Ochrana osobních údajů

1. Úvod, základní pojmy a cíle právní úpravy

Ochrana osobních údajů představuje velice aktuální problém, protože dopadá na velké množství případů zpracování dat v informačních systémech. Vzhledem k nárůstu možností výpočetních technologií došlo k výraznému rozšíření možností, jak osobní údaje zpracovávat, stejně jako celkovému množství probíhajících procesů zpracování. S ochranou osobních údajů se tak dostáváme dennodenně do kontaktu ať už v pozici správce údajů (tedy toho, kdo osobní údaje zpracovává ať už za cíli profesními jako například při vedení databáze zákazníků, nebo volnočasovými jako v případě vytvoření studentské stránky, na které je možné hodnotit kvalitu výuky konkrétních pedagogů), nebo v pozici subjektu údajů (tedy toho, jehož údaje jsou zpracovávány; jako příklad je možné uvést prakticky jakékoli sociální sítě a další online služby, hodnocení kredibility v bankách, zákaznické programy v obchodech atd.). Téma ochrany osobních údajů je v poslední době předmětem veřejné debaty i vzhledem k nedávné legislativní proměně, kdy evropský zákonodárce nahradil dosavadní právní úpravu novým nařízením č. 2016/679, Obecné nařízení o ochraně osobních údajů (známé pod akronymem „GDPR" z anglického „General Data Protection Regulation", dále jako „Obecné nařízení"), které tak představuje základní dokument, se kterým je třeba pracovat.

Tato kapitola si klade za cíl představit základní principy, na kterých systém ochrany osobních údajů spočívá, stručně pojednat o povinnostech správců a právech subjektů údajů a nabídnout odkazy na další zdroje pro hlubší studium.

1.1 Přehled relevantních dokumentů

Mezinárodní úroveň

- **Evropská úmluva o ochraně lidských práv a základních svobod**
  - Základní lidskoprávní dokument, který stanoví povinnost států garantovat základní lidská práva a svobody.
  - Čl. 8 obsahuje garanci práva na respektování rodinného a soukromého života, do kterého spadá rovněž ochrana osobních údajů.
  - Viz: Sdělení federálního ministerstva zahraničních věcí č. 209/1992 Sb. m. s., o sjednání Úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících.
- **Úmluva Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních dat (Úmluva č. 108)**
  - Mezinárodní smlouva z roku 1981 věnovaná výslovně ochraně osobních údajů. Obsahuje základní principy a pravidla, která můžeme najít ve všech modernějších předpisech do dnešního dne.
  - Viz: Sdělení ministerstva zahraničních věcí č. 115/2001 Sb. m. s., o přijetí Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat.

Evropská úroveň

- **Listina základních práv Evropské Unie (Dokument č. 2010/C 83/02)**
  - Čl. 8 zakládá ochranu osobních údajů jako přímo formulované základní právo.

    1. *Každý má právo na ochranu osobních údajů, které se ho týkají.*

    2. *Tyto údaje musí být zpracovány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu*

stanoveného zákonem. Každý má právo na přístup k údajům, které o něm byly shromážděny, a má právo na jejich opravu.

3. Na dodržování těchto pravidel dohlíží nezávislý orgán.

- **Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů**
    - Již zrušená směrnice, kterou nahradilo Obecné nařízení. Stále je však do určité míry relevantní, protože je na ni navázáno velké množství rozhodnutí Soudního dvora Evropské unie, které vykládají některé klíčové aspekty právní úpravy. Jejich použitelnost je dána tím, že Obecné nařízení vychází ze stejných zásad a principů jako zrušená směrnice.
- **Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích)**
    - Směrnice, která obsahuje zvláštní úpravu pro ochranu soukromí a zpracování osobních údajů v oblasti elektronických komunikací. Upravuje například pravidla pro užívání cookies, nebo zakazuje odposlechy telekomunikací.
- **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) (Text s významem pro EHP)**
    - Základní a obecný právní předpis, který upravuje pravidla ochrany osobních údajů. Vzhledem k tomu, že se jedná o nařízení, jeho ustanovení jsou přímo účinná v národním právu. Jde tedy o dokument, se kterým při řešení otázek ochrany osobních údajů primárně pracujeme.
- **Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV**
    - Tzv. „Policejní směrnice“, která upravuje pravidla pro zpracování osobních údajů v kontextu vyšetřování a stíhání trestné činnosti. V těchto oblastech se Obecné nařízení neuplatňuje.

