia potrebné na dosiahnutie súladu tohto systému s uvedenými požiadavkami, na jeho stiahnutie z trhu alebo od používateľa, alebo zabezpečí, aby uvedené nápravné opatrenia prijal poskytovateľ, dovozca alebo prípadne akýkoľvek relevantný prevádzkovateľ. Ak vysokorizikový systém umelej inteligencie predstavuje riziko v zmysle článku 65 ods. 1, distribútor o tom bezodkladne informuje príslušné vnútroštátne orgány členských štátov, v ktorých výrobok sprístupnil, pričom uvedie podrobnosti najmä o nedodržaní požiadaviek a o všetkých prijatých nápravných opatreniach.

5. Na základe odôvodnenej žiadosti príslušného vnútroštátneho orgánu distribútori vysokorizikových systémov umelej inteligencie poskytnú tomuto orgánu všetky informácie a dokumentáciu potrebné na preukázanie zhody vysokorizikového systému s požiadavkami stanovenými v kapitole 2 tejto hlavy. Distribútori spolupracujú s týmto príslušným vnútroštátnym orgánom aj pri každom opatrení, ktoré tento orgán prijme.

#### Článok 28

##### *Povinnosti distribútorov, dovozcov, používateľov alebo iných tretích strán*

1. Každý distribútor, dovozca, používateľ alebo iná tretia strana sa na účely tohto nariadenia považuje za poskytovateľa a vzťahujú sa na neho povinnosti poskytovateľa podľa článku 16 za ktorýchkoľvek z týchto okolností:
  - a) pod svojím menom alebo ochrannou známkou uvádzajú na trh alebo do prevádzky vysokorizikový systém umelej inteligencie;
  - b) menia zamýšľaný účel vysokorizikového systému umelej inteligencie, ktorý už bol uvedený na trh alebo do prevádzky;
  - c) vykonávajú podstatnú zmenu vysokorizikového systému umelej inteligencie.
2. Ak nastanú okolnosti uvedené v odseku 1 písm. b) alebo c), poskytovateľ, ktorý uviedol vysokorizikový systém umelej inteligencie na trh alebo do prevádzky pôvodne, sa už na účely tohto nariadenia za poskytovateľa nepovažuje.

#### Článok 29

##### *Povinnosti používateľov vysokorizikových systémov umelej inteligencie*

1. Používatelia vysokorizikových systémov umelej inteligencie musia tieto systémy používať v súlade s návodom na použitie k nim priloženým, a to podľa odsekov 2 a 5.
2. Povinnosťami uvedenými v odseku 1 nie sú dotknuté iné povinnosti používateľov vyplývajúce z právnych predpisov Únie alebo vnútroštátneho práva ani rozhodovanie používateľov pri organizovaní vlastných zdrojov a činností na účely vykonávania opatrení na zabezpečenie ľudského dohľadu uvedených poskytovateľom.
3. Bez toho, aby bol dotknutý odsek 1 a pokiaľ má používateľ kontrolu nad vstupnými údajmi, tento používateľ zabezpečí, aby vstupné údaje boli relevantné z hľadiska zamýšľaného účelu vysokorizikového systému umelej inteligencie.
4. Používatelia monitorujú prevádzku vysokorizikového systému umelej inteligencie na základe návodu na použitie. Ak majú dôvody domnievať sa, že používanie v súlade s návodom na použitie môže viesť k tomu, že systém umelej inteligencie bude predstavovať riziko v zmysle článku 65 ods. 1, informujú poskytovateľa alebo distribútora a pozastavia používanie systému. Poskytovateľa alebo distribútora informujú aj vtedy, keď zistia akýkoľvek závažný incident alebo akúkoľvek poruchu v zmysle článku 62, a používanie systému umelej inteligencie prerušia. V prípade, že používateľ sa s poskytovateľom nedokáže spojiť, uplatňuje sa *mutatis mutandis* článok 62.
5. V prípade používateľov, ktorí sú úverovými inštitúciami regulovanými smernicou 2013/36/EÚ, sa povinnosť monitorovania stanovená v prvom pododseku považuje za splnenú, ak sa dodržia pravidiel týkajúce sa opatrení, postupov a mechanizmov vnútorného riadenia podľa článku 74 uvedenej smernice.



6. Používatelia vysokorizikových systémov umelej inteligencie uchovávajú logy automaticky generované týmito systémami, pokiaľ sú tieto logy pod ich kontrolou. Logy sa uchovávajú počas obdobia, ktoré je primerané vzhľadom na zamýšľaný účel vysokorizikového systému umelej inteligencie a uplatniteľné právne povinnosti podľa právnych predpisov Únie alebo vnútroštátneho práva.  
Používatelia, ktorí sú úverovými inštitúciami regulovanými smernicou 2013/36/EÚ, uchovávajú logy ako súčasť dokumentácie týkajúcej sa opatrení, postupov a mechanizmov vnútorného riadenia podľa článku 74 uvedenej smernice.
7. Na splnenie svojej povinnosti vykonať posúdenie vplyvu na ochranu údajov podľa článku 35 nariadenia (EÚ) 2016/679 alebo prípadne článku 27 smernice (EÚ) 2016/680 využijú používatelia vysokorizikových systémov umelej inteligencie informácie poskytnuté podľa článku 13.

## KAPITOLA 4

### NOTIFIKUJÚCE ORGÁNY A NOTIFIKOVANÉ OSOBY

#### Článok 30

##### *Notifikujúce orgány*

1. Každý členský štát určí alebo zriadi notifikujúci orgán zodpovedný za stanovenie a vykonávanie nevyhnutných postupov na posudzovanie, určovanie a notifikáciu orgánov posudzovania zhody a za ich monitorovanie.
2. Členské štáty môžu ako notifikujúci orgán určiť vnútroštátny akreditačný orgán uvedený v nariadení (ES) č. 765/2008.
3. Notifikujúce orgány sa zriaďujú, organizujú a prevádzkujú tak, aby nedochádzalo ku konfliktu záujmov s orgánmi posudzovania zhody a aby bola zabezpečená objektivita a nestrannosť ich činností.
4. Notifikujúce orgány majú takú organizačnú štruktúru, aby rozhodnutia týkajúce sa notifikácie orgánov posudzovania zhody prijímali príslušné osoby iné ako osoby, ktoré vykonali posudzovanie týchto orgánov.
5. Notifikujúce orgány nesmú ponúkať ani poskytovať žiadne činnosti, ktoré vykonávajú orgány posudzovania zhody, ani žiadne poradenské služby na komerčnom či konkurenčnom základe.
6. Notifikujúce orgány musia zabezpečiť dôvernosť informácií, ktoré získajú.
7. Notifikujúce orgány majú na riadne vykonávanie svojich úloh k dispozícii dostatočný počet odborne spôsobilých zamestnancov.
8. Notifikujúce orgány zabezpečia, aby sa posudzovanie zhody vykonávalo primeraným spôsobom, ktorým sa predíde zbytočnému zaťaženiu poskytovateľov, a aby notifikované osoby vykonávali svoje činnosti s náležitým zreteľom na veľkosť podniku, odvetvie, v ktorom podnik pôsobí, jeho štruktúru a stupeň zložitosti príslušného systému umelej inteligencie.

### Článok 31

#### *Žiadosť orgánov posudzovania zhody o notifikáciu*

1. Žiadosť o notifikáciu predkladajú orgány posudzovania zhody notifikujúcemu orgánu členského štátu, v ktorom sú usadené.
2. Súčasťou žiadosti o notifikáciu je opis činností posudzovania zhody, modulu alebo modulov posudzovania zhody a technológií umelej inteligencie, v súvislosti s ktorými orgán posudzovania zhody tvrdí, že je odborne spôsobilý, a ak existuje, aj osvedčenie o akreditácii vydané vnútroštátnym akreditačným orgánom, ktorým sa potvrdzuje, že orgán posudzovania zhody spĺňa požiadavky stanovené v článku 33. Priložia sa všetky platné dokumenty týkajúce sa existujúcich prípadov, v ktorých bola žiadajúca notifikovaná osoba určená podľa iných harmonizačných právnych predpisov Únie.
3. Ak dotknutý orgán posudzovania zhody nemôže poskytnúť osvedčenie o akreditácii, poskytne notifikujúcemu orgánu všetky písomné doklady, ktoré sú potrebné na overenie, uznanie a pravidelné monitorovanie toho, či plní požiadavky stanovené v článku 33. V prípade notifikovaných osôb, ktoré boli určené podľa iných harmonizačných právnych predpisov Únie, sa ako podklady pre postup ich určenia podľa tohto nariadenia môžu podľa potreby použiť všetky dokumenty a osvedčenia súvisiace s týmito určeniami.

### Článok 32

#### *Notifikačný postup*

1. Notifikujúce orgány môžu notifikovať iba o tých orgánoch posudzovania zhody, ktoré splnili požiadavky stanovené v článku 33.
2. Komisii a ostatným členským štátom podávajú notifikujúce orgány notifikácie prostredníctvom elektronického notifikačného nástroja vyvinutého a spravovaného Komisiou.
3. Notifikácia musí obsahovať úplné údaje o činnostiach posudzovania zhody, module alebo moduloch posudzovania zhody a dotknutých technológiách umelej inteligencie.
4. Dotknutý orgán posudzovania zhody môže vykonávať činnosti notifikovanej osoby iba vtedy, ak Komisia ani ostatné členské štáty nevzniesli do jedného mesiaca od notifikácie námietky.
5. Akékoľvek následné relevantné zmeny notifikácie oznámia notifikujúce orgány Komisii a ostatným členským štátom.

### Článok 33

#### *Notifikované osoby*

1. Notifikované osoby overujú zhodu vysokorizikového systému umelej inteligencie v súlade s postupmi posudzovania zhody uvedenými v článku 43.
2. Notifikované osoby musia spĺňať požiadavky týkajúce sa organizácie, riadenia kvality, zdrojov a postupov potrebné na plnenie svojich úloh.
3. Organizačná štruktúra, rozdelenie zodpovedností, hierarchické vzťahy a fungovanie notifikovaných osôb musia byť také, aby sa zabezpečila dôvera v ich konanie a vo výsledky činností posudzovania zhody, ktoré notifikované osoby vykonávajú.

4. Notifikované osoby musia byť nezávislé od poskytovateľa vysokorizikového systému umelej inteligencie, v súvislosti s ktorým vykonávajú činnosti posudzovania zhody. Takisto musia byť nezávislé od akéhokoľvek iného prevádzkovateľa, ktorý má na posudzovanom vysokorizikovom systéme umelej inteligencie hospodársky záujem, ako aj od akýchkoľvek konkurentov poskytovateľa.
5. Notifikované osoby musia mať takú organizačnú štruktúru a fungovať tak, aby sa zaručila nezávislosť, objektivita a nestrannosť ich činností. Notifikované osoby musia zdokumentovať a zaviesť štruktúru a postupy, ktorými sa zaručí nestrannosť a ktorými sa budú presadzovať a uplatňovať zásady nestrannosti v celej ich organizačnej štruktúre, u všetkých zamestnancov a pri všetkých činnostiach posudzovania.
6. Notifikované osoby musia mať zavedené zdokumentované postupy, ktorými sa zabezpečí, aby ich zamestnanci, výbory, dcérske spoločnosti, subdodávatelia a akýkoľvek pridružený subjekt alebo zamestnanci externých subjektov zachovávali dôvernosť informácií, ktoré získajú počas vykonávania činností posudzovania zhody, s výnimkou prípadov, keď sa zverejnenie týchto informácií vyžaduje podľa zákona. Zamestnanci notifikovaných osôb sú povinní zachovávať služobné tajomstvo, pokiaľ ide o všetky informácie, ktoré získali pri vykonávaní svojich úloh podľa tohto nariadenia; táto povinnosť sa neuplatňuje vo vzťahu k notifikujúcim orgánom členského štátu, v ktorom sa ich činnosti vykonávajú.
7. Na vykonávanie činností musia mať notifikované osoby postupy, pri ktorých sa náležite zohľadňuje veľkosť podniku, odvetvie, v ktorom podnik pôsobí, jeho štruktúra a stupeň zložitosti príslušného systému umelej inteligencie.
8. Notifikované osoby musia v súvislosti so svojimi činnosťami posudzovania zhody uzavrieť primerané poistenie zodpovednosti, ak na seba v súlade s vnútroštátnym právom neprevzal zodpovednosť dotknutý členský štát alebo ak za posudzovanie zhody nezodpovedá priamo tento členský štát.
9. Všetky úlohy, ktoré im prináležia podľa tohto nariadenia, musia byť notifikované osoby schopné vykonávať na najvyššej úrovni profesijnej bezúhonnosti a s náležitou odbornou spôsobilosťou v danej oblasti bez ohľadu na to, či tieto úlohy vykonávajú samotné notifikované osoby alebo sa vykonávajú v ich mene a na ich zodpovednosť.
10. Notifikované osoby musia byť na internej úrovni dostatočne spôsobilé, aby mohli účinne hodnotiť úlohy, ktoré v ich mene vykonávajú externé subjekty. Na tento účel musia mať notifikované osoby vždy a pre každý prípad postupu posudzovania zhody, ako aj pre každý typ vysokorizikového systému umelej inteligencie, pre ktorý boli určené, neustále k dispozícii dostatočný počet administratívnych, technických a vedeckých zamestnancov, ktorí majú skúsenosti a vedomosti týkajúce sa príslušných technológií umelej inteligencie, údajov a ich spracovania, ako aj požiadaviek stanovených v kapitole 2 tejto hlavy.
11. Notifikované osoby sa zúčastňujú na koordinačných činnostiach uvedených v článku 38. Takisto sa priamo zúčastňujú na činnosti európskych normalizačných organizácií alebo sú v nich zastúpené, alebo zabezpečia, aby boli neustále informované o aktuálnom stave príslušných noriem.
12. Notifikujúcemu orgánu uvedenému v článku 30 notifikované osoby sprístupnia a na požiadanie predložia všetky príslušné dokumenty vrátane dokumentácie poskytovateľa, aby tento orgán mohol vykonávať svoje činnosti posudzovania,

určovania, notifikácie, monitorovania a dohľadu a aby sa uľahčilo posudzovanie podľa tejto kapitoly.

#### *Článok 34*

##### *Dcérske spoločnosti a subdodávatelia notifikovaných osôb*

1. Ak notifikovaná osoba zadáva osobitné úlohy spojené s posudzovaním zhody subdodávateľovi alebo ich prenesie na dcérsku spoločnosť, musí zabezpečiť, aby tento subdodávateľ alebo táto dcérska spoločnosť spĺňali požiadavky stanovené v článku 33, a náležite o tom informuje notifikujúci orgán.
2. Notifikované osoby nesú plnú zodpovednosť za úlohy vykonávané subdodávateľmi alebo dcérskymi spoločnosťami bez ohľadu na to, kde sú usadené.
3. Vykonávanie činností sa môže zadať subdodávateľovi alebo preniesť na dcérsku spoločnosť iba so súhlasom poskytovateľa.
4. Notifikované osoby musia mať pre notifikujúci orgán k dispozícii príslušnú dokumentáciu týkajúcu sa posúdenia kvalifikácie subdodávateľa alebo dcérskej spoločnosti a práce, ktorú tento subdodávateľ alebo táto dcérska spoločnosť vykonali podľa tohto nariadenia.

#### *Článok 35*

##### *Identifikačné čísla a zoznamy notifikovaných osôb určených podľa tohto nariadenia*

1. Každý notifikovanej osobe prideli Komisia identifikačné číslo. Notifikovanej osobe prideli len jedno číslo, a to aj keď je notifikovaná na základe viacerých aktov Únie.
2. Komisia zverejní zoznam osôb notifikovaných podľa tohto nariadenia vrátane identifikačných čísiel, ktoré im boli pridelené, a činností, v súvislosti s ktorými boli notifikované. Komisia zabezpečuje aktuálnosť tohto zoznamu.

