6. 5. 2026

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Digital Omnibus: Revoluce v datech, nebo jen nová zátěž pro podnikatele?

Dne 19. listopadu 2025 zveřejnila Evropská komise legislativní balíček známý jako Digitální Omnibus. Tento krok navazuje na strategické zprávy politiků Maria Draghiho a Enrica Letty, které shodně identifikovaly regulatorní fragmentaci a vysokou administrativní zátěž jako hlavní překážky evropské konkurenceschopnosti. Pod heslem „A simpler and faster Europe“ se Evropská unie pokouší o zásadní obrat v digitální regulaci: od extenzivní normotvorby směrem k efektivnější harmonizaci, deregulaci a funkčnímu propojení již existujících předpisů.

Balíček Digitálního Omnibusu není izolovaným zásahem, ale komplexním souborem úprav rozděleným do dvou hlavních větví. První z nich, obecný **Digital Omnibus**[1], cílí na provázání a úpravu klíčových norem, jako jsou obecné nařízení o ochraně osobních údajů[2] („**GDPR**“), směrnice ePrivacy[3], směrnice NIS2[4] a Akt o datech (Data Act)[5]. Druhá větev, **Digital Omnibus on AI**[6], pak specificky modifikuje nedávno přijatý Akt o umělé inteligenci[7] („**AI Act**“). Společným cílem je odstranit výkladové nejasnosti a duplicitu povinností, které dosud brzdily zejména malé a střední podniky v inovativním nakládání s daty.

Rozsah navrhovaných změn týkajících se GDPR je nakonec poměrně překvapivý. Zatímco původní debaty a stanoviska Evropského sboru pro ochranu osobních údajů („**EDPB**“) naznačovaly spíše „kosmetické“ úpravy (akcentovaly např. zjednodušení záznamů o činnostech zpracování), finální návrh Komise jde mnohem dále. Předložený text reflektuje novou generaci datových předpisů EU – a pokouší se o hlubší integraci principů ochrany soukromí s potřebami digitální ekonomiky a sdílení dat.

Je však nutné zdůraznit, že se v současné době nacházíme na počátku legislativního procesu. Návrh Digital Omnibus bude teprve předmětem vyjednávání v rámci trialogu, jehož zahájení se očekává ve třetím čtvrtletí 2026.

Níže předložený článek si klade za cíl analyzovat navrhované změny, posoudit jejich potenciální dopad na správce a zpracovatele údajů a kriticky zhodnotit, zda navržená deregulace skutečně přinese proklamované zjednodušení, aniž by došlo ke snížení standardu ochrany subjektů údajů.

Redefinice pojmu osobní údaj?

Jednou z nejdiskutovanějších změn, které měl Digital Omnibus přinést, je koncepční posun v chápání pojmu „osobní údaj” ve smyslu čl. 4 odst. 1 GDPR. Stávající definice vymezuje osobní údaj jako jakoukoliv informaci o identifikované nebo identifikovatelné fyzické osobě. Tento pojem byl tradičně chápán spíše jako absolutní kategorie - informace buď osobním údajem je, nebo není, bez ohledu na to, kdo s ní nakládá. Judikatura Soudního dvora Evropské unie („**SDEU**“)[8] ovšem zdůrazňuje, že posouzení identifikovatelnosti musí probíhat s ohledem na konkrétní kontext zpracování a zejména prostředky, které má daný správce či zpracovatel k dispozici.

Evropská komise navrhla toto relativní pojetí osobního údaje zakotvit přímo do textu GDPR. Nově by se posuzovalo, zda je informace osobním údajem z perspektivy konkrétní organizace a s ohledem na

to, zda je skutečně schopna danou osobu identifikovat. Praktický dopad by byl zásadní: tatáž informace by pro jednu organizaci byla osobním údajem, zatímco pro jinou nikoli.

Návrh vzbudil vlnu diskuzí. Kritika zaznívala zejména ze strany dozorových orgánů a odborné veřejnosti. EDPB a Evropský inspektor ochrany údajů ve společném stanovisku[9] upozornili, že navrhovaná změna nepředstavuje pouze technické zpřesnění, ale fakticky zasahuje do samotné podstaty pojmu osobních údajů, což může vést k fragmentaci ochrany a k právní nejistotě. Podobně nevládní organizace[10] poukazovaly na riziko, že by relativní pojetí mohlo být zneužíváno k vyvázání určitých forem zpracování z působnosti GDPR, a to zejména v oblasti online sledování a cílené reklamy.

Tyto výhrady se promítly i do legislativního procesu. **V aktuální fázi projednávání Digital Omnibus Rada Evropské unie navrhovanou redefinici pojmu osobní údaj ze svého kompromisního textu vypustila**[11] a její právní zakotvení do textu GDPR se proto jeví jako nepravděpodobné.

Diskuse otevřená návrhem digitálního nařízení nicméně ukazuje na přetrvávající napětí mezi snahou o regulatorní zjednodušení a zachováním vysoké úrovně ochrany osobních údajů v digitální ekonomice. Lze očekávat, že tato otázka bude i nadále řešena prostřednictvím judikatury a metodických pokynů dozorových orgánů, spíše než změnou samotné definice v primárním textu GDPR.

Nová výjimka z informační povinnosti

Další změnou, kterou Digital Omnibus přináší, je rozšíření výjimky z informační povinnosti správce podle článků 13 a 14 GDPR. V současné době platí, že správce je povinen poskytnout subjektu údajů při získávání osobních údajů široké spektrum informací – od identity správce přes účely zpracování až po kategorie příjemců a práva subjektů údajů. Výjimka existuje pouze v případě, že subjekt údajů *„již tyto informace má"*.

Návrh digitálního nařízení tuto výjimku rozšiřuje na situace, kdy existuje jasný a vymezený vztah mezi správcem a subjektem údajů v rámci činnosti, která není náročná na data, a současně existují oprávněné důvody se domnívat, že subjekt údajů již informace zná.

Tato změna reflektuje kritiku ze strany zejména malých a středních podniků, které dosud musely plnit náročné informační povinnosti i v případech, kdy jejich splnění nepřinášelo žádnou přidanou hodnotu pro ochranu subjektů údajů.

Komise uvádí typické příklady, kdy bude možné novou výjimku aplikovat:

- **Řemeslníci a poskytovatelé služeb**: vztah mezi řemeslníkem (například truhlářem, elektrikářem) a jeho klienty je jasně vymezený, zpracování dat není datově intenzivní a je zřejmé, že klient zná účel zpracování (například kontaktní údaje pro fakturaci a realizaci zakázky).
- **Sportovní kluby a sdružení**: vedení evidence členů, komunikace se členy a organizace sportovních akcí představuje nízce rizikové zpracování, kdy je vztah mezi správcem a subjektem údajů zcela transparentní.

Výjimka se neuplatní a informační povinnost je ovšem třeba plnit vždy, pokud jde o:

- zpracování údajů zaměstnanců (kde existuje nerovné postavení mezi správcem a subjektem údajů);

- zapojení dalšího příjemce (například externího zpracovatele);
- předání údajů mimo EU;
- automatizované rozhodování;
- vysoce rizikové zpracování (například zpracování zvláštní kategorie osobních údajů podle článku 9 GDPR).

Cílem této změny mělo být zejména usnadnění fungování malým podnikatelům, u nichž administrativní náklady na sestavení formálních informačních dokumentů představují nepřiměřenou zátěž vzhledem k povaze jejich činnosti. Praxe však bude zřejmě složitější. Výjimka totiž operuje s řadou neurčitých právních pojmů (jasný a vymezený vztah, datově náročná činnost nebo oprávněné důvody). Navíc výjimka odpadá vždy, jakmile do zpracování vstoupí externí subjekt – například běžný IT dodavatel nebo účetní software v cloudu. Situace typického malého podnikatele tak paradoxně může být po přijetí nové úpravy administrativně náročnější než dříve: místo vyhotovení dnes již standardní informační doložky bude muset provést právní posouzení, zda vůbec podmínky pro výjimku splňuje.

Nový důvod pro odmítnutí žádosti o přístup

Právo na přístup k osobním údajům zakotvené v článku 15 GDPR patří mezi základní práva subjektů údajů. V praxi však správci stále častěji čelí zneužívání tohoto práva, kdy subjekty údajů podávají žádosti nikoli za účelem ochrany svých osobních údajů, ale s úmyslem vyvolat odmítnutí správce a následně požadovat odškodnění nebo hrozit právními kroky. Tyto situace představují značnou administrativní a finanční zátěž pro správce, kteří jsou nuceni věnovat významné zdroje vyřizování žádostí, které nejsou vedeny legitimním zájmem.

Současná právní úprava v článku 12 odst. 5 GDPR sice umožňuje správci odmítnout žádost, pokud je *„zjevně nedůvodná nebo nepřiměřená“*, nicméně praxe ukazuje, že důkazní břemeno spočívá na správci a prokazování zneužití práva je často velmi obtížné.

Digital Omnibus reaguje na tyto problémy zavedením nového důvodu pro odmítnutí žádosti o přístup, **pokud existují *„rozumné důvody“* se domnívat, že žádost byla podána pro jiné účely než ochranu osobních údajů**. Dochází tedy k významnému snížení důkazního břemene pro správce – místo zjevné nedůvodnosti či nepřiměřenosti postačí, aby správce měl rozumné důvody pro svůj závěr.

Podle Komise by mělo jít o případy, kdy subjekt údajů opakovaně podává identické žádosti v krátkém časovém období, zjevně útočí na správce v médiích nebo na sociálních sítích před podáním žádosti, nebo kdy z jeho komunikace vyplývá primární záměr získat finanční kompenzaci spíše než skutečně vykonávat právo na informace.

V takových případech může správce žádost odmítnout nebo může účtovat přiměřený poplatek za její vyřízení. Tato změna by měla správcům umožnit efektivněji vyřizovat legitimní žádosti, které přispívají k ochraně práv subjektů údajů.

Na druhou stranu je třeba upozornit na riziko, že nová úprava může být zneužita samotnými správci k odmítání nepříjemných, ale legitimních žádostí. Snížení důkazního břemene a neurčitý pojem *„rozumných důvodů“* mohou vést k situacím, kdy správci budou příliš ochotně klasifikovat žádosti jako zneužívající, čímž dojde k oslabení práv subjektů údajů. Bude proto klíčové, jak dozorové úřady a judikatura následně tento nový důvod odmítnutí vyloží.

Výjimka pro zpracování biometrických údajů za účelem verifikace

Článek 9 odst. 1 GDPR zakazuje zpracování zvláštních kategorií osobních údajů, mezi které patří i **biometrické údaje zpracovávané za účelem jedinečné identifikace fyzické osoby**. V praxi však tento obecný zákaz způsoboval nejasnosti zejména u technologií, jako je Face ID nebo Touch ID na mobilních zařízeních, kde jsou biometrické údaje používány čistě k verifikaci identity uživatele (tedy k ověření, že jde o oprávněného uživatele daného zařízení), nikoli k identifikaci ve smyslu určení totožnosti neznámé osoby.

Digital Omnibus zavádí **novou výjimku**, podle které zpracování biometrických údajů za účelem verifikace nebude podléhat zákazu článku 9 odst. 1 GDPR, pokud tyto údaje **zůstávají pod výlučnou kontrolou subjektu údajů**. Typickým příkladem je právě Face ID na iPhone, kde je biometrický vzor tváře uložen pouze lokálně v zabezpečeném prostoru zařízení (Secure Enclave) a není sdílen s výrobcem zařízení ani žádnou třetí stranou.

Tato změna reaguje na technologický vývoj a snaží se harmonizovat právní úpravu s realitou každodenního používání biometrických technologií. Současně však klade důraz na zásadní podmínku, a to výlučnou kontrolu subjektu údajů, což znamená, že biometrické údaje nesmí opustit zařízení ani být sdíleny s dalšími subjekty.

Pro výrobce zařízení a poskytovatele služeb bude klíčové prokázat, že jejich systémy skutečně splňují podmínku výlučné kontroly subjektu údajů. To bude vyžadovat technickou dokumentaci prokazující, že biometrické údaje jsou ukládány pouze lokálně v zabezpečeném prostředí a transparentní informace pro uživatele o tom, jak jsou jejich biometrické údaje zpracovávány a že nejsou předávány třetím stranám, případně nezávislé audity nebo certifikace systémů, které mají posílit důvěru uživatelů.

Je pravděpodobné, že EDPB vydá další pokyny k výkladu pojmu *„výlučná kontrola subjektu údajů"*, zejména v kontextu cloudových služeb a vzdáleného zálohování dat. Otázkou zůstává, zda bude možné aplikovat výjimku i na situace, kdy jsou biometrické údaje zálohované v šifrované podobě na cloudových serverech výrobce. Technicky by měl přístup pouze subjekt údajů, avšak jeho kontrola nad daty není v takovém případě zcela *„výlučná"*.

Ohlašování jen vysoce rizikových incidentů

Současná úprava v článku 33 GDPR vyžaduje, aby správce oznámil dozorovému úřadu porušení zabezpečení osobních údajů **bez zbytečného odkladu, nejpozději do 72 hodin**, ledaže je nepravděpodobné, že by takový incident měl za následek riziko pro práva a svobody fyzických osob. Tato negativně formulovaná podmínka vytváří nejistotu ohledně toho, kdy je oznamování skutečně nutné. Oproti tomu článek 34 GDPR stanovuje povinnost informovat o incidentu subjekty údajů, pokud je pravděpodobné, že bude mít za následek vysoké riziko pro jejich práva a svobody.

Změna navrhovaná v Digital Omnibus sjednocuje prahy pro oznamování mezi články 33 a 34 GDPR a zavádí jednotnou hranici *„vysokého rizika"* i pro hlášení dozorovému úřadu. Správce bude povinen oznamovat pouze ta porušení zabezpečení, která pravděpodobně povedou k vysokému riziku pro práva a svobody fyzických osob. Současně se **prodlužuje lhůta pro oznamování na 96 hodin**, což má správcům poskytnout dostatečný čas na řádné vyhodnocení incidentu a jeho dopadů.

EDPB bude pověřen vypracováním jednotného evropského formuláře pro oznamování a společného seznamu okolností, které představují vysoké riziko. Tento přístup má odstranit současnou

nejednotnost mezi členskými státy a zjednodušit situaci zejména pro mezinárodně působící správce.

Klíčovou inovací je zavedení **jednotného kontaktního místa** (Single Entry Point - SEP) spravovaného Agenturou Evropské unie pro kybernetickou bezpečnost.[12] Tento systém vychází z principu *„nahlásit jednou, sdílet s mnoha"* a má odstranit překrývající se oznamovací povinnosti napříč různými regulacemi jako je GDPR, směrnice NIS 2 nebo nařízení DORA.[13]

Revoluce v cookies: Konec *„lištového"* teroru?

Navrhovaná reforma představuje významnou korekci současného stavu, který je poznamenán roztříštěností mezi směrnicí e-Privacy a nařízením GDPR. Tento duální režim v praxi generuje značné transakční náklady a právní nejistotu, neboť k téže operaci často přistupují různé dozorové orgány s odlišnou metodikou.

Dosavadní striktní požadavky na aktivní a svobodný souhlas, uplatňované bez ohledu na to, zda ukládané informace představují osobní údaje, vedly v praxi k neudržitelné *„bannerové únavě"*. Navrhovaná reforma se proto snaží tento stav překonat příklonem k technologické neutralitě a automatizaci správy uživatelských preferencí.[14]

Podle nové právní úpravy se má veškeré zpracování osobních údajů v koncovém zařízení řídit výhradně nařízením GDPR. Tím má dojít k odstranění interpretačních rozporů a sjednocení dohledu pod mechanismus *„one-stop-shop"*.

Návrh dává Evropské komisi mandát k vytvoření navazujících norem pro automatizované předávání preferencí subjektu údajů. Správci budou povinni respektovat **signály vysílané prohlížečem**[15] či **agentní umělou inteligencí**.

Návrh zavádí v článku 88a hierarchickou strukturu pravidel, která kombinuje ochranu soukromí s pragmatickým přístupem k fungování digitálních služeb. Výchozím pravidlem zůstává **princip opt-in**: jakýkoliv přístup k datům v zařízení uživatele je primárně podmíněn jeho svobodným souhlasem. Návrh však ponechává prostor pro specifické výjimky stanovené právem Unie nebo členského státu, pokud sledují důležité veřejné zájmy (například bezpečnost státu či vymáhání práva dle čl. 23 GDPR).