Národní úroveň

- **Listina základních práv a svobod (usnesení č. 2/1993 Sb.)**
    - Jde o základní lidskoprávní dokument v českém právním řádu a má sílu ústavního zákona. Pro ochranu osobních údajů je podstatný zejména Čl. 10, který ve svém odst. 3 uvádí: „Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.“
- **Zákon č. 110/2019 Sb., o zpracování osobních údajů**
    - Český zákon, který specifikuje několik otázek, které nechalo Obecné nařízení otevřené a umožnilo tak členským státům, aby si je upravily dle svých národních potřeb. Implementuje rovněž policejní směrnici a upravuje zpracování osobních údajů pro oblasti, kam Obecné nařízení nedosáhne vzhledem k limitům evropského práva (např. činnost zpravodajských služeb, armády a podobně).
    - Zákon tedy funguje jako doplněk k Obecnému nařízení.

Podzákonné dokumenty

- **Doporučení a stanoviska WP 29 a EDPB**
  - WP 29 (Pracovní skupina zřízená podle čl. 29 směrnice 95/46/ES) byla tvořena zástupci národních úřadů pro ochranu osobních údajů, a byla poradním orgánem Evropské Komise pro otázky ochrany osobních údajů. Po účinnosti Obecného nařízení byla přetvořena v Evropský sbor pro ochranu osobních údajů (European Data Protection Board – „EDPB").
  - Publikuje řadu stanovisek a doporučení, ve kterých se detailně věnuje vybraným problematickým oblastem ochrany osobních údajů. Tato stanoviska mají velkou informační a argumentační hodnotu.
  - Nalezneme je na webových stránkách:
    - https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec5
    - https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en
- **Stanoviska a doporučení Úřadu pro ochranu osobních údajů (ÚOOÚ)**
  - Na stránkách ÚOOÚ nalezneme množství doplňkových dokumentů, které vykládají otázky ochrany osobních údajů specificky pro české prostředí. Můžeme tam rovněž najít české překlady dokumentů WP 29 a EDPB.
    - https://www.uoou.cz/

1.2 Základní pojmy

Osobní údaj

Obecné nařízení vymezuje pojem osobní údaj v čl. 4 odst. 1 následovně:

„***veškeré informace*** *o* ***identifikované*** *nebo* ***identifikovatelné fyzické osobě*** *(dále jen „subjekt údajů"); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.*"

Osobní údaje jsou opravdu všechny informace, které mohou přímo nebo nepřímo vést k identifikaci fyzické osoby (tedy člověka). Právní úprava ochrany osobních údajů se nevztahuje na právnické osoby. Přímo identifikující osobní údaje jsou takové informace nebo záznamy, u kterých je přímo z jejich vlastního kontextu jednoznačné, že mohou identifikovat člověka. Jde tak například o jméno a příjmení, trvalé bydliště, číslo občanského průkazu, nebo telefonní číslo. České soudy totiž tradičně osobní údaje mimo jiné pojí s možností daného člověka kontaktovat. Nepřímo identifikující jsou naopak takové údaje, které sice samy o sobě k identifikaci vést nemohou, ale pokud se spojí dohromady s dalšími údaji ve správném kontextu, už k identifikaci daného člověka mohou být použity. Jde tak například o IP adresy, které identifikují osobní zařízení uživatelů, a které mohou být použity při vyšetřování trestné činnosti. Je potřeba zdůraznit, že nepřímo identifikující osobní údaje jsou opravdu osobními údaji i tehdy, pokud je člověk v danou chvíli nedokáže použít ke ztotožnění. Pokud existuje někdo, kdo je legálními prostředky k identifikaci člověka použít dokáže, a toto použití nebude zásadně nepřiměřeně nákladné nebo technicky neproveditelné, jedná se o osobní údaje.

> *Příklad 1: Společnost ABC Security s.r.o., která poskytuje kyber bezpečnostní služby, sleduje provoz na síti svého klienta, aby detekovala případné hrozby a mohla jim zabránit. Při této činnosti zaznamenává IP adresy zařízení, které se do sítě připojují, časovou známku připojení a stručnou charakteristiku probíhajícího přenosu. Se zaznamenanými IP adresami musí společnost ABC Security nakládat*

jako s osobními údaji, a to i přesto, že sama není schopná na jejich základě člověka využívajícího dané zařízení ztotožnit. Může však údaje poskytnout policii, která už tento proces dokáže.

V souvislosti s vymezením osobních údajů se ještě můžeme setkat s pojmy anonymní a pseudonymní údaj. Anonymní údaje jsou takové, které prošly procesem jednostranné nevratné anonymizace a již je není možné použít k tomu, aby pomocí nich byl identifikován konkrétní člověk. Jde tedy o „ex-osobní údaje". Problém anonymizace spočívá v tom, že data je možné jen ve velmi výjimečných případech hodnotit jednoznačně jako „anonymní" nebo „neanonymní". Vhodnější je o anonymizaci přemýšlet jako o škále mezi identifikací a absolutní anonymitou, protože čím jsou data anonymnější, tím nesou nižší informační hodnotu a naopak. Za anonymní můžeme považovat takové údaje, jejichž opětovná identifikace by byla vzhledem ke stavu techniky zjevně nepřiměřeně náročná nebo nákladná. Anonymní údaje se často používají pro statistické účely.

