Weinhold Legal

Digital Legal Update

LEDEN 2026

Níže přinášíme aktuální informace z DIGITAL oblasti. Budete-li mít k níže uvedenému jakékoliv dotazy, neváhejte se na nás obrátit.

Obsah

AKTUALITY Z LEGISLATIVY

Zákon o kybernetické bezpečnosti

Nový zákon o kybernetické bezpečnosti (č. 264/2025 Sb.), který provádí směrnici NIS2, nabyl účinnosti dne 1. listopadu 2025.

Spolu s ním nabyly účinnosti jeho prováděcí předpisy, kterými jsou zejména následující vyhlášky Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB):

- č. 334/2025 Sb., o Portálu Národního úřadu pro kybernetickou a informační bezpečnost a požadavcích na některé úkony,
- č. 408/2025 Sb., o regulovaných službách,
- č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností,
- č. 410/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností.

Poskytovatelé regulovaných služeb byli povinni provést ohlášení regulovaných služeb do 31. prosince 2025.

Zákon o odolnosti subjektů kritické infrastruktury

Nový zákon č. 266/2025 Sb., o odolnosti subjektů kritické infrastruktury (zákon o kritické infrastruktuře), transponuje směrnici 2022/2557 o odolnosti kritických subjektů (směrnice CER - Critical Entities Resilience). **Účinnosti zákon nabyl dne 19. srpna 2025**.

Systém kritické infrastruktury není novinkou, v českém

právním řádu byl již zakotven od roku 2010, a to konkrétně v krizovém zákoně.

Dříve se zákon zaměřoval na prvky kritické infrastruktury, tedy objekty, stavby, zařízení nebo sítě, které byly odpovědnými orgány určovány.

V rámci nového přístupu je pozornost zaměřená na poskytování základní služby daným provozovatelem. Neurčují se již „prvky kritické infrastruktury“, ale **„subjekty kritické infrastruktury“**, které následně samy definují svou kritickou infrastrukturu nezbytnou pro poskytování základní služby.

Nový zákon vymezuje, co se považuje za základní službu. Jde například o dodávky energie, zdravotní péči, dopravu, vodní hospodářství, digitální infrastrukturu nebo fungování veřejné správy.

Poskytovatelem základní služby je každý, kdo ji na území České republiky zajišťuje a současně naplňuje alespoň jedno z kritérií významnosti, například počtem uživatelů, tržním podílem nebo závislostí dalších odvětví.

Poskytovatel základní služby, který nejpozději k 30. listopadu 2025 zahájil poskytování základní služby, je povinen poskytnout informace příslušným úřadům **do 1. března 2026**. Zatím však nebyly přijaty prováděcí předpisy:

- nařízení vlády o základních službách a kritériích významnosti,
- vyhláška o náležitostech a zpracování plánu odolnosti, posouzení rizik a obsahu opatření k zajištění odolnosti subjektů kritické infrastruktury,
- vyhláška k podrobnostem hlášení incidentů v souvislosti se subjekty kritické infrastruktury, a
- vyhláška o portálu kritické infrastruktury.

NAVRHOVANÁ LEGISLATIVA

Digital Omnibus

Evropská komise dne 19. listopadu 2025 představila nový balíček legislativních návrhů s názvem Digital Omnibus. Hlavním motivem tohoto balíčku je **snaha po zjednodušení a snížení administrativní zátěže.** Digital Omnibus se dotýká zejména Digital Services Act (DSA), Digital Markets Act (DMA), AI Act, Data Governance Act, Data Act a okrajově také GDPR a ePrivacy.

Digital Services Act

Ve vztahu k DSA digitální omnibus nemění samotný obsah povinností platforem ani odpovědnost za nezákonný obsah, ale soustředí se na procesní a institucionální sladění jeho uplatňování s dalšími digitálními předpisy EU, zejména GDPR, AI Act, DMA a Data Act. Jeho cílem je zvýšit právní jistotu a předvídatelnost dohledu, omezit duplicitní řízení a nekoordinované sankce a vyjasnit rozdělení kompetencí mezi dozorové orgány, aniž by docházelo ke zmírnění nebo zjednodušení věcných povinností vyplývajících z DSA.

AI Act

Úlevy čekají společnosti, které vyvíjejí nebo používají systémy umělé inteligence. Původní pravidla nařízení označovaného jako AI Act ukládají společnostem povinnost registrovat určité vysoce rizikové systémy v databázi EU. Nový návrh tuto povinnost navrhuje zrušit pro ty systémy, které sice spadají do kategorie vysoce rizikových, ale v praxi nepředstavují zásadní hrozbu pro základní práva (například systémy určené jen pro úzké procedurální úkoly). Místo registrace bude nově stačit, pokud si společnost zpracuje vlastní hodnocení a uloží si jej pro případnou kontrolu.

Weinhold Legal

Digital Legal Update

LEDEN 2026

Změna se má dotknout i vzdělávání. AI Act zavedl provozovatelům a poskytovatelům AI systémů (tj. i zaměstnavatelů) povinnost zajistit AI gramotnost (schopnost rozumět fungování AI). Digital Omnibus navrhuje tuto odpovědnost přesunout primárně na členské státy a Komisi, kteří mají za úkol zajistit potřebnou osvětu a nástroje.

Pro vývojáře se navíc od roku 2028 plánují celoevropská „pískoviště“ (sandboxy), kde bude možné AI bezpečně testovat v reálném prostředí bez obav z okamžitých sankcí.

GDPR

V oblasti ochrany osobních údajů je cílem návrhu zvýšit právní jistotu a předvídatelnost pro vývojáře a provozovatele digitálních technologií, zejména tím, že zpřesňuje vztah GDPR k dalším evropským digitálním předpisům a podporuje jednotnou aplikační praxi.

Návrh nemění pravidla pro určení právního základu podle GDPR, ale vyjasňuje, že oprávněný zájem podle čl. 6 odst. 1 písm. f) GDPR může být za určitých okolností posuzován jako relevantní právní základ i pro účely trénování AI modelů či vědeckého výzkumu, pokud je splněn test proporcionality a jsou přijata odpovídající ochranná opatření, jako je např. pseudonymizace nebo omezení účelu. Návrh tak posiluje důraz na rizikově orientovaný a kontextový přístup, nikoli na plošné rozšíření možnosti využívání osobních údajů.

Cookies

Novinkou pro uživatele i provozovatele webů má být plánované omezení vyskakovacích oken pro udělení souhlasu s cookies. Navíc pro cookies, které nejsou pro soukromí uživatele rizikové (například pro základní měření návštěvnosti nebo funkčnost webu), nebude již nutné vyžadovat souhlas.

NIS2

V souvislosti s hlášením incidentů má dojít ke sjednocení pravidel. V současnosti společnosti musí hlásit jeden incident více úřadům podle různých předpisů (GDPR, NIS2, DORA). Nově by mělo vzniknout jen jedno kontaktní místo pro všechna hlášení incidentů.

Data Act

Ve vztahu k Data Act se digitální omnibus zaměřuje na zpřesnění a koordinaci jeho uplatňování s dalšími digitálními předpisy EU, zejména GDPR, DSA a AI Act. Jeho cílem je zvýšit právní jistotu adresátů Data Actu, omezit duplicitní oznamovací a kontrolní povinnosti, vyjasnit procesy při žádostech veřejného sektoru o data a sladit role dozorových orgánů, aniž by docházelo k omezení samotné povinnosti sdílení dat v případech stanovených tímto nařízením.

European Business Wallet

Poslední novinkou je zavedení Evropské obchodní peněženky (European Business Wallet). Půjde o digitální nástroj, který má společnostem umožnit snadno prokazovat svou identitu a ověřovat obchodní partnery napříč celou EU, což si klade za cíl zrychlit a zabezpečit přeshraniční obchodování.

Celý balíček je nyní ve fázi návrhu Evropské komise, která zároveň spustila veřejnou konzultaci tzv. „Digital Fitness Check“. Veřejná konzultace poběží do března 2026. **Finální podoba pravidel se tedy může ještě měnit.**

Implementace AI Actu v ČR

Ministerstvo průmyslu a obchodu připravilo návrh zákona o umělé inteligenci.

Jelikož je evropská legislativa přímo použitelná, tuzemský zákon nezavádí nová pravidla pro fungování AI, ale soustředí

se minimalisticky pouze na nezbytné procesní a institucionální úpravy, které jsou v kompetenci členských států.

Roli hlavního gestora a koordinátora bude mít Ministerstvo průmyslu a obchodu, zatímco dohled nad trhem a funkci jednotného kontaktního místa bude vykonávat Český telekomunikační úřad. Zapojeny budou rovněž Česká národní banka a Úřad pro ochranu osobních údajů, zatímco Úřad pro technickou normalizaci převezme roli oznamujícího orgánu a bude akreditovat subjekty posouzení shody. V oblasti ochrany základních práv bude hrát významnou roli Veřejný ochránce práv, současně se počítá se vznikem národního regulačního sandboxu, který má společnostem umožnit bezpečné testování AI systémů před jejich uvedením na trh a vytvořit odpovídající prostředí také pro vznik oznámených subjektů odpovědných za certifikaci vybraných systémů umělé inteligence.

Návrh dále definuje skutkové podstaty přestupků a nastavuje proces ukládání sankcí za porušení pravidel, přičemž maximální výše pokut vychází přímo z evropského nařízení a může dosáhnout až 35 milionů eur nebo 7 % celosvětového obratu podniku.

U návrhu bylo ukončeno meziresortní připomínkové řízení, jednotlivé připomínky jsou teď zpracovávány.

Chat Control

Rada EU schválila dne 27. listopadu 2025 svou vyjednávací pozici k návrhu nařízení CSAM (někdy označovanému jako „chat control“), jehož cílem je ochrana dětí v digitálním prostředí a boj proti sexuálnímu zneužívání dětí online. Návrh počítá s tím, že poskytovatelé digitálních služeb budou povinni posuzovat rizika zneužití svých služeb a v odůvodněných případech zavádět opatření ke snížení těchto rizik, včetně detekce a hlášení nelegálního obsahu.

Možnost automatizované detekce obsahu, která by v krajním případě mohla vést k zásahům do soukromé komunikace a tlaku na oslabení end-to-end šifrování, vyvolala rozsáhlé kontroverze. Rada EU se proto snažila nalézt kompromis, který by umožnil ochranu dětí, aniž by vedl k plošnému sledování komunikace. Přesto zůstává návrh politicky citlivý a některé členské státy, včetně České republiky, se nadále staví proti řešením, která by mohla znamenat plošný monitoring obsahu nebo oslabení šifrovaných služeb.

NOVINKY Z OBLASTI GDPR

Nové procesní nařízení pro přeshraniční stížnosti týkající se ochrany údajů

Dne 12. prosince 2025 bylo na poli EU zveřejněno nové procesní nařízení, které má za cíl zrychlit a zefektivnit vymáhání GDPR v přeshraničních případech. Dosavadní systém vyřizování přeshraničních stížností často vedl k dlouhým a nejasným řízením, které zvyšovaly náklady i právní nejistotu pro organizace i fyzické osoby.

Klíčovým prvkem je harmonizace kritérií přípustnosti stížností napříč členskými státy a posílení procesních práv účastníků, včetně možnosti vyjádřit se k podstatným podkladům a předběžným zjištěním.

Nařízení stanoví závazné lhůty pro postup v přeshraničních věcech (včetně rámce 15 měsíců s možností jednorázového prodloužení o 12 měsíců u výjimečně složitých případů). Nařízení zavádí také mechanismus „early resolution“, který umožňuje řízení ukončit, pokud bylo porušení napraveno a stížnost ztratila předmět, při zachování procesních záruk

Weinhold Legal

Digital Legal Update

LEDEN 2026

pro stěžovatele.

Nová procesní pravidla se začnou plně uplatňovat od 2. dubna 2027.

DMA a GDPR – Společné pokyny EDPB a Komise

Evropský sbor pro ochranu osobních údajů (EDPB) a Komise zveřejnily dne 9. října 2025 společné pokyny k vyjasnění povinností podle nařízení o digitálních trzích (Digital Markets Act – DMA) a nařízení GDPR.

Cílem pokynů je zajistit jednotný výklad obou předpisů a poskytnout právní jistotu tzv. *gatekeeperům* (velkým digitálním platformám - např. Meta, Google, Apple), kteří musí naplnit požadavky DMA a zároveň respektovat zásady GDPR. Klíčovým poselstvím těchto společných pokynů je skutečnost, že oba předpisy se uplatňují paralelně, a že DMA nenahrazuje GDPR ani nezavádí nový právní základ pro zpracování osobních údajů.

Hlavní témata pokynů jsou:

- požadavky na platný souhlas uživatele podle čl. 5 (2) DMA a GDPR jsou stanovené tak, aby *gatekeepeři* mohli legálně kombinovat nebo křížově využívat osobní údaje v hlavních službách platforem;
- povinnost nabídnout „méně personalizovanou, ale ekvivalentní“ verzi služby;
- určení právních základů zpracování a jejich omezení;
- interoperabilita (povinnost gatekeeperů technicky umožnit propojení svých služeb s jinými) a nutnost provádět posouzení vlivu na ochranu osobních údajů (DPIA);
- koordinace dohledu mezi Komisí a dozorovými úřady.

Společné pokyny potvrzují, že DMA a GDPR se doplňují, nikoli nahrazují, a že ochrana osobních údajů zůstává nepřekročitelnou hranicí i při plnění povinností digitální regulace.

Pokyny jsou zveřejněny jako návrh ke konzultaci, připomínky bylo možné zasílat do 4. prosince 2025. Publikace finální verze se očekává v průběhu roku 2026.

Stanovisko EDPB k odpovídající ochraně UK

EDPB přijal v říjnu 2025 dvě stanoviska k návrhu Evropské komise na prodloužení rozhodnutí o odpovídající ochraně pro Spojené království (podle GDPR a podle Směrnice o ochraně údajů při prosazování práva – LED). Komise navrhuje prodloužit platnost rozhodnutí o odpovídající ochraně o dalších šest let, tedy až do **27. prosince 2031**.

EDPB dospěl k závěru, že britský právní rámec se nadále v zásadě shoduje s rámcem EU a že osobní údaje mohou být nadále předávány bez dodatečných záruk. Zároveň však identifikoval několik oblastí, v nichž by měl být budoucí vývoj britského práva pečlivě monitorován. Jde zejména o nový britský test pro předávání údajů do třetích zemí založený na kritériu, že ochrana nesmí být „materiálně nižší“, o benevolentnější přístup k automatizovanému rozhodování a možná omezení práva na lidský přezkum, jakož i o rozšíření výjimek z některých zásad ochrany údajů v souvislosti s národní bezpečností a vymáháním práva. Komise bude muset tyto aspekty zohlednit ve finálním rozhodnutí a zajistit jejich důsledné průběžné sledování.

Koordinovaná kontrolní akce 2026

EDPB vybral jako téma pro svou pátou koordinovanou kontrolní akci, která proběhne v roce 2026, dodržování

Weinhold Legal

Digital Legal Update

LEDEN 2026

povinnosti transparentnosti a informování subjektů údajů.

Dozorové úřady jednotlivých členských států se zaměří na prověřování toho, zda správci plní požadavky článků 12, 13 a 14 GDPR a zda řádně informují jednotlivce o zpracování jejich osobních údajů.

Výsledky národních šetření budou následně agregovány do společné zprávy pro případná další cílená opatření. Tato akce je klíčovou součástí dlouhodobé strategie EDPB pro roky 2024–2027 a navazuje na předchozí ročníky kontrol zaměřené na využívání cloudových služeb veřejným sektorem, postavení pověřenců, právo na přístup či aktuálně vyhodnocované právo na výmaz.

Pokyny EDPS k řízení rizik u AI

Evropský inspektor ochrany údajů (EDPS) vydal dne 11. listopadu 2025 nové pokyny týkající se identifikace a zmírnění rizik spojených s vývojem, nákupem a provozem systémů umělé inteligence. Hlavním cílem těchto pokynů je pomoci identifikovat a zmírnit rizika pro základní práva jednotlivců, která vznikají při zpracování osobních údajů pomocí systémů AI. Pokyny se zaměřují na technická opatření k zajištění souladu s klíčovými zásadami ochrany osobních údajů, kterými jsou spravedlnost, přesnost, minimalizace údajů a bezpečnost.

EDPS zdůrazňuje význam interpretovatelnosti a vysvětlitelnosti AI systémů jako předpokladu pro plnění dalších právních povinností a upozorňuje na zvýšená rizika spojená s využíváním tzv. black box modelů. V oblasti spravedlnosti se věnuje eliminaci předpojatosti vznikající v datech i v návrhu algoritmů, která může vést k diskriminačním výstupům. U zásady přesnosti upozorňuje mimo jiné na halucinace generativních modelů a na riziko data driftu (tj. zhoršování kvality dat v čase). Významná část pokynů se zabývá také bezpečnostními hrozbami, včetně útoků typu model inversion (při nichž lze z výstupů modelu rekonstruovat trénovací data), a praktickými obtížemi při uplatňování práv subjektů údajů.

Pokyny posouvají důraz od formálního plnění GDPR k aktivnímu a průběžnému řízení rizik AI systémů. V praxi to znamená, že nasazení umělé inteligence není jednorázovým krokem, ale kontinuálním procesem vyžadujícím systematickou dokumentaci, technické kontroly a pravidelné vyhodnocování dopadů na základní práva; správci již při výběru či nákupu AI musí posuzovat vysvětlitelnost, kvalitu dat, bezpečnost a možnost uplatnění práv subjektů údajů, tyto požadavky smluvně i technicky zajistit a průběžně monitorovat rizika jako halucinace, bias či data drift. Odpovědnost za soulad s právními předpisy zůstává vždy na správci, nikoli na dodavateli AI.

EVROPSKÁ JUDIKATURA

Vztah GDPR a ePrivacy

Rozsudek Soudního dvora C-654/23 ze dne 13. listopadu 2025 řešil spor mezi rumunskou společností provozující právní zpravodajský web a rumunským vnitrostátním orgánem pro dohled nad zpracováním osobních údajů. V tomto sporu šlo o posouzení, zda provozovatel mohl zasílat denní e-mailový newsletter uživatelům s bezplatným účtem bez jejich výslovného souhlasu, a to na základě výjimky „soft opt-in“ podle směrnice ePrivacy, aniž by bylo nutné opírat se o samostatný právní základ podle GDPR.

Společnost argumentovala tím, že registrace uživatele představovala formu prodeje služby, což jí dává právo posílat nabídky na podobné služby i bez speciálního souhlasu.
Soudní dvůr se postavil na stranu společnosti a potvrdil, že

v digitálním světě slovo prodej neznamená jen výměnu peněz. Pokud se uživatel zaregistruje, aby získal přístup k obsahu, který by jinak neviděl, uzavírá tím se společností smlouvu. Emailovou adresu uživatele získá společnost tedy **v souvislosti s prodejem výrobku nebo služby**, jelikož zaslání takového informačního zpravodaje představuje použití elektronické pošty **pro účely přímého marketingu svých vlastních obdobných výrobků nebo služeb**.

Provozovatel tak může využít své oprávnění zasílat na tyto adresy nevyžádaná sdělení týkající se vlastních obdobných výrobků či služeb (tzv. soft opt-in), aniž by potřeboval samostatný souhlas, pokud zákazníkům umožní toto využití jednoduše a zdarma odmítnout. Pokud jsou splněny tyto specifické podmínky čl. 13 odst. 2 směrnice 2002/58 (ePrivacy směrnice), která působí jako lex specialis, neuplatní se na toto zpracování obecné podmínky zákonnosti stanovené v čl. 6 odst. 1 nařízení GDPR.

Vymezení pseudonymizace

Soudní dvůr EU rozhodl dne 4. září 2025 v případu C-413/23 P spor mezi EDPS a Evropským úřadem pro řešení krizí (dále jen „Úřad“), který řešil krizi španělské banky Banco Popular. Jádrem sporu bylo vyřešení, zda jsou pseudonymizované připomínky akcionářů a věřitelů banky po předání externímu poradci stále osobními údaji, pokud tento příjemce nemá rozumně dostupné prostředky k jejich zpětné identifikaci konkrétních osob, a zda tedy bylo nutné plnit informační povinnosti vůči subjektům údajů i ve vztahu k tomuto předání.

Konkrétně se v daném případě jednalo o situaci, kdy Úřad předtím, než data odeslal svému externímu poradci, nahradil jména konkrétních osob číselnými kódy, tedy provedl tzv. pseudonymizaci, v jejímž důsledku tento poradce neměl možnost osoby identifikovat.

Výsledkem sporu bylo, že Soudní dvůr EU potvrdil, že pseudonymizované připomínky akcionářů a věřitelů banky předané externímu poradci nepředstavovaly pro tohoto příjemce osobní údaje, pokud neměl žádné rozumně dostupné prostředky k identifikaci dotčených osob. Soudní dvůr však zdůraznil, že pro Úřad samotný osobními údaji zůstávaly, protože disponoval re-identifikačním klíčem. Úřad nebyl povinen plnit informační povinnosti vůči subjektům údajů ve vztahu k samotnému předání pseudonymizovaných dat poradci, nicméně jeho povinnosti ochrany osobních údajů jako původního správce tím nebyly dotčeny a měl tedy informovat o předání osobních údajů v souladu s čl. 13 a 14 GDPR.

DALŠÍ AKTUALITY

Komise uložila společnosti X pokutu za porušení DSA

Komise uložila společnosti X pokutu ve výši 120 milionů eur za porušení povinností podle nařízení o digitálních službách (DSA). Konkrétně společnost X porušila povinnosti velmi velkých online platforem v oblasti řízení systémových rizik, transparentnosti fungování služby a nakládání s nezákonným a škodlivým obsahem. Komise dospěla k závěru, že společnost X nepřijala dostatečná a přiměřená opatření k ochraně uživatelů a veřejného diskurzu, jak nařízení DSA vyžaduje.

Případ je významný tím, že potvrzuje reálnou vymahatelnost DSA a ukazuje, že povinnosti platforem nejsou jen formální – Komise hodnotila nejen existenci interních pravidel, ale i jejich skutečnou účinnost v praxi. Rozhodnutí je silným signálem pro další velké online platformy, že nedostatečné řízení rizik, netransparentní algoritmy či slabý dohled nad

obsahem mohou vést k citelným sankcím na úrovni EU.

Jedná se o první rozhodnutí o nesouladu podle DSA.

Komise: Možné protisoutěžní jednání společnosti SAP

Komise má předběžný názor, že společnost SAP omezovala soutěž na trhu údržby a podpory on-premise softwaru pro plánování podnikových zdrojů (Enterprise Resource Planning – ERP).

Společnost SAP mohla zneužít svého dominantního postavení (na trhu EHP s poprodejními službami údržby a podpory on-premise softwaru pro ERP od společnosti SAP) tím, že:

a) zákazníkům vnucuje politiku „všechno nebo nic“, která vyžaduje, aby zákazníci od společnosti SAP odebírali údržbu a podporu pro veškerý svůj on-premise software pro ERP od společnosti SAP na stejné úrovni podpory;
b) zákazníkům brání v ukončení služeb údržby a podpory pro nepoužívané softwarové licence („shelfware“);
c) prodlužuje počáteční dobu platnosti licencí pro on-premise ERP, během níž údržbu a podporu nelze ukončit;
d) účtuje poplatky za obnovení a za zpětnou údržbu zákazníkům, kteří se po období nepřítomnosti přihlásí k údržbě a podpoře od společnosti SAP.

Společnost SAP nabídla závazky (i když nesouhlasí s předběžným názorem Komise):

Mezi klíčové prvky závazků patří:

a) **Politika „všechno nebo nic“**: Zákazníci společnosti SAP mohou požádat o rozdělení svého digitálního prostředí, jež integruje všechny on-premise softwarové produkty a licence pro ERP od společnosti SAP, do samostatných komerčních instalací. Pro každou komerční instalaci si zákazníci budou moci vybrat různé poskytovatele údržby a podpory a/nebo různé úrovně podpory od společnosti SAP, nebo budou moci ponechat své komerční instalace bez podpory.
b) **Shelfware**: Společnost SAP se zavazuje, že nabídne větší transparentnost a širší přístup ke smlouvám s jednou metrikou, v jejichž rámci jsou licenční poplatky – včetně poplatků za údržbu a podporu – vypočítány na základě dohodnuté metriky, např. příjmů. Kromě toho budou mít zákazníci rovněž možnost si zřídit samostatné komerční instalace, které zahrnují shelfware, a ukončit údržbu a podporu takové komerční instalace.
c) **Prodloužení počáteční doby platnosti**: Společnost SAP se zavazuje, že vyjasní svá smluvní ustanovení týkající se prodloužení počáteční doby platnosti a nebude vyžadovat její opětovné zahájení při každém dalším nákupu licence.
d) **Poplatky za zpětnou údržbu a obnovení**: Společnost SAP se zavazuje, že zruší poplatky za obnovení a sníží poplatky za zpětnou údržbu na 50 % výše poplatků za údržbu a podporu, které by zákazník zaplatil, pokud by podporu neukončil, s omezením na šest měsíců. Společnost SAP se rovněž zavazuje, že zcela upustí od poplatků za zpětnou údržbu u seznamu produktů, které již nejsou společností SAP podporovány a na něž se nevztahuje licence napříč produkty.

Komise má v úmyslu tyto závazky přijmout.

ÚOHS prověřoval možné zneužití dominantního postavení v oblasti inzerce na pracovních portálech

Úřad prověřoval možné zneužití dominantního postavení společností skupiny Alma Career na českém trhu poskytování služeb inzerce na online pracovních portálech.

Skupina Alma Career provozuje nejznámější inzertní portály *jobs.cz* a *prace.cz*, přičemž sama je současně výrobcem software pro správu náboru zaměstnanců (tzv. ATS).

Úřad vyšetřoval podezření, že skupina Alma Career zneužívá své výsadní postavení a prostřednictvím cenových i technických překážek znesnadňuje propojení konkurenčních ATS a konkurenčních pracovních portálů se systémy Alma Career.

Úřad pro ochranu hospodářské soutěže zastavil správní řízení poté, co účastník řízení předložil závazky, které mají zajistit interoperabilitu s konkurenčními službami poskytovanými na dotčených trzích.

Martin Lukáš
Partner
martin.lukas@weinholdlegal.com

Tereza Hošková
Vedoucí advokátka
tereza.hoskova@weinholdlegal.com

Nikola Faltová
Advokátka
nikola.faltova@weinholdlegal.com

Jana Duchoňová
Advokátka
jana.duchonova@weinholdlegal.com