#### *Článok 36*

##### *Zmeny notifikácií*

1. Ak má notifikujúci orgán podozrenie alebo bol informovaný o tom, že notifikovaná osoba už nespĺňa požiadavky stanovené v článku 33 alebo že si neplní svoje povinnosti, notifikujúci orgán túto záležitosť bezodkladne a čo najdôkladnejšie vyšetrí. V tejto súvislosti informuje dotknutú notifikovanú osobu o vznesených námietkach a poskytne jej možnosť na vyjadrenie stanoviska. Ak notifikujúci orgán dospeje k záveru, že notifikovaná osoba, ktorá je predmetom vyšetrovania, už nespĺňa požiadavky stanovené v článku 33 alebo že si neplní svoje povinnosti, notifikujúci orgán podľa potreby a v závislosti od závažnosti nesplnenia požiadaviek alebo neplnenia povinností obmedzí, pozastaví alebo stiahne notifikáciu. Takisto o tom okamžite informuje Komisiu a ostatné členské štáty.
2. V prípade obmedzenia, pozastavenia alebo stiahnutia notifikácie, alebo ak notifikovaná osoba prestala vykonávať činnosť, notifikujúci orgán prijme náležité kroky, ktorými zabezpečí, aby spisovú dokumentáciu uvedenej notifikovanej osoby prevzala iná notifikovaná osoba alebo aby bola na požiadanie sprístupnená zodpovedným notifikujúcim orgánom.

### Článok 37

#### *Napadnutie spôsobilosti notifikovaných osôb*

1. Komisia v prípade potreby vyšetrí všetky prípady, v ktorých sú odôvodnené pochybnosti o tom, či notifikovaná osoba spĺňa požiadavky stanovené v článku 33.
2. Notifikujúci orgán poskytne na požiadanie Komisii všetky relevantné informácie týkajúce sa notifikácie dotknutej notifikovanej osoby.
3. Komisia zabezpečí dôverné zaobchádzanie so všetkými dôvernými informáciami získanými počas jej vyšetrení.
4. Keď Komisia zistí, že notifikovaná osoba nespĺňa alebo prestala spĺňať požiadavky stanovené v článku 33, prijme odôvodnené rozhodnutie, ktorým notifikujúci členský štát požiada, aby prijal potrebné nápravné opatrenia vrátane prípadného stiahnutia notifikácie. Uvedený vykonávací akt sa prijme v súlade s postupom preskúmania uvedeným v článku 74 ods. 2.

### Článok 38

#### *Koordinácia notifikovaných osôb*

1. Komisia zabezpečí, aby sa so zreteľom na oblasti, na ktoré sa vzťahuje toto nariadenie, medzi notifikovanými osobami pôsobiacimi v oblasti postupov posudzovania zhody systémov umelej inteligencie podľa tohto nariadenia zaviedla a riadne vykonávala primeraná koordinácia a spolupráca v podobe odvetvovej skupiny notifikovaných osôb.
2. Členské štáty zabezpečia, aby sa osoby, ktoré notifikovali, priamo alebo prostredníctvom určených zástupcov zúčastňovali na práci tejto skupiny.

### Článok 39

#### *Orgány posudzovania zhody tretích krajín*

Orgány posudzovania zhody zriadené podľa práva tretej krajiny, s ktorou Únia uzavrela dohodu, môžu byť oprávnené vykonávať činnosti notifikovaných osôb podľa tohto nariadenia.

## KAPITOLA 5

### NORMY, POSUDZOVANIE ZHODY, CERTIFIKÁTY, REGISTRÁCIA

### Článok 40

#### *Harmonizované normy*

Vysokorizikové systémy umelej inteligencie, ktoré sú v zhode s harmonizovanými normami alebo ich časťami, na ktoré boli uverejnené odkazy v *Úradnom vestníku Európskej únie*, sa považujú za systémy, ktoré sú v zhode s požiadavkami stanovenými v kapitole 2 tejto hlavy, pokiaľ sa uvedené normy na tieto požiadavky vzťahujú.

### Článok 41

#### *Spoločné špecifikácie*

1. Ak harmonizované normy uvedené v článku 40 neexistujú alebo ak sa Komisia domnieva, že príslušné harmonizované normy sú nedostatočné alebo že je potrebné

riešiť osobitné obavy týkajúce sa bezpečnosti alebo základných práv, môže prostredníctvom vykonávacích aktov prijať spoločné špecifikácie, pokiaľ ide o požiadavky stanovené v kapitole 2 tejto hlavy. Uvedené vykonávacie akty sa prijímú v súlade s postupom preskúmania uvedeným v článku 74 ods. 2.

2. Komisia pri vypracúvaní spoločných špecifikácií uvedených v odseku 1 zozbiera stanoviská príslušných orgánov alebo expertných skupín zriadených podľa príslušných odvetvových právnych predpisov Únie.
3. Vysokorizikové systémy umelej inteligencie, ktoré sú v zhode so spoločnými špecifikáciami uvedenými v odseku 1, sa považujú za systémy, ktoré sú v zhode s požiadavkami stanovenými v kapitole 2 tejto hlavy, pokiaľ sa uvedené spoločné špecifikácie na tieto požiadavky vzťahujú.
4. Ak poskytovatelia nedodržiavajú spoločné špecifikácie uvedené v odseku 1, musia riadne odôvodniť, že prijali technické riešenia, ktoré sú s uvedenými špecifikáciami aspoň rovnocenné.

#### *Článok 42*

##### *Predpoklad zhody s určitými požiadavkami*

1. Vzhľadom na zamýšľaný účel vysokorizikových systémov umelej inteligencie, ktoré boli trénované a testované na údajoch týkajúcich sa konkrétnych geografických, behaviorálnych a funkčných podmienok, v ktorých sa majú používať, sa predpokladá, že tieto systémy sú v súlade s požiadavkou stanovenou v článku 10 ods. 4.
2. Vysokorizikové systémy umelej inteligencie, pre ktoré bol v rámci systému kybernetickej bezpečnosti podľa nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881<sup>63</sup> vydaný certifikát alebo vyhlásenie o zhode a na ktoré boli uverejnené odkazy v *Úradnom vestníku Európskej únie*, sa považujú za systémy, ktoré sú v súlade s kyberneticko-bezpečnostnými požiadavkami stanovenými v článku 15 tohto nariadenia, pokiaľ sa certifikát kybernetickej bezpečnosti alebo vyhlásenie o zhode alebo ich časti na tieto požiadavky vzťahujú.

#### *Článok 43*

##### *Posudzovanie zhody*

1. Ak poskytovateľ pri preukazovaní súladu vysokorizikového systému umelej inteligencie uvedeného v bode 1 prílohy III s požiadavkami stanovenými v kapitole 2 tejto hlavy uplatnil harmonizované normy uvedené v článku 40 alebo prípadne spoločné špecifikácie uvedené v článku 41, musí dodržať jeden z týchto postupov:
  - a) postup posudzovania zhody na základe vnútornej kontroly uvedený v prílohe VI;
  - b) postup posudzovania zhody na základe posúdenia systému riadenia kvality a posúdenia technickej dokumentácie za účasti notifikovanej osoby uvedený v prílohe VII.

---

<sup>63</sup> Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (Ú. v. EÚ L 151, 7.6.2019, s. 1).

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

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

2. V prípade vysokorizikových systémov umelej inteligencie uvedených v bodoch 2 až 8 prílohy III poskytovatelia musia dodržať postup posudzovania zhody na základe vnútornej kontroly uvedený v prílohe VI, v ktorom sa nestanovuje účasť notifikovanej osoby. V prípade vysokorizikových systémov umelej inteligencie podľa bodu 5 písm. b) prílohy III uvedených na trh alebo do prevádzky úverovými inštitúciami regulovanými smernicou 2013/36/EÚ sa posudzovanie zhody vykonáva ako súčasť postupu uvedeného v článkoch 97 až 101 uvedenej smernice.
3. V prípade vysokorizikových systémov umelej inteligencie, na ktoré sa vzťahujú právne akty uvedené v oddiele A prílohy II, sa poskytovateľ riadi príslušným posúdením zhody vyžadovaným podľa uvedených právnych aktov. Na uvedené vysokorizikové systémy umelej inteligencie sa vzťahujú požiadavky stanovené v kapitole 2 tejto hlavy a musia byť zahrnuté do tohto posúdenia. Uplatňujú sa aj body 4.3, 4.4, 4.5 a piaty odsek bodu 4.6 prílohy VII.

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

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

4. Vždy, keď dôjde k podstatnej zmene vysokorizikových systémov umelej inteligencie, podrobia sa novému postupu posudzovania zhody, a to bez ohľadu na to, či je upravený systém určený na ďalšiu distribúciu alebo či ho ďalej používa súčasný používateľ.

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

5. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 73 na účely aktualizácie príloh VI a VII s cieľom zaviesť prvky postupov posudzovania zhody, ktorých potreba vznikne vzhľadom na technický pokrok.
6. Komisia je splnomocnená prijímať delegované akty na zmenu odsekov 1 a 2 s cieľom podrobiť vysokorizikové systémy umelej inteligencie uvedené v bodoch 2 až 8 prílohy III postupu posudzovania zhody uvedenému v prílohe VII alebo jeho častiam. Pri prijímaní takýchto delegovaných aktov Komisia zohľadní účinnosť postupu posudzovania zhody na základe vnútornej kontroly uvedeného v prílohe VI pri predchádzaní alebo minimalizácii rizík pre zdravie, bezpečnosť a ochranu základných práv, ktoré takéto systémy predstavujú, ako aj dostupnosť primeraných kapacít a zdrojov notifikovaných osôb.

#### *Článok 44* *Certifikáty*

1. Certifikáty vydané notifikovanými osobami v súlade s prílohou VII sa vyhotovia v niektorom z úradných jazykov Únie, ktorý určí členský štát, v ktorom je notifikovaná osoba usadená, alebo v inom úradnom jazyku Únie prijateľnom pre notifikovanú osobu.
2. Certifikáty platia na obdobie, ktoré sa v nich uvádza a ktoré nesmie presiahnuť päť rokov. Na žiadosť poskytovateľa možno platnosť certifikátu predĺžiť na ďalšie obdobia, z ktorých žiadne nesmie presiahnuť päť rokov, a to na základe opätovného posúdenia v súlade s uplatniteľnými postupmi posudzovania zhody.
3. Ak notifikovaná osoba zistí, že systém umelej inteligencie už nespĺňa požiadavky stanovené v kapitole 2 tejto hlavy, pozastaví so zreteľom na zásadu primeranosti platnosť vydaného certifikátu alebo ho stiahne, alebo jeho platnosť obmedzí, pokiaľ sa v primeranej lehote stanovenej notifikovanou osobou vhodnými nápravnými opatreniami prijatými poskytovateľom systému nezabezpečí súlad s týmito požiadavkami. Notifikovaná osoba svoje rozhodnutie zdôvodní.

#### *Článok 45* *Odvolanie proti rozhodnutiam notifikovaných osôb*

Členské štáty zabezpečia, aby strany, ktoré majú oprávnený záujem na rozhodnutiach notifikovaných osôb, mohli proti týmto rozhodnutiam využiť odvolacie konanie.

#### *Článok 46* *Informačné povinnosti notifikovaných osôb*

1. Notifikované osoby informujú notifikujúci orgán:
  - a) o všetkých certifikátoch Únie o posúdení technickej dokumentácie, všetkých dodatkoch k týmto certifikátom a schváleniach systémov riadenia kvality vydaných v súlade s požiadavkami prílohy VII;
  - b) o všetkých zamietnutiach, obmedzeniach platnosti, pozastaveniach platnosti alebo stiahnutiach certifikátov Únie o posúdení technickej dokumentácie alebo schválení systémov riadenia kvality vydaných v súlade s požiadavkami prílohy VII;
  - c) o všetkých okolnostiach, ktoré majú vplyv na rozsah alebo podmienky notifikácie;



- d) o každej žiadosti o informácie, ktorú dostali od orgánov dohľadu nad trhom v súvislosti s činnosťami posudzovania zhody;
  - e) na požiadanie o činnostiach posudzovania zhody vykonaných v rozsahu ich notifikácie a o akejkoľvek inej vykonanej činnosti vrátane cezhraničných činností a zadávania činností subdodávateľom.
2. Každá notifikovaná osoba informuje ostatné notifikované osoby o:
- a) schváleniach systémov riadenia kvality, ktoré zamietla, ktorých platnosť pozastavila alebo ktoré stiahla, a na požiadanie o schváleniach systémov kvality, ktoré vydala;
  - b) certifikátoch EÚ o posúdení technickej dokumentácie alebo ich dodatkoch, ktoré zamietla, stiahla, ktorých platnosť pozastavila alebo inak obmedzila, a na požiadanie o certifikátoch a/alebo ich dodatkoch, ktoré vydala.
3. Každá notifikovaná osoba poskytne ostatným notifikovaným osobám, ktoré vykonávajú podobné činnosti posudzovania zhody vzťahujúce sa na rovnaké technológie umelej inteligencie, relevantné informácie o otázkach týkajúcich sa negatívnych a na požiadanie aj pozitívnych výsledkov posudzovania zhody.

#### *Článok 47*

##### *Výnimka z postupu posudzovania zhody*

1. Odchyľne od článku 43 môže každý orgán dohľadu nad trhom z výnimočných dôvodov verejnej bezpečnosti alebo ochrany života a zdravia osôb, ochrany životného prostredia a ochrany kľúčových priemyselných a infraštruktúrnych aktív povoliť uvedenie špecifických vysokorizikových systémov umelej inteligencie na trh alebo do prevádzky na území dotknutého členského štátu. Toto povolenie sa udelí na obmedzené obdobie, kým sa vykonávajú potrebné postupy posudzovania zhody, a po ukončení týchto postupov sa jeho platnosť končí. Uvedené postupy sa ukončia bez zbytočného odkladu.
2. Povolenie uvedené v odseku 1 sa vydá len vtedy, ak orgán dohľadu nad trhom dospeje k záveru, že vysokorizikový systém umelej inteligencie spĺňa požiadavky kapitoly 2 tejto hlavy. O každom povolení vydanom podľa odseku 1 informuje orgán dohľadu nad trhom Komisiu a ostatné členské štáty.
3. Ak žiaden členský štát ani Komisia do 15 kalendárnych dní od prijatia informácií uvedených v odseku 2 nevznesú námietku proti povoleniu vydanému orgánom dohľadu na trhom členského štátu v súlade s odsekom 1, toto povolenie sa považuje za opodstatnené.
4. Ak do 15 kalendárnych dní od prijatia oznámenia uvedeného v odseku 2 členský štát vznesie námietky proti povoleniu vydanému orgánom dohľadu nad trhom iného členského štátu alebo ak sa Komisia domnieva, že povolenie je v rozpore s právnymi predpismi Únie alebo že záver členských štátov, pokiaľ ide o súlad systému uvedeného v odseku 2, je neopodstatnený, Komisia bezodkladne začne konzultácie s príslušným členským štátom; s príslušným prevádzkovateľom (prevádzkovateľmi) sa vedú konzultácie a má možnosť vyjadriť svoje stanovisko. Vzhľadom na to Komisia rozhodne, či je povolenie opodstatnené alebo nie. Svoje rozhodnutie Komisia oznámi dotknutému členskému štátu a príslušnému prevádzkovateľovi, príp. prevádzkovateľom.

5. Ak sa povolenie považuje za neopodstatnené, orgán dohľadu nad trhom dotknutého členského štátu ho stiahne.
6. Odchyľne od odsekov 1 až 5 sa v prípade vysokorizikových systémov umelej inteligencie určených na používanie ako bezpečnostné komponenty zariadení, na ktoré sa vzťahuje nariadenie (EÚ) 2017/745 a nariadenie (EÚ) 2017/746, alebo ktoré sú samy takýmito zariadeniami, článok 59 nariadenia (EÚ) 2017/745 a článok 54 nariadenia (EÚ) 2017/746 uplatňujú aj vzhľadom na výnimku z posudzovania zhody, pokiaľ ide o súlad s požiadavkami stanovenými v kapitole 2 tejto hlavy.

