Council of the European Union

Brussels, 26 March 2026
(OR. en, cs)

7720/26

Interinstitutional Files:
2025/0358 (COD)
2025/0359 (COD)
2025/0360 (COD)

SIMPL 46
ANTICI 51
DATAPROTECT 103
CYBER 144
TELECOM 145
CODEC 542
COMPET 374
PROCIV 62
JAI 397
MI 295
INST 114
PARLNAT 53
PARLNAT

COVER NOTE

From:	Parliament of the Czech Republic, Chamber of Deputies
date of receipt:	23 March 2026
To:	The President of the Council of the European Union
Subject:	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL DATA UNION STRATEGY UNLOCKING DATA FOR AI [15712/25 - COM(2025)835] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI) [15708/25 - COM(2025)836] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus) [15698/25 - COM(2025)837] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the establishment of European Business Wallets [15701/25 - COM(2025)838]

- Opinion on the application of the Principles of Subsidiarity and Proportionality

Delegations will find enclosed the opinion[1] of Chamber of Deputies of the Czech Republic on the above, followed by a courtesy English translation.

[1] The translation(s) of the opinion may be available on the Interparliamentary EU Information Exchange website (IPEX) at the following address:
https://secure.ipex.eu/IPEXL-WEB/document/COM-2025-0836
https://secure.ipex.eu/IPEXL-WEB/document/COM-2025-0837
https://secure.ipex.eu/IPEXL-WEB/document/COM-2025-0835
https://secure.ipex.eu/IPEXL-WEB/document/COM-2025-0838

The Commission reply will be available at the following address: https://national-parliaments-opinions.ec.europa.eu/home

POSLANECKÁ SNĚMOVNA PARLAMENTU ČESKÉ REPUBLIKY

2026
10. volební období

37.
USNESENÍ

Výboru pro evropské záležitosti
ze 7. schůze ze dne 18. března 2026

ke sdělení Komise Evropskému parlamentu a Radě – Strategie evropské datové unie: zpřístupnění dat pro umělou inteligenci /kód Rady 15712/25, KOM(2025) 835 v konečném znění/ (dále jen sdělení o datové strategii)

k návrhu nařízení Evropského parlamentu a Rady, kterým se mění nařízení (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 a směrnice 2002/58/ES, (EU) 2022/2555 a (EU) 2022/2557, pokud jde o zjednodušení digitálního právního rámce, a kterým se zrušují nařízení (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868 a směrnice (EU) 2019/1024 (souhrnný balíček pro digitální oblast) /kód Rady 15698/25, KOM(2025) 837 v konečném znění/ (dále jen digitální omnibus)

k návrhu nařízení Evropského parlamentu a Rady o zřízení evropských podnikatelských peněženek /kód Rady 15701/25, KOM(2025) 838 v konečném znění/ (dále jen nařízení o EPP)

k návrhu nařízení Evropského parlamentu a Rady, kterým se mění nařízení (EU) 2024/1689 a (EU) 2018/1139, pokud jde o zjednodušení provádění harmonizovaných pravidel pro umělou inteligenci (souhrnný balíček pro digitální oblast týkající se umělé inteligence) /kód Rady 15708/25, KOM(2025) 836 v konečném znění/ (dále jen omnibus pro UI)

Výbor pro evropské záležitosti Poslanecké sněmovny Parlamentu ČR po vyslechnutí informace poradkyně předsedy vlády pro záležitosti Evropské unie Mileny Hrdinkové, ředitele Odboru právního a legislativního Digitální a informační agentury Víta Křížky, zástupce vrchního ředitele Sekce výzkumu, vývoje a inovací Ministerstva průmyslu a obchodu Daniela Všetečky, po vyslechnutí zpravodajské zprávy poslankyně Ireny Ferčíkové Konečné a po rozpravě

1. **b e r e n a v ě d o m í** sdělení o datové strategii, návrh digitálního omnibusu, návrh nařízení o EPP a návrh omnibusu pro UI (dále vše jen **digitální balíček**);

2. **v y j a d ř u j e s o u h l a s** se stanoviskem vlády ČR k těmto dokumentům, zejména v částech podporujících snižování administrativní zátěže pro malé a střední podniky, avšak s výhradami k opatřením, která oslabují transparentnost a právní jistotu, a **u k l á d á** vládě, aby jej informovala o průběhu dalšího projednávání návrhu digitálního omnibusu, omnibusu pro UI a nařízení o EPP v Radě;

3. **po důkladném posouzení těchto návrhů d o s p ě l k z á v ě r u ,** že předložený digitální balíček v navržené podobě **v některých aspektech obsahuje riziko nedodržení p r i n c i p u p r o p o r c i o n a l i t y ,** neboť administrativní zjednodušení může přinést rovněž zásahy do základních práv na ochranu osobních údajů a soukromí, a to konkrétně v následujících bodech:

   a. Zúžení definice osobních údajů: V souladu se stanoviskem vlády ČR i společným stanoviskem Evropského sboru pro ochranu osobních údajů (EDPB) a Evropského inspektora ochrany údajů (EDPS) výbor vyjadřuje zásadní výhrady k navrhované změně definice osobních údajů. Tato úprava podle EDPB neodpovídá judikatuře Soudního dvora EU. Ačkoli výbor plně podporuje potřebu snížit zbytečnou byrokratickou zátěž pro podniky i výzkumné instituce, je tak nutné činit při respektování ochrany pseudonymizovaných údajů, aby nedošlo k oslabení ochrany soukromí. Zároveň se výbor v souladu s EDPB, EDPS a RPV vyjadřuje rezervovaně k přenesení pravomoci určovat pravidla pseudonymizace na Komisi, což by mělo zůstat v kompetenci nezávislých dozorových úřadů a judikatury. (Digitální Omnibus)

   b. Ohrožení práva subjektů údajů na přístup: Digitální omnibus zavádí možnost odmítnout žádost o přístup k údajům z důvodu jiného účelu, než je ochrana osobních údajů. Tento krok považují EDPB i EDPS za problematický a v rozporu s horizontální povahou práva na ochranu údajů. V souladu s vládními obavami o právní jistotu výbor varuje, že takové omezení vytváří prostor pro libovůli správců při vyřizování žádostí. Výbor vyzývá k hledání vyváženého řešení, lepší specifikace či definice, která povede ke snížení zbytečné byrokratické zátěže v případech možného zneužití práva subjektů k přístupu za jiným účelem, než je ochrana osobních údajů. Současně výbor zdůrazňuje, že jakékoliv omezení nesmí narušit práva zaměstnanců v platformové ekonomice na přezkum algoritmického rozhodování. (Digitální Omnibus)

   c. Omezení transparentnosti u vysoce rizikové UI: Výbor se ztotožňuje s názorem vlády, která nesouhlasí se zrušením povinnosti registrace vysoce rizikových systémů UI v databázi EU v případech vlastního posouzení poskytovatelem. Takový krok by v rozporu s principem transparentnosti podle čl. 49 odst. 2 aktu o UI a umožnil by poskytovatelům se netransparentně a jednostranně vyhnout všem povinnostem pro vysoce rizikovou UI, což drasticky omezuje možnosti dohledu a ohrožuje bezpečnost občanů. Výbor se ztotožňuje se stanoviskem vlády požadujícím zjednodušení celého procesu registrace, namísto jejího kompletního zrušení. (Omnibus pro UI)

   d. Problematický právní základ pro trénování AI na citlivých údajích: Výbor vyjadřuje znepokojení ze zavedení výjimek z povinnosti výmazu citlivých dat při „nepřiměřeném úsilí“, které oslabují ochranu nejzranitelnějších údajů, aniž by byla provedena řádná analýza proporcionality. Výbor konstatuje soulad se stanoviskem EDPB, který nepovažuje

navrhované výjimky pro zpracování citlivých údajů systémy UI za nezbytné a doporučuje jejich přísné omezení, současně si je však vědom důležitosti využití dat pro detekci a odstraňování biasu modelů umělé inteligence. Výbor proto apeluje, aby v případě zavedení jakýchkoliv výjimek bylo toto doplněno jasnými garancemi proti zneužití. Současně apeluje na vyjasněním definice termínu „nepřiměřené úsilí". Stanovisko vlády v této souvislosti správně upozorňuje na rizika plynoucí z nejasného vymezení prováděcích pravomocí Komise v této oblasti. (Omnibus pro UI)

e. Zákaz systémů UI pro sexuální manipulaci (nudifying): V souladu s aktuální pozicí Rady výbor naléhavě žádá, aby byl do článku 5 odst. 1 prvního pododstavce aktu o UI doplněn nový bod (ha) zakazující uvádění na trh, uvádění do provozu nebo používání systémů UI, které bez souhlasu identifikovatelné fyzické osoby upravují, manipulují nebo uměle generují realistické obrazy či videa zobrazující sexuálně explicitní aktivity nebo intimní části těla. Tento zákaz se nevztahuje na poskytovatele s účinnými bezpečnostními opatřeními zamezujícími zneužití, ani nebrání vývoji technických schopností pro legitimní účely. (Omnibus pro UI);

4. **ž á d á** , aby v souladu s mandátem daným Aktem o UI Komise prioritně zavedla harmonizované metodiky pro měření a transparentní vykazování environmentální stopy a energetické náročnosti systémů UI a datových center při zachování principu nezvyšování administrativní zátěže;

5. **v í t á** iniciativu zřízení evropských podnikatelských peněženek (EPP), která má potenciál významně snížit administrativní zátěž firem a usnadnit jejich přeshraniční interakce; v souladu se stanoviskem vlády zdůrazňuje nezbytnost, aby tento unijní rámec v maximální možné míře reflektoval a integroval již existující národní systémy elektronického doručování a identifikace. Apeluje na důsledné dodržování standardů ochrany údajů a zajištění kybernetické bezpečnosti (*security by design*), při současném zachování principu dobrovolnosti využívání tohoto nástroje pro hospodářské subjekty. V zájmu ochrany soukromí výbor doporučuje využití decentralizované architektury (SSI), která zamezí plošnému sledování transakcí a komerčnímu profilování firem;

6. **v í t á** Strategii evropské datové unie a v souladu se stanoviskem vlády ČR podporuje její ambici posílit konkurenceschopnost a technologickou suverenitu Unie prostřednictvím tří stěžejních pilířů: rozšíření přístupu ke kvalitním datům pro umělou inteligenci a inovace, zjednodušení pravidel pro data a ochrany datové suverenity EU prostřednictvím strategické mezinárodní datové politiky, přičemž klade důraz na podporu open-source řešení a otevřených standardů jako základu pro skutečnou technologickou nezávislost a transparentnost EU; zároveň **k o n s t a t u j e** , že tento přístup je konzistentní s Národní strategií umělé inteligence ČR 2030;

7. **p o v ě ř u j e** předsedu Výboru pro evropské záležitosti, aby v rámci politického dialogu postoupil toto usnesení předsedkyni Evropské komise.