Přínosem pro konkurenceschopnost má být **rozšíření tzv. zákonných licencí**, kdy je zpracování zákonné bez nutnosti souhlasu. Jedná se o situace, kdy je operace nezbytná pro:

a. **Technický přenos** - tj. zajištění samotné elektronické komunikace v síti.
b. **Vyžádanou službu** - tj. poskytnutí funkce, kterou uživatel výslovně aktivoval (tzv. funkční cookies).
c. **Vlastní analytiku (měření návštěvnosti)** - jde o vytváření agregovaných statistik výhradně pro potřeby správce, což de facto legalizuje analytické nástroje bez nutnosti banneru, pokud data nejsou sdílena s třetími stranami.
d. **Kybernetickou bezpečnost** – operace pro zajištění integrity a obnovu bezpečnosti služby, o kterou uživatel či jeho zařízení požádalo.

Pro situace, kde souhlas zůstává nezbytný, tj. zejména **marketingový tracking**, zavádí článek 88a procesní pravidla pro zamezení manipulativních technik. Jde jednak o zdůraznění zavedeného principu, že odmítnutí souhlasu musí být stejně jednoduché jako jeho udělení. Návrh explicitně vyžaduje tlačítko pro odmítnutí na první úrovni banneru (**princip** „**Single Click**"). Dále návrh zavádí **ochranu před „re-promptingem"**, tj. pokud uživatel souhlas udělí, správce jej nesmí zbytečně žádat znovu. Pokud uživatel souhlas **odmítne**, vzniká **šestiměsíční lhůta**, během které je

zakázáno uživatele se stejnou žádostí znovu kontaktovat.

Posun v automatizovaném rozhodování: Konec doktríny *„lidského faktoru“*

Významnou bariéru pro digitální inovace dosud představovala rigidní interpretace článku 22 GDPR, který v základu zakazuje rozhodnutí založená výhradně na automatizovaném zpracování. Ačkoliv existuje výjimka pro případy, kdy je takové rozhodování **nezbytné pro plnění smlouvy**, dozorové orgány a judikatura tento pojem vykládají poměrně restriktivně.[16] Pokud totiž bylo teoreticky možné proces zajistit lidskou silou, byla automatizace často shledána jako *„postradatelná“*.

Navrhovaná revize tento přístup zásadně mění a zavádí **objektivnější standard nezbytnosti**. Automatizované rozhodování bude nově přípustné vždy, pokud je logickou součástí smluvního plnění, a to bez ohledu na hypotetickou možnost zapojení člověka do rozhodovacího procesu. Pokud však existuje několik stejně účinných řešení automatizovaného zpracování, měl by správce použít to méně rušivé.

Podnikům ve finančním sektoru, pojišťovnictví či logistice to může zlepšit pozici při nasazování pokročilých algoritmů a představovat impulz pro zvyšování konkurenceschopnosti na globálním trhu.

Harmonizace DPIA: Konec národní fragmentace

Dalším významným krokem může být navrhovaná unifikace procesu **posouzení vlivu na ochranu osobních údajů** („**DPIA**“). Současný stav, kdy seznamy operací vyžadujících DPIA (dle čl. 35 odst. 4 a 5 GDPR) definují jednotlivé národní dozorové orgány, vytváří pro subjekty působící ve více členských státech nepřehledné a často protichůdné regulatorní prostředí. Tato fragmentace zvyšuje právní nejistotu a administrativní náklady zejména u inovativních projektů s přeshraničním přesahem.

Reforma tuto pravomoc přenáší na **Evropskou komisi**, která nově vydá **jednotný unijní seznam** operací zpracování, jež DPIA podléhají, i těch, která jsou od této povinnosti explicitně osvobozena. Klíčovým přínosem pro praktické fungování podniků bude zavedení závazné **jednotné metodiky a šablony**. Pro správce to znamená nejen významné snížení nákladů na právní poradenství, ale především možnost spolehnout se na presumpci shody při dodržení jednotných metodických pokynů napříč celým jednotným trhem.

