10 LET S GDPR

10 let od schválení GDPR

Letos v dubnu uplyne deset let od schválení zásadní reformy ochrany osobních údajů v Evropské unii - přijetí obecného nařízení o ochraně osobních údajů (GDPR). Toto nařízení zásadním způsobem ovlivnilo řadu oborů a stalo se inspiračním zdrojem pro řadu obdobných právních úprav po celém světě. Při této příležitosti vám přinášíme několik textů o významu GDPR připravených zástupci českého Úřadu pro ochranu osobních údajů, který je dozorovým orgánem ve věcech ochrany osobních údajů v České republice, a neziskové organizace Spolek pro ochranu osobních údajů.

Úřad pro ochranu osobních údajů

Spolek pro ochranu osobních údajů

Co je GDPR?

GDPR je evropské nařízení platící ve všech státech EU a také v Norsku, Lichtenštejnsku a na Islandu.

Jeho oficiální název je **Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)**

Unifikační význam GDPR a mezinárodní spolupráce

GDPR přineslo sjednocení pravidel ochrany osobních údajů napříč členskými státy Evropské unie. Namísto národních úprav s významnými odlišnostmi vznikl přímo použitelný právní rámec, který stanovil jednotná pravidla pro správce i zpracovatele, a zároveň posílil práva subjektů údajů. Tento unifikační efekt významně přispěl k právní jistotě subjektů, které působí ve více členských státech EU. GDPR však mělo i významný vliv mimo EU, když ovlivnilo legislativu i aplikační praxi v třetích zemích. To byl ostatně i hlavní závěr nedávné mezinárodní konference Spolku pro ochranu osobních údajů.

Sjednocení pravidel je úzce propojeno s mechanismy mezinárodní spolupráce mezi dozorovými úřady. GDPR zakotvilo princip tzv. one-stop-shop a vytvořilo strukturovaný systém spolupráce a konzistence, který umožňuje koordinované rozhodování v přeshraničních případech. Tento rámec byl nedávno dále posílen přijatými změnami zaměřenými na zefektivnění a urychlení spolupráce mezi dozorovými orgány, zejména pokud jde o sdílení informací, procesní koordinaci a vydávání společných stanovisek.

Evropský sbor pro ochranu osobních údajů zde plní klíčovou roli při sjednocování výkladu a řešení sporů mezi dozorovými orgány. Význam těchto mechanismů ilustruje i rozhodovací praxe – například rozhodnutí Úřadu pro ochranu osobních údajů, kterým byla uložena dosud nejvyšší pokuta za dobu účinnosti GDPR, bylo výsledkem právě tohoto procesu mezinárodní spolupráce.

Význam GDPR tedy spočívá zejména ve sjednocení pravidel napříč Evropskou unií, ale i vytyčení institucionálního rámce, který umožňuje jeho jednotné uplatňování napříč Evropskou unií. Celkový dopad GDPR je však globální, když jeho přijetí postupně ovlivnilo legislativu a praxi i v řadě zemí mimo EU.

EDPB – Nový orgán pro novou éru ochrany osobních údajů

Jednou z nejvýznamnějších institucionálních inovací, které GDPR přineslo, je vznik Evropského sboru pro ochranu osobních údajů (EDPB). Nejedná se již o poradní pracovní skupinu, nýbrž o nezávislý orgán s pravomocí vydávat vlastní závazná rozhodnutí a výkladové pokyny či stanoviska, kterými jsou usměrňovány nejen mechanismus spolupráce a jednotnosti, zvláště rozhodování přeshraničních případů s využitím jednotného kontaktního místa (one-stop-shop), ale i výklad GDPR bezprostředně aplikovaný správci osobních údajů a profesionály napříč EHP. Zvláště v poslední době se zaměřuje na praktické nástroje a vzory pro každodenní využití.

Po deseti letech od schválení GDPR je zřejmé, že EDPB zastřešující soustavu dozorových úřadů má zásadní vliv na vymahatelnost práva. Jen za rok 2025 uložily dozorové úřady pokuty v celkové výši 1 145 760 374 EUR. Zároveň EDPB přispívá k pojetí GDPR jako globálního referenčního rámce, který ovlivňuje legislativu daleko za hranicemi EU.

Do budoucna bude stěžejní, jak EDPB naplní svůj mandát v současném prostředí dynamicky se rozvíjejících technologií - počínaje umělou inteligencí až po datovou ekonomiku - a zda personální a odborné kapacity dozorových úřadů porostou úměrně k novým úkolům a narůstajícím výzvám, jimž čelí.