Marie KRŠKOVÁ
ověřovatelka

Irena FERČÍKOVÁ KONEČNÁ
zpravodajka

Petr SOKOL
předseda

Příloha k usnesení č. 37

POSLANECKÁ SNĚMOVNA PARLAMENTU ČESKÉ REPUBLIKY

PARLAMENTNÍ INSTITUT

DOKUMENTY EU

Digitální balíček

Informační podklad k:

- návrhu nařízení, kterým se mění nařízení (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 a směrnice 2002/58/ES, (EU) 2022/2555 a (EU) 2022/2557, pokud jde o zjednodušení digitálního právního rámce, a kterým se zrušují nařízení (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868 a směrnice (EU) 2019/1024 (souhrnný balíček pro digitální oblast),
- návrhu nařízení o zřízení evropských podnikatelských peněženek,
- návrhu nařízení, kterým se mění nařízení (EU) 2024/1689 a (EU) 2018/1139, pokud jde o zjednodušení provádění harmonizovaných pravidel pro umělou inteligenci (souhrnný balíček pro digitální oblast týkající se umělé inteligence), a
- sdělení Strategie evropské datové unie: zpřístupnění dat pro umělou inteligenci

NÁVRH NAŘÍZENÍ

Návrh nařízení Evropského parlamentu a Rady, kterým se mění nařízení (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 a směrnice 2002/58/ES, (EU) 2022/2555 a (EU) 2022/2557, pokud jde o zjednodušení digitálního právního rámce, a kterým se zrušují nařízení (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868 a směrnice (EU) 2019/1024 (souhrnný balíček pro digitální oblast)

COM(2025) 837 final, kód Rady 15698/25

Interinstitucionální spis 2025/0360/COD

NÁVRH NAŘÍZENÍ

Návrh nařízení Evropského parlamentu a Rady o zřízení evropských podnikatelských peněženek

COM(2025) 838 final, kód Rady 15701/25

Interinstitucionální spis 2025/0358/COD

NÁVRH NAŘÍZENÍ

Návrh nařízení Evropského parlamentu a Rady, kterým se mění nařízení (EU) 2024/1689 a (EU) 2018/1139, pokud jde o zjednodušení provádění harmonizovaných pravidel pro umělou inteligenci (souhrnný balíček pro digitální oblast týkající se umělé inteligence)

COM(2025) 836 final, kód Rady 15708/25

Interinstitucionální spis 2025/0359/COD

SDĚLENÍ

Sdělení Komise Evropskému parlamentu a Radě – Strategie evropské datové unie: zpřístupnění dat pro umělou inteligenci

COM(2025) 835 final, kód Rady 15712/25

- **Právní základ:**
  Článek 16 a 114 Smlouvy o fungování Evropské unie. (COM(2025) 837 final)
  Článek 114 Smlouvy o fungování Evropské unie. (COM(2025) 838 final, COM(2025) 836 final)

- **Datum zaslání Poslanecké sněmovně prostřednictvím VEZ:**
  20. 11. 2025

- **Datum projednání ve VEZ:**
  19. 2. 2026 (1. kolo)

- **Procedura:**
  Řádný legislativní postup.

- **Předběžná stanoviska vlády (dle § 109a odst. 1 jednacího řádu PS):**
  Datovaná dnem 6. a 27. 1. a 5. 2. 2026, doručená do výboru pro evropské záležitosti dne 7., 8. a 29. 1. a 10. 2. 2026 prostřednictvím systému ISAP.

- **Hodnocení z hlediska principu subsidiarity:**
  Dokumenty jsou v souladu s principem subsidiarity.

- **Odůvodnění a předmět:**
  Komise dne 19. 11. 2025 předložila **nový balíček pro digitální oblast, který zjednodušuje pravidla v digitální oblasti.** Cílem je snížit administrativní zátěž, podpořit konkurenceschopnost a přinést jasnější pravidla pro podniky, veřejnou správu i občany.

  Balíček pro digitální oblast tvoří:
  Návrh nařízení o digitálním omnibusu, který usiluje o zjednodušení a zpřehlednění právního rámce EU v oblasti nakládání s daty, ochrany osobních údajů, kybernetické bezpečnosti a vztahů mezi online platformami a podniky, čímž má vytvářet jednotnější a právně předvídatelné prostředí (dále též „**digitální omnibus**“),

  Návrh nařízení o digitálním omnibusu pro umělou inteligenci, jenž zahrnuje soubor opatření, která mají sladit zavádění pravidel aktu o umělé inteligenci s dostupností podpůrných nástrojů, snížit administrativní zátěž (zejména pro menší podniky) a zvýšit flexibilitu i praktičnost regulace při zachování ochrany údajů a možnosti testování v reálných podmínkách (dále též „**digitální omnibus pro UI**“),

  Návrh nařízení o evropské podnikatelské peněžence, který zavádí nový digitální nástroj pro zjednodušení interakcí mezi podniky v EU a veřejnými orgány, umožňující ověřování totožnosti, digitální podpisy a výměnu informací (dále též „**nařízení o EPP**“).

  Současně s balíčkem pro digitální oblast Komise zveřejnila sdělení **Strategie evropské datové unie** stanovující cíle a priority v oblasti dostupnosti a sdílení dat a zahájila digitální kontrolu účelnosti, která zahrnuje obsáhlou veřejnou konzultaci a je druhou fází plánu Komise na zjednodušení digitálních pravidel EU.

  Evropská komise v **politických směrech 2024–2029** deklarovala, že bude zjednodušovat předpisy EU a jejich implementaci s cílem zvýšit konkurenceschopnost a prosperitu evropského hospodářství. Reagovala tak na závěry v **Draghiho zprávě** vydané v září 2024, že nahromadění pravidel v průběhu času na různých úrovních, jejich větší složitost a problémy při jejich provádění mají významný dopad na konkurenceschopnost Evropy.

  Sdělení Komise Evropa jednodušší a rychlejší z února 2025 pak představilo vizi programu v oblasti provádění a zjednodušování a komplexní soubor nástrojů k dosažení výsledků. **Pracovní program Komise na rok 2025** tuto vizi dále rozpracoval a konkretizoval s důrazem na zjednodušování prostřednictvím souhrnných balíčků a návrhů zaměřených na prioritní oblasti. **Cílem je snížit administrativní zátěž do konce roku 2029 alespoň o 25 % a pro malé a střední podniky o 35 %. Balíček pro digitální oblast představuje sedmý souhrnný balíček** (tzv. Omnibus).

- **Obsah a dopad:**
  1. Digitální omnibus

  V rámci digitálního omnibusu Komise navrhuje změny ve třech oblastech:
  - **Oblast dat:** Konsoliduje a zefektivňuje se regulační rámec pro data do dvou právních aktů, a to aktu o datech a GDPR;

- **Kybernetická bezpečnost:** Zjednodušuje se hlášení kybernetických bezpečnostních incidentů, které se týká několika předpisů EU, a to prostřednictvím vytvoření jednotného kontaktního místa;
- **Vztahy mezi online platformami a podniky:** Zrušují se zastaralé či duplicitní předpisy.

A. Změny v oblasti dat

Změny nařízení (EU) 2023/2854 – akt o datech

Navrhovaná novela **aktu o datech (Data Act)** zjednodušuje pravidla v oblasti dat a integruje vybraná ustanovení z jiných předpisů EU (nařízení o volném toku neosobních údajů v EU, aktu o správě dat a směrnice o otevřených datech). Cílem je vytvořit jasnější pravidla pro přístup k datům, jejich využívání a opakované použití. Klíčovými změnami jsou:

- **Ochrana a zpřístupnění dat:** Nově mohou držitelé dat odmítnout zpřístupnění obchodního tajemství při vysokém riziku zneužití, zejména ve třetích zemích s nižší úrovní ochrany. Krizové situace, **jejich zmírňování a následná obnova** jsou nově jediným důvodem pro povinné sdílení dat s veřejným sektorem (např. ohrožení veřejného zdraví, velké přírodní katastrofy nebo závažné kybernetické incidenty), přičemž je stanoveno, jaká data lze požadovat. (*Pozn. PI: Dřívější „výjimečná potřeba" zahrnovala i jiné úkoly veřejného zájmu, např. vypracování statistik mimo krizovou situaci.)*

- **Výjimky pro změnu poskytovatele služeb zpracování dat**: Zjednodušuje se proces změny poskytovatele služeb zpracování dat pro malé a střední podniky, malé podniky se střední tržní kapitalizací a poskytovatele služeb na zakázku, což má vést k jednorázovým úsporám ve výši přibližně 1,5 miliardy eur.

Poznámka PI:

Digitální omnibus navrhuje rozšířit některá příznivá opatření pro malé a střední podniky (MSP), jejichž počet v EU je cca 26,1 mil., i na novou kategorii **malých podniků se střední tržní kapitalizací (SMC)**, kterých je v EU cca 38 000. Do této kategorie mají spadat podniky, které mají 250–749 zaměstnanců a roční obrat ≤ 150 milionům eur nebo bilanční sumu ≤ 129 milionům eur. Cílem je snížit náklady na dodržování předpisů a administrativu, podpořit růst a umožnit investovat do klíčových činností, jako je vývoj produktů a expanze. Opatření mají posílit konkurenceschopnost evropských MSP a SMC ve srovnání s firmami v jurisdikcích bez podobné podpory.

- **Služby zprostředkování dat a datový altruismus:** Ruší se povinný oznamovací režim pro poskytovatele služeb zprostředkování dat a je nahrazen dobrovolnou registrací, u organizací pro datový altruismus zůstává dobrovolná registrace. V obou skupinách se ruší některé povinnosti a je zavedena možnost dobrovolného zápisu do unijních rejstříků a používání označení „uznaný v Unii" a společného loga.

Poznámka PI:

Akt o správě dat definuje **datový altruismus** jako dobrovolné a nekomerční sdílení dat na základě souhlasu uděleného fyzickými nebo právnickými osobami pro cíle obecného zájmu, jako jsou zdravotní péče, boj proti změně klimatu, zlepšení mobility, usnadnění vývoje, tvorby a šíření oficiálních statistik, zlepšení poskytování veřejných služeb, tvorba veřejné politiky nebo účely vědeckého výzkumu ve veřejném zájmu. (Zdroj: Český telekomunikační úřad. Datový altruismus)

- **Opakované použití dat veřejného sektoru:** Sjednocují se pravidla pro opakované použití otevřených dat i určitých kategorií chráněných dat, u nichž se stanovují podmínky bezpečného přístupu a procesní pravidla. Zavádí se možnost přiměřených poplatků pro velmi velké podniky na základě objektivních kritérií a stanovuje se, že klíčové datové soubory s vysokou hodnotou

budou zpřístupněny zdarma. Přesně jsou definovány postupy při výjimkách a získávání souhlasů.

Změny nařízení (EU) 2016/679 – GDPR

GDPR je novelizováno s cílem vyjasnit a zjednodušit pravidla ochrany osobních údajů při zachování hlavních zásad a požadavků. **Zásadní navrhované změny zahrnují zejména**:

- **Definici pojmu osobní údaje a pravidla pseudonymizace**: Upřesňuje se **definice pojmu osobní údaje** tak, že se vkládá nový odstavec, který ji doplňuje. Za **osobní údaje** by se již nepovažovaly informace o fyzické osobě, na jejichž základě by nemohla jiná osoba nebo subjekt identifikovat tuto osobu prostředky, o nichž lze rozumně předpokládat, že je použije, a informace by se pro ni nestávaly osobními údaji jen proto, že **potenciální následný příjemce těchto informací** by měl prostředky k identifikaci. Pokud jde o **pseudonymizaci**, Komise se zmocňuje, aby prováděcími akty stanovila, za jakých okolností mohou pseudonymizované údaje přestat být považovány za osobní údaje pro určité kategorie správců nebo konkrétní situace.

Poznámka PI:

Co jsou osobní údaje?

Osobními údaji jsou podle čl. 4 odst. 1 GDPR veškeré informace o identifikované osobě (víme, kdo to je), **nebo identifikovatelné fyzické osobě** (lze zjistit, kdo to je, pokud máme další informace). Při určování, zda je fyzická osoba identifikovatelná, by se podle rec. 26 GDPR mělo přihlédnout ke **všem prostředkům**, o nichž lze rozumně předpokládat, že je správce (tj. osoba určující proč a jak jsou osobní údaje zpracovávány) nebo jiná osoba použijí pro přímou či nepřímou identifikaci dané fyzické osoby. Ke stanovení toho, zda lze rozumně předpokládat použití prostředků k identifikaci fyzické osoby, by měly být vzaty v úvahu všechny objektivní faktory, jako jsou náklady a čas, které si identifikace vyžádá, s přihlédnutím k technologii dostupné v době zpracování i k technologickému rozvoji. Soudní dvůr EU např. v rozsudku C-582/14 – Breyer vysvětlil, že **dynamická IP adresa sama o sobě nepředstavuje informaci o identifikované osobě**, protože přímo neodhaluje totožnost fyzické osoby, která počítač používá, ani jiné osoby. **Aby však IP adresa představovala osobní údaj, není nutné, aby sama o sobě umožňovala identifikovat subjekt údajů ani aby všechny informace potřebné k identifikaci byly v rukou jediné osoby**. Stačí, pokud se provozovatel internetových stránek může obrátit na příslušný orgán a získat od **poskytovatele internetového připojení** další informace potřebné k identifikaci uživatele. V takovém případě existuje **prostředek, který může být rozumně použit pro identifikaci subjektu údajů** a IP adresa se považuje za osobní údaj. Odborná literatura tento přístup interpretuje jako **objektivní test identifikovatelnosti**, při němž se posuzuje, zda **obecně existují realisticky dostupné prostředky k identifikaci** (např. jiné databáze, externí informace, technologie), které by vedly k identifikaci osoby.

Co by v praxi znamenala navrhovaná změna definice osobních údajů?

Identifikovatelnost fyzické osoby by se posuzovala **pouze z pohledu konkrétního subjektu zpracovávajícího tyto informace**, tzn. zda má prostředky k tomu, aby osobu, jíž se informace týkají, identifikoval. To se stalo předmětem **silné kritiky ze strany odborníků i jiných orgánů EU** (viz dále), neboť taková úprava zcela neodpovídá dosavadní judikatuře Soudního dvora a neznamenala by jen upřesnění definice osobních údajů, ale její zúžení, a tím zásah do ochrany soukromí.

Co je pseudonymizace?

Pseudonymizace je ve smyslu **čl. 4 GDPR odst. 5** způsob zpracování osobních údajů, při němž jsou přímé identifikátory osoby (např. jméno nebo rodné číslo) nahrazeny kódem nebo jiným označením, např. pseudonymem, a doplňující údaje umožňující zpětné přiřazení k osobě (např. seznam kódů) jsou uchovávány odděleně a zabezpečeny. Takto zpracovaná data nelze přímo přiřadit ke konkrétní osobě, ale identitu lze teoreticky zjistit, pokud někdo získá přístup k těmto

doplňujícím údajům. Například škola při analýze výsledků testů nahradí jména žáků kódy (např. Ž001, Ž002), takže učitelé pracují pouze s kódy a výsledky. Seznam, který přiřazuje kódy ke konkrétním žákům, je uložen odděleně a má k němu přístup jen omezený okruh osob.

Co by v praxi znamenaly navrhované změny?

Podle názoru Evropského sboru pro ochranu osobních údajů a Evropského inspektora a občanských organizací by změny mohly vést k tomu, že pseudonymizované údaje by již nebyly chráněny, pokud by osoba zpracovávající tyto informace tvrdila, že nemá prostředky k identifikaci osob, kterých se týkají. Dále upozorňují na to, že pravidla pseudonymizace jsou v rámci ochrany osobních údajů zásadní a jejich specifikace by neměla být definována Komisí, ale ponechána na judikatuře Soudního dvora EU.

- **Nová pravidla pro vědecký výzkum:** Zavádí se **nová definice vědeckého výzkumu**, která reaguje na dosavadní právní nejistotu ohledně toho, které činnosti a subjekty lze za vědecký výzkum považovat. Zároveň se stanovuje, že další zpracování údajů pro vědecké účely je považováno za kompatibilní s původním účelem (bez nutnosti posuzování) a může představovat oprávněný zájem.

- **Výjimky ze zvláštních kategorií osobních údajů:** Zavádí se dvě nové výjimky umožňující zpracování (1) **zvláštních kategorii osobních údajů v UI systémech**, u nichž je povoleno jejich dočasné zpracování, pokud se objeví v datech pro vývoj nebo provoz UI a jsou přijata vhodná technická a organizační opatření k zabránění jejich zpracování, jsou ihned odstraňovány nebo jsou chráněny před použitím k výrobě výstupů, zpřístupněním nebo jiným poskytnutím třetím stranám, pokud odstranění vyžaduje nepřiměřené úsilí, a (2) **biometrických údajů**, u nichž se umožňuje jejich zpracování výhradně pro ověření totožnosti, pokud jsou pod výhradní kontrolou subjektu údajů a přístup správce je omezen na nezbytné minimum.

Poznámka PI:

Co jsou zvláštní kategorie osobních údajů?

Do zvláštní kategorie osobních údajů podle čl. 9 odst. 1 GDPR spadají údaje vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání nebo členství v odborech, genetické údaje, biometrické údaje za účelem jedinečné identifikace fyzické osoby a údaje o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby. GDPR poskytuje těmto osobním údajům vyšší úroveň ochrany, neboť mají citlivý charakter. Dříve se pro tyto údaje používalo označení „citlivé údaje". Platí pravidlo, že zpracování této kategorie osobních údajů je zakázáno, ale je taxativně stanoveno 10 výjimek, které stanovují zvláštní podmínky, při jejichž splnění je lze zpracovávat.