#### *Článok 48* *EÚ vyhlásenie o zhode*

1. Pre každý systém umelej inteligencie poskytovateľ vyhotoví EÚ vyhlásenie o zhode v písomnej podobe, ktoré desať rokov po uvedení systému umelej inteligencie na trh alebo do prevádzky uchováva k dispozícii pre potreby príslušných vnútroštátnych orgánov. V EÚ vyhlásení o zhode musí byť uvedený systém umelej inteligencie, pre ktorý bolo vyhotovené. Na požiadanie sa kópia EÚ vyhlásenia o zhode poskytne príslušným vnútroštátnym orgánom.
2. V EÚ vyhlásení o zhode sa uvedie, že príslušný vysokorizikový systém umelej inteligencie spĺňa požiadavky stanovené v kapitole 2 tejto hlavy. EÚ vyhlásenie o zhode musí obsahovať informácie uvedené v prílohe V a musí byť preložené do toho úradného jazyka alebo tých úradných jazykov Únie, ktoré sú požadované v členských štátoch, kde sa vysokorizikový systém umelej inteligencie sprístupňuje.
3. Ak sa na vysokorizikové systémy umelej inteligencie vzťahujú ďalšie harmonizačné právne predpisy Únie, v ktorých sa takisto vyžaduje EÚ vyhlásenie o zhode, vyhotoví sa vo vzťahu k všetkým právnym predpisom Únie uplatniteľným na daný vysokorizikový systém umelej inteligencie jedno EÚ vyhlásenie o zhode. Toto vyhlásenie musí obsahovať všetky informácie potrebné na to, aby bolo možné identifikovať harmonizačné právne predpisy Únie, na ktoré sa vyhlásenie vzťahuje.
4. Vypracovaním EÚ vyhlásenia o zhode poskytovateľ preberá zodpovednosť za splnenie požiadaviek stanovených v kapitole 2 tejto hlavy. Poskytovateľ EÚ vyhlásenie o zhode podľa potreby aktualizuje.
5. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 73 na účely aktualizácie obsahu EÚ vyhlásenia o zhode stanoveného v prílohe V s cieľom zaviesť prvky, ktorých potreba vznikne vzhľadom na technický pokrok.

#### *Článok 49* *Označenie zhody CE*

1. Označenie CE sa na vysokorizikové systémy umelej inteligencie umiestni tak, aby bolo viditeľné, čitateľné a neodstrániteľné. Ak to nie je možné alebo odôvodnené z hľadiska povahy vysokorizikového systému umelej inteligencie, označenie sa umiestni na obale alebo prípadne v sprievodnej dokumentácii.
2. Označenie CE uvedené v odseku 1 tohto článku podlieha všeobecným zásadám stanoveným v článku 30 nariadenia (ES) č. 765/2008.
3. V relevantných prípadoch za označením CE nasleduje identifikačné číslo notifikovanej osoby zodpovednej za postupy posudzovania zhody stanovené v článku 43. Identifikačné číslo sa uvedie aj v akomkoľvek reklamnom materiáli, v ktorom sa

nachádza informácia, že vysokorizikový systém umelej inteligencie spĺňa požiadavky na označenie CE.

#### *Článok 50* *Uchovávanie dokumentov*

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

- a) technickú dokumentáciu uvedenú v článku 11;
- b) dokumentáciu týkajúcu sa systému riadenia kvality uvedenú v článku 17,
- c) dokumentáciu týkajúcu sa prípadných zmien schválených notifikovanými osobami;
- d) prípadné rozhodnutia a iné dokumenty vydané notifikovanými osobami;
- e) EÚ vyhlásenie o zhode uvedené v článku 48.

#### *Článok 51* *Registrácia*

Pred uvedením vysokorizikového systému umelej inteligencie podľa článku 6 ods. 2 na trh alebo do prevádzky poskytovateľ alebo prípadne jeho splnomocnený zástupca zaregistruje tento systém v databáze EÚ uvedenej v článku 60.

### **HLAVA IV**

## **POVINNOSTI TRANSPARENTNOSTI PRE URČITÉ SYSTÉMY UMELEJ INTELIGENCIE**

#### *Článok 52* *Povinnosti transparentnosti pre určité systémy umelej inteligencie*

1. Poskytovatelia zabezpečia, aby systémy umelej inteligencie určené na interakciu s fyzickými osobami boli koncipované a vyvinuté tak, aby boli fyzické osoby informované o tom, že komunikujú so systémom umelej inteligencie, pokiaľ to nie je zrejmé z okolností a kontextu používania. Táto povinnosť sa nevzťahuje na systémy umelej inteligencie, ktoré sa podľa zákona môžu používať na odhaľovanie, prevenciu, vyšetrovanie a stíhanie trestných činov, pokiaľ tieto systémy nie sú sprístupnené verejnosti na oznamovanie trestných činov.
2. Používatelia systému na rozpoznávanie emócií alebo systému biometrickej kategorizácie musia o prevádzke takéhoto systému informovať fyzické osoby, ktoré sú mu vystavené. Táto povinnosť sa nevzťahuje na systémy umelej inteligencie používané na biometrickú kategorizáciu, ktoré sa podľa zákona môžu používať na odhaľovanie, prevenciu a vyšetrovanie trestných činov.
3. Používatelia systému umelej inteligencie, ktorý vytvára obrazový, zvukový obsah alebo videoobsah, alebo s takýmto obsahom manipuluje, pričom tento obsah sa zjavne podobá existujúcim osobám, predmetom, miestam alebo iným subjektom či udalostiam a niektorým osobám by sa mohol mylne javiť ako pravý alebo pravdivý („deepfake“), musia informovať, že tento obsah bol umelo vytvorený alebo zmanipulovaný.

Prvý pododsek sa však neuplatňuje, ak toto použitie povoľuje zákon na odhaľovanie, prevenciu, vyšetrovanie a stíhanie trestných činov alebo je nevyhnutné na výkon práva na slobodu prejavu a práva na slobodu umenia a vedeckého bádania, ktoré sú zaručené Chartou základných práv EÚ, a pod podmienkou primeraných záruk pre práva a slobody tretích strán.

4. Odsekmi 1, 2 a 3 nie sú dotknuté požiadavky a povinnosti stanovené v hlave III tohto nariadenia.

## HLAVA V

### OPATRENIA NA PODPORU INOVÁCIÍ

#### Článok 53

##### *Experimentálne regulačné prostredia pre umelú inteligenciu*

1. Experimentálne regulačné prostredia pre umelú inteligenciu zriadené jedným alebo viacerými príslušnými orgánmi členských štátov alebo európskym dozorným úradníkom pre ochranu údajov musia poskytovať kontrolované prostredie, ktoré na obmedzený čas pred uvedením inovačných systémov umelej inteligencie na trh alebo do prevádzky podľa konkrétneho plánu uľahčuje ich vývoj, testovanie a validáciu. Uskutočňuje sa to pod priamym dohľadom a vedením príslušných orgánov s cieľom zabezpečiť súlad s požiadavkami tohto nariadenia a prípadne s inými právnymi predpismi Únie a členských štátov, nad ktorým sa v rámci regulačného prostredia vykonáva dohľad.
2. Pokiaľ inovačné systémy umelej inteligencie spracúvajú osobné údaje alebo na inom základe podliehajú dohľadu ďalších vnútroštátnych orgánov alebo príslušných orgánov, ktoré poskytujú alebo podporujú prístup k údajom, členské štáty zabezpečia, aby do prevádzky experimentálneho regulačného prostredia pre umelú inteligenciu boli zapojené vnútroštátne orgány na ochranu údajov a ďalšie vnútroštátne orgány.
3. Právomoci príslušných orgánov v oblasti dohľadu a nápravy nie sú experimentálnymi regulačnými prostriedkami pre umelú inteligenciu dotknuté. Akékoľvek významné riziká pre zdravie a bezpečnosť, ako aj pre základné práva, ktoré sa zistia počas vývoja a testovania takýchto systémov, musia mať za následok okamžité zmiernenie rizík, a ak to nie je možné, pozastavenie procesu vývoja a testovania, až kým k takémuto zmierneniu nedôjde.
4. Účastníci experimentálneho regulačného prostredia pre umelú inteligenciu sú podľa uplatniteľných právnych predpisov Únie a členských štátov týkajúcich sa zodpovednosti zodpovední za akúkoľvek škodu spôsobenú tretím stranám v dôsledku experimentov, ktoré sa v takomto prostredí uskutočňujú.
5. Príslušné orgány členských štátov, ktoré experimentálne regulačné prostredia pre umelú inteligenciu zriadili, koordinujú svoje činnosti a spolupracujú v rámci Európskej rady pre umelú inteligenciu. O výsledkoch zavádzania uvedených systémov predkladajú Európskej rade pre umelú inteligenciu a Komisii výročné správy, v ktorých uvedú osvedčené postupy, získané skúsenosti a odporúčania týkajúce sa štruktúry systémov a prípadne aj uplatňovania tohto nariadenia a iných právnych predpisov Únie, nad ktorým sa v rámci regulačného prostredia vykonáva dohľad.

6. Spôsoby a podmienky fungovania experimentálnych regulačných prostredí pre umelú inteligenciu vrátane kritérií oprávnenosti a postupu podávania žiadostí, výberu, účasti a ukončenia účasti v takomto prostredí, ako aj práva a povinnosti účastníkov sa stanovujú vo vykonávacích aktoch. Uvedené vykonávacie akty sa prijímajú v súlade s postupom preskúmania uvedeným v článku 74 ods. 2.

#### *Článok 54*

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

1. Osobné údaje zákonne zozbierané na iné účely sa v experimentálnom regulačnom prostredí pre umelú inteligenciu spracúvajú na účely vývoja a testovania určitých inovačných systémov umelej inteligencie v regulačnom prostredí za týchto podmienok:
  - a) inovačné systémy umelej inteligencie sa vyvíjajú na ochranu významného verejného záujmu v jednej alebo viacerých z týchto oblastí:
    - i) predchádzanie trestným činom, ich vyšetrovanie, odhaľovanie alebo stíhanie, alebo výkon trestných sankcií vrátane ochrany pred ohrozením verejnej bezpečnosti a predchádzania takémuto ohrozeniu pod kontrolou a v zodpovednosti príslušných orgánov. Spracovanie prebieha podľa právnych predpisov členského štátu alebo Únie;
    - ii) verejná bezpečnosť a verejné zdravie vrátane prevencie, kontroly a liečby chorôb;
    - iii) vysoká úroveň ochrany životného prostredia a zlepšovanie jeho kvality;
  - b) spracúvané údaje sú potrebné na splnenie jednej alebo viacerých požiadaviek uvedených v hlave III kapitole 2, ak tieto požiadavky nie je možné účinne splniť spracovaním anonymizovaných, syntetických alebo iných ako osobných údajov;
  - c) existujú účinné mechanizmy monitorovania umožňujúce zistiť, či počas experimentovania v regulačných prostrediach môžu vzniknúť vysoké riziká pre základné práva dotknutých osôb, ako aj mechanizmus reakcie na rýchle zmiernenie týchto rizík a v prípade potreby na zastavenie spracúvania;
  - d) všetky osobné údaje, ktoré sa majú spracúvať v rámci regulačného prostredia, sú vo funkčne oddelenom, izolovanom a chránenom prostredí spracovania údajov pod kontrolou účastníkov a prístup k týmto údajom majú len oprávnené osoby;
  - e) spracúvané osobné údaje sa nezasielajú ani neprenášajú iným stranám, a tieto strany k nim ani nemajú prístup na inom základe;
  - f) spracovanie osobných údajov v rámci regulačného prostredia nevedie k opatreniam alebo rozhodnutiam, ktoré majú vplyv na dotknuté osoby;
  - g) všetky osobné údaje spracúvané v rámci regulačného prostredia sa po ukončení účasti v regulačnom prostredí alebo po skončení obdobia uchovávanía osobných údajov vymažú;
  - h) logy zo spracovania osobných údajov v rámci regulačného prostredia sa uchovávajú počas trvania účasti v regulačnom prostredí a 1 rok po jej ukončení, a to výlučne na účely plnenia povinností týkajúcich sa

zodpovednosti a vedenia dokumentácie podľa tohto článku alebo iných uplatniteľných právnych predpisov Únie alebo členských štátov a len tak dlho, ako je to na plnenie týchto povinností potrebné;

- i) ako súčasť technickej dokumentácie podľa prílohy IV sa spolu s výsledkami testovania uchováva úplný a podrobný opis procesu a dôvodov tréovania, testovania a validácie systému umelej inteligencie;
  - j) na webovom sídle príslušných orgánov sa zverejní krátke zhrnutie projektu umelej inteligencie vyvinutého v regulačnom prostredí, jeho cieľov a očakávaných výsledkov.
2. Odsekom 1 nie sú dotknuté právne predpisy Únie alebo členských štátov, ktoré vylučujú spracovanie na iné účely, než sú v nich výslovne uvedené.

#### *Článok 55*

##### *Opatrenia pre malých poskytovateľov a používateľov*

1. Členské štáty prijímú tieto opatrenia:
  - a) malým poskytovateľom a startupom poskytnú prednostný prístup k experimentálnym regulačným prostriediam pre umelú inteligenciu, pokiaľ spĺňajú podmienky oprávnenosti;
  - b) organizujú osobitné činnosti na zvyšovanie informovanosti o uplatňovaní tohto nariadenia prispôsobené potrebám malých poskytovateľov a používateľov;
  - c) v prípade potreby vytvoria vyhradený kanál na komunikáciu s malými poskytovateľmi a používateľmi, ako aj s ďalšími inovátormi s cieľom poskytovať usmernenia a odpovedať na otázky týkajúce sa vykonávania tohto nariadenia.
2. Pri stanovovaní poplatkov za posudzovanie zhody podľa článku 43 sa zohľadnia osobitné záujmy a potreby malých poskytovateľov tak, že sa tieto poplatky znížia úmerne k ich veľkosti a veľkosti ich trhu.

## **HLAVA VI**

### **SPRÁVA A RIADENIE**

#### **KAPITOLA 1**

##### **EURÓPSKA RADA PRE UMELÚ INTELIGENCIU**

#### *Článok 56*

##### *Zriadenie Európskej rady pre umelú inteligenciu*

1. Zriaďuje sa Európska rada pre umelú inteligenciu (ďalej len „rada pre umelú inteligenciu“).
2. Táto rada pre umelú inteligenciu poskytuje Komisii poradenstvo a pomoc s cieľom:
  - a) prispievať k účinnej spolupráci vnútroštátnych dozorných orgánov a Komisie, pokiaľ ide o záležitosti, na ktoré sa vzťahuje toto nariadenie;

- b) koordinovať a prispievať k usmerneniam a analýze, ktoré poskytujú Komisia a vnútroštátne dozorné orgány, ako aj ďalšie príslušné orgány k problémom vznikajúcim na vnútornom trhu v súvislosti so záležitosťami, na ktoré sa vzťahuje toto nariadenie;
- c) pomáhať vnútroštátnym dozorným orgánom a Komisii pri zabezpečovaní konzistentného uplatňovania tohto nariadenia.

#### Článok 57

##### *Štruktúra rady pre umelú inteligenciu*

1. Rada pre umelú inteligenciu pozostáva z vnútroštátnych dozorných orgánov, ktoré sú zastúpené vedúcimi alebo rovnocennými vysokopostavenými úradníkmi týchto orgánov, a z európskeho dozorného úradníka pre ochranu údajov. Na zasadnutia môžu byť prizvané iné vnútroštátne orgány, ak sú pre ne prerokúvané otázky relevantné.
2. Rada pre umelú inteligenciu prijme svoj rokovací poriadok jednoduchou väčšinou hlasov svojich členov po odsúhlasení Komisiou. Rokovací poriadok musí obsahovať aj operačné aspekty súvisiace s plnením úloh rady pre umelú inteligenciu uvedených v článku 58. Na účely preskúmania konkrétnych otázok môže rada pre umelú inteligenciu podľa potreby zriaďovať podskupiny.
3. Rade pre umelú inteligenciu predsedá Komisia. Komisia zvoláva zasadnutia a pripravuje program v súlade s úlohami rady pre umelú inteligenciu podľa tohto nariadenia a s rokovacím poriadkom rady pre umelú inteligenciu. Činnosti rady pre umelú inteligenciu podľa tohto nariadenia poskytuje Komisia administratívnu a analytickú podporu.
4. Rada pre umelú inteligenciu môže k účasti na svojich zasadnutiach prizývať externých odborníkov a pozorovateľov a môže uskutočňovať výmeny informácií so zainteresovanými tretími stranami s cieľom využiť ich v primeranom rozsahu pri svojich činnostiach. Na tento účel môže Komisia poskytovať podporu pri výmenách informácií medzi radou pre umelú inteligenciu a inými orgánmi, úradmi, agentúrami a poradnými skupinami Únie.

#### Článok 58

##### *Úlohy rady pre umelú inteligenciu*

Pri poskytovaní poradenstva a pomoci Komisii v kontexte článku 56 ods. 2 plní rada pre umelú inteligenciu najmä tieto úlohy:

- a) zhromažďovanie a výmena odborných znalostí a najlepších postupov medzi členskými štátmi;
- b) prispievanie k jednotným administratívnym postupom v členských štátoch, a to aj pokiaľ ide o fungovanie regulačných prostredí uvedených v článku 53;
- c) vydávanie stanovísk, odporúčaní alebo písomných príspevkov k otázkam týkajúcim sa vykonávania tohto nariadenia, najmä
  - i) k technickým špecifikáciám alebo existujúcim normám v súvislosti s požiadavkami stanovenými v hlave III kapitole 2;
  - ii) k používaniu harmonizovaných noriem alebo spoločných špecifikácií uvedených v článkoch 40 a 41;

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

## KAPITOLA 2

### PRÍSLUŠNÉ VNÚTROŠTÁTNE ORGÁNY

#### Článok 59

#### *Určenie príslušných vnútroštátnych orgánov*

1. Na účely zabezpečenia uplatňovania a vykonávania tohto nariadenia každý členský štát zriadi alebo určí príslušné vnútroštátne orgány. Príslušné vnútroštátne orgány majú takú organizačnú štruktúru, aby zabezpečili objektivitu a nestrannosť vykonávania svojich činností a úloh.
2. Spomedzi príslušných vnútroštátnych orgánov každý členský štát určí vnútroštátny dozorný orgán. Pokiaľ členský štát nemá organizačné a administratívne dôvody na určenie viac ako jedného orgánu, koná vnútroštátny dozorný orgán ako notifikujúci orgán a orgán dohľadu nad trhom.
3. Členské štáty informujú Komisiu o orgáne, príp. orgánoch, ktoré určili, a prípadne o dôvodoch na určenie viac ako jedného orgánu.
4. Členské štáty zabezpečia, aby príslušné vnútroštátne orgány mali na plnenie svojich úloh podľa tohto nariadenia k dispozícii primerané finančné a ľudské zdroje. Príslušné vnútroštátne orgány musia mať predovšetkým neustále k dispozícii dostatočný počet zamestnancov, ktorých spôsobilosti a odborné znalosti zahŕňajú dôkladné pochopenie technológií umelej inteligencie, údajov a ich spracovania, základných práv, zdravotných a bezpečnostných rizík a znalosť existujúcich noriem a právnych požiadaviek.
5. Členské štáty každoročne podávajú Komisii správu o stave finančných a ľudských zdrojov príslušných vnútroštátnych orgánov spolu s posúdením ich primeranosti. Komisia tieto informácie postúpi rade pre umelú inteligenciu na prerokovanie a prípadné odporúčania.
6. Komisia podporuje výmenu skúseností medzi príslušnými vnútroštátnymi orgánmi.
7. Príslušné vnútroštátne orgány môžu poskytovať usmernenia a poradenstvo týkajúce sa vykonávania tohto nariadenia, a to aj malým poskytovateľom. Vždy, keď príslušné vnútroštátne orgány zamýšľajú poskytnúť usmernenia a poradenstvo v súvislosti so systémom umelej inteligencie v oblastiach, na ktoré sa vzťahujú iné právne predpisy Únie, podľa potreby uskutočnia konzultácie s vnútroštátnymi orgánmi, ktoré sú príslušné podľa uvedených právnych predpisov Únie. Členské štáty môžu takisto zriadiť jedno centrálné kontaktné miesto na komunikáciu s prevádzkovateľmi.
8. Pokiaľ do rozsahu pôsobnosti tohto nariadenia spadajú inštitúcie, agentúry a orgány Únie, koná ako príslušný orgán pre dohľad nad nimi európsky dozorný úradník pre ochranu údajov.



## HLAVA VII

### DATABÁZA EÚ PRE SAMOSTATNÉ VYSOKORIZIKOVÉ SYSTÉMY UMELEJ INTELIGENCIE

#### Článok 60

##### *Databáza EÚ pre samostatné vysokorizikové systémy umelej inteligencie*

1. Komisia v spolupráci s členskými štátmi zriadi a spravuje databázu EÚ obsahujúcu informácie uvedené v odseku 2 týkajúce sa vysokorizikových systémov umelej inteligencie uvedených v článku 6 ods. 2, ktoré sú registrované v súlade s článkom 51.
2. Údaje uvedené v prílohe VIII vkladajú do databázy EÚ poskytovatelia. Komisia im poskytuje technickú a administratívnu podporu.
3. Informácie obsiahnuté v databáze EÚ sú prístupné verejnosti.
4. Osobné údaje obsahuje databáza EÚ len v rozsahu nevyhnutnom na zber a spracovanie informácií v súlade s týmto nariadením. Súčasťou týchto informácií sú mená a kontaktné údaje fyzických osôb, ktoré sú zodpovedné za registráciu systémov a majú právomoc zastupovať poskytovateľa.
5. Prevádzkovateľom databázy EÚ je Komisia. Zabezpečuje aj primeranú technickú a administratívnu podporu poskytovateľov.

## HLAVA VIII

### MONITOROVANIE PO UVEDENÍ NA TRH, VÝMENA INFORMÁCIÍ, DOHLAD NAD TRHOM

#### KAPITOLA 1

##### MONITOROVANIE PO UVEDENÍ NA TRH

#### Článok 61

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

1. Poskytovatelia zavedú a zdokumentujú systém monitorovania po uvedení na trh spôsobom, ktorý je primeraný povahe technológií umelej inteligencie a rizikám vysokorizikového systému umelej inteligencie.
2. Systém monitorovania po uvedení na trh musí aktívne a systematicky zbierať, dokumentovať a analyzovať relevantné údaje o výkonnosti vysokorizikových systémov umelej inteligencie počas celej ich životnosti poskytnuté používateľmi alebo zozbierané z iných zdrojov a umožňovať poskytovateľovi hodnotiť nepretržitý súlad systémov umelej inteligencie s požiadavkami stanovenými v hlave III kapitole 2.
3. Systém monitorovania po uvedení na trh sa musí zakladať na pláne monitorovania po uvedení na trh. Plán monitorovania po uvedení na trh tvorí súčasť technickej

dokumentácie uvedenej v prílohe IV. Komisia prijme vykonávací akt, v ktorom stanoví podrobné ustanovenia, ktorými sa vytvorí vzor plánu monitorovania po uvedení na trh a zoznam prvkov, ktoré sa majú do plánu zahrnúť.

4. V prípade vysokorizikových systémov umelej inteligencie, na ktoré sa vzťahujú právne akty uvedené v prílohe II a pre ktoré sú systém a plán monitorovania po uvedení na trh už zavedené podľa uvedených právnych predpisov, sa prvky opísané v odsekoch 1, 2 a 3 podľa potreby začlenia do tohto systému a plánu.

Prvý pododsek sa uplatňuje aj na vysokorizikové systémy umelej inteligencie uvedené v bode 5 písm. b) prílohy III uvádzané na trh alebo do prevádzky úverovými inštitúciami regulovanými smernicou 2013/36/EÚ.

## KAPITOLA 2

### VÝMENA INFORMÁCIÍ O INCIDENTOCH A PORUCHÁCH

#### Článok 62

##### *Podávanie správ o závažných incidentoch a poruchách*

1. Poskytovatelia vysokorizikových systémov umelej inteligencie uvedených na trh Únie podávajú o akomkoľvek závažnom incidente alebo poruche týchto systémov, ktorá predstavuje porušenie povinností podľa právnych predpisov Únie určených na ochranu základných práv, správy orgánom dohľadu nad trhom členských štátov, v ktorých k tomuto závažnému incidentu alebo porušeniu povinností došlo.

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

2. Po prijatí oznámenia týkajúceho sa porušenia povinností podľa právnych predpisov Únie určených na ochranu základných práv orgán dohľadu nad trhom informuje vnútroštátne orgány verejnej moci alebo subjekty uvedené v článku 64 ods. 3. Na uľahčenie plnenia povinností stanovených v odseku 1 vypracuje Komisia osobitné usmernenia. Tieto usmernenia sa vydajú najneskôr 12 mesiacov po nadobudnutí účinnosti tohto nariadenia.
3. V prípade vysokorizikových systémov umelej inteligencie uvedených v bode 5 písm. b) prílohy III uvádzaných na trh alebo do prevádzky poskytovateľmi, ktorí sú úverovými inštitúciami regulovanými smernicou 2013/36/EÚ, a v prípade vysokorizikových systémov umelej inteligencie, ktoré sú bezpečnostnými komponentmi zariadení alebo sú samy zariadeniami a na ktoré sa vzťahuje nariadenie (EÚ) 2017/745 a nariadenie (EÚ) 2017/746, sa oznamovanie závažných incidentov alebo porúch obmedzuje na tie incidenty alebo poruchy, ktoré predstavujú porušenie povinností podľa právnych predpisov Únie určených na ochranu základných práv.

## KAPITOLA 3

### PRESADZOVANIE PRÁVA

#### Článok 63

##### *Dohľad nad trhom a kontrola systémov umelej inteligencie na trhu Únie*

1. Na systémy umelej inteligencie v rozsahu pôsobnosti tohto nariadenia sa vzťahuje nariadenie (EÚ) 2019/1020. Na účely účinného presadzovania tohto nariadenia sa však:
  - a) každý odkaz na hospodársky subjekt podľa nariadenia (EÚ) 2019/1020 chápe tak, že zahŕňa všetkých prevádzkovateľov uvedených v hlave III kapitole 3 tohto nariadenia;
  - b) každý odkaz na výrobok podľa nariadenia (EÚ) 2019/1020 chápe tak, že zahŕňa všetky systémy umelej inteligencie, ktoré patria do rozsahu pôsobnosti tohto nariadenia.
2. O výsledkoch príslušných činností dohľadu nad trhom podáva vnútroštátny dozorný orgán pravidelne správy Komisii. Všetky informácie zistené v priebehu činností dohľadu nad trhom, ktoré by mohli mať potenciálny význam pre uplatňovanie právnych predpisov Únie o pravidlách hospodárskej súťaže, národný dozorný orgán bezodkladne oznámi Komisii a príslušným vnútroštátnym orgánom na ochranu hospodárskej súťaže.
3. V prípade vysokorizikových systémov umelej inteligencie súvisiacich s výrobkami, na ktoré sa vzťahujú právne akty uvedené v oddiele A prílohy II, je orgánom dohľadu nad trhom na účely tohto nariadenia orgán zodpovedný za činnosti dohľadu nad trhom určený podľa uvedených právnych aktov.
4. V prípade systémov umelej inteligencie, ktoré uvádzajú na trh, do prevádzky alebo používajú finančné inštitúcie regulované právnymi predpismi Únie o finančných službách, je orgánom dohľadu nad trhom na účely tohto nariadenia príslušný orgán zodpovedný za finančný dohľad nad týmito inštitúciami podľa uvedených právnych predpisov.
5. V prípade systémov umelej inteligencie uvedených v bode 1 písm. a) a pokiaľ sa tieto systémy používajú na účely presadzovania práva podľa bodov 6 a 7 prílohy III, určia členské štáty ako orgány dohľadu nad trhom na účely tohto nariadenia buď príslušné dozorné orgány pre ochranu údajov podľa smernice (EÚ) 2016/680 alebo nariadenia 2016/679, alebo príslušné vnútroštátne orgány vykonávajúce dohľad nad činnosťami orgánov presadzovania práva, imigračných alebo azylových orgánov, ktoré tieto systémy uvádzajú do prevádzky alebo používajú.
6. Pokiaľ do rozsahu pôsobnosti tohto nariadenia spadajú inštitúcie, agentúry a orgány Únie, koná ako ich orgán pre dohľad nad trhom európsky dozorný úradník pre ochranu údajov.
7. Členské štáty podporujú koordináciu medzi orgánmi dohľadu nad trhom určenými podľa tohto nariadenia a inými príslušnými vnútroštátnymi orgánmi alebo subjektmi, ktoré vykonávajú dohľad nad uplatňovaním harmonizačných právnych predpisov Únie uvedených v prílohe II alebo iných právnych predpisov Únie, ktoré by mohli byť relevantné pre vysokorizikové systémy umelej inteligencie uvedené v prílohe III.

*Článok 64*  
*Prístup k údajom a dokumentácii*

1. Orgánom dohľadu nad trhom sa v rámci ich činností poskytne úplný prístup k súborom tréningových, validačných a testovacích údajov, ktoré používa poskytovateľ, a to aj prostredníctvom aplikačných programovacích rozhraní (*application programming interfaces* – API) alebo iných vhodných technických prostriedkov a nástrojov umožňujúcich diaľkový prístup.
2. Ak je to potrebné na posúdenie zhody vysokorizikového systému umelej inteligencie s požiadavkami stanovenými v hlave III kapitole 2, a na základe odôvodnenej žiadosti sa orgánom dohľadu nad trhom udelí prístup k zdrojovému kódu systému umelej inteligencie.
3. Vnútroštátne orgány verejnej moci alebo subjekty, ktoré dohliadajú na dodržiavanie povinností podľa právnych predpisov Únie na ochranu základných práv v súvislosti s používaním vysokorizikových systémov umelej inteligencie uvedených v prílohe III alebo dodržiavanie týchto povinností presadzujú, majú právomoc požadovať akúkoľvek dokumentáciu vytvorenú alebo udržiavanú podľa tohto nariadenia a mať k nej prístup, ak je prístup k tejto dokumentácii potrebný na plnenie právomocí v rámci ich mandátu a jurisdikcie. O každej takejto žiadosti príslušný orgán verejnej moci alebo subjekt informuje orgán dohľadu nad trhom dotknutého členského štátu.
4. Do 3 mesiacov od nadobudnutia účinnosti tohto nariadenia každý členský štát určí orgány verejnej moci alebo subjekty uvedené v odseku 3 a ich zoznam zverejní na webovom sídle vnútroštátneho dozorného orgánu. Tento zoznam členské štáty oznámia Komisii a všetkým ostatným členským štátom a udržujú ho v aktuálnom stave.
5. Ak dokumentácia uvedená v odseku 3 nepostačuje na zistenie toho, či došlo k porušeniu povinností podľa právnych predpisov Únie určených na ochranu základných práv, orgán verejnej moci alebo subjekt uvedený v odseku 3 môže orgánu dohľadu nad trhom predložiť odôvodnenú žiadosť, aby zorganizoval testovanie vysokorizikového systému umelej inteligencie technickými prostriedkami. Orgán dohľadu nad trhom zorganizuje testovanie v primeranom čase od podania žiadosti v úzkej spolupráci so žiadajúcim orgánom verejnej moci alebo subjektom.
6. So všetkými informáciami a s dokumentáciou, ktoré vnútroštátne orgány verejnej moci alebo subjekty uvedené v odseku 3 získali podľa ustanovení tohto článku, sa zaobchádza v súlade s povinnosťami zachovávaní dôvernosti stanovenými v článku 70.

*Článok 65*  
*Postup zaobchádzania so systémami umelej inteligencie, ktoré predstavujú riziko na vnútroštátnej úrovni*

1. Systémy umelej inteligencie predstavujúce riziko sa chápu ako výrobky predstavujúce riziko vymedzené v článku 3 bode 19 nariadenia (EÚ) 2019/1020, pokiaľ ide o riziká pre zdravie alebo bezpečnosť, alebo pre ochranu základných práv osôb.
2. Ak má orgán dohľadu nad trhom členského štátu dostatočné dôvody domnievať sa, že systém umelej inteligencie predstavuje riziko uvedené v odseku 1, vykoná hodnotenie dotknutého systému umelej inteligencie, pokiaľ ide o jeho súlad so všetkými požiadavkami a povinnosťami stanovenými v tomto nariadení. Ak existujú

riziká pre ochranu základných práv, orgán dohľadu nad trhom informuje aj príslušné vnútroštátne orgány verejnej moci alebo subjekty uvedené v článku 64 ods. 3. S orgánmi dohľadu nad trhom a ostatnými vnútroštátnymi orgánmi verejnej moci alebo subjektmi uvedenými v článku 64 ods. 3 podľa potreby spolupracujú príslušní prevádzkovatelia.

Ak v priebehu uvedeného hodnotenia orgán dohľadu nad trhom zistí, že systém umelej inteligencie nespĺňa požiadavky a povinnosti stanovené v tomto nariadení, bezodkladne požiada príslušného prevádzkovateľa, aby prijal všetky primerané nápravné opatrenia, ktoré vedú k zosúladieniu systému umelej inteligencie s uvedenými požiadavkami a povinnosťami, jeho stiahnutiu z trhu alebo od používateľa v rámci primeranej lehoty úmernej povahy rizika, ktorú môže orgán stanoviť.

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

3. Ak sa orgán dohľadu nad trhom domnieva, že nesúlad s požiadavkami a povinnosťami sa neobmedzuje na územie jeho štátu, informuje Komisiu a ostatné členské štáty o výsledkoch hodnotenia a opatreniach, o ktorých prijatie požiadal prevádzkovateľa.
4. Prevádzkovateľ zabezpečí prijatie všetkých primeraných nápravných opatrení v súvislosti so všetkými dotknutými systémami umelej inteligencie, ktoré sprístupnil na trhu v celej Únii.
5. Ak prevádzkovateľ systému umelej inteligencie v lehote uvedenej v odseku 2 neprijme primerané nápravné opatrenia, orgán dohľadu nad trhom prijme všetky primerané predbežné opatrenia s cieľom zakázať alebo obmedziť sprístupňovanie systému umelej inteligencie na svojom vnútroštátnom trhu, výrobok z uvedeného trhu stiahnuť alebo ho stiahnuť od používateľa. O týchto opatreniach uvedený orgán bezodkladne informuje Komisiu a ostatné členské štáty.
6. Informácie uvedené v odseku 5 musia obsahovať všetky podrobné údaje, ktoré sú k dispozícii, najmä údaje potrebné na identifikáciu nevyhovujúceho systému umelej inteligencie, jeho pôvod, povahu údajného nesúladu a z neho vyplývajúce riziko, povahu a trvanie prijatých vnútroštátnych opatrení a stanoviská, ktoré predložil príslušný prevádzkovateľ. Orgány dohľadu nad trhom musia predovšetkým uviesť, či k nesúladu došlo v dôsledku jedného alebo viacerých z týchto dôvodov:
  - a) systém umelej inteligencie nespĺňa požiadavky stanovené v hlave III kapitole 2;
  - b) existujú nedostatky v harmonizovaných normách alebo spoločných špecifikáciách uvedených v článkoch 40 a 41, ktoré sú základom pre predpoklad zhody.
7. Orgány dohľadu nad trhom členských štátov iné než orgán dohľadu nad trhom členského štátu, ktorý postup začal, bezodkladne oboznámia Komisiu a ostatné členské štáty so všetkými prijatými opatreniami a s akýmikoľvek dodatočnými informáciami týkajúcimi sa nesúladu dotknutého systému umelej inteligencie, ktoré majú k dispozícii, a v prípade, že nesúhlasia s oznámeným vnútroštátnym opatrením, aj so svojimi námietkami.

8. Ak do troch mesiacov od prijatia informácií uvedených v odseku 5 žiaden členský štát ani Komisia nevznesú námietku proti predbežnému opatreniu prijatému členským štátom, opatrenie sa považuje za opodstatnené. Týmto nie sú dotknuté procesné práva dotknutého prevádzkovateľa v súlade s článkom 18 nariadenia (EÚ) 2019/1020.
9. Orgány dohľadu nad trhom všetkých členských štátov zabezpečia, aby sa vo vzťahu k dotknutému výrobku bezodkladne prijali primerané reštriktívne opatrenia, ako je napríklad stiahnutie výrobku z ich trhu.

#### *Článok 66* *Ochranný postup Únie*

1. Ak do troch mesiacov od prijatia oznámenia uvedeného v článku 65 ods. 5 členský štát vznesie námietky proti opatreniu prijatému iným členským štátom alebo ak Komisia pokladá toto opatrenie za také, ktoré je v rozpore s právnymi predpismi Únie, Komisia bezodkladne začne konzultácie s príslušným členským štátom a prevádzkovateľom, príp. prevádzkovateľmi a vnútroštátne opatrenie vyhodnotí. Na základe výsledkov tohto hodnotenia Komisia do deviatich mesiacov od oznámenia uvedeného v článku 65 ods. 5 rozhodne, či je vnútroštátne opatrenie opodstatnené, a oznámi toto rozhodnutie dotknutému členskému štátu.
2. Ak sa vnútroštátne opatrenie považuje za opodstatnené, všetky členské štáty prijímú opatrenia potrebné na zabezpečenie stiahnutia nevyhovujúceho systému umelej inteligencie zo svojho trhu a informujú o nich Komisiu. Ak sa vnútroštátne opatrenie považuje za neopodstatnené, dotknutý členský štát toto opatrenie zruší.
3. Ak sa vnútroštátne opatrenie považuje za opodstatnené a nesúlad systému umelej inteligencie sa pripisuje nedostatkom v harmonizovaných normách alebo spoločných špecifikáciách uvedených v článkoch 40 a 41 tohto nariadenia, Komisia uplatní postup stanovený v článku 11 nariadenia (EÚ) č. 1025/2012.

#### *Článok 67* *Vyhovujúce systémy umelej inteligencie, ktoré predstavujú riziko*

1. Ak po vykonaní hodnotenia podľa článku 65 orgán dohľadu nad trhom členského štátu zistí, že systém umelej inteligencie, ktorý je v súlade s týmto nariadením, napriek tomu predstavuje riziko pre zdravie alebo bezpečnosť osôb, pre dodržiavanie povinností podľa právnych predpisov Únie alebo vnútroštátnych právnych predpisov určených na ochranu základných práv alebo pre iné hľadiská ochrany verejného záujmu, požiada príslušného prevádzkovateľa, aby prijal všetky primerané opatrenia, ktorými sa zabezpečí, aby dotknutý systém umelej inteligencie pri uvedení na trh alebo do prevádzky už takéto riziko nepredstavoval alebo aby v primeranej lehote úmernej povahe rizika, ktorú môže orgán stanoviť, došlo k jeho stiahnutiu z trhu alebo od používateľa.
2. Poskytovateľ alebo iní relevantní prevádzkovatelia v lehote predpísanej orgánom dohľadu nad trhom členského štátu v zmysle odseku 1 zabezpečia prijatie nápravných opatrení v súvislosti so všetkými dotknutými systémami umelej inteligencie, ktoré sprístupnili na trhu v celej únii.
3. Členský štát o tom okamžite informuje Komisiu a ostatné členské štáty. Tieto informácie musia obsahovať všetky podrobnosti, ktoré sú k dispozícii, najmä údaje potrebné na identifikáciu dotknutého systému umelej inteligencie, jeho pôvod

a dodávateľský reťazec, povahu z neho vyplývajúceho rizika a povahu a trvanie prijatých vnútroštátnych opatrení.

4. Komisia začne bezodkladne konzultovať s členskými štátmi a príslušným prevádzkovateľom a prijaté vnútroštátne opatrenia vyhodnotí. Na základe výsledkov tohto hodnotenia Komisia rozhodne, či je opatrenie opodstatnené, a podľa potreby navrhne primerané opatrenia.
5. Rozhodnutie Komisie je určené členským štátom.

#### *Článok 68*

##### *Formálny nesúlad*

1. Orgán dohľadu na trhom členského štátu požiada príslušného prevádzkovateľa o odstránenie predmetného nesúladu, ak dospeje k jednému z týchto zistení:
  - a) označenie zhody bolo umiestnené v rozpore s článkom 49;
  - b) označenie zhody nebolo umiestnené;
  - c) nebolo vyhotovené EÚ vyhlásenie o zhode;
  - d) EÚ vyhlásenie o zhode nebolo vyhotovené správne;
  - e) nebolo umiestnené identifikačné číslo notifikovanej osoby zapojenej v relevantných prípadoch do postupu posudzovania zhody.
2. Ak nesúlad uvedený v odseku 1 pretrváva, dotknutý členský štát prijme všetky náležité opatrenia na obmedzenie alebo zákaz sprístupňovania vysokorizikového systému umelej inteligencie na trhu alebo zabezpečí jeho stiahnutie od používateľa alebo z trhu.

## **HLAVA IX**

### **KÓDEXY SPRÁVANIA**

#### *Článok 69*

##### *Kódexy správania*

1. Komisia a členské štáty nabádajú k vypracúvaniu kódexov správania určených na podporu dobrovoľného uplatňovania požiadaviek stanovených v hlave III kapitole 2 na systémy umelej inteligencie, ktoré nie sú vysokorizikovými systémami umelej inteligencie, na základe technických špecifikácií a riešení, ktoré sú vzhľadom na zamýšľaný účel systémov vhodnými prostriedkami na zabezpečenie súladu s takýmito požiadavkami, a vypracúvanie takýchto kódexov podporujú.
2. Komisia a rada pre umelú inteligenciu nabádajú k vypracúvaniu kódexov správania určených na podporu dobrovoľného uplatňovania požiadaviek týkajúcich sa napríklad environmentálnej udržateľnosti, prístupnosti pre osoby so zdravotným postihnutím, účasti zainteresovaných strán na koncipovaní a vývoji systémov umelej inteligencie a rozmanitosti vývojových tímov na základe jasných cieľov a kľúčových ukazovateľov výkonnosti na meranie dosahovania týchto cieľov, a podporujú vypracúvanie takýchto kódexov.
3. Kódexy správania môžu vypracovať jednotliví poskytovatelia systémov umelej inteligencie alebo organizácie, ktoré ich zastupujú, alebo obaja, a to aj v spolupráci s používateľmi a akýmkoľvek zainteresovanými stranami a organizáciami, ktoré ich

zastupujú. Kódexy správania sa môžu vzťahovať na jeden alebo viacero systémov umelej inteligencie, pričom sa zohľadní podobnosť zamýšľaného účelu príslušných systémov.

4. Komisia a rada pre umelú inteligenciu pri nabádaní k vypracovaniu kódexov správania a jeho podpore zohľadňujú osobitné záujmy a potreby malých poskytovateľov a startupov.

## **HLAVA X**

### **DÔVERNOSŤ A SANKCIE**

#### *Článok 70*

#### *Dôvernosť*

1. Príslušné vnútroštátne orgány a notifikované osoby, ktoré sa zúčastňujú na uplatňovaní tohto nariadenia, musia dodržiavať dôvernosť informácií a údajov získaných pri vykonávaní svojich úloh a činností takým spôsobom, aby chránili najmä:
  - a) práva duševného vlastníctva a dôverné obchodné informácie alebo obchodné tajomstvo fyzickej alebo právnickej osoby vrátane zdrojového kódu, s výnimkou prípadov uvedených v článku 5 smernice 2016/943 o ochrane nesprístupneného know-how a obchodných informácií (obchodného tajomstva) pred ich neoprávneným získaním, využitím a sprístupnením;
  - b) účinné vykonávanie tohto nariadenia, najmä na účely inšpekcií, vyšetrovaní alebo auditov; verejný záujem a záujmy národnej bezpečnosti;
  - c) integritu trestného alebo správneho konania.
2. Bez toho, aby bol dotknutý odsek 1, sa informácie, ktoré sa vymieňajú na dôvernom základe medzi príslušnými vnútroštátnymi orgánmi navzájom a medzi príslušnými vnútroštátnymi orgánmi a Komisiou, nezverejňujú bez predchádzajúcej konzultácie s príslušným vnútroštátnym orgánom, od ktorého pochádzajú, a používateľom, ak vysokorizikové systémy umelej inteligencie uvedené v bodoch 1, 6 a 7 prílohy III používajú orgány presadzovania práva, imigračné alebo azylové orgány a ak by takéto zverejnenie ohrozilo verejný záujem a záujmy národnej bezpečnosti.

Ak sú poskytovateľmi vysokorizikových systémov umelej inteligencie uvedených v bodoch 1, 6 a 7 prílohy III orgány presadzovania práva, imigračné alebo azylové orgány, technická dokumentácia uvedená v prílohe IV musí zostať v priestoroch týchto orgánov. Tieto orgány zabezpečia, aby orgány dohľadu nad trhom uvedené v článku 63 ods. 5 a 6 mali na požiadanie okamžitý prístup k dokumentácii alebo aby okamžite dostali jej kópiu. Prístup k dokumentácii alebo akejkoľvek jej kópii majú len zamestnanci orgánu dohľadu nad trhom, ktorí sú držiteľmi bezpečnostnej previerky na primeranej úrovni.
3. Odsekmi 1 a 2 nie sú dotknuté práva a povinnosti Komisie, členských štátov a notifikovaných osôb, pokiaľ ide o výmenu informácií a šírenie upozornení, ani povinnosti dotknutých strán poskytovať informácie podľa trestného práva členských štátov.
4. Komisia a členské štáty si v prípade potreby môžu vymieňať dôverné informácie s regulačnými orgánmi tretích krajín, s ktorými uzavreli bilaterálne alebo



multilaterálne dohody o zachovaní dôvernosti zaručujúce primeranú úroveň dôvernosti.

### Článok 71 Sankcie

1. Členské štáty v súlade s podmienkami stanovenými v tomto nariadení stanovujú pravidlá týkajúce sa sankcií vrátane správnych pokút, ktoré sa uplatňujú pri porušeníach tohto nariadenia, a prijímajú všetky opatrenia potrebné na zabezpečenie ich riadneho a účinného vykonávania. Stanovené sankcie musia byť účinné, primerané a odrádzajúce. Musia zohľadňovať najmä záujmy malých poskytovateľov a startupov a ich ekonomickú životaschopnosť.
2. Členské štáty o týchto pravidlách a opatreniach informujú Komisiu a bezodkladne jej oznámia každú následnú zmenu, ktorá ich ovplyvní.
3. Správne pokuty až do výšky 30 000 000 EUR, alebo ak je poruшитelom spoločnosť, až do výšky 6 % jej celkového svetového ročného obratu za predchádzajúci účtovný rok, podľa toho, ktorá suma je vyššia, sa ukladajú za tieto porušenia:
  - a) nedodržovanie zákazu praktík v oblasti umelej inteligencie uvedených v článku 5;
  - b) nesúlad systému umelej inteligencie s požiadavkami stanovenými v článku 10.
4. Za nesúlad systému umelej inteligencie s požiadavkami alebo povinnosťami podľa tohto nariadenia, ktoré nie sú stanovené v článkoch 5 a 10, sa ukladajú správne pokuty až do výšky 20 000 000 EUR, alebo ak je poruшитelom spoločnosť, až do výšky 4 % jej celkového svetového ročného obratu za predchádzajúci účtovný rok, podľa toho, ktorá suma je vyššia.
5. Za poskytnutie nesprávnych, neúplných alebo zavádzajúcich informácií v odpovedi na žiadosť notifikovaných osôb a príslušných vnútroštátnych orgánov sa ukladajú správne pokuty až do výšky 10 000 000 EUR, alebo ak je poruшитelom spoločnosť, až do výšky 2 % jej celkového svetového ročného obratu za predchádzajúci účtovný rok, podľa toho, ktorá suma je vyššia.
6. Pri rozhodovaní o výške správnej pokuty sa v každom jednotlivom prípade zohľadnia všetky relevantné okolnosti konkrétnej situácie a náležite sa vezme do úvahy:
  - a) povaha, závažnosť a trvanie porušenia a jeho dôsledkov;
  - b) či už tomu istému prevádzkovateľovi uložili za to isté porušenie správne pokuty iné orgány dohľadu nad trhom;
  - c) veľkosť a trhovú podiel prevádzkovateľa, ktorý sa dopustil porušenia.
7. Každý členský štát stanoví pravidlá, či a v akom rozsahu sa môžu správne pokuty uložiť orgánom verejnej moci a subjektom zriadeným v danom členskom štáte.
8. V závislosti od právneho systému členských štátov sa pravidlá o správnych pokutách môžu uplatňovať tak, aby pokuty podľa pravidiel uplatniteľných v daných členských štátoch ukladali príslušné vnútroštátne súdy alebo iné orgány. Uplatňovanie takýchto pravidiel v uvedených členských štátoch má rovnocenný účinok.

## Článok 72

### *Správne pokuty uložené inštitúciám, agentúram a orgánom Únie*

1. Európsky dozorný úradník pre ochranu údajov môže uložiť správne pokuty inštitúciám, agentúram a orgánom Únie, ktoré patria do rozsahu pôsobnosti tohto nariadenia. Pri rozhodovaní o uložení správnej pokuty a o jej výške sa v každom jednotlivom prípade zohľadnia všetky relevantné okolnosti konkrétnej situácie a náležite sa vezme do úvahy:
  - a) povaha, závažnosť a trvanie porušenia a jeho dôsledkov;
  - b) spolupráca s európskym dozorným úradníkom pre ochranu údajov s cieľom napraviť porušenie a zmierniť možné nepriaznivé účinky porušenia vrátane dodržiavania všetkých opatrení, ktoré predtým nariadil európsky dozorný úradník pre ochranu údajov dotknutej inštitúcii, agentúre alebo dotknutému orgánu Únie v rovnakej veci;
  - c) všetky podobné predchádzajúce porušenia, ku ktorým došlo zo strany inštitúcie, agentúry alebo orgánu Únie.
2. Správne pokuty až do výšky 500 000 EUR sa ukladajú za tieto porušenia:
  - a) nedodržiavanie zákazu praktík v oblasti umelej inteligencie uvedených v článku 5;
  - b) nesúlad systému umelej inteligencie s požiadavkami stanovenými v článku 10.
3. Za nesúlad systému umelej inteligencie s požiadavkami alebo povinnosťami podľa tohto nariadenia, ktoré nie sú stanovené v článkoch 5 a 10, sa ukladajú správne pokuty až do výšky 250 000 EUR.
4. Pred prijatím rozhodnutí podľa tohto článku európsky dozorný úradník pre ochranu údajov poskytne inštitúcii, agentúre alebo orgánu Únie, voči ktorým vedie konanie, príležitosť na vyjadrenie v záležitostiach týkajúcich sa možného porušenia. Európsky dozorný úradník pre ochranu údajov pri svojich rozhodnutiach vychádza len z prvkov a okolností, ku ktorým sa dotknuté strany mohli vyjadriť. Prípadní sťažovatelia sú do konania úzko zapojení.
5. V konaní sa v plnej miere rešpektuje právo dotknutých strán na obhajobu. S výhradou oprávneného záujmu fyzických osôb alebo podnikov na ochrane svojich osobných údajov alebo obchodného tajomstva majú strany právo na prístup k spisu európskeho dozorného úradníka pre ochranu údajov.
6. Prostriedky získané z pokút uložených podľa tohto článku sú príjmom všeobecného rozpočtu Únie.

## HLAVA XI

### DELEGOVANIE PRÁVOMOCI A POSTUP VÝBORU

## Článok 73

### *Vykonávanie delegovania právomoci*

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

2. Delegovanie právomoci uvedené v článku 4, článku 7 ods. 1, článku 11 ods. 3, článku 43 ods. 5 a 6 a článku 48 ods. 5 sa Komisii udeľuje na neurčitý čas odo dňa [nadobudnutia účinnosti nariadenia].
3. Delegovanie právomoci uvedené v článku 4, článku 7 ods. 1, článku 11 ods. 3, článku 43 ods. 5 a 6 a článku 48 ods. 5 môže Európsky parlament alebo Rada kedykoľvek odvolať. Rozhodnutím o odvolaní sa ukončuje delegovanie právomoci, ktoré sa v ňom uvádza. Rozhodnutie nadobúda účinnosť dňom nasledujúcim po jeho uverejnení v *Úradnom vestníku Európskej únie* alebo k neskoršiemu dátumu, ktorý je v ňom určený. Nie je ním dotknutá platnosť delegovaných aktov, ktoré už nadobudli účinnosť.
4. Komisia oznamuje delegovaný akt hneď po jeho prijatí súčasne Európskemu parlamentu a Rade.
5. Delegovaný akt prijatý podľa článku 4, článku 7 ods. 1, článku 11 ods. 3, článku 43 ods. 5 a 6 a článku 48 ods. 5 nadobudne účinnosť, len ak Európsky parlament alebo Rada voči nemu nevzniesli námietku v lehote troch mesiacov odo dňa oznámenia uvedeného aktu Európskemu parlamentu a Rade, alebo ak pred uplynutím uvedenej lehoty Európsky parlament a Rada informovali Komisiu o svojom rozhodnutí nevzniesť námietku. Na podnet Európskeho parlamentu alebo Rady sa táto lehota predĺži o tri mesiace.

*Článok 74*  
*Postup výboru*

1. Komisii pomáha výbor. Uvedený výbor je výborom v zmysle nariadenia (EÚ) č. 182/2011.
2. Ak sa odkazuje na tento odsek, uplatňuje sa článok 5 nariadenia (EÚ) č. 182/2011.

**HLAVA XII**

**ZÁVEREČNÉ USTANOVENIA**

*Článok 75*  
*Zmena nariadenia (ES) č. 300/2008*

V článku 4 ods. 3 nariadenia (ES) č. 300/2008 sa dopĺňa tento pododsek:

„Pri prijímaní podrobných opatrení súvisiacich s technickými špecifikáciami a postupmi schvaľovania a používania bezpečnostných zariadení týkajúcich sa systémov umelej inteligencie v zmysle nariadenia Európskeho parlamentu a Rady (EÚ) RRR/XX [o umelej inteligencii]\* sa zohľadňujú požiadavky stanovené v hlave III kapitole 2 uvedeného nariadenia.

---

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

*Článok 76*  
*Zmena nariadenia (EÚ) č. 167/2013*

V článku 17 ods. 5 nariadenia (EÚ) č. 167/2013 sa dopĺňa tento pododsek:

„Pri prijímaní delegovaných aktov podľa prvého pododseku týkajúcich sa systémov umelej inteligencie, ktoré sú bezpečnostnými komponentmi v zmysle nariadenia Európskeho parlamentu a Rady (EÚ) RRR/XX [o umelej inteligencii]\*, sa zohľadňujú požiadavky stanovené v hlave III kapitole 2 uvedeného nariadenia.

---

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

*Článok 77  
Zmena nariadenia (EÚ) č. 168/2013*

V článku 22 ods. 5 nariadenia (EÚ) č. 168/2013 sa dopĺňa tento pododsek:

„Pri prijímaní delegovaných aktov podľa prvého pododseku týkajúcich sa systémov umelej inteligencie, ktoré sú bezpečnostnými komponentmi v zmysle nariadenia Európskeho parlamentu a Rady (EÚ) RRR/XX [o umelej inteligencii]\*, sa zohľadňujú požiadavky stanovené v hlave III kapitole 2 uvedeného nariadenia.

---

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

*Článok 78  
Zmena smernice 2014/90/EÚ*

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

„4. V prípade systémov umelej inteligencie, ktoré sú bezpečnostnými komponentmi v zmysle nariadenia Európskeho parlamentu a Rady (EÚ) RRR/XX [o umelej inteligencii]\*, Komisia pri vykonávaní svojich činností podľa odseku 1 a pri prijímaní technických špecifikácií a skúšobných noriem v súlade s odsekmi 2 a 3 zohľadní požiadavky stanovené v hlave III kapitole 2 uvedeného nariadenia.

---

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

*Článok 79  
Zmena smernice (EÚ) 2016/797*

V článku 5 smernice (EÚ) 2016/797 sa dopĺňa tento odsek:

„12. Pri prijímaní delegovaných aktov podľa odseku 1 a vykonávacích aktov podľa odseku 11 týkajúcich sa systémov umelej inteligencie, ktoré sú bezpečnostnými komponentmi v zmysle nariadenia Európskeho parlamentu a Rady (EÚ) RRR/XX [o umelej inteligencii]\*, sa zohľadňujú požiadavky stanovené v hlave III kapitole 2 uvedeného nariadenia.

---

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

*Článok 80  
Zmena nariadenia (EÚ) 2018/858*

V článku 5 nariadenia (EÚ) 2018/858 sa dopĺňa tento odsek:

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

---

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

### *Článok 81 Zmena nariadenia (EÚ) 2018/1139*

Nariadenie (EÚ) 2018/1139 sa mení takto:

1. V článku 17 sa dopĺňa tento odsek:

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

---

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

2. V článku 19 sa dopĺňa tento odsek:

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

3. V článku 43 sa dopĺňa tento odsek:

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

4. V článku 47 sa dopĺňa tento odsek:

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

5. V článku 57 sa dopĺňa tento odsek:

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

6. V článku 58 sa dopĺňa tento odsek:

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

*Článok 82*  
*Zmena nariadenia (EÚ) 2019/2144*

V článku 11 nariadenia (EÚ) 2019/2144 sa dopĺňa tento odsek:

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

---

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

*Článok 83*

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

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

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

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

*Článok 84*

*Hodnotenie a preskúmanie*

1. Komisia raz ročne po nadobudnutí účinnosti tohto nariadenia posúdi potrebu zmeny zoznamu v prílohe III.
2. Komisia do [tri roky od dátumu začatia uplatňovania tohto nariadenia uvedeného v článku 85 ods. 2] a potom každé štyri roky predloží Európskemu parlamentu a Rade správu o hodnotení a preskúmaní tohto nariadenia. Správy sa zverejnia.
3. Správy uvedené v odseku 2 venujú osobitnú pozornosť:
  - a) stavu finančných a ľudských zdrojov príslušných vnútroštátnych orgánov na účinné vykonávanie úloh, ktoré im boli pridelené podľa tohto nariadenia;
  - b) stavu sankcií, a najmä správnych pokút uvedených v článku 71 ods. 1, ktoré členské štáty uplatňujú za porušenie ustanovení tohto nariadenia.
4. Do [tri roky od dátumu začatia uplatňovania tohto nariadenia uvedeného v článku 85 ods. 2] a potom každé štyri roky Komisia vyhodnotí vplyv a účinnosť kódexov správania na podporu uplatňovania požiadaviek stanovených v hlave III kapitole 2

a prípadne ďalších dodatočných požiadaviek na systémy umelej inteligencie, ktoré nie sú vysokorizikovými systémami umelej inteligencie.

5. Rada pre umelú inteligenciu, členské štáty a príslušné vnútroštátne orgány poskytnú Komisii na jej žiadosť informácie na účely odsekov 1 až 4.
6. Pri hodnoteniach a preskúmaniach uvedených v odsekoch 1 až 4 Komisia zohľadní stanoviská a zistenia rady pre umelú inteligenciu, Európskeho parlamentu, Rady a iných relevantných subjektov alebo zdrojov.
7. V prípade potreby Komisia predloží vhodné návrhy na zmenu tohto nariadenia, pričom zohľadní najmä vývoj v oblasti technológií a vezme do úvahy aktuálny stav pokroku v informačnej spoločnosti.

#### *Článok 85*

##### *Nadobudnutie účinnosti a uplatňovanie*

1. Toto nariadenie nadobúda účinnosť dvadsiatym dňom po jeho uverejnení v *Úradnom vestníku Európskej únie*.
2. Toto nariadenie sa uplatňuje od [24 mesiacov po nadobudnutí účinnosti nariadenia].
3. Odchylne od odseku 2:
  - a) hlava III kapitola 4 a hlava VI sa uplatňujú od [*tri mesiace po nadobudnutí účinnosti tohto nariadenia*];
  - b) článok 71 sa uplatňuje od [dvanásť mesiacov po nadobudnutí účinnosti tohto nariadenia].

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

V Bruseli

*Za Európsky parlament  
predseda*

*Za Radu  
predseda*

## LEGISLATÍVNY FINANČNÝ VÝKAZ

### **1. RÁMEC NÁVRHU/INICIATÍVY**

- 1.1. Názov návrhu/iniciatívy
- 1.2. Príslušné oblasti politiky
- 1.3. Návrh/iniciatíva sa týka:
- 1.4. Ciele
  - 1.4.1. Všeobecné ciele
  - 1.4.2. Špecifické ciele
  - 1.4.3. Očakávané výsledky a vplyv
  - 1.4.4. Ukazovatele výkonnosti
- 1.5. Dôvody návrhu/iniciatívy
  - 1.5.1. Potreby, ktoré sa majú uspokojiť v krátkodobom alebo dlhodobom horizonte vrátane podrobného harmonogramu prvotnej fázy vykonávania iniciatívy
  - 1.5.2. Prínos zapojenia Únie (môže byť výsledkom rôznych faktorov, napr. lepšej koordinácie, právnej istoty, väčšej účinnosti alebo komplementárnosti). Na účely tohto bodu je „prínos zapojenia Únie“ hodnota vyplývajúca zo zásahu Únie, ktorá dopĺňa hodnotu, ktorú by inak vytvorili len samotné členské štáty.
  - 1.5.3. Poznatzky získané z podobných skúseností v minulosti
  - 1.5.4. Zlučiteľnosť s viacročným finančným rámcom a možná synergia s inými vhodnými nástrojmi
  - 1.5.5. Posúdenie rôznych disponibilných možností financovania vrátane možnosti prerozdelenia
- 1.6. Trvanie a finančný vplyv návrhu/iniciatívy
- 1.7. Plánovaný spôsob riadenia

### **2. OPATRENIA V OBLASTI RIADENIA**

- 2.1. Opatrenia týkajúce sa monitorovania a predkladania správ
- 2.2. Systém riadenia a kontroly
  - 2.2.1. Opodstatnenie navrhovaných spôsobov riadenia, mechanizmov vykonávania financovania, spôsobov platby a stratégie kontroly
  - 2.2.2. Informácie o zistených rizikách a systémoch vnútornej kontroly zavedených na ich zmierňovanie
  - 2.2.3. Odhad a opodstatnenie nákladovej účinnosti kontrol (pomer medzi nákladmi na kontroly a hodnotou súvisiacich riadených finančných prostriedkov) a posúdenie očakávaných úrovní rizika chyby (pri platbe a uzavretí)



2.3. Opatrenia na predchádzanie podvodom a nezrovnalostiam

**3. ODHADOVANÝ FINANČNÝ VPLYV NÁVRHU/INICIATÍVY**

3.1. Príslušné okruhy viacročného finančného rámca a rozpočtové riadky výdavkov

3.2. Odhadovaný finančný vplyv návrhu na rozpočtové prostriedky

*3.2.1. Zhrnutie odhadovaného vplyvu na operačné rozpočtové prostriedky*

*3.2.2. Odhadované výsledky financované z operačných rozpočtových prostriedkov*

*3.2.3. Zhrnutie odhadovaného vplyvu na administratívne rozpočtové prostriedky*

*3.2.4. Súlad s platným viacročným finančným rámcom*

*3.2.5. Príspevky od tretích strán*

3.3. Odhadovaný vplyv na príjmy

## LEGISLATÍVNY FINANČNÝ VÝKAZ

### 1. RÁMEC NÁVRHU/INICIATÍVY

#### 1.1. Názov návrhu/iniciatívy

Nariadenie Európskeho parlamentu a Rady, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie (akt o umelej inteligencii) a menia niektoré legislatívne akty Únie

#### 1.2. Príslušné oblasti politiky

Komunikačné siete, obsah a technológie;  
Vnútorný trh, priemysel, podnikanie a MSP;  
Vplyv na rozpočet sa týka nových úloh zverených Komisii vrátane podpory Rada EÚ pre umelú inteligenciu;  
Činnosť: Formovanie digitálnej budúcnosti Európy.

#### 1.3. Návrh/iniciatíva sa týka:

**novej akcie**

**novej akcie, ktorá nadväzuje na pilotný projekt/prípravnú akciu<sup>64</sup>**

**predĺženia trvania existujúcej akcie**

**akcie presmerovanej na novú akciu**

#### 1.4. Ciele

##### 1.4.1. Všeobecné ciele

Všeobecným cieľom zásahu je zabezpečiť správne fungovanie jednotného trhu vytvorením podmienok pre vývoj a používanie dôveryhodnej umelej inteligencie v Únii.

##### 1.4.2. Špecifické ciele

###### Špecifický cieľ č. 1

Stanoviť požiadavky špecifické pre systémy umelej inteligencie a povinnosti pre všetkých účastníkov hodnotového reťazca s cieľom zabezpečiť, aby systémy umelej inteligencie uvedené na trh a používané boli bezpečné a v súlade s platnými právnymi predpismi týkajúcimi sa základných práv a hodnôt Únie.

###### Špecifický cieľ č. 2

Zabezpečiť právnu istotu na uľahčenie investícií a inovácií v oblasti umelej inteligencie objasnením toho, aké základné požiadavky, povinnosti, ako aj postupy overovania súladu a zabezpečenia súladu je potrebné dodržiavať pri uvádzaní systému umelej inteligencie na trh Únie alebo jeho používaní na ňom.

###### Špecifický cieľ č. 3

Zlepšiť riadenie a účinné presadzovanie platných právnych predpisov týkajúcich sa základných práv a bezpečnostných požiadaviek platných pre systémy umelej

<sup>64</sup>

Podľa článku 54 ods. 2 písm. a) alebo b) nariadenia o rozpočtových pravidlách.

inteligencie zabezpečením nových právomocí, zdrojov a jasných pravidiel pre príslušné orgány v oblasti postupov posudzovania zhody a postupov monitorovania *ex post*, ako aj rozdelenia úloh v oblasti riadenia a dohľadu medzi vnútroštátnu úroveň a úroveň EÚ.

#### Špecifický cieľ č. 4

Uľahčiť rozvoj jednotného trhu v záujme zákonných, bezpečných a dôveryhodných aplikácií umelej inteligencie a zabrániť roztrieštenosti trhu prijatím opatrení na úrovni EÚ s cieľom stanoviť minimálne požiadavky na systémy umelej inteligencie, ktoré sa majú uviesť a používať na trhu Únie v súlade s platnými právnymi predpismi o základných právach a bezpečnosti.

### 1.4.3. Očakávané výsledky a vplyv

*Uved'te, aký vplyv by mal mať návrh/iniciatíva na prijímateľov/cieľové skupiny.*

Dodávatelia umelej inteligencie by mali mať prospech z minimálneho, ale jasného súboru požiadaviek, ktorým sa vytvára právna istota a zabezpečuje sa prístup k celému jednotnému trhu.

Používatelia umelej inteligencie by mali mať prospech z právnej istoty, že vysokorizikové systémy umelej inteligencie, ktoré kupujú, sú v súlade s európskymi právnymi predpismi a hodnotami.

Spotrebitelia by mali mať prospech zo zníženia rizika porušovania ich bezpečnosti alebo základných práv.

### 1.4.4. Ukazovatele výkonnosti

*Uved'te ukazovatele, pomocou ktorých je možné sledovať uskutočňovanie návrhu/iniciatívy.*

#### Ukazovateľ 1

Počet závažných incidentov alebo prípadov činnosti umelej inteligencie, ktoré predstavujú závažný incident alebo porušenie povinností v oblasti základných práv (polročne) podľa oblastí uplatňovania a vypočítaný a) v absolútnom vyjadrení; b) ako podiel zavedených aplikácií a c) ako podiel dotknutých občanov.

#### Ukazovateľ 2

a) celkové investície do umelej inteligencie v EÚ (ročné);

b) celkové investície do umelej inteligencie podľa členských štátov (ročné);

c) podiel spoločností využívajúcich umelú inteligenciu (ročný);

d) podiel malých a stredných podnikov využívajúcich umelú inteligenciu (ročný);

a) a b) sa vypočítajú na základe oficiálnych zdrojov a porovnávajú sa so súkromnými odhadmi;

c) a d) sa budú získať prostredníctvom pravidelných prieskumov spoločností.

## 1.5. Dôvody návrhu/iniciatívy

### 1.5.1. *Potreby, ktoré sa majú uspokojiť v krátkodobom alebo dlhodobom horizonte vrátane podrobného harmonogramu prvotnej fázy vykonávania iniciatívy*

Nariadenie by sa malo v plnom rozsahu uplatňovať jeden a pol roka po jeho prijatí. Prvky riadiacej štruktúry by však mali byť zavedené ešte predtým. Členské štáty predovšetkým dovedy určia existujúce orgány a/alebo vytvoria nové orgány, ktoré majú plniť úlohy stanovené v právnych predpisoch skôr a mala by sa zriadiť a fungovať Rada EÚ pre umelú inteligenciu. Európska databáza systémov umelej inteligencie by mala byť plne funkčná do začiatku uplatňovania. Súbežne s procesom prijímania je preto potrebné rozvíjať databázu, aby sa jej vývoj dokončil, kým nariadenie nadobudne účinnosť.

- 1.5.2. *Prínos zapojenia Únie (môže byť výsledkom rôznych faktorov, napr. lepšej koordinácie, právnej istoty, väčšej účinnosti alebo komplementárnosti). Na účely tohto bodu je „prínos zapojenia Únie“ hodnota vyplývajúca zo zásahu Únie, ktorá dopĺňa hodnotu, ktorú by inak vytvorili len samotné členské štáty.*

Vznikajúci nerovnomerný rámec potenciálne odlišných vnútroštátnych pravidiel bude brániť plynulému poskytovaniu systémov umelej inteligencie v celej EÚ a je neúčinný pri zaisťovaní bezpečnosti a ochrany základných práv a hodnôt Únie v jednotlivých členských štátoch. Spoločné legislatívne opatrenia EÚ v oblasti umelej inteligencie by mohli podporiť vnútorný trh a majú veľký potenciál poskytnúť európskemu priemyslu konkurenčnú výhodu na globálnej scéne a úspory z rozsahu, ktoré členské štáty nemôžu dosiahnuť samy.

- 1.5.3. *Poznatzky získané z podobných skúseností v minulosti*

V smernici 2000/31/ES o elektronickom obchode sa stanovuje základný rámec fungovania jednotného trhu a dohľadu nad digitálnymi službami a základná štruktúra mechanizmu všeobecnej spolupráce medzi členskými štátmi, pričom pokrýva v zásade všetky požiadavky uplatniteľné na digitálne služby. V hodnotení smernice sa poukázalo na nedostatky vo viacerých aspektoch tohto mechanizmu spolupráce vrátane významných procesných aspektov, ako je nedostatok jasných časových rámcov reakcie členských štátov spojený so všeobecne nedostatočnou schopnosťou reagovať na žiadosti ich partnerov. V priebehu rokov to viedlo k strate dôvery medzi členskými štátmi pri riešení obáv týkajúcich sa poskytovateľov ponúkajúcich digitálne služby cezhranične. Hodnotenie smernice ukázalo potrebu vymedziť diferencovaný súbor pravidiel a požiadaviek na európskej úrovni. Preto by si zavedenie osobitných povinností stanovených v tomto nariadení vyžiadalo osobitný mechanizmus spolupráce na úrovni EÚ s riadiacou štruktúrou zabezpečujúcou koordináciu konkrétnych zodpovedných orgánov na úrovni EÚ.

- 1.5.4. *Zlučiteľnosť s viacročným finančným rámcom a možná synergie s inými vhodnými nástrojmi*

V nariadení, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a menia niektoré legislatívne akty Únie, sa vymedzuje nový spoločný rámec požiadaviek platných pre systémy umelej inteligencie, ktorý výrazne prekračuje rámec stanovený v platných právnych predpisoch. Preto je potrebné stanoviť v tomto návrhu nové potreby týkajúce sa fungovania regulácie a koordinácie na vnútroštátnej a európskej úrovni.

Pokiaľ ide o možnú synergiu s inými vhodnými nástrojmi, úlohu notifikujúcich orgánov na vnútroštátnej úrovni môžu vykonávať vnútroštátne orgány, ktoré plnia podobné funkcie podľa iných právnych predpisov EÚ.

Navyše zvýšením dôvery v umelú inteligenciu, a teda podporením investícií do vývoja a zavedenia umelej inteligencie sa dopĺňa program Digitálna Európa, v rámci ktorého je podpora šírenia umelej inteligencie jednou z piatich priorit.

- 1.5.5. *Posúdenie rôznych disponibilných možností financovania vrátane možnosti prerozdelenia*

Zamestnanci budú prerozdelení. Ostatné náklady budú podporené z finančného krytia na program Digitálna Európa (DEP) vzhľadom na to, že cieľ tohto nariadenia – zabezpečenie dôveryhodnej umelej inteligencie – priamo prispieva

k jednému z kľúčových cieľov programu Digitálna Európa – urýchlenie vývoja a zavedenia umelej inteligencie v Európe.

## 1.6. Trvanie a finančný vplyv návrhu/iniciatívy

### obmedzené trvanie

- v platnosti od [DD/MM]RRRR do [DD/MM]RRRR
- Finančný vplyv na viazané rozpočtové prostriedky od RRRR do RRRR a na platobné rozpočtové prostriedky od RRRR do RRRR.

### neobmedzené trvanie

- Počiatočná fáza implementácie bude trvať **jeden/dva (určí sa)** roky,
- a potom bude implementácia pokračovať v plnom rozsahu.

## 1.7. Plánovaný spôsob riadenia<sup>65</sup>

### Priame riadenie na úrovni Komisie

- prostredníctvom jej útvarov vrátane zamestnancov v delegáciách Únie
- prostredníctvom výkonných agentúr

### Zdieľané riadenie s členskými štátmi

#### Nepriame riadenie, pri ktorom sa plnením rozpočtu poveria:

- tretie krajiny alebo subjekty, ktoré tieto krajiny určili,
  - medzinárodné organizácie a ich agentúry (uved'te),
  - Európska investičná banka (EIB) a Európsky investičný fond,
  - subjekty uvedené v článkoch 70 a 71 nariadenia o rozpočtových pravidlách,
  - verejnoprávne subjekty,
  - súkromnoprávne subjekty poverené vykonávaním verejnej služby, pokiaľ tieto subjekty poskytujú dostatočné finančné záruky,
  - súkromnoprávne subjekty spravované právom členského štátu, ktoré sú poverené vykonávaním verejno-súkromného partnerstva a ktoré poskytujú dostatočné finančné záruky,
  - osoby poverené vykonávaním osobitných činností v oblasti SZBP podľa hlavy V Zmluvy o Európskej únii a určené v príslušnom základnom akte.
- *V prípade viacerých spôsobov riadenia uved'te v oddiele „Poznámky“ presnejšie vysvetlenie.*

Poznámky:

--

<sup>65</sup> Vysvetlenie spôsobov riadenia a odkazy na nariadenie o rozpočtových pravidlách sú k dispozícii na webovej stránke BudgWeb: [http://www.cc.cec/budg/man/budgmanag/budgmanag\\_en.html](http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html).

## 2. OPATRENIA V OBLASTI RIADENIA

### 2.1. Opatrenia týkajúce sa monitorovania a predkladania správ

*Uveďte časový interval a podmienky, ktoré sa vzťahujú na tieto opatrenia.*

Nariadenie sa preskúma a vyhodnotí päť rokov odo dňa nadobudnutia účinnosti tohto nariadenia. Komisia musí o zisteniach pri hodnotení podať správu Európskemu parlamentu, Rade a Európskemu hospodárskemu a sociálnemu výboru.

### 2.2. Systémy riadenia a kontroly

#### 2.2.1. *Opodstatnenie navrhovaných spôsobov riadenia, mechanizmov vykonávania financovania, spôsobov platby a stratégie kontroly*

Týmto nariadením sa stanovuje nová politika, pokiaľ ide o harmonizované pravidlá poskytovania systémov umelej inteligencie na vnútornom trhu pri súčasnom zabezpečení dodržiavania bezpečnosti a základných práv. Tieto nové pravidlá si vyžadujú mechanizmus konzistentnosti pri cezhraničnom uplatňovaní povinností podľa tohto nariadenia vo forme novej poradnej skupiny koordinujúcej činnosti vnútroštátnych orgánov.

Na tieto nové úlohy je potrebné vybaviť útvary Komisie primeranými zdrojmi. Odhaduje sa, že presadzovanie nového nariadenia si vyžiada 10 ekvivalentov plného pracovného času (ďalej len „FTE“) v každom režime (5 FTE na podporu činností rady a 5 FTE na európskeho dozorného úradníka pre ochranu údajov pôsobiaceho ako notifikujúci orgán pre systémy umelej inteligencie zavedené orgánom Európskej únie).

#### 2.2.2. *Informácie o zistených rizikách a systémoch vnútornej kontroly zavedených na ich zmierňovanie*

S cieľom zabezpečiť, aby členovia rady mali možnosť vykonať informovanú analýzu na základe faktických dôkazov, sa predpokladá, že rada by mala byť podporovaná administratívnou štruktúrou Komisie a mala by sa vytvoriť expertná skupina s cieľom poskytovať ďalšie odborné znalosti, ak je to potrebné.

#### 2.2.3. *Odhad a opodstatnenie nákladovej účinnosti kontrol (pomer medzi nákladmi na kontroly a hodnotou súvisiacich riadených finančných prostriedkov) a posúdenie očakávaných úrovní rizika chyby (pri platbe a uzavretí)*

Pokiaľ ide o výdavky na zasadnutia, vzhľadom na nízku hodnotu na jednu transakciu (napr. preplatenie cestovných nákladov delegátovi za zasadnutie), štandardné kontrolné postupy sa zdajú postačujúce. Pokiaľ ide o rozvoj databázy, zadávanie zákaziek má zavedený spoľahlivý systém vnútornej kontroly v GR CNECT prostredníctvom centralizovaného obstarávania.

### 2.3. Opatrenia na predchádzanie podvodom a nezrovnalostiam

*Uveďte existujúce a plánované preventívne a ochranné opatrenia, napr. zo stratégie na boj proti podvodom.*

Existujúce opatrenia boja proti podvodom uplatniteľné na Komisiu sa budú vzťahovať na dodatočné rozpočtové prostriedky potrebné pre toto nariadenie.



### 3. ODHADOVANÝ FINANČNÝ VPLYV NÁVRHU/INICIATÍVY

#### 3.1. Príslušné okruhy viacročného finančného rámca a rozpočtové riadky výdavkov

- Existujúce rozpočtové riadky

V poradí, v akom za sebou nasledujú okruhy viacročného finančného rámca a rozpočtové riadky.

Okruh viacročného finančného rámca	Rozpočtový riadok	Druh výdavkov	Príspevky			
	Číslo	DRP/NRP <sup>66</sup>	krajín EZVO <sup>67</sup>	kandidátskych krajín <sup>68</sup>	tretích krajín	v zmysle článku 21 ods. 2 písm. b) nariadenia o rozpočtových pravidlách
7	20 02 06 Administratívne výdavky	NRP	NIE	NIE	NIE	NIE
1	02 04 03 DEP umelá inteligencia	DRP	ÁNO	NIE	NIE	NIE
1	02 01 30 01 Výdavky na podporu programu Digitálna Európa	NRP	ÁNO	NIE	NIE	NIE

#### 3.2. Odhadovaný finančný vplyv návrhu na rozpočtové prostriedky

##### 3.2.1. Zhrnutie odhadovaného vplyvu na výdavky na operačné rozpočtové prostriedky

- Návrh/iniciatíva si nevyžaduje použitie operačných rozpočtových prostriedkov.
- Návrh/iniciatíva si vyžaduje použitie operačných rozpočtových prostriedkov, ako je uvedené v tejto tabuľke:

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

<b>Okruh viacročného finančného</b>	1	
-------------------------------------	---	--

<sup>66</sup> DRP = diferencované rozpočtové prostriedky / NRP = nediferencované rozpočtové prostriedky.

<sup>67</sup> EZVO: Európske združenie voľného obchodu.

<sup>68</sup> Kandidátske krajiny a prípadne potenciálni kandidáti zo západného Balkánu.

<b>rámca</b>		
--------------	--	--

GR: CNECT				Rok 2022	Rok 2023	Rok 2024	Rok 2025	Rok 2026	Rok 2027 <sup>69</sup>	SPOLU
• Operačné rozpočtové prostriedky										
Rozpočtový riadok <sup>70</sup> 02 04 03	Závazky	(1a)		1,000						<b>1,000</b>
	Platby	(2a)		0,600	0,100	0,100	0,100	0,100		<b>1,000</b>
Rozpočtový riadok	Závazky	(1b)								
	Platby	(2b)								
Administratívne rozpočtové prostriedky financované z finančného krytia na vykonávanie osobitných programov <sup>71</sup>										
Rozpočtový riadok 02 01 30 01		(3)		0,240	0,240	0,240	0,240	0,240		<b>1,200</b>
<b>Rozpočtové prostriedky pre GR CNECT</b>		Závazky	= 1a + 1b + 3		<b>1,240</b>		<b>0,240</b>	<b>0,240</b>	<b>0,240</b>	<b>2,200</b>
		Platby	= 2a + 2b + 3		<b>0,840</b>	<b>0,340</b>	<b>0,340</b>	<b>0,340</b>	<b>0,340</b>	<b>2,200</b>

• Operačné rozpočtové prostriedky SPOLU	Závazky	(4)		1,000						<b>1,000</b>
---	---------	-----	--	-------	--	--	--	--	--	--------------

<sup>69</sup> Orientačne a v závislosti od dostupnosti rozpočtu.

<sup>70</sup> Podľa oficiálnej rozpočtovej nomenklatúry.

<sup>71</sup> Technická a/alebo administratívna pomoc a výdavky určené na financovanie vykonávania programov a/alebo akcií Európskej únie (pôvodné rozpočtové riadky „BA“), nepriamy výskum, priamy výskum.

	Platby	(5)		0,600	0,100	0,100	0,100	0,100		<b>1,000</b>
• Administratívne rozpočtové prostriedky financované z finančného krytia na vykonávanie osobitných programov SPOLU		(6)		<b>0,240</b>	<b>0,240</b>	<b>0,240</b>	<b>0,240</b>	<b>0,240</b>		<b>1,200</b>
<b>Rozpočtové prostriedky OKRUHU 1</b> viacročného finančného rámca <b>SPOLU</b>		Závazky	= 4 + 6	1,240	0,240	0,240	0,240	0,240		<b>2,200</b>
		Platby	= 5 + 6	0,840	0,340	0,340	0,340	0,340		<b>2,200</b>

**Ak má návrh/iniciatíva vplyv na viaceré okruhy, zopakujte oddiel uvedený vyššie:**

• Operačné rozpočtové prostriedky SPOLU (všetky operačné okruhy)	Závazky	(4)								
	Platby	(5)								
• Administratívne rozpočtové prostriedky financované z finančného krytia na vykonávanie osobitných programov SPOLU (všetky operačné okruhy)		(6)								
<b>Rozpočtové prostriedky OKRUHOV 1 až 6</b> viacročného finančného rámca <b>SPOLU</b> (referenčná suma)		Závazky	= 4 + 6							
		Platby	= 5 + 6							

<b>Okruh viacročného finančného rámca</b>	<b>7</b>	„Administratívne výdavky“
---	----------	---------------------------

Tento oddiel sa vyplní s použitím „rozpočtových údajov administratívnej povahy“, ktoré budú po prvýkrát uvedené v [prílohe k legislatívnemu finančnému výkazu](#) (príloha V k interným predpisom), ktorá sa na účely konzultácie medzi útvarmi vloží do aplikácie DECIDE.

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

		Rok 2023	Rok 2024	Rok 2025	Rok 2026	Rok 2027	Po roku 2027 <sup>72</sup>	SPOLU
<b>GR: CNECT</b>								
• Ľudské zdroje		0,760	0,760	0,760	0,760	0,760	0,760	<b>3,800</b>
• Ostatné administratívne výdavky		<b>0,010</b>	<b>0,010</b>	<b>0,010</b>	<b>0,010</b>	<b>0,010</b>	<b>0,010</b>	<b>0,050</b>
<b>GR CNECT SPOLU</b>		<b>Rozpočtové prostriedky</b>		<b>0,760</b>	<b>0,760</b>	<b>0,760</b>	<b>0,760</b>	<b>3,850</b>
Európsky dozorný úradník pre ochranu údajov								
• Ľudské zdroje		0,760	0,760	0,760	0,760	0,760	0,760	<b>3,800</b>
• Ostatné administratívne výdavky								
<b>EDPS SPOLU</b>		<b>Rozpočtové prostriedky</b>		<b>0,760</b>	<b>0,760</b>	<b>0,760</b>	<b>0,760</b>	<b>3,800</b>
<b>Rozpočtové prostriedky OKRUHU 7 viacročného finančného rámca SPOLU</b>		(Závazky spolu = Platby spolu)		1,530	1,530	1,530	1,530	<b>7,650</b>

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

		Rok 2022	Rok 2023	Rok 2024	Rok 2025	Rok 2026	Rok 2027	SPOLU
<b>Rozpočtové prostriedky</b>	Závazky		2,770	1,770	1,770	1,770	1,770	<b>9,850</b>

<sup>72</sup> Všetky údaje v tomto stĺpci sú orientačné a závisia od pokračovania programov a dostupnosti rozpočtových prostriedkov.

<b>OKRUHOV 1 až 7</b> viacročného finančného rámca <b>SPOLU</b>	Platby		2,370	1,870	1,870	1,870	1,870	<b>9,850</b>
--	--------	--	-------	-------	-------	-------	-------	--------------

3.2.2. *Odhadované výsledky financované z operačných rozpočtových prostriedkov*

viazané rozpočtové prostriedky v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Uveďte ciele a výstupy ↓			Rok 2022	Rok 2023	Rok 2024	Rok 2025	Rok 2026	Rok 2027	Po roku 2027 <sup>73</sup>	SPOLU								
	Druh	Priemerné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet spolu	Náklady spolu
<b>VÝSTUPY</b>																		
ŠPECIFICKÝ CIEĽ č. 1 <sup>74</sup> ...																		
Databáza					1	1,000	1		1		1		1		1	0,100	1	1,000
Zasadnutia – výstup					10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	50	1,000
Komunikačné činnosti					2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	10	0,040
Špecifický cieľ č. 1 medzisúčet																		
ŠPECIFICKÝ CIEĽ č. 2...																		
– Výstup																		
Špecifický cieľ č. 2 medzisúčet																		
<b>SPOLU</b>					13	0,240	13	0,240	13	0,240	13	0,240	13	0,240	13	0,100	65	2,200

<sup>73</sup>

Všetky údaje v tomto stĺpci sú orientačné a závisia od pokračovania programov a dostupnosti rozpočtových prostriedkov.

<sup>74</sup>

Ako je uvedené v bode 1.4.2. „Špecifické ciele...“.

### 3.2.3. Zhrnutie odhadovaného vplyvu na administratívne rozpočtové prostriedky

- Návrh/iniciatíva si nevyžaduje použitie administratívnych rozpočtových prostriedkov
- Návrh/iniciatíva si vyžaduje použitie administratívnych rozpočtových prostriedkov, ako je uvedené v nasledujúcej tabuľke:

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

	Rok 2022	Rok 2023	Rok 2024	Rok 2025	Rok 2026	Rok 2027	Ročne po roku 2027 <sup>75</sup>	SPOLU
--	-------------	-------------	-------------	-------------	-------------	-------------	--	-------

<b>OKRUH 7</b> <b>viacročného finančného</b> <b>rámca</b>								
Eudské zdroje		1,520	1,520	1,520	1,520	1,520	<b>1,520</b>	<b>7,600</b>
Ostatné administratívne výdavky		0,010	0,010	0,010	0,010	0,010	<b>0,010</b>	<b>0,050</b>
<b>Medzisúčet OKRUHU 7</b> <b>viacročného finančného</b> <b>rámca</b>		1,530	1,530	1,530	1,530	1,530	<b>1,530</b>	<b>7,650</b>

<b>Mimo OKRUHU 7</b> <sup>76</sup> <b>of the multiannual</b> <b>financial framework</b>								
Eudské zdroje								
Ostatné administratívne výdavky		0,240	0,240	0,240	0,240	0,240	<b>0,240</b>	<b>1,20</b>
<b>Medzisúčet</b> <b>mimo OKRUHU 7</b> <b>viacročného finančného</b> <b>rámca</b>		0,240	0,240	0,240	0,240	0,240	<b>0,240</b>	<b>1,20</b>

<b>SPOLU</b>		<b>1,770</b>	<b>1,770</b>	<b>1,770</b>	<b>1,770</b>	<b>1,770</b>	<b>1,770</b>	<b>8,850</b>
--------------	--	--------------	--------------	--------------	--------------	--------------	--------------	--------------

Rozpočtové prostriedky potrebné na ľudské zdroje a na ostatné administratívne výdavky budú pokryté rozpočtovými prostriedkami GR, ktoré už boli pridelené na riadenie akcie a/alebo boli prerozdelené v rámci GR, a v prípade potreby budú doplnené zdrojmi, ktoré sa môžu prideliť riadiacemu GR v rámci ročného postupu pridelovania zdrojov a v závislosti od rozpočtových obmedzení.

<sup>75</sup> Všetky údaje v tomto stĺpci sú orientačné a závisia od pokračovania programov a dostupnosti rozpočtových prostriedkov.

<sup>76</sup> Technická a/alebo administratívna pomoc a výdavky určené na financovanie vykonávania programov a/alebo akcií Európskej únie (pôvodné rozpočtové riadky „BA“), nepriamy výskum, priamy výskum.

### 3.2.3.1. Odhadované potreby ľudských zdrojov

- Návrh/iniciatíva si nevyžaduje použitie ľudských zdrojov.
- Návrh/iniciatíva si vyžaduje použitie ľudských zdrojov, ako je uvedené v nasledujúcej tabuľke:

odhady sa vyjadrujú v jednotkách ekvivalentu plného pracovného času

	Rok 2023	Rok 2024	Rok 2025	2026	2027	Po roku 2027 <sup>77</sup>	
<b>• Plán pracovných miest (úradníci a dočasní zamestnanci)</b>							
20 01 02 01 (ústredie a zastúpenia Komisie)	10	10	10	10	10	10	
20 01 02 03 (delegácie)							
01 01 01 01 (nepriamy výskum)							
01 01 01 11 (priamy výskum)							
Iné rozpočtové riadky (uved'te)							
<b>• Externí zamestnanci (ekvivalent plného pracovného času FTE)<sup>78</sup></b>							
20 02 01 (ZZ, VNE, DAZ z celkového balíka prostriedkov)							
20 02 03 (ZZ, MZ, VNE, DAZ, PED v delegáciách)							
<b>XX 01 xx yy zz<sup>79</sup></b>	– ústredie						
	– delegácie						
01 01 01 02 (ZZ, VNE, DAZ – nepriamy výskum)							
01 01 01 12 (ZZ, VNE, DAZ – priamy výskum)							
Iné rozpočtové riadky (uved'te)							
<b>SPOLU</b>	<b>10</b>	<b>10</b>	<b>10</b>	<b>10</b>	<b>10</b>	<b>10</b>	

**XX** predstavuje príslušnú oblasť politiky alebo rozpočtovú hlavu.

Potreby ľudských zdrojov budú pokryté úradníkmi GR, ktorí už boli pridelení na riadenie akcie a/alebo boli interne prerozdelení v rámci GR, a v prípade potreby budú doplnené zdrojmi, ktoré sa môžu prideliť riadiacemu GR v rámci ročného postupu pridelovania zdrojov v závislosti od rozpočtových obmedzení.

Očakáva sa, že EDPS poskytne polovicu potrebných zdrojov.

Opis úloh, ktoré sa majú vykonať:

Úradníci a dočasní zamestnanci	<p>Na prípravu celkovo 13 až 16 zasadnutí, vypracovanie návrhov správ, pokračovanie v práci v oblasti politiky, napr. v súvislosti s budúcimi zmenami zoznamu vysokorizikových aplikácií umelej inteligencie, a udržiavanie vzťahov s orgánmi členských štátov sa budú vyžadovať 4 AD FTE a 1 AST FTE.</p> <p>Za systémy umelej inteligencie vyvinuté inštitúciami EÚ zodpovedá európsky dozorný úradník pre ochranu údajov. Na základe minulých skúseností možno odhadnúť, že na splnenie zodpovedností EDPS podľa návrhu právneho predpisu sa vyžaduje 5 AD</p>
--------------------------------	---

<sup>77</sup> Všetky údaje v tomto stĺpci sú orientačné a závisia od pokračovania programov a dostupnosti rozpočtových prostriedkov.

<sup>78</sup> ZZ = zmluvný zamestnanec; MZ = miestny zamestnanec; VNE = vyslaný národný expert; DAZ = dočasný agentúrny zamestnanec; PED = pomocný expert v delegácii.

<sup>79</sup> Čiastkový strop pre externých zamestnancov financovaných z operačných rozpočtových prostriedkov (pôvodné rozpočtové riadky „BA“).



	FTE.
Externí zamestnanci	

### 3.2.4. Súlad s platným viacročným finančným rámcom

Návrh/iniciatíva:

- môže byť v plnej miere financovaná prerozdelením v rámci príslušného okruhu viacročného finančného rámca (VFR).

Nie je potrebné preprogramovanie.

- si vyžaduje použitie nepridelenej rezervy v rámci príslušného okruhu VFR a/alebo použitie osobitných nástrojov vymedzených v nariadení o VFR.

Vysvetlite potrebu a uveďte príslušné okruhy, rozpočtové riadky, zodpovedajúce sumy a nástroje, ktorých použitie sa navrhuje.

- si vyžaduje revíziu VFR.

Vysvetlite potrebu a uveďte príslušné okruhy, rozpočtové riadky a zodpovedajúce sumy.

### 3.2.5. Príspevky od tretích strán

Návrh/iniciatíva:

- nezahŕňa spolufinancovanie tretími stranami
- zahŕňa spolufinancovanie tretími stranami, ako je odhadnuté v nasledujúcej tabuľke:

rozpočtové prostriedky v mil. EUR (zaokrúhlené na 3 desatinné miesta)

	Rok N <sup>80</sup>	Rok N + 1	Rok N + 2	Rok N + 3	Uveďte všetky roky, počas ktorých vplyv trvá (pozri bod 1.6)			Spolu
Uveďte spolufinancujúci subjekt								
Prostriedky zo spolufinancovania SPOLU								

<sup>80</sup>

Rok N je rokom, v ktorom sa návrh/iniciatíva začína vykonávať. Nahraďte „N“ očakávaným prvým rokom vykonávania (napríklad: 2021). To isté urobte aj pri nasledujúcich rokoch.

### 3.3. Odhadovaný vplyv na príjmy

- Návrh/iniciatíva má finančný vplyv na príjmy, ako je uvedené v nasledujúcej tabuľke:
- Návrh/iniciatíva má finančný vplyv na príjmy, ako je uvedené v nasledujúcej tabuľke:
  - vplyv na iné príjmy
  - vplyv na iné príjmy
  - Uved'te, či sú príjmy pripísané rozpočtovým riadkom výdavkov

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Rozpočtový príjmov:	riadok	Rozpočtové prostriedky k dispozícii v bežnom rozpočtovom roku	Vplyv návrhu/iniciatívy <sup>81</sup>					
			Rok N	Rok N + 1	Rok N + 2	Rok N + 3	Uved'te všetky roky, počas ktorých vplyv trvá (pozri bod 1.6)	
Článok .....								

V prípade pripísaných príjmov uved'te príslušné rozpočtové riadky výdavkov.

Ďalšie poznámky (napr. spôsob/vzorec použitý na výpočet vplyvu na príjmy alebo akékoľvek ďalšie informácie).

<sup>81</sup> Pokiaľ ide o tradičné vlastné zdroje (clá, odvody z produkcie cukru), uvedené sumy musia predstavovať čisté sumy, t. j. hrubé sumy po odčítaní 20 % na náklady na výber.