Flexibilní právní rámec pro éru umělé inteligence

Významnou inovací, kterou Digitální Omnibus přináší, je vyplnění legislativního vakua v oblasti trénování a nasazování modelů umělé inteligence.

Pro vývoj AI je nyní explicitně připuštěn **oprávněný zájem** (čl. 6 odst. 1 písm. f GDPR) jako dostatečný právní titul, jsou-li splněny specifické podmínky transparentnosti a bezpečnosti.

Návrh obsahuje i novou **výjimku pro využití zvláštních kategorií osobních údajů** (například údaje o zdravotním stavu) pro účely vývoje a používání AI. Tato možnost je podmíněna zavedením robustních technických a organizačních opatření. Je však otázka, do jaké míry tato opatření představují další vrstvu povinností nad rámec požadavků kladených **Aktem o umělé inteligenci**, což může v praxi vyžadovat další harmonizaci compliance procesů.

Návrh dále zavádí logickou posloupnost nakládání s daty v AI systémech. Primárním cílem je data

nezpracovávat, pokud to není nezbytné. Pokud k tomu dojde, má být zajištěno jejich včasné **odstranění** (např. po fázi trénování). V poslední instanci je třeba **zajistit jejich ochranu přímo ve výstupech AI**, aby nedocházelo k neoprávněné identifikaci subjektů údajů skrze vygenerovaný obsah.

Posílení inovačního potenciálu skrze vědecký a komerční výzkum

Závěrečný pilíř reformy se zaměřuje na modernizaci pravidel pro vědecký a historický výzkum. Návrh Digitálního Omnibusu **explicitně uznává komerční výzkum jako legitimní formu vědecké činnosti** požívající stejných privilegií jako výzkum akademický.

Pro vědecké účely nově nebude nutné striktně dodržovat pravidlo slučitelnosti s původním účelem sběru dat (tzv. purpose compatibility), pokud budou implementovány vhodné záruky. Tato úleva (která se však netýká zpracování založeného na souhlasu) umožní efektivní sekundární využití velkých datových sad pro další výzkum bez nutnosti získávat nové právní tituly.

Významnou procesní úlevu představuje rozšíření **výjimky z informační povinnosti**. Ta se nově uplatní i v případech, kdy byla data získána přímo od subjektu údajů, pokud by následné informování o výzkumném využití vyžadovalo **nepřiměřené úsilí**.

Tato opatření v souhrnu mají vytvořit pro evropské firmy i výzkumné instituce prostředí s nižší administrativní zátěží, které umožňuje rychlejší přechod od sběru dat k inovativním objevům a produktům.

Závěrečné shrnutí

Digital Omnibus odráží snahu Evropské unie najít rovnováhu mezi ochranou osobních údajů a potřebami digitální ekonomiky. Pro podnikatele to v praxi znamená méně administrativních povinností v některých oblastech, zároveň však novou nejistotu tam, kde návrh operuje s neurčitými právními pojmy. Z dlouhodobého hlediska však může konsolidace digitální regulace posílit stabilitu právního prostředí a podpořit důvěru v evropský digitální trh.

Mgr. Andrea Diligent,
senior právník, Pražská energetika, a.s.

Mgr. Michaela Vimpelová, LL.M.,
advokátka

PIERSTONE

PIERSTONE s.r.o., advokátní kancelář

Perlová 371/5
110 00 Praha 1

Tel.: +420 224 234 958
E-mail: michaela.vimpelova@pierstone.com

[1] Evropská komise, ‘Návrh nařízení o souhrnném digitálním nařízení’ (Policy and legislation, zveřejněno dne 19. listopadu 2025) k dispozici >>> zde cit.19 ledna 2026

[2] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů [2016] OJ L 119/1

[3] Směrnice evropského parlamentu a Rady (EU) 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací [2002] OJ L 201/37

[4] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii [2022] OJ L 333/80

[5] Nařízení Evropského parlamentu a Rady (EU) 2023/2854 ze dne 13. prosince 2023 o harmonizovaných pravidlech pro spravedlivý přístup k datům a jejich využívání [2023] OJ L 1/71

[6] Evropská komise, ‘Digitální souhrnný návrh na nařízení o umělé inteligenci’ (Policy and legislation, zveřejněno dne 19. listopadu 2025) k dispozici >>> zde cit.19 leden 2026

[7] Nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci [2024] OJ L 1/144

[8] Rozsudek Soudního dvora EU ve věci C-319/22 Gesamtverband Autoteile-Handel v. Scania ze dne 9. listopadu 2023 a rozsudek Soudního dvora EU ve věci C-413/23 EDPS v. SRB ze dne 4. září 2025

[9] EDPB-EDPS Joint opinion 2/2026 on the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus), zveřejněno dne 11. února 2026, dostupné >>> zde.

[10] NOYB – European Center for Digital Rights. Digital Omnibus: Analysis of Select GDPR and ePrivacy Proposals by the European Commission, Version 2.0, leden 2026, dostupné >>> zde.

[11] Claudie Moreau, ‘Council deletes revised definition of personal data from GDPR Omnibus’ (Euractiv, 20. února 2026), informující o uniklém kompromisním textu kyperského předsednictví Rady EU ze dne 20. února 2026, ze kterého byla navrhovaná redefinice pojmu osobní údaj vypuštěna; k dispozici >>> zde.

[12] Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA (Agentuře Evropské unie pro kybernetickou bezpečnost) a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 (akt o

kybernetické bezpečnosti) [2019] OJ L 151/15

[13] Nařízení Evropského parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011 [2022] OJ L 333/1

[14] Srov. rozsudek Soudního dvora EU ve věci C-673/17 Planet49 [2019], úř. věst. C 413, s. 4, který potvrdil nepřípustnost předem zaškrtnutých políček a definitivně propojil věcnou působnost směrnice o soukromí a elektronických komunikacích s požadavky nařízení GDPR

[15] S ohledem na nařízení Evropského parlamentu a Rady (EU) 2024/1083 (EMFA) ze dne 11. 4. 2024, kterým se stanoví společný rámec pro mediální služby na vnitřním trhu [2024] OJ L 1/37, je však zachována výjimka pro poskytovatele mediálních služeb. Ti nebudou povinni automatizované signály respektovat, čímž je chráněn jejich obchodní model založený na přímé interakci a personalizovaném financování nezávislé žurnalistiky

[16]Evropská komise, Restriktivní přístup dozorových orgánů k pojmu nezbytnosti potvrzují Pokyny k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679 (wp251rev.01), (Pokyny, zveřejněno dne 22. srpna 2018) k dispozici >>> zde cit. 28 ledna 2026, podle nichž musí správce prokázat, že neexistuje žádná jiná, k soukromí šetrnější alternativa k dosažení stejného cíle. Tento trend vyvrcholil v nedávném rozsudku SDEU ve věci C-634/21 SCHUFA Holding (Scoring) [2023] Úř. věst. C 37, který za automatizované rozhodnutí označil i dílčí procesy (scoring), pokud mají určující vliv na finální rozhodnutí, čímž zásadně zúžil prostor pro flexibilní využití algoritmů v rámci smluvních vztahů

Další články:

- Digital Omnibus: Revoluce v datech, nebo jen nová zátěž pro podnikatele?
- Darování pro případ smrti nemovité věci zapsané v katastru nemovitostí a určení výše odměny soudního komisaře
- Flotilová novela: Kdo a kdy musí nově získat licenci k distribuci pojištění?
- Nová pravidla pro ground handling v EU a jejich dopady na letecký sektor
- Právní due diligence nemovitostí: na co se v praxi skutečně zaměřit
- Hmotněprávní opatrovník obchodní korporace: mezi efektivní ochranou a zásahem do korporační autonomie
- Byznys a paragrafy, díl 32.: Konkurenční doložka
- Skryté ujednání v realitní smlouvě – zbytečná hra na schovávanou
- Odpovědnost člena voleného orgánu dle § 159 OZ a vymezení škody způsobené právnické osobě
- Vnosy do společného jmění manželů a jejich valorizace v aktuální judikatuře Nejvyššího soudu a Ústavního soudu
- Právo na přístup ke kamerovým záznamům: střet GDPR, informačního zákona a praxe veřejných institucí