- **Právo na přístup k osobním údajům:** Nově se jako **důvod odmítnutí přístupu** stanoví **zneužití práv subjektu** k jiným účelům než ochraně jeho údajů (např. vymáhání odškodnění, poškození správce, získání výhod). U **nepřiměřených žádostí** by správce nově dokládal jen existenci rozumných důvodů pro nepřiměřenost.

Co je právo na přístup k osobním údajům?

V souladu s čl. 15 GDPR má fyzická osoba, jejíž údaje jsou zpracovávány (tzv. subjekt údajů), právo získat prostřednictvím podané žádosti informace o tom, zda jsou či nejsou jeho osobní údaje zpracovávány. V čl. 12 odst. 5 GDPR jsou stanoveny důvody odmítnutí přístupu, pokud jsou žádosti zjevně nedůvodné nebo nepřiměřené, zejména pokud se opakují. Tyto důvody prokazoval vždy správce.

- **Omezení informační povinnosti o zpracování osobních údajů:** Zavádí se dvě výjimky, kdy se informační povinnost neuplatní, a to jde-li o (1) **běžné smluvní vztahy s nízkým rizikem**, je-li jasně vymezený vztah mezi subjekty údajů a správcem, jde-li o nenáročné zpracování a lze rozumně předpokládat, že subjekt údajů již informace má (např. ve vztahu mezi řemeslníkem a jeho klientem, nebo u sportovních klubů); to však neplatí při předávání údajů, automatizovaném

rozhodování nebo vysoce rizikovém zpracování, a (2) **vědecký výzkum**, pokud by to nebylo možné, vyžadovalo neúměrné úsilí nebo ohrozilo cíle výzkumu, přičemž správce musí přijmout ochranná opatření, zejména zveřejnit informace obecně.

- **Výjimku pro automatizované rozhodování:** Objasňuje se požadavek na využití automatizovaného individuálního rozhodování v souvislosti s uzavřením nebo plněním smlouvy mezi subjektem údajů a správcem údajů tak, že požadavek na nezbytnost platí bez ohledu na to, zda by rozhodnutí mohlo být přijato jinak než výhradně automatizovanými prostředky.

Co je automatizované rozhodování?
Automatizované zpracování osobních údajů je prováděno prostředky výpočetní techniky, např. prostřednictvím počítačů či chytrých mobilních telefonů. Podle čl. 22 odst. 1 GDPR má subjekt údajů právo nebýt předmětem žádného rozhodnutí, které je založeno výhradně na automatizovaném zpracování (nedochází k lidskému zásahu) a má-li pro něho právní účinky či se ho obdobným způsobem významně dotýká. Z tohoto obecného zákazu jsou stanoveny výjimky v čl. 22 odst. 2 GDPR.

- **Oznamování porušení zabezpečení:** Nově se má oznámení vyžadovat, je-li pravděpodobné, že porušení zabezpečení osobních údajů bude mít **za následek vysoké riziko** pro práva subjektu, a lhůta pro oznámení se prodlužuje na **96 hodin** (ze 72 hodin). Zavádí se jednotné kontaktní místo pro oznamování a společná šablona.

Co je oznamování porušení zabezpečení?
Pokud dojde k porušení zabezpečení ochrany osobních údajů, tj. porušení důvěrnosti, dostupnosti nebo integrity, která má za následek pravděpodobnost vzniku rizika pro subjekty údajů, je správce povinen do 72 hodin oznámit tuto událost dozorovému úřadu.

- **Souhlas s cookies:** Pravidla směrnice o soukromí a elektronických komunikacích (směrnice e-Privacy) se pro osobní údaje v koncovém zařízení přenášejí do GDPR. Zachovává se přitom princip, podle něhož je přístup k těmto údajům **založen na souhlasu uživatele a jsou stanoveny výjimky**. Výjimky, které jsou označovány jako **tzv. whitelist nízkorizikových cookies, umožňují přístup i bez souhlasu,** přičemž **nově se tento okruh výjimek rozšiřuje**.

- Má se zajistit, aby uživatel mohl **souhlas udělit nebo odmítnout** jedním klikem, a správce nesmí znovu žádat o souhlas pro stejný účel během platnosti souhlasu nebo po jeho odmítnutí nejméně po dobu 6 měsíců, včetně následného zpracování. Návrh otevírá cestu **k automatizovanému a strojově čitelnému označování jednotlivých voleb subjektu údajů v koncovém zařízení** a k jejich respektování poskytovateli internetových stránek a mobilních aplikací, jakmile budou k dispozici příslušné harmonizované normy. Správci by byli povinni umožnit udělení nebo odmítnutí souhlasu a vznesení námitky automatizovaně prostřednictvím volby ve strojově čitelném formátu nastavené přímo v prohlížeči nebo operačním systému, s výjimkou poskytovatelů mediálních služeb. **Důsledkem přenesení právní úpravy do GDPR je mj. i to, že p**orušení pravidel by mělo podléhat jeho sankčnímu režimu (mj. pokuty až do výše 4 % z celosvětového obratu).

Co jsou cookies a jak jsou upraveny?
Cookies jsou malé textové soubory, které si webová stránka uloží do počítače nebo mobilního zařízení uživatele po jejím navštívení. Umožňují webu **pamatovat si akce uživatele a nastavení** (např. jazyk, přihlášení nebo preference), takže je při příští návštěvě nemusí znovu zadávat. (Zdroj: Evropská unie: Co jsou cookies.) Podle čl. 5 odst. 3 směrnice ePrivacy musí subjekt údajů k použití cookies nebo srovnatelných sledovacích technologií poskytnout specifický a informovaný souhlas, tj. uchovávání informací nebo získávání přístupu k již uchovávaným informacím v koncovém zařízení účastníka nebo uživatele je povoleno **pouze pod podmínkou souhlasu pro konkrétní účely** stanovené v uvedeném článku.

Současně jsou stanoveny výjimky, kdy souhlas není vyžadován, a to pro případy technického ukládání nebo přístupu, jehož jediným účelem je provedení přenosu sdělení prostřednictvím sítě elektronických komunikací, nebo je-li to nezbytně nutné k tomu, aby mohl poskytovatel služeb informační společnosti poskytovat služby, které si účastník nebo uživatel výslovně vyžádal. Cílem tohoto ustanovení je podle rec. 24 chránit koncová zařízení uživatelů, neboť jsou součástí soukromí uživatelů. Rec. 66 pak uvádí, že souhlas může být vyjádřen nastavením prohlížeče nebo jiné aplikace, kde je to technicky možné a efektivní, nicméně je diskutovanou otázkou, za jakých podmínek splňuje požadavky platného souhlasu. Souhlas se často získává pomocí lišt, které informují o účelu zpracování a typech cookies.

Co by v praxi znamenaly navrhované změny u cookies?

V praxi by návrh především **rozšířil okruh situací, kdy lze používat nízkorizikové cookies bez souhlasu uživatele**, zejména při poskytování služby výslovně požadované uživatelem, při anonymizovaném měření návštěvnosti nebo při zajištění nebo obnovení bezpečnosti služby. Další změny by současně **zjednodušily práci se souhlasem** a omezily opakované zobrazování cookie lišt, čímž by mohly přispět ke snížení tzv. „cookie fatigue" (únavy z cookies). Evropský sbor pro ochranu osobních údajů a Evropský inspektor a občanské organizace tyto cíle obecně podporují, současně však varují zejména před právní nejistotou a úskalími automatizovaného a strojově čitelného označování jednotlivých voleb v koncovém zařízení a upozorňují na potřebu jasnějších definic jednotlivých výjimek.

- **Zpracování osobních údajů pro vývoj a provoz UI**: Zpracování je umožněno na základě předpokládaného **oprávněného zájmu správce**, pokud nepřeváží práva subjektu údajů a pokud jiné předpisy výslovně nevyžadují souhlas, přičemž musí být zajištěna minimalizace údajů, ochrana před neoprávněným zpřístupněním, transparentnost a právo subjektu vznést námitku.

B. Kybernetická bezpečnost

Zjednodušení podávání hlášení o kybernetických incidentech: Zavádí se jednotné kontaktní místo, prostřednictvím kterého mohou společnosti plnit všechny povinnosti týkající se oznamování kybernetických incidentů podle směrnice NIS2, obecného nařízení o ochraně osobních údajů (GDPR), nařízení o digitální provozní odolnosti (DORA), nařízení o elektronické identitě (eIDAS) a nařízení o odolnosti kritických subjektů (CER). Rozhraní bude vyvinuto agenturou ENISA se spolehlivými bezpečnostními zárukami a bude podrobeno komplexnímu testování. Cílem je zjednodušit proces oznamování a zvýšit jeho efektivitu. Jednotné kontaktní místo by se mělo začít používat do 18 měsíců od vstupu digitálního omnibusu v platnost, avšak za určitých okolností může být povinnost jej používat odložena na 24 měsíců od vstupu nařízení v platnost.

C. Vztahy mezi online platformami a podniky

Zrušení nařízení Platform-to-Business (P2B): Zrušují se zastaralá či duplicitní ustanovení, která již byla převzata aktem o digitálních službách (DSA) a aktem o digitálních trzích (DMA). Po zrušení předpisů zůstanou některá vybraná ustanovení platná až do roku 2032.

Stanovisko vlády ČR k digitálnímu omnibusu:

Vláda ČR v obecné rovině **vítá návrh digitálního omnibusu** a podporuje opatření vedoucí ke snižování administrativní zátěže a zjednodušení legislativních pravidel, zejména pro malé a střední podniky. Je však nutné zajistit, aby skutečně představoval zjednodušení, nepřinesl zvýšenou administrativní zátěž nebo nezpůsobil právní nejistotu. Případné změny, které vyplynou z probíhající digitální kontroly účelnosti, by bylo vhodné zavést spolu s digitálním omnibusem, aby byla právní situace stabilní a předvídatelná. Ve vztahu k datové legislativě vláda požaduje zejména vysvětlení nebo úpravy a u GDPR nesouhlasí zvláště se změnou definice osobních údajů.

2. Digitální omnibus pro umělou inteligenci

Komise navrhuje cílená zjednodušující opatření, která mají zajistit včasné, bezproblémové a přiměřené provádění některých ustanovení **aktu o UI**.

Mezi tato opatření patří:

- **Harmonogram uplatnění pravidel pro vysoce rizikovou UI:** Navrhuje se změnit datum počátku uplatňování (původně 2. 8. 2026) tak, že bude vázáno na dostupnost harmonizovaných norem nebo jiných nástrojů podporujících dodržování aktu o umělé inteligenci. Pravidla by se začala uplatňovat po potvrzení dostupnosti těchto nástrojů Komisí, a to za 6 měsíců pro systémy v příloze III (nejpozději do 2. 12. 2027) a za 12 měsíců pro systémy v příloze I (nejpozději do 2. 8. 2028).
- **Rozšíření zvláštního režimu uplatňovaného na MSP**: Zjednodušená technická dokumentace a zvláštní zohlednění při uplatňování sankcí pro malé a střední podniky (MSP) se mají rozšířit i na malé podniky se střední tržní kapitalizací.
- **Gramotnost v oblasti UI**: Povinnost poskytovatelů a zavádějících subjektů zajistit gramotnost v oblasti UI se zrušuje. Nově mají členské státy a Komise gramotnost v oblasti UI pouze podporovat prostřednictvím školení a nezávazných opatření. Zvláštní povinnosti odborné přípravy u zavádějících subjektů vysoce rizikových systémů UI však zůstávají zachovány.
- **Flexibilnější monitorování po uvedení na trh:** Zrušuje se předepsaný harmonizovaný plán monitorování po uvedení na trh a místo toho se ponechává poskytovatelům vysoce rizikových systémů UI flexibilita při nastavení tohoto systému. Komise má vydat pouze výkladové pokyny.
- **Výjimka pro povinnost registrace vysoce rizikových systémů UI:** Poskytovatelé by již nemuseli registrovat systémy UI v EU databázi, pokud by dospěli k závěru, že tyto systémy nejsou vysoce rizikové, protože se používají pouze pro úzce vymezené nebo procedurální úkoly. (*Pozn. PI: Vysoce rizikovými systémy UI jsou např. systémy biometrické identifikace osob, nástroje pro výběr a hodnocení zaměstnanců a systémy posuzující přístup k úvěrům nebo sociálním dávkám.*)
- **Centralizace dohledu nad určitými systémy UI:** Posiluje se pravomoc dohledu úřadu EU pro UI nad všemi systémy UI založenými na obecných modelech, pokud model i systém vyvinul tentýž poskytovatel, a nad všemi systémy zabudovanými do velmi velkých online platforem nebo vyhledávačů, i když poskytovatel systému a modelu není stejný. Ostatní systémy UI zůstávají pod dohledem členských států.

Poznámka PI:

Příkladem systémů UI založených na obecných modelech jsou generativní systémy umělé inteligence, které jsou schopné na základě rozsáhlých trénovacích dat vytvářet nový obsah, například text, obrázky nebo kód, jako je např. ChatGPT (Zdroj: Digitální a informační agentura. Generativní AI)

- **Výjimka pro zpracování zvláštních kategorií osobních údajů:** Poskytovatelům a zavádějícím subjektům všech systémů a modelů UI se má umožnit zpracovávat zvláštní kategorie osobních údajů za účelem zajišťování odhalování a nápravy zkreslení, a to s využitím příslušných záruk.
- **Širší využívání regulačních sandboxů a testování v reálných podmínkách**: Posiluje se spolupráce mezi Komisí a členskými státy při správě regulačních sandboxů pro UI, sjednocuje se jejich řízení a umožňuje se začlenit testování vysoce rizikových systémů UI v reálných podmínkách přímo do plánů sandboxů. Testování mimo sandboxy se rozšiřuje na vysoce rizikové systémy podle příloh I a III a umožňují se dobrovolné dohody mezi Komisí a

členskými státy pro určité systémy z přílohy I, aniž by byly dotčeny jiné právní předpisy. Zakotvuje se právní základ pro zřízení regulačního sandboxu na úrovni Unie.

Poznámka PI:

Regulační sandboxy pro UI poskytují kontrolované prostředí, kde mohou poskytovatelé po omezenou dobu vyvíjet, testovat a ověřovat své systémy UI před uvedením na trh, s dohodnutým plánem testování a vhodnými zárukami, včetně případného testování v reálných podmínkách. (čl. 53 aktu o UI)

- **Vztah mezi aktem o UI a dalšími právními předpisy EU**: Cílené změny mají vyjasnit působnost aktu ve vztahu k GDPR a pravidlům v oblasti civilního letectví.
- **Jediná žádost o posouzení shody:** Navrhuje se, aby subjekty posuzování shody vysoce rizikových systémů UI, které ověřují splnění všech požadavků, včetně bezpečnosti a kvality, před uvedením systému na trh, mohly podat pouze jednu žádost a projít jediným postupem posuzování, pokud žádají o jmenování podle aktu o UI i harmonizačních právních předpisů Unie.
- **Přechodné období pro generativní UI:** Pro poskytovatele generativních systémů UI uvedených na trh před 2. 8. 2026 se navrhuje šestiměsíční přechodné období k úpravě označování, tedy k informování uživatelů, že jde o generativní UI, včetně jejího fungování a jejích omezení.

Stanovisko vlády ČR k digitálnímu omnibusu pro umělou inteligenci:

Vláda vítá a oceňuje zohlednění řady priorit a podnětů ČR v **návrhu digitálního omnibusu k UI**. Pozitivně hodnotí zejména rozšíření výjimek a podpůrných opatření pro malé a střední podniky a malé společnosti se střední tržní kapitalizací, jakož i prodloužení časových rámců pro poskytovatele systémů obecných modelů UI. Vláda však nesouhlasí se zrušením povinnosti registrace systému UI pro určité případy a upozorňuje, že je třeba řešit přetrvávající nejasnosti u povolovacích postupů, ustanovení o spolupráci mezi orgány a prováděcích pravomocí Komise.

Stanovisko Senátu PČR k digitálnímu omnibusu pro umělou inteligenci:
Senát přijal usnesení č. 363, ve kterém souhlasí se stanoviskem vlády, konkrétně s většinou návrhů na zjednodušení práva EU v oblasti umělé inteligence a s odkladem účinnosti některých ustanovení, přičemž zdůrazňuje potřebu zachovat standardy ochrany a zaměřit se na administrativní zjednodušení a právní vyjasnění. Podporuje celkové zjednodušení registrace systémů UI místo odstranění požadavku registrace na základě vlastního posouzení poskytovatele, které by mohlo být zneužitelné a oslabit dohled. Zároveň upozorňuje, že některé nejasně formulované změny by mohly snížit odpovědnost poskytovatelů a uživatelů UI systémů.

Poznámka PI:

V souvislosti s připravovanými změnami GDPR **se k návrhu vyjadřují také instituce EU**, mimo jiné **Evropský sbor pro ochranu osobních údajů (EDPB)**, který je nezávislým orgánem EU sdružujícím národní úřady pro ochranu osobních údajů členských států a Evropského inspektora ochrany údajů. Jeho úkolem je zajišťovat jednotné uplatňování pravidel ochrany osobních údajů, zejména GDPR, a podporovat spolupráci mezi dozorovými úřady při jejich vymáhání. V přeshraničních případech, kdy mezi úřady nedojde ke shodě, může EDPB přijímat závazná rozhodnutí. Sbor má sekretariát v Bruselu. (Zdroj: EDPB. The European Data Protection Board)

Evropský sbor pro ochranu osobních údajů a **Evropský inspektor ochrany údajů** ve **společném stanovisku 2/2026** z 10. 2. 2026 upozorňují, že navrhované změny **definice**

osobních údajů vyvolávají závažné obavy z hlediska ochrany soukromí jednotlivců, stejně jako navrhované zmocnění Komise stanovit prováděcím aktem, které údaje již po pseudonymizaci nepředstavují osobní údaje. Zákonodárce důrazně vyzývají, aby tyto změny nepřijímal. Současně však vítají ty části návrhu, které mohou přispět k vyšší harmonizaci, konzistentnímu výkladu a posílení právní jistoty nebo ke snížení administrativní zátěže. Konkrétně podporují novou **definici vědeckého výzkumu**, úpravu kompatibility dalšího zpracování pro tyto účely, nové odchylky od **informační povinnosti**, výjimku pro zpracování **biometrických údajů** při ověřování totožnosti pod kontrolou uživatele za předpokladu odpovídajících záruk, zvýšení prahu pro **oznamování porušení zabezpečení osobních údajů** a prodloužení oznamovací lhůty na 96 hodin včetně zavedení jednotné šablony oznámení. V některých oblastech sice podporují základní cíl navrhovaných změn, považují však za nezbytné jejich zpřesnění. Pokud jde o zpracování osobních údajů prostřednictvím **systémů umělé inteligence**, nepovažují navrhované změny za nezbytné, pro případ jejich přijetí však doporučují doplnit specifická ustanovení týkající se posuzování **oprávněného zájmu** a výkonu **práva vznést námitku**. Ve vztahu k navrhované výjimce pro zpracování **zvláštních kategorií osobních údajů** v kontextu vývoje a provozu systémů nebo modelů umělé inteligence doporučují, aby bylo přímo v **normativní části právního aktu** (nikoli pouze v recitálu 33) výslovně stanoveno, že se tato výjimka vztahuje výhradně na zpracování nahodilé či zbytkové, nikoli na zpracování nezbytné pro účely vývoje a provozu těchto systémů či modelů, současně navrhují upřesnit rozsah této výjimky a zajistit odpovídající záruky po celý životní cyklus systému. Jde-li o navrhované **omezení práva na přístup**, doporučují blíže vymezit, co lze považovat za zneužití práva, například jeho podmíněním existencí zneužívajícího úmyslu. **Zjednodušení požadavků na informační povinnost a snížení administrativní zátěže zejména pro malé a střední podniky** hodnotí pozitivně, avšak navrhují další upřesnění s cílem zajistit právní jistotu a skutečné snížení zátěže při současném zachování možnosti jednotlivců získat informace o zpracování jejich osobních údajů. **Zákaz automatizovaného individuálního rozhodování** by měl být podle jejich názoru zachován v souladu s výkladem Soudního dvora EU. Ačkoli připouštějí možnost výjimek, nesouhlasí s tím, aby bylo takové rozhodování obecně považováno za přípustné vždy, existuje-li smlouva bez ohledu na splnění kritéria nezbytnosti, a doporučují upřesnit postup posuzování této nezbytnosti. Navrhované zjednodušení směrnice **ePrivacy** a úpravy týkající se **cookies** vítají, vyjadřují však obavy, že oddělení pravidel o přístupu k osobním a neosobním údajům může vést k právní nejistotě, a doporučují další úpravy směřující k posílení právní jistoty, minimalizaci rizik a podpoře odpovědných inovací.

Rovněž některé občanské organizace **formulují svá stanoviska** k navrhovaným změnám GDPR a směrnice ePrivacy. Například noyb i EDRi upozorňují, že navrhované změny digitálního omnibusu nepředstavují jen technické zjednodušení, ale přinášejí zásadní změny, které mohou oslabit ochranu osobních údajů. Kriticky hodnotí **zúžení definice osobních údajů**, které by mohlo vyjmout data jako cookies či identifikátory zařízení z působnosti GDPR, a **omezení práv subjektů údajů**, například přístupu k vlastním datům a kontroly nad zpracováním. Varují také před **rozšířeným zpracováním dat pro účely UI**, včetně používání citlivých osobních údajů, bez dostatečných ochranných mechanismů, což by mohlo omezit práva subjektů údajů a zvýšit riziko nedostatečné kontroly nad jejich daty. Dále upozorňují, že **rozšířené výjimky a nejasně definovaná pravidla** by mohly **ovlivnit sběr a zpracování cookies** uložených v koncovém zařízení, přičemž **právní nejistota by ztěžovala uživatelům kontrolu nad jejich daty**, firmám zajištění souladu s pravidly a dozorovým orgánům **efektivní vymáhání**. Noyb doporučuje tyto části upravit tak, aby byla ochrana uživatelů zachována, výjimky přísně vymezeny a proces byl transparentní, včetně možnosti jasného souhlasu uživatele, a aby automatizované udělování souhlasu či námitky ve strojově čitelném formátu bylo právně a technicky jasně definováno a respektovalo svobodnou a informovanou volbu

uživatele. Obě organizace zdůrazňují, že návrh by mohl vést ke **snížení právní jistoty a efektivity ochrany**, a proto požadují pečlivé přehodnocení či odmítnutí navrhovaných změn.

3. Evropská podnikatelská peněženka: nový digitální nástroj pro zjednodušení administrativy

Návrh nařízení o EPP zavádí **evropskou podnikatelskou peněženku (EPP)** jako **digitální nástroj pro bezpečné přeshraniční interakce mezi podniky a veřejnou správou i mezi podniky navzájem**. EPP má umožnit ověřování identity, elektronické podepisování dokumentů, časová razítka a výměnu ověřených digitálních informací. Úkony provedené jejím prostřednictvím by měly **stejné právní účinky jako úkony provedené osobně nebo v listinné podobě.**

EPP by mohli poskytovat pouze **oprávnění poskytovatelé** zapsaní na **důvěryhodném seznamu** a musela by splňovat stanovené funkční a technické požadavky. Totožnost vlastníka EPP by byla ověřována na základě **identifikačních údajů** vydaných kvalifikovanými poskytovateli nebo veřejnými orgány. Každému držiteli by byl přiřazen **jedinečný identifikátor** umožňující jeho jednoznačnou a jednotnou identifikaci v celé EU. EPP by umožnila, aby **oprávněný zástupce** jednal jménem vlastníka při používání a provozování jejích funkcí na základě jím uděleného oprávnění. Součástí infrastruktury by byl **evropský digitální adresář** vytvořený a spravovaný Komisí pro automatickou a bezpečnou identifikaci adresáta a doručování dokumentů s právními účinky. EPP by současně povinně využívaly jednotnou **kvalifikovanou službu elektronického doporučeného doručování**, kterou by Komise určila prostřednictvím prováděcího aktu podle nařízení eIDAS, jako standardní bezpečný právní komunikační kanál, přičemž její technická integrace by byla závazná pro všechny poskytovatele peněženek. V prováděcích aktech by Komise stanovila normy, technické specifikace a kategorie informací sdělovaných Komisi. **Dohled nad poskytovateli** by vykonávaly **vnitrostátní dozorové orgány podle eIDAS**, zatímco na EPP používané orgány EU by dohlížela **Komise**.

Poznámka PI:

eIDAS je nařízení (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu, které stanoví právní rámec pro používání prostředků elektronické identifikace a důvěryhodných služeb v EU. (Zdroj: Digitální a informační agentura. eIDAS, služby vytvářející důvěru a elektronická identifikace).

Subjekty veřejného sektoru by musely do 24 měsíců umožnit hospodářským subjektům používat EPP k identifikaci, autentizaci, podepisování, předkládání dokumentů a zasílání či přijímání oznámení v rámci správních postupů. Pro předkládání dokumentů a doručování by musely mít vlastní peněženku včetně kvalifikované služby elektronického doporučeného doručování, přičemž po dobu 36 měsíců by mohly dočasně podporovat i rovnocenná řešení podle eIDAS.

Návrh umožňuje Komisi uznat **podnikatelské peněženky a obdobné systémy třetích zemí** za rovnocenné EPP, pokud jsou interoperabilní s rámcem eIDAS a zajišťují identifikaci, autentizaci a výměnu potvrzení atributů. Komise je oprávněna uznání změnit, pozastavit nebo zrušit. Návrh stanoví také podmínky pro **vydávání EPP hospodářským subjektům usazeným mimo Unii**, kterým může být vydán pouze jeden soubor identifikačních údajů a jedinečný identifikátor po ověření totožnosti podle eIDAS. Členské státy a orgány dohledu mají spolupracovat, aby se zabránilo duplicitnímu vydávání identifikačních údajů.

Stanovisko vlády ČR k nařízení o EPP:

Vláda v obecné rovině vítá cíle návrhu **nařízení o EPP**, avšak některé aspekty shledává jako problematické s ohledem na již zavedené a využívané systémy a procesy na národní úrovni, které návrh nařízení nereflektuje dostatečným způsobem. Zejména se jedná o úmysl plošně zavést jednu konkrétní kvalifikovanou službu elektronického doporučeného doručování v rámci EPP bez ohledu na stávající systémy elektronického doručování dokumentů v členských státech (v ČR informační systém datových schránek). Zvláštní pozornost je třeba věnovat dopadům na malé podnikatele/OSVČ.

4. Strategie evropské datové unie: zpřístupnění dat pro umělou inteligenci

Nová **Strategie evropské datové unie** v návaznosti na Evropskou strategii pro data z roku 2020 nastiňuje další opatření v oblasti dat. Stávající legislativa o datech vytvořila základ pro jednotný trh s daty, EU však stále čelí třem zásadním výzvám: (1) nedostatku rozsáhlých, kvalitních a interoperabilních datových souborů, které brzdí inovace v oblasti UI, zejména u malých a středních podniků, (2) fragmentaci a složitosti pravidel pro přístup k datům a jejich používání (včetně souběhu s GDPR) a (3) rostoucí globální konkurenci v mezinárodním kontextu. Strategie má zajistit bezpečné a zodpovědné využívání dat pro umělou inteligenci a inovace, zapojit průmysl a veřejný sektor a posílit konkurenceschopnost a technologickou suverenitu EU.

Strategie stojí na třech pilířích.

1. **Rozšíření přístupu k datům pro umělou inteligenci** s cílem zajistit přístup k vysoce kvalitním datům potřebným pro inovace, a to prostřednictvím (a) **rozšiřování společných evropských datových prostorů** s podporou ve výši cca 100 milionů eur napříč klíčovými odvětvími, jako jsou zdravotnictví, mobilita, energetika, veřejná správa, životní prostředí a obrana, (b) **datových laboratoří**, které budou nabízet komplexní služby umožňující bezpečné využívání dat pro vývoj UI v souladu s právními předpisy, zejména jejich sdružování, zpřístupňování a technickou přípravu pro trénování a testování modelů, které budou zahrnovat např. anonymizaci a pseudonymizaci, generování syntetických dat, poskytování bezpečného výpočetního prostředí a cílené regulační poradenství, (c) **aktu o rozvoji cloudu a umělé inteligence**, který Komise předloží v prvním čtvrtletí roku 2026 k zajištění dostupnosti udržitelné infrastruktury datových center a suverénních cloudových a UI služeb prostřednictvím podpory inovací v celém hodnotovém řetězci a urychlení budování potřebných kapacit, (d) **rozšíření a zpřístupnění strategických datových fondů** veřejného sektoru, vědy, kultury a jazyků pro trénování modelů, včetně otevřených dat s vysokou hodnotou (rozšířených o právní, soudní, správní a další data), evropského cloudu pro vědu a digitalizovaných kulturních a jazykových zdrojů, a (e) **podpory horizontálních opatření pro datovou ekonomiku** k zajištění důvěryhodného používání syntetických dat, právně bezpečného a efektivního sdružování dat mezi podniky napříč odvětvími a jednotných standardů kvality, sběru a anotace dat, což usnadní trénování a opakované využívání modelů UI.

2. **Zjednodušení pravidel pro údaje** s cílem zjednodušit a modernizovat pravidla pro data tak, aby podporovala inovace a malé a střední podniky, a to: (a) **aktualizací a konsolidací *acquis* EU**, sjednocením sdílení dat veřejného sektoru a pravidel pro cookies a ochranu soukromí, (b) **vytvořením předvídatelného a soudržného rámce pro data** s posíleným prosazováním a důvěrou při zprostředkování dat, (c) zavedením **„dodržování předpisů jedním kliknutím“** přes digitální nástroje a EPP pro snadné ověřování souladu s regulacemi a (d) **pomocí podnikům** prostřednictvím vzorových smluv, standardních doložek, pokynů k přiměřené kompenzaci a právních konzultací, aby mohly plně využít akt o datech a soustředit se na inovace.

3. **Zajištění svrchovanosti EU v oblasti údajů** s cílem posílit celosvětovou pozici EU v

oblasti mezinárodních datových toků. Komise konkrétně: (**a**) stanoví **spravedlivé podmínky pro přeshraniční datové toky** a účinnou kontrolu v rámci mezinárodního digitálního obchodu, **vydá pokyny** k hodnocení zacházení s daty EU třetími zeměmi, přijme nástroje proti lokalizaci, diskriminačním omezením a únikům dat a přijme první balíček opatření na ochranu citlivých neosobních údajů v EU, (b) podpoří **propojení ekosystémů EU s podobně smýšlejícími třetími zeměmi**, včetně evropských datových prostorů, standardních smluvních doložek a závazků v mezinárodních dohodách, a (**c**) posílí **vliv EU v globální správě dat**, bude prosazovat hodnoty EU v digitálních dohodách a fórech a podporovat spolupráci s kandidátskými a sousedními zeměmi.

Stanovisko vlády ČR ke Strategii evropské datové unie:

Vláda v obecné rovině vítá **Strategii evropské datové unie** a podporuje její cíl posílit konkurenceschopnost EU prostřednictvím lepší dostupnosti a využitelnosti kvalitních dat pro umělou inteligenci, inovace a modernizaci veřejného sektoru.

- **Předpokládaný harmonogram projednávání v orgánech EU:**
  K přijetí navrhovaných nařízení je vyžadováno, aby se Evropský parlament a Rada shodly na jejich znění. V Evropském parlamentu je pro **digitální omnibus** výborem odpovědným za projednání návrhu Výbor pro průmysl, výzkum a energetiku (ITRE) a Výbor pro občanské svobody, spravedlnost a vnitřní věci (LIBE). Zpravodajkou ITRE byla určena Aura Salla (EPP) a zpravodajkou LIBE Marina Kaljurand (S&D). Návrh byl také postoupen k vyjádření stanoviska Výboru pro vnitřní trh a ochranu spotřebitelů (IMCO) a Výboru pro právní záležitosti (JURI).

  Digitální omnibus pro umělou inteligenci byl přidělen Výboru pro vnitřní trh a ochranu spotřebitelů (IMCO) a Výboru pro občanské svobody, spravedlnost a vnitřní věci (LIBE). Zpravodajkou IMCO je Arba Kokalari (EPP) a zpravodajem LIBE Michael McNamara (Renew). K vyjádření stanoviska byl návrh předložen také Výboru pro průmysl, výzku a energetiku (ITRE), Výboru pro pro dopravu a cestovní ruch (TRAN), Výboru pro pro kulturu a vzdělávání (CULT) a Výboru pro právní záležitosti (JURI).

  Jedním ze stínových zpravodajů je k oběma digitálním omnibusům česká europoslankyně Markéta Gregorová (Greens/EFA).

  Poznámka PI:

  Dne 26. 1. 2026 Komise představila členům výboru **LIBE** zjednodušující balíčky týkající se digitálních pravidel a umělé inteligence. U cílených změn **GDPR** někteří poslanci varovali, že změna definice osobních údajů by mohla ohrozit standardy ochrany soukromí. Byly také vyjádřeny obavy ohledně nových výjimek, které umožňují **systémům** UI zpracovávat zvláštní kategorie osobních údajů. Vnímané oslabení povinností transparentnosti v rámci aktu o UI dále přispělo k obavám, že **vysoce** rizikové **systémy** UI by **mohly** být klasifikovány jako nerizikové, což by mohlo ovlivnit dohled a odpovědnost. Další členové zdůrazňovali význam evropské konkurenceschopnosti a inovací.

  Návrh zprávy (Draft report PE782.530v01-00) s pozměňovacími návrhy, který představuje oficiální první pozici Evropského parlamentu k návrhu digitálního omnibusu pro UI, byl dne 5. 2. 2026 společně přijat **výbory IMCO a LIBE**. Obsahuje přibližně 24 pozměňovacích návrhů a podporuje zjednodušení a zpřehlednění uplatňování aktu o UI. Doporučuje odklad účinnosti s pevnými daty 2. 12. 2027 pro systémy z přílohy III a 2. 8. 2028 pro systémy z přílohy I. Zahrnuje úpravy týkající se gramotnosti v oblasti UI, zpracování zvláštní kategorie osobních údajů pro odhalování a omezení nespravedlivých vlivů algoritmů, fungování notifikovaných orgánů, kybernetické bezpečnosti a testovacích prostředí (sandboxů). Dne 12. 2. 2026 se konalo

mimořádné zasedání výboru JURI, kde byl projednáván návrh stanoviska k této zprávě IMCO a LIBE. Dne 26. 2. 2026 bylo přijato stanovisko výboru JURI.

Dne 26. 2. 2026 byla na výboru IMCO představena nová studie analyzující digitální balíček. Studie upozorňuje, že některé návrhy mohou ohrozit právní jistotu a ochranu práv jednotlivců a podniků. **Změna definice osobních údajů** může oslabit jednotnou ochranu podle GDPR, vyloučit pseudonymizovaná a nepřímo identifikovatelná data, ohrozit dodržování pravidel i právní jistotu, práva subjektů údajů a kybernetickou bezpečnost, přičemž není jasné, zda skutečně přispěje ke zjednodušení a konkurenceschopnosti. **Omezení přístupu k údajům** se odchyluje od judikatury Soudního dvora EU a bylo by v rozporu s Chartou základních práv EU, ohrozilo by právní jistotu a ochranu subjektů údajů. **Automatizovaná a strojově čitelná označení voleb subjektu údajů v koncovém zařízení fyzických osob** spíše nepřinesou skutečnou kontrolu uživatelů, ale jen technicky přesunou problém, delegují rozhodování na prohlížeče, umožní vliv dominantních firem a širokou interpretaci výjimek u nízkorizikových cookies. **Výjimky pro mediální služby** vytvářejí dvojí standard. Návrh má omezenou účinnost proti „dark patterns" a neřeší „cookie fatigue". **Konsolidace aktu o datech** snižuje roztříštěnost pravidel, ale ponechává mezery v implementaci a může posílit postavení držitelů dat na úkor veřejného sektoru a práv uživatelů. **Zavedení jednotného kontaktního místa (SEP)** je vítáno, ale nedostatečné zdroje pro správu a provoz platformy a nesladěné definice mohou centralizovat fragmentaci a vést k duplicitním požadavkům. **Zpracování osobních údajů pro vývoj a provoz UI na základě oprávněného zájmu** obchází balanční test, umožňuje rozsáhlé zpracování dat bez dostatečného dohledu a záruk a uplatnění práva na námitku je v praxi téměř nemožné. **Rozšířené zpracování zvláštní kategorie osobních údajů pro testování zkreslení UI** u širšího okruhu systémů, možnost jejich reziduální přítomnosti při nepřiměřeném úsilí o odstranění a posílení využití oprávněného zájmu namísto souhlasu může stírat hranici mezi „testováním zkreslení" a tréninkem, vytvářet nejistotu ohledně právního základu a záruk a zvyšovat riziko diskriminace. **Změny v harmonogramu povinností vysoce rizikových systémů UI, oslabení povinnosti zajistit gramotnost v oblasti UI a nedostatečně vymezený EU sandbox a reálné testování** snižují právní jistotu a mohou ohrozit ochranu základních práv. Studie proto doporučuje, aby Evropský parlament trval na důkladném odůvodnění navrhovaných změn, postupoval etapově, nejprve posílil nástroje pro praktické uplatňování pravidel namísto otevírání jejich struktury, zajistil silnější dohled a záruky u zvláštní kategorie osobních údajů a využil proces k harmonizaci právních definic, posílení spolupráce regulačních orgánů a zohlednění sociálních, pracovních a strategických dopadů, zejména v kontextu postavení Evropy v oblasti umělé inteligence.

Za projednání nařízení o EPP a Strategie evropské datové unie je odpovědný Výbor pro průmysl, výzkum a energetiku (ITRE), zpravodajkou pro nařízení o EPP byla určena Eero Heinäluoma (S&D). O stanovisko byl požádán také Výbor pro vnitřní trh a ochranu spotřebitelů (IMCO), Výbor pro právní záležitosti (JURI) a Výbor pro občanské svobody, spravedlnost a vnitřní věci (LIBE).

V Radě se návrhy zabývají její přípravné orgány. Digitální omnibus a digitální omnibus pro umělou inteligenci projednává pracovní skupina pro zjednodušování (AGS), nařízení o EPP a Strategii evropské datové unie pracovní skupina pro telekomunikace a informační společnost v rámci Rady pro dopravu, telekomunikace a energetiku (TTE) – část telekomunikace a informační společnost.

Ve spolupráci se zpravodajkou výboru pro evropské záležitosti Irenou Ferčíkovou Konečnou zpracovala Mgr. Andrea Pokorná, odborná konzultantka Parlamentního institutu Kanceláře PS PČR.

15

PARLIAMENT
OF THE CZECH REPUBLIC
Chamber of Deputies
Petr Sokol
Chairman
Committee on European Affairs

Prague, 18th March 2026

Dear Ms. President,

I would like to inform you on the opinion of the Committee on European Affairs of the Chamber of Deputies of the Parliament of the Czech Republic

on the Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus) /Concil Code 15698/25, COM(2025) 837 final/;

on the Proposal for a Regulation of the European Parliament and of the Council on the establishment of European Business Wallets /Council Code 15701/25, COM(2025) 838 final/;

on the Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI) /Council Code 15708/25, COM(2025) 836 final/ and

on the Communication from the Commission to the European Parliament and the Council – Data Union Strategy Unlocking Data for AI /Council Code 15712/25, COM(2025) 835 final/.

The respective documents were included in the agenda of the 7th session of the Committee on European Affairs and were scrutinized on 18th March 2026. According to the Rules of Procedure a Deputy Minister of Industry and Trade and a representative of the Office of the Government were present at the session to introduce the preliminary Government's Framework Position.

Parliament of the Czech Republic, Chamber of Deputies, Sněmovní 3, 118 26 Praha 1
tel.: +420-257 173 411, fax: +420-257 173 415
http://www.psp.cz/vez

After the hearing of the rapporteur's review and after the discussion the Committee has adopted the **Resolution No. 37 in the context of the Political Dialogue** which is enclosed to this letter.

Yours sincerely

Ms. Ursula von der Leyen
President of the European Commission
B r u s s e l s

Parliament of the Czech Republic, Chamber of Deputies, Sněmovni 3, 118 26 Praha 1
tel.: +420-257 173 411, fax: +420-257 173 415
http://www.psp.cz/vez

Parliament of the Czech Republic
Chamber of Deputies
2026
10th election period

Resolution No. 37
of the Committee on European Affairs

7th Session on 18 March 2026

Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus) /Concil Code 15698/25, COM(2025) 837 final/;

Proposal for a Regulation of the European Parliament and of the Council on the establishment of European Business Wallets /Council Code 15701/25, COM(2025) 838 final/;

Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI) /Council Code 15708/25, COM(2025) 836 final/ and

Communication from the Commission to the European Parliament and the Council – Data Union Strategy Unlocking Data for AI /Council Code 15712/25, COM(2025) 835 final/

Committee on European Affairs

1. **takes note of** the Communication on the Data Strategy, the Proposal for a Digital Omnibus, the Proposal for a Regulation on the EPP, and the Proposal for an Omnibus on the AI (hereinafter collectively referred to as the "Digital Package");

2. **expresses its agreement** with the Czech Government's Framework Position on these documents, particularly in the sections supporting the reduction of the administrative burden on small and medium-sized enterprises, but with reservations regarding measures that undermine transparency and legal certainty, and instructs the Government to keep it informed of the progress of further discussions on the draft Digital Omnibus, the AI Omnibus, and the EPP Regulation in the Council of the EU;

3. **after a thorough assessment of these proposals has concluded** that the submitted Digital Package, **in certain aspects carries a risk of non-compliance with the principle of proportionality**, as administrative simplification may also entail interference with the fundamental rights to the protection of personal data and privacy, specifically in the following areas:

Parliament of the Czech Republic, Chamber of Deputies, Sněmovní 3, 118 26 Praha 1
tel.: +420-257 173 411, fax: +420-257 173 415
http://www.psp.cz/vez

a. Narrowing the definition of personal data: In line with the Position of the Czech Government and the joint opinion of the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS), the Committee expresses serious reservations regarding the proposed amendment to the definition of personal data. According to the EDPB, this amendment is not in line with the case law of the Court of Justice of the European Union. Although the Committee fully supports the need to reduce unnecessary bureaucratic burdens on businesses and research institutions, this must be done while respecting the protection of pseudonymized data to avoid weakening privacy protection. At the same time, in line with the EDPB, EDPS, and RPV, the Committee expresses reservations about transferring the authority to set pseudonymization rules to the Commission, as this should remain within the competence of independent supervisory authorities and the courts. (Digital Omnibus)
b. Threat to data subjects' right of access: The Digital Omnibus introduces the possibility of refusing a request for access to data on grounds other than the protection of personal data. Both the EDPB and the EDPS consider this step problematic and contrary to the horizontal nature of the right to data protection. In line with the Government's concerns regarding legal certainty, the Board warns that such a restriction creates room for arbitrariness on the part of controllers when handling requests. The Committee calls for a balanced solution, better specification, or definition that will reduce unnecessary bureaucratic burdens in cases of potential abuse of data subjects' right of access for purposes other than the protection of personal data. At the same time, the Committee emphasizes that any restrictions must not undermine the rights of workers in the platform economy to review algorithmic decision-making. (Digital Omnibus)
c. Restrictions on transparency for high-risk AI: The Committee agrees with the Government's Position, which does not agree with the removal of the obligation to register high-risk AI systems in the EU database in cases where the provider conducts its own assessment. Such a step would be contrary to the principle of transparency under Article 49(2) of the AI Act and would allow providers to avoid all obligations for high-risk AI in a non-transparent and unilateral manner, which drastically limits oversight capabilities and endanger the safety of citizens. The Committee agrees with the Government's Position calling for a simplification of the entire registration process, rather than its complete abolition. (Omnibus for AI)
d. Problematic legal basis for training AI on sensitive data: The Committee expresses concern over the introduction of exceptions to the obligation to erase sensitive data in cases of "disproportionate effort," which weaken the protection of the most vulnerable data without a proper proportionality analysis having been conducted. The Committee notes alignment with the EDPB's opinion, which does not consider the proposed exceptions for the processing of sensitive data by AI systems to be necessary and recommends their strict limitation; at the same time, however, it is aware of the importance of using data to detect and eliminate bias in artificial intelligence models. The Committee therefore urges that, should any exceptions be introduced, they be accompanied by clear safeguards against misuse. At the same time, it calls for clarification of the definition of the term "disproportionate effort." In this context, the Government's opinion correctly highlights the risks arising from the unclear definition of the Commission's implementing powers in this area. (Omnibus for AI)
e. Ban on AI systems for sexual manipulation (nudifying): In line with the Council's current position, the Committee urges that a new point should be added to the first subparagraph of Article 5(1) of the AI Act, prohibiting the placing on the market, putting into service, or use of AI systems that, without the consent of an identifiable natural person, modify, manipulate, or artificially generate realistic images or videos depicting sexually explicit activities or intimate body parts without the consent of an identifiable natural person. This prohibition does not apply to providers with effective safeguards against misuse, nor does it hinder the development of technical capabilities for legitimate purposes. (AI Omnibus);

4. **calls on the Commission**, in accordance with the mandate set out in the Act on the Digital Single Market, to prioritize the introduction of harmonized methodologies for measuring and

Parliament of the Czech Republic, Chamber of Deputies, Sněmovní 3, 118 26 Praha 1
tel.: +420-257 173 411, fax: +420-257 173 415
http://www.psp.cz/vez

transparently reporting the environmental footprint and energy consumption of digital single market systems and data centers, while ensuring that the administrative burden is not increased;

5. **welcomes** the initiative to establish European Business Wallets (EBWs), which has the potential to significantly reduce the administrative burden on businesses and facilitate their cross-border interactions. In line with the Government's Position, emphasizes the necessity for this EU Framework to reflect and integrate existing national electronic delivery and identification systems to the greatest extent possible. It calls for strict adherence to data protection standards and the assurance of cybersecurity (security by design), while maintaining the principle of voluntary use of this tool for economic operators. In the interest of privacy protection, the committee recommends the use of a decentralized architecture (SSI) that prevents blanket monitoring of transactions and commercial profiling of companies;

6. **welcomes** the European Data Union Strategy and, in line with the Government's Position, supports its ambition to strengthen the Union's competitiveness and technological sovereignty through three key pillars: expanding access to high-quality data for artificial intelligence and innovation, simplifying data rules and protecting EU data sovereignty through a strategic international data policy, while emphasizing support for open-source solutions and open standards as the foundation for genuine EU technological independence and transparency; at the same time, **notes** that this approach is consistent with the Czech Republic's National Artificial Intelligence Strategy 2030;

6. **authorizes** the Chairman of the Committee on European Affairs to inform on this Resolution the President of the European Commission **in the context of the political dialogue.**

Parliament of the Czech Republic, Chamber of Deputies, Sněmovní 3, 118 26 Praha 1
tel.: +420-257 173 411, fax: +420-257 173 415
http://www.psp.cz/vez