Úřad pro ochranu osobních údajů

Spolek pro ochranu osobních údajů

www.uoou.gov.cz

www.ochranaudaju.cz

Práva subjektů údajů

Svoboda každé lidské bytosti určovat svůj osud nedílně zahrnuje i svobodnou dispozici vlastními osobními údaji. Tato idea, zrozená z hořkých zkušeností se státním i korporátním zneužíváním dat ve 20. století, stála u zrodu práv subjektů údajů jako středobodu ochrany osobních údajů vůbec.

Proto již původní směrnice 95/46/ES obsahovala jak práva subjektů na přístup k údajům, jejich opravu a výmaz, tak i právo na námitku proti zpracování a právo nebýt předmětem rozhodnutí založených výhradně na automatizovaném zpracování.

Obecné nařízení o ochraně osobních údajů tato základní práva přesněji vymezilo a v některých detailech rozšířilo, a zároveň doplnilo paletu práv subjektů údajů o právo na omezení zpracování a právo na přenositelnost údajů. Ale především byly stanoveny jasné procedury a lhůty, které musí správci dodržet při odpovědi na uplatnění subjektivních práv, takže lze konstatovat, že postavení subjektů údajů bylo významně posíleno.

O rostoucím významu práv subjektů svědčí mimo jiné i pozornost, kterou věnují dozorové úřady jak samostatně, tak i v rámci práce Evropského sboru pro ochranu osobních údajů, jejich výkladu i jejich uplatňování v praxi. Řadu výkladových dokumentů k jednotlivým dílčím právům zahájil Evropský sbor vydáním Pokynů EDPB 01/2022 k právům subjektů údajů – právo na přístup. Na implementaci práva na přístup ze strany správců osobních údajů byla zaměřena také jedna z prvních koordinovaných dozorových akcí evropských dozorových úřadů, která proběhla v roce 2024.

Procesní nařízení (EU) 2025/2518 jako posílení procesních práv

Dosavadní zkušenost s prosazováním GDPR ukázala, že mechanismus jednotného kontaktního místa, tedy systém, v němž vedoucí dozorový úřad řeší přeshraniční případy ve spolupráci s ostatními dotčenými dozorovými úřady, trpí slabinou: absencí harmonizovaných procesních pravidel. Nové procesní nařízení tak nemění hmotné právo, nýbrž stanoví postupy dozorových úřadů a procesní práva stěžovatele a vyšetřovaných stran řízení, včetně ochrany před případnou nečinností. Důraz je dán na právo účastníků řízení vyjádřit se k věci i na přesné stanovení rozsahu informací, které si úřady povinně vyměňují. Zachován je však princip, dle něhož stěžovatel není protistranou vyšetřované strany, ale samostatným účastníkem se svébytnými právy.

Zákonodárce se pokusil harmonizovat jen ty instituty, jež vykazovaly problémy, při zachování procesní autonomie členských států. Výsledkem má být stav, v němž dozorové úřady povedou přeshraniční řízení účelně a efektivně, a budou účinně spolupracovat. Ke kontrole výkonnosti mají sloužit i povinně zveřejňované statistické výkazy. Předpis je nicméně provázen obavami, že skokové zvýšení administrativního zatížení dozorových úřadů bez adekvátního personálního posílení ve skutečnosti dozorovou kapacitu úřadů ani jejich efektivitu nezvýší. Nařízení vstoupí v účinnost 2. dubna 2027.

Úřad pro ochranu osobních údajů

Spolek pro ochranu osobních údajů

www.uoou.gov.cz

www.ochranaudaju.cz

Pověřenec pro ochranu osobních údajů (DPO)

Pověřenec pro ochranu osobních údajů (označovaný také jako „DPO“ neboli Data Protection Officer), je dnes již zavedeným institutem obecného nařízení o ochraně osobních údajů (GDPR). Pověřenec u stanovených správců a zpracovatelů osobních údajů dohlíží na to, zda zpracování osobních údajů probíhá v souladu s právními předpisy, slouží jako poradce ve věci ochrany osobních údajů, a zároveň funguje jako kontaktní bod pro dozorový úřad a osoby, jejichž údaje jsou zpracovávány.

Povinnost jmenovat pověřence nemají všichni správci a zpracovatelé. GDPR ji výslovně ukládá orgánům veřejné moci a veřejným subjektům, a dále těm osobám, jejichž hlavní činnost spočívá v rozsáhlém, pravidelném a systematickém zpracování osobních údajů, nebo které ve velkém rozsahu zpracovávají zvláštní kategorie údajů (tzv. citlivé údaje, např. o zdravotním stavu apod.).

Správce a zpracovatel, který pověřence jmenuje, musí zajistit jeho nezávislost. Tak může pověřenec garantovat objektivní posuzování a upozorňování na případné nedostatky bez tlaku ze strany dotčeného správce a nebo zpracovatele. Odpovědnost za soulad s předpisy ve věci zpracování osobních údajů však nadále nese dotčený správce/zpracovatel (jeho vedení a zaměstnanci). Pověřenec jejich činnosti monitoruje, upozorňuje na rizika a navrhuje opatření k nápravě.

Pověřenec může být ve vztahu ke svému správci či zpracovateli zaměstnanec nebo externista. Pověřenec by měl disponovat odbornými znalostmi práva a praxe v oblasti ochrany údajů, nemusí však nezbytně mít právní vzdělání.

Role pověřence se za dobu účinnosti GDPR výrazně proměnila. Rostoucí využívání umělé inteligence, nové regulace v oblasti kybernetické bezpečnosti i digitálních služeb kladou na pověřence stále vyšší nároky. Spolek pro ochranu osobních údajů, který řadu pověřenců sdružuje, na tyto výzvy reaguje průběžným vzděláváním svých členů, činností odborných komisí a každoročním oceňováním nejlepších pověřenců za veřejný i soukromý sektor v soutěži Pověřenec roku.

Deset let GDPR: Rekordní počet stížností potvrzuje význam ochrany osobních údajů

Rok 2025 se zapsal do historie dohledu nad ochranou osobních údajů jako zcela mimořádný. Úřad v tomto roce obdržel nejvyšší počet podnětů a stížností od nabytí účinnosti GDPR. Celkem Úřad obdržel 3 854 podání, což představuje meziroční nárůst o více než 68 %.

Z uvedeného počtu tvořilo 2 514 stížností a 1 340 podnětů, přičemž tento bezprecedentní nárůst reflektuje nejen rostoucí povědomí veřejnosti o právech v oblasti ochrany osobních údajů, ale také proměňující se technologické prostředí. Zejména masivní rozšiřování nástrojů umělé inteligence v běžném životě přináší nové výzvy a mimořádné nároky na činnost Úřadu a jednotlivé zaměstnance. Nástroje AI výrazně usnadňují veřejnosti přístup k informacím o právech subjektů údajů a také samotné podávání stížností dozorovému úřadu. Moderní nástroje AI dnes bez větší námahy dokáží stěžovatelům osvětlit, jaká práva jim plynou z GDPR, a zároveň poradit, jakým způsobem tato práva uplatnit jak u správce, tak u dozorového úřadu. Nástroje umělé inteligence rovněž umožňují automaticky vytvářet samotné texty stížností a podnětů, nezřídka ovšem obsahující některé faktické a právní chyby. Obdobný trend sleduje také většina ostatních dozorových úřadů, a to jak ve smyslu nárůstu počtu stížností, tak využití nástrojů AI při jejich tvorbě.

Zvláštní pozornosti si dlouhodobě zaslouží stížnosti na zpracování osobních údajů prostřednictvím kamerových systémů, které představují přibližně 20 % všech došlých stížností, z toho pak téměř polovinu celkového počtu tvoří stížnosti na kamery provozované z obydlí. Jedná se o téma, které je pro subjekty údajů nadále velmi citlivé, avšak současně obtížně řešitelné. Úřad se těmito stížnostmi zabývá a ve vhodném rozsahu prošetřuje, je však třeba mít na paměti, že jádro sporu v řadě případů netkví pouze v ochraně osobních údajů jako takové, ale v dlouhodobě narušených sousedských vztazích. Úřad proto důsledně informuje jak stěžovatele, tak správce kamerových systémů o jejich právech a povinnostech, a současně i na dostupné prostředky právní ochrany, které mohou být v konkrétních případech vhodné k řešení sporu.

Deset let od přijetí GDPR tak jasně ukazuje, že ochrana osobních údajů zůstává živou a dynamickou oblastí, která si vyžaduje odpovídající institucionální i personální kapacity na straně státu, a současně naznačuje, že GDPR se stalo pevnou součástí právního vědomí veřejnosti.

Úřad pro ochranu osobních údajů

Spolek pro ochranu osobních údajů

www.uoou.gov.cz

www.ochranaudaju.cz

GDPR a nová digitální regulace

V dubnu uplyne 10 let od podpisu obecného nařízení o ochraně osobních údajů. Ačkoliv se GDPR od té doby nezměnilo, výrazně se změnil svět, ve kterém tato regulace funguje. Za těch 10 let se také výrazně zvýšila digitalizace celé společnosti. Jeden příklad za všechny – v České republice užívalo sociální sítě v roce 2016 podle ČSÚ cca 41 % osob, v roce 2024 již 63 % osob (pro srovnání, v roce 2010 to bylo pouhých 9,4 %).

K GDPR jako obecné normě upravující ochranu osobních údajů přibyla řada dalších právních předpisů. Ty lze rozdělit do několika skupin. První skupinou je sektorová regulace. Ta obvykle upravuje pravidla zpracování osobních údajů pro některé specifické obory či oblasti. Příkladem může být tzv. Digital Services Act (2022/2065/EU), který obsahuje mj. regulaci sociálních sítí. Dalším příkladem může být nařízení regulující zpracování zdravotních údajů, tzv. nařízení European Health Data Space (2025/327/EU). Druhou skupinou jsou regulace upravující postavení specifických kategorií osob. Příkladem může být tzv. Digital Markets Act (2022/1925/EU). Toto nařízení upravuje postavení tzv. správců přístupu (nejsilnějších digitálních platforem), kterým opětovně stanoví řadu omezení ohledně zpracování osobních údajů, např. zakazuje určitá zpracování údajů bez souhlasu uživatelů. Třetí skupinou jsou pak právní předpisy upravující specifické způsoby zpracování dat a osobních údajů, jako je např. AI Act (2024/1689/EU),. Ten upravuje kupř. specifičtější pravidla pro transparentnost při automatizovaném rozhodování. Podobně lze odkázat na směrnici Platform2Work (2024/2831/EU), tedy směrnici o zlepšení pracovních podmínek při práci prostřednictvím platformy. Čtvrtou skupinou předpisů jsou předpisy dotvářející pravidla pro zpracování osobních údajů v rámci veřejného sektoru anebo neziskových organizací, jako je např. nařízení Data Governance Act (2022/868/EU), které stanoví např. pravidla pro některá sdílení dat ze strany veřejné správy podnikatelskému sektoru (nad rámec pravidel podle tzv. směrnice Open Data (2019/1024/EU).

Specifickou skupinu pak tvoří předpisy zabývající se kybernetickou bezpečností, které také stanoví řadu speciálních postupů týkajících se zpracování dat. Zde došlo oproti stavu v roce 2016, kdy byla přijata původní směrnice NIS1, také k výraznému vývoji. Příkladem může být směrnice NIS2 (2022/2555/EU), nařízení DORA (2022/2554/EU), vztahující se na finanční sektor, nebo tzv. Cyber Resilience Act zabývající se kybernetickou bezpečností produktů s digitálními prvky (2024/2847/EU). Zcela specifickou kategorii pak představuje Data Act (2023/2854/EU) – zásadní nařízení dotýkající se celé řady prvků digitální ekonomiky, jehož centrální význam se pravděpodobně ještě zvýší v případě přijetí změn v rámci návrhu tzv. Digitálního Omnibusu.

I když se tedy samotné nařízení GDPR nezměnilo, změnil se výrazně celý právní řád, v jehož rámci GDPR funguje. Ten je nyní mnohem komplexnější, s řadou specifických předpisů, a vyžaduje mnohem pečlivější zkoumání toho, jaké všechny předpisy na dotčené zpracování dopadají.

Vedle toho došlo ale k další změně, která je sice méně viditelná, ale možná o to významnější. Dochází totiž k celé řadě úprav výkladu pravidel GDPR a to jednak díky rozhodnutím Soudního dvora EU, jednak výkladovým pokynům EDPB. Příkladem za všechny může být výrazné posunutí hranice pojmu zvláštních kategorií osobních údajů, jak ho SDEU judikoval např. v rozsudcích C-184/20 anebo C-21/23. SDEU sice „jenom“ vykládá zákonná pravidla, ale fakticky často dosavadní výklad výrazně mění.

I díky těmto změnám lze tedy říci, že úprava zpracování osobních údajů v rámci digitální ekonomiky se neustále dynamicky vyvíjí a mění.

Vše výše uvedené na jedné straně klade na profesionály zabývající se ochranou a zpracováním osobních údajů stále vyšší nároky, na druhé straně to pro ně znamená také příležitost – význam řádné „datové compliance“ se výrazně zvyšuje a tato pravidla přináší pro dotčené správce a zpracovatele sice řadu nových rizik, ale také řadu nových příležitostí.

Úřad pro ochranu osobních údajů

Spolek pro ochranu osobních údajů

Připraveno ve spolupráci Úřadu pro ochranu osobních údajů a Spolku pro ochranu osobních údajů. Na přípravě se podíleli: Ing. Kateřina Hrubešová, Mgr. Mária Chvajová Staňková, Mgr. Bc. David Burian, Ing. Mgr. Zdeněk Hrach, Mgr. Petr Jäger, Ph.D., Mgr. Michal Nulíček, LL.M., FCIArb, JUDr. Vladan Rámiš, Ph.D.