Pseudonymní údaje jsou takové, kdy se přímé identifikátory nahradí identifikátory nepřímými. Jde tak například o nahrazení jména a příjmení číslem nebo bezvýznamovou přezdívkou. Jak ale už vyplývá z výše řečeného, stále se jedná o osobní údaje, byť lépe zabezpečené.

Vedle „běžných" osobních údajů Obecné nařízení rozeznává tzv. „zvláštní kategorie osobních údajů", které byly dříve nazývány „citlivé" osobní údaje. Jde o údaje, „*které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby*" (viz čl. 9 Obecného nařízení).

Správce a zpracovatel osobních údajů

Správce osobních údajů je osoba (ať už fyzická nebo právnická), instituce, úřad nebo jakýkoli jiný subjekt, který **určuje účel** daného **zpracování** osobních údajů a je za ně primárně odpovědný. Jeho vymezení najdeme v čl. 4 odst. 7) Obecného nařízení. V případě, že se vícero správců dohodne, že si rozdělí odpovědnost za zpracování, hovoříme o tzv. „společných správcích". Jedna společnost tak může například zajišťovat sběr dat a komunikaci se subjekty údajů, druhá jejich archivaci a analýzu.

Účel zpracování je zcela zásadním prvkem v kontextu celé právní úpravy ochrany osobních údajů. Vůči účelu, který správce na začátku zpracování určil, se následně poměřuje, jak zajistit, aby zpracování mohlo legálně probíhat (viz dále „právní tituly"), jak dlouho mohou být údaje uchovávány, kdo k nim může mít přístup a podobně (více viz část Základní principy a koncepty). Správce osobních údajů často zpracovává údaje za různými účely a odpovídá tak za vícero procesů zpracování.

Příklad 2: ABC Security s.r.o. z minulého příkladu je správce osobních údajů, protože určuje účel zpracování údajů, které sbírá a analyzuje ze síťového provozu, mezi kterými jsou i IP adresy (účelem je zajištění kybernetické bezpečnosti). Obchodní divize ABC Security dále nabízí na e-shopu kyber bezpečnostní produkty (firewall a antivirus) a zpracovává proto osobní údaje svých zákazníků, kteří si tyto produkty pořídili (účelem zpracování je prodej zboží a služeb). Vedle toho dále ABC Security zpracovává osobní údaje svých zaměstnanců, aby jim mohla posílat výplaty a plnila zákonné povinnosti, které jí jako zaměstnavateli náleží (účelem zpracování je zajištění pracovně právního vztahu).

Zpracovatel osobních údajů (definován v čl. 4 odst. 8 Obecného nařízení) je osoba, instituce, úřad nebo jakýkoli jiný subjekt, který **zpracovává osobní údaje pro správce**. Sám tedy účel neurčuje, ale dělá to, co mu správce řekne. Správce a zpracovavatel mezi sebou musí uzavřít smlouvu, ve které se upraví detaily jejich vztahu (minimální požadavky na tuto smlouvu jsou uvedeny v čl. 28 Obecného nařízení). Primární odpovědnost za zpracování nese sice správce, subjekt údajů se však může obrátit i na zpracovatele.

> *Příklad 3: ABC Security využívá služeb personální a daňové agentury Veselé finance k.s., která se stará o počítání daní a mezd jejích zaměstnanců. ABC Security je správcem těchto osobních údajů, protože určuje účel jejich zpracování. Společnost Veselé finance se nachází v pozici zpracovatele osobních údajů, protože účel neurčuje a je v mezích zákona povinna s nimi dělat to, co jí ABC Security nakáže.*

Zpracování osobních údajů

Obecné nařízení vymezuje v čl. 4 odst. 2) zpracování osobních údajů jako:

„*[]akákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.*“

Podobně jako v případě osobních údajů je definice zpracování nesmírně široká. Obecně jde tedy o jakoukoli činnost, kterou správce nebo zpracovatel s osobními údaji v průběhu jejich životního cyklu provádí. O zpracování osobních údajů je vhodné uvažovat procedurálně v průběhu času. Jeden proces zpracování, který je vymezen určeným účelem, tak může obsahovat více dílčích činností nakládání s osobními údaji.

1.3 Cíle právní úpravy ochrany osobních údajů

Základem pro právo na ochranu osobních údajů je **právo na informační sebeurčení**. To garantuje každému člověku možnost určit si, jak bude nakládáno s informacemi o jeho osobě. Nejde o právo absolutní a existují z něj výjimky, například v podobě zpracování informací státními orgány. Obecně však právo na informační sebeurčení dává každému člověku možnost určit si, jak se bude na veřejnosti prezentovat, jaké informace chce, aby o něm byly známy, a v konečném důsledku i jaké informace chce přijímat.

Právní úprava ochrany osobních údajů sleduje dva cíle. Prvním z nich je zajistit, že nebude docházet k zásahu do práva na ochranu osobních údajů fyzických osob (subjektů údajů). Právní úprava ochrany osobních údajů upravuje chování povinných subjektů ve vztahu k osobním údajům, které zpracovávají. Pokud se někdo rozhodne nakládat s osobními údaji, bude v naprosté většině případů docházet k jejich zpracování. Následkem toho musí tento správce osobních údajů dodržovat povinnosti, které mu z právní úpravy vyplývají. Z hlediska práva na ochranu osobních údajů v základu nehraje příliš velkou roli, komu osobní údaje patří. Ať už je člověk známou veřejnou osobností, nebo zcela soukromou osobou, jsou jeho osobní údaje v základu chráněny stejně. V tom se ochrana osobních údajů liší od ochrany soukromí, kdy známé osobnosti musí snést vyšší míru zásahu do svého soukromí než lidé, kteří si své soukromí chrání.

Právo na ochranu osobních údajů upravuje to, jak je s osobními údaji nakládáno. Jedná se o preventivní nástroj, v jehož základu stojí předpoklad, že pokud správce údajů dodržuje povinnosti, které jsou mu předepsány, zmenšuje se riziko škody, újmy nebo zneužití osobních údajů, které by mohlo být zpracováním způsobeno. Díky tomu jsou nepřímo chráněna další

základní práva, do kterých by mohlo být špatným nakládáním s osobními údaji zasaženo. Předně jde o právo na soukromí, protože při správném zacházení s osobními údaji je limitováno riziko, že dojde k prozrazení citlivých informací o člověku. Dále je však jako příklad takto nepřímo chráněného práva možné uvést vlastnické právo (špatné zpracování osobních údajů může vést například ke krádeži identity a zneužití platebních karet), nebo zákaz diskriminace (na základě zneužití zpracování osobních údajů může docházet k diskriminačním praktikám). Právo na ochranu osobních údajů je ve své podstatě procedurální právo. Je jako slunečník chránící další práva, která by zpracováním osobních údajů mohla být porušena.

Druhým cílem právní úpravy je obecně umožnit takové zpracování osobních údajů, které je v souladu s právem, a které ctí ochranu práv subjektů údajů. Právní úprava ochrany osobních údajů je vrcholně pragmatická, protože v jejím základu stojí předpoklad, že se zpracování osobních údajů děje a obecně je pro společnost vhodné, aby se dělo. Oblíbená glosa praví, že osobní údaje jsou novou ropou, protože umožňují ekonomické využití a pokrok. Právní úprava ochrany osobních údajů proto nemá za cíl naprosté zakázání zpracování osobních údajů. Zpracování je obecně možné, pokud k němu správce údajů přistupuje zodpovědně tak, aby minimalizoval rizika, která zpracování může pro subjekt údajů znamenat.

Oba zmíněné cíle se vzájemně dynamicky doplňují. Předmětem každého procesu zpracování osobních údajů je nalezení rovnováhy mezi nimi.

2. Působnost a základní zásady Obecného nařízení

2.1 Působnost

Věcná působnost

Pravidla, která stanoví Obecné nařízení je třeba použít vždy tehdy, když dochází k automatizovanému zpracování osobních údajů (čímž máme na mysli takové situace, ve kterých je alespoň částečně využito informačních technologií), případně i v případech neautomatizovaného zpracování, pokud mají být osobní údaje zařazeny do nějaké evidence, například kartotéky. Velmi zjednodušeně můžeme říct, že se nebude jednat o zpracování osobních údajů tehdy, když by neautomatizovaná činnost zpracování byla provedena zcela nahodile a nesystematicky (např. pokud donesu do práce noviny, ve kterých jsou osobní údaje, neprovádím jejich zpracování). Krom toho se Obecné nařízení nevztahuje na několik případů výjimek, které jsou z jeho působnosti vyloučeny. Jde zejména o následující:

1) Případy, na které se nevztahuje právo Evropské unie. Tyto případy jsou pak upraveny národními zákony, jako je například zákon č. 110/2019 Sb., o zpracování osobních údajů. Jedná se kupříkladu o zpracování osobních údajů, které provádí při plnění svých úkolů tajné služby, nebo armáda.
2) Případy, kdy osobní údaje zpracovávají orgány činné v trestním řízení při zajišťování prevence, vyšetřování, odhalování či stíhání trestných činů a výkonů trestu. Tyto činnