Ochrana osobních údajů

Ochrana osobních údajů

Veřejnoprávní ochrana osobních údajů je svým vývojem úzce propojena s mezinárodním vnímáním potřeby ochrany osobnosti, zvláště pak jejího soukromí. Je základní řada specifických práv subjektů údajů, jakými jsou: právo na informaci o zpracování, rozsahu zpracování, účelu zpracování nebo o jeho zpracovateli, právo na opravu či odstranění neoprávněně zpracovávaných osobních údajů. Ty se dají odvodit již z výkladu čl. 17 Mezinárodního paktu o občanských a politických právech.

Z Paktu však nelze bez dalšího dovozovat základní principy zpracování osobních údajů. Již dříve bylo možné jejich formulaci zaznamenat v pravidlech OECD (Organizace pro hospodářskou spolupráci a rozvoj) vydaných roku 1980. Obdobně jako pro ochranu osobnosti však pochází nadnárodní úprava významná pro české právní prostředí především z činnosti Rady Evropy. Úmluva č. 108 o ochraně osob s důrazem na automatizované zpracování osobních údajů byla přijata již v roce 1981. Pro Českou Republiku však nabyla platnosti až v roce 1981. Lze ji považovat za vůbec první detailněji zabývající se mezinárodní úpravu této problematiky.

Skrze tuto úmluvu byl položen základ národních právních předpisů, který následně umožnil snazší implementaci požadavků evropské směrnice č. 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Úmluva je považována za zásadní evropský předpis v této oblasti práva.

K 25. květnu 2018 vstoupil v účinnost Evropský reformní balíček pravidel pro zpracování osobních údajů, který reflektuje posun v prostoupení společnosti informačními a komunikačními technologiemi a reaguje na nově vzniklé výzvy. Cílila na harmonizaci a posílení ochrany osobních údajů a soukromí podle dosavadního právního rámce, přinesla tudíž řadu změn, ať již v celkové koncepci regulace a zajištění souladu s ní, tak v podobě nově upravených dílčích práv či povinností. Klíčové postavení nově jednotně zaujímá Obecné nařízení o ochraně osobních údajů č. 2016/679 (General Data Protection Regulation, dále jen „GDPR“), které je ve zvláštních oblastech doplněno dalšími evropskými právními předpisy či národní úpravou.

Účel úpravy

Zásahy do osobnostních či jiných základních práv a svobod skrze zpracování osobních údajů mohou nabývat různé intenzity. Může jít o různé formy narušení soukromí, resp. újmy na cti či vážnosti, např. skrze neoprávněné zveřejnění intimních informací o osobním životě či o preferencích, zálibách nebo jednání jednotlivce. Osobní údaje mohou být také využity pro profilování jedince skrze kombinaci údajů o jeho návycích, zájmech a slabostech za účelem jeho následného ovlivnění

při jednání, rozhodování či tvorbě názorů.

Údaje ale mohou také sloužit k vydírání či manipulaci vybraných jedinců. Zřejmě nejzávažnější formou zneužití osobních údajů je pak tzv. krádež identity, kdy dojde k neoprávněnému převzetí jedné či více významných virtuálních identit jedince, které umožní narušiteli neoprávněně jednat jménem oběti a na její účet bez možnosti snadného odhalení.

Z důvodu tohoto nerovného postavení mezi subjekty údajů a subjekty zpracovávajícími jejich osobní údaje je v zájmu ochrany před zmíněnými zásadními zásahy do základních práv a svobod dotčených osob namístě uložit těmto subjektům,1924 aby při nakládání s osobními údaji zohledňovaly a bilancovaly vlastní ekonomické či společenské zájmy s riziky a dopady do sféry dotčených fyzických osob.

Základní zásady zpracování osobních údajů

Zpracování musí probíhat zákonným, korektním a transparentním způsobem pro vymezený a legitimní účel, přičemž rozsah zpracovávaných údajů tomu musí být přiměřený a osobní údaje mají být pokud možno přesné, případně opravitelné. Ukládání osobních údajů je přípustné pouze po nezbytnou dobu danou účelem zpracování a při veškerém nakládání s osobními údaji je nutno klást důraz na zajištění jejich náležitého zabezpečení zejména před neoprávněným zneužitím či náhodným narušením.

Tyto zásady jsou však rozšířeny o podstatný prvek, který posouvá koncepci úpravy k formě regulované samoregulace. Tím je výslovné zakotvení odpovědnosti správce za dodržování základních zásad zpracování a požadavek jeho schopnosti tento soulad doložit.

Požadavky na zákonné zpracování osobních údajů

Je nutno posuzovat kombinaci tří aspektů nakládání s osobními údaji. Je nutno určit účel, pro který dochází ke zpracování, nalézt či zajistit právní základ daného zpracování a vymezit okruh dotčených osobních údajů, který musí být přiměřený tomuto účelu a podložený právním základem. Obecné právní základy jsou upraveny v článku 6 GDPR.

Zpracování může být oprávněno nezbytností pro plnění smlouvy se subjektem údajů. Jeho nezbytnost lze také nalézat v plnění právní povinnosti uložené správci nebo v plnění úkolu ve veřejném zájmu či výkonu veřejné moci pověřeným správcem. Obsah těchto dvou kategorií právních základů může případně blíže vymezovat právo členského státu.

V omezené míře lze za podklad vnímat i nezbytnost zpracování pro ochranu životně důležitých zájmů fyzické osoby či ochranu oprávněných zájmů správce či třetí osoby. V druhém zmíněném případě je však nutno zohledňovat poměřování se zájmy či základními právy a svobodami subjektu údajů, především pokud se jedná o dítě.

GDPR naopak roli souhlasu do jisté míry zesiluje, když zavádí zvláštní požadavky na souhlas u zpracování osobních údajů dětí (mladších 13–16 let, podle národní úpravy). Jádrem úpravy je požadavek, aby správce při snaze o získání souhlasu při poskytování služby informační společnosti (např. sociální sítě, online prodej, online herní platformy apod.) vyvinul přiměřené úsilí odhalit, zda zpracovávané osobní údaje přísluší dítěti pod zmíněnou věkovou hranicí, a v případě takového zjištění zajistil souhlas se zpracováním od osoby s rodičovskou odpovědností.

Tímto ustanovením je sledován chvályhodný záměr, jelikož je zřejmé, že dítě nízkého věku si je méně vědomo možných rizik a důsledků nakládání s jeho osobními údaji, zvláště pokud jde o profilování, marketingové účely či služby cílící na děti.

Mohou tím však vznikat jiná dříve pominutelná rizika a překážky. Předně je nutné ze strany správce zvažovat přiměřenou míru profilování uživatele, aby zjistil jeho věk.

Výše popsané dosud nebralo zřetel na skutečnost, že zpracovávané osobní údaje mohou mít různě citlivý charakter. Již od sjednání úmluvy č. 108 je přijímáno, že určité specifické kategorie osobních údajů vyžadují přísnější režim zpracování, který poskytuje dodatečné záruky ochrany před jejich zneužitím. Jedná se o údaje, které se váží k citlivým, intimním aspektům osobnosti či jednání jedince, které lze vzhledem k různým režimům dle GDPR dělit na pět kategorií

Obecné povinnosti správce a zpracovatele

Druhou rovinou k těmto povinnostem je pak potřeba vytváření záznamů, které v případě potřeby umožní správci doložit vnitřní procesy posuzování a bilancování předvídané nařízením a které dokumentují zavedená opatření a zdůvodnění jejich vhodnosti.

Je předvídáno, že řada správců pro mnoho forem zpracování bude spoléhat na jiný subjekt, který představuje v tomto ohledu zpracovatele. Po správci je tudíž vyžadováno, aby posuzoval vhodnost těchto poskytovatelů a vstupoval s nimi do právního vztahu pouze na základě smlouvy (příp. jiného právního aktu), která upravuje základní parametry zpracování a vzájemných práv a povinností, jak blíže vymezeno v článku 28 GDPR. Zpracovateli tak touto formou vzniká sekundární odpovědnost za soulad zpracování s právní úpravou, kterou nese především vůči správci. Je současně povinen jednat v mezích jeho pokynů a smí do zpracování zapojit dalšího zpracovatele pouze na základě písemného svolení správce, přičemž tímto nemůže snížit úroveň požadovaných záruk a povinností stanovených mu správcem.

Zabezpečení zpracování osobních údajů

Velká část rizik zpracování je spojena s únikem osobních údajů mimo sféru vlivu správce či zpracovatele a jejich následným neoprávněným zneužíváním a šířením. Nosnou premisou právní úpravy ochrany osobních údajů zajišťující prevenci proti těmto narušením zabezpečení osobních údajů je, že pokud správce či zpracovatel zpracovává osobní údaje, musí tak činit při zavedení vhodných technických a organizačních opatření přiměřených rizikům, která se váží k jejich

náhodnému či neoprávněnému úniku, změně, zničení či zpřístupnění. Výchozím bodem pro určení potřebné úrovně zabezpečení je posouzení zpracování co do jeho povahy, kontextu, rozsahu a účelu. V následujícím kroku je pak příhodné načrtnout možné rizikové scénáře a roztřídit je s ohledem na dostupné informace podle stupně závažnosti a pravděpodobnosti. Kategorie narušení zabezpečení lze dělit podle tradičního přístupu informační bezpečnosti na zásah do důvěrnosti údajů, do dostupnosti údajů a do integrity údajů.

Ohlašování případů porušení zabezpečení osobních údajů

Povinnost ohlášení se odvíjí od zjištění, zda porušení má za následek riziko pro práva a svobody fyzických osob. Na rozdíl od jiných režimů posuzování rizik v rámci GDPR se zde řeší konkrétní důsledky reálně nastalého porušení. Pro určení míry rizika hrají roli kritéria zahrnující především: formu porušení; povahu, citlivost a množství dotčených osobních údajů; identifikovatelnost jednotlivce z dotčených údajů; předpokládanou závažnost dopadů na jednotlivce; možný dopad na děti či jiné zvlášť zranitelné kategorie subjektů údajů; odhadované množství dotčených osob či případné specifické postavení správce.

Správce má povinnost ohlásit porušení zabezpečení Úřadu pro ochranu osobních údajů zásadně bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl. Pokud porušení zjistí zpracovatel, je povinen o něm bez zbytečného odkladu informovat správce (Minimální požadovaný obsah ohlášení je stanoven v článku 33 odst. 3 GDPR).

Má-li porušení natolik závažnou formu, že hrozí vysoké riziko pro práva a svobody fyzických osob, je správce povinen bez zbytečného odkladu oznámit porušení zabezpečení dotčeným subjektům údajů. Oznámení není nutné, pokud byly údaje subjektu zajištěny opatřením, které je činí nesrozumitelnými při neoprávněném přístupu

Každý případ porušení zabezpečení osobních údajů musí být správcem zdokumentován, výše popsané ohlášení dozorovému orgánu však není povinné pro případy, kdy riziko pro práva a svobody dotčených subjektů údajů není pravděpodobné.

Záměrná a standardní ochrana osobních údajů

Smyslem záměrné ochrany osobních údajů je pak od úvodní fáze procesu zpracování účinně chránit osobní údaje, např. formou pseudonymizace. Tímto procesem je podoba údajů skryta převedením na nepřímé identifikátory, které vyžadují ke ztotožnění s fyzickou osobou dodatečnou informaci, která je za vhodných opatření uchovávána odděleně.

Pověřenec pro ochranu osobních údajů

Pověřenec pro ochranu osobních údajů plní v rámci operací správce či zpracovatele několik význačných rolí, které směřují ke zkvalitnění nakládání s osobními údaji. Předně se jedná o specializovaného konzultanta, který má hluboké odborné povědomí o právní úpravě i praxi ochrany osobních údajů, a má tedy radit a poskytovat informace jak správci či zpracovateli, tak zaměstnancům, kteří provádějí zpracování osobních údajů. Zároveň se jedná o formu interního kontrolního orgánu či „hlídacího psa“, který v zájmu subjektů údajů a v rámci garantované funkční nezávislosti a absence střetu zájmů monitoruje soulad činností daného povinného subjektu s požadavky právní úpravy. Zatřetí pak pověřenec funguje jako kontaktní bod pro dozorový úřad či případně pro dotčené subjekty údajů.

Tato funkce může být zřízena libovolným správcem či zpracovatelem, některé významné subjekty ji však musejí zřídit mandatorně. Případný jmenovaný pověřenec může být jak interní zaměstnanec, tak poskytovatel služby formou outsourcingu.

Práva subjektu údajů

Obecné povinnosti správce směřující k usnadnění uplatňování práv subjektu údajů. Ten na ně musí upozornit srozumitelným, stručným a transparentním způsobem, poskytnout náležitou součinnost k jejich realizaci a zásadně v měsíční lhůtě informovat subjekt o formě vyřízení jeho žádosti včetně odůvodnění.

Správce odpovídá za kontrolu oprávněnosti požadavků, jelikož poskytnutí informací (osobních údajů) o subjektu údajů neoprávněné třetí osobě na základě její žádosti představuje porušení zabezpečení zpracování osobních údajů.

Výchozím právem subjektu údajů je právo na informace. To má dvě formy, podle toho, zda jsou osobní údaje získány přímo od subjektu údajů nebo od třetí osoby. Při získávání údajů přímo od subjektu údajů je v podstatě nutné mu v okamžiku získání poskytnout přehled o základních parametrech užití údajů, tedy např. účelu zpracování, totožnosti a kontaktu na správce či okruhu dalších subjektů, kterým správce získané osobní údaje bude předávat.

Specifické právo na informace se vztahuje k profilování a automatizovanému individuálnímu rozhodování, o kterém je pojednáno v sekci patnácté této části. Subjekt údajů musí být předně důsledně informován o svých právech. Pro tyto účely bude zřejmě v převážné míře odkazováno na webové stránky správce poskytující tuto informaci.

Specifickou formou práva na kopii údajů, nově zavedenou GDPR, je právo na přenositelnost údajů. To se váže na ztíženou změnu poskytovatele informační služby v situacích, kdy je požitek ze služby vázán na soubor osobních údajů poskytnutý uživatelem (např. komunikační platformy sociálních sítí či jiné služby, kde významným prvkem je, že si uživatel vytváří specifickou virtuální identitu).

Vzhledem k tomu, že jednou ze zásad zpracování osobních údajů je požadavek jejich přesnosti a správnosti, má subjekt údajů také právo žádat opravu či doplnění nepřesných údajů. Současně dostalo v GDPR zakotvení judikaturně dovozené právo na výmaz (také označováno jako právo na zapomnění či právo být zapomenut). Jeho smyslem je možnost subjektu údajů domoci se v duchu zásady minimalizace rozsahu a doby uchovávaných údajů odstranění osobních údajů, které již neslouží k přiměřenému či legitimnímu zpracování.

Právní ochrana subjektu údajů

Na podporu zmíněných práv a zmocnění jednotlivce k větší kontrole nad svými osobními údaji má subjekt údajů k dispozici prostředky právní ochrany. V první řadě jde o možnost obrátit se na dozorový orgán (především Úřad pro ochranu osobních údajů, ale případně i na orgán jiného členského státu) se stížností na porušení právní úpravy.2064 Tato stížnost má formu podnětu, ve zvlášť neupravených ohledech se tedy užije obecná úprava dle zákona č. 500/2004 Sb., správního řádu. Zde je také upravena procesní stránka ochrany před nečinností dozorového orgánu, kterou předvídá článek 78 GDPR. Ve srovnatelné formě přijímal a vyřizoval Úřad pro ochranu osobních údajů stížnosti dle dosavadní úpravy zákona č. 101/2000 o ochraně osobních údajů, v tomto směru tedy nedochází pro subjekt údajů k viditelným změnám. Subjekt údajů má mimoto právo i na účinnou soudní ochranu přímo proti správci či zpracovateli, který porušením nařízení zasahuje do jeho práv.

Činnost dozorového orgánu

Jelikož jde však v případě ochrany osobních údajů o veřejnoprávní úpravu, je její dodržování, bez ohledu na výše zmíněné nároky subjektu údajů, primárně vynucováno činností dozorového orgánu. Tím je již zmíněný Úřad pro ochranu osobních údajů, resp. ekvivalentní orgány jiných členských států. Působnost a pravomoci úřadu konkrétně upravuje národní legislativa, přesto lze v GDPR v článcích 51 až 59 dohledat obecné požadavky na úpravu členskými státy. Předně je vyžadována jeho nezávislost, dále je pak kladen důraz na spolupráci mezi úřady napříč Evropskou unií.

Zde stojí alespoň za zmínku role vedoucího dozorového úřadu. Tím je úřad příslušný pro jedinou nebo hlavní provozovnu správce či zpracovatele, přičemž ostatní dozorové úřady tento informují o stížnostech či řízeních proti danému subjektu a je na vedoucím dozorovém úřadu, aby rozhodl, zda se věcí bude primárně zabývat on či úřad oznamující.

Věci jsou zásadně řešeny na bázi spolupráce mezi dozorujícími orgány se snahou o jednotný postup a konsensus. Úřady tak vykonávají úkony na základě vyžádání úřadu z jiného členského státu, případně postupují v některých šetřeních či donucovacích opatřeních společně.

V rámci rozhodnutí či opatření s obecným dopadem je využíván mechanismus jednotnosti, kterým je především Evropský sbor pro ochranu osobních údajů, tedy útvar, který navazuje na fungování Pracovní skupiny podle článku 29 směrnice č. 95/46/ES (zjednodušeně označována WP29, z anglického Article 29 Working Party). Sbor je nově subjektem Unie s vlastní právní subjektivitou, jeho fungování se tedy oproti pracovní skupině formalizovalo a jeho pravomoci a působnost jsou

rozšířeny. Podrobný popis však přesahuje možnosti této kapitoly.

Rozhodnutí o udělení správní pokuty je individuálním správním aktem, který je výsledkem správního řízení ve smyslu zákona č. 500/2004 Sb., správní řád, adresát má tedy možnost instančního přezkumu v rámci činnosti Úřadu pro ochranu osobních údajů a případně následného přezkumu ve správním soudnictví podle zákona č. 150/2002 Sb., soudní řád správní. Nárok na právní přezkum vyplývá také přímo z ustanovení GDPR.

Vedle popsané funkce dozoru Úřad i nadále plní funkce vzdělávací, informativní a konzultační ve vztahu k oblasti ochrany osobních údajů. V GDPR je pak z těchto zdůrazňována především funkce iniciace a monitorování přípravy a dodržování odvětvových kodexů chování.

Nad rámec zmíněných rolí, které měl ve srovnatelné míře Úřad již na základě implementace směrnice 95/46/ES skrze zákon č. 101/2000 Sb., o ochraně osobních údajů, vyplývají z GDPR některé dodatečné pravomoci, které mají regulatorní povahu. Ty se týkají především nově zavedené koncepce mechanismů pro vydávání osvědčení o ochraně osobních údajů a zavedení pečetí a známek dokládajících soulad s požadavky nařízení. Ty mají být vydávány subjekty akreditovanými na základě prokázání nezávislosti, odborné znalosti a adekvátnosti vnitřních struktur a postupů.

Posouzení vlivu na ochranu osobních údajů

Pod pojmem profilování je zapotřebí vnímat libovolnou formu zpracování osobních údajů, které je prováděno automatizovaně a které současně spočívá v užití osobních údajů k hodnocení určitých osobních aspektů dotčených subjektů údajů. Za hodnocení je pak předně namístě považovat analýzu, klasifikaci či odhad nejrůznějších parametrů, sahajících od místa, kde se osoba nachází, přes její preference a zájmy až po její spolehlivost či pracovní výkonnost. Profilováním je tedy i prosté rozdělení osob podle pohlaví či věku, mnohem významnější jsou však pokročilé mechanismy, kterými za pomoci kombinace dostatečného množství zdánlivě běžných údajů (např. podrobné aktuální údaje o spotřebě elektrické energie v kombinaci s veřejně dostupnými údaji pro zjištění vybavení domácnosti a odhad ekonomické situace, příp. skrze dlouhodobé sledování polohy mobilního telefonu pro vyvození návyků a preferencí) lze získat intimní vhled do osobní sféry velkého množství fyzických osob.

> Profilování jako takové musí být na základě GDPR prováděno v souladu s požadavky na transparentnost, zákonnost, limitaci účelem, přesnost a minimalizaci údajů.

Předávání údajů do zemí mimo Evropskou unii

V rámci Evropské unie platí princip volného pohybu osobních údajů a smyslem GDPR rozhodně není omezovat toto směřování k jednotnému vnitřnímu digitálnímu trhu. S ohledem na požadavek zajistit adekvátní ochranu subjektům údajů z Evropské unie a absenci reálných hranic v kyberprostoru je však nutné řešit záruky a omezení, které se vztahují na nakládání s osobními údaji, které se dostanou do sféry jiné země než členských států (např. jsou uloženy či zpracovávány na serverech, které se nacházejí mimo území Evropské unie, ačkoliv jde o údaje o fyzických osobách z Evropské unie).

Tyto nástroje lze zjednodušeně dělit na dvě kategorie. U první jde o činnost Evropské komise, která může na mezistátní úrovni vyjednávat a posuzovat obecnou úroveň ochrany určité třetí země a následně rozhodnout o odpovídající ochraně (dosud přijímaných dle článku 25 směrnice č. 95/46/ES, nově pak dle článku 45 GDPR).

Při absenci tohoto plošného nástroje pro předávání osobních údajů do třetí země jsou správci a zpracovatelé nuceni individuálně zajistit vhodné záruky, a to především pro vymahatelnost práv subjektů údajů a jejich účinnou právní ochranu.

Vedle standardních smluvních doložek mohou být vhodné záruky zajištěny právně závaznými a vymahatelnými nástroji mezi orgány veřejné moci, závaznými podnikovými pravidly, dodržováním schváleného kodexu chování, příp. osvědčeními na základě schváleného mechanismu, která obsahují vymahatelné závazky uplatňovat ve třetí zemi vhodné záruky a chránit práva subjektu údajů.

Specifické výjimky a zvláštní úprava

Je namístě zdůraznit, co již bylo zmíněno v úvodu tohoto pojednání o ochraně osobních údajů, tedy že právní rámec GDPR představuje pouze základní harmonizační předpis, často doplňován o specifickou úpravu. Tato specifická úprava je k nalezení mj. v připravovaném zákoně o zpracování osobních údajů a doprovodném zákoně, kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů, které představují specifickou národní úpravu předvídanou GDPR. Jde především o zpracování pro novinářské účely a pro účely akademického, uměleckého či literárního projevu (s ohledem na svobodu projevu a informací),2142 přístup veřejnosti k osobním údajům v úředních dokumentech,2143 nakládání s národními identifikačními čísly (tedy s rodným číslem),2144 specifickým parametrům zpracování v rámci zaměstnaneckého poměru,2145 výjimek pro zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely,2146 zvláštní režim komplexních pravidel pro ochranu údajů uplatňovaných církvemi a náboženskými sdruženími2147 či zvláštní pravidla pro dozorovou činnost ve vztahu k subjektům podléhajícím služebnímu tajemství či srovnatelné povinnosti mlčenlivosti.

Významným alternativním režimem je pak především úprava ochrany osobních údajů a soukromí v prostředí elektronických komunikací. S ohledem na rozsah změn, které přináší GDPR, je i pro tuto oblast zapotřebí revize dosavadního režimu směrnice č. 2002/58/ES o soukromí a elektronických komunikacích .

Neopominutelnou odchylkou je pak nakonec již v na začátku zmíněný odlišný režim pro zpracování orgány veřejné moci za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo

výkonu trestů.

Revision #1
Created 2025-05-28 13:03:53 UTC by Magdalena Dobešová
Updated 2025-05-28 13:08:14 UTC by Magdalena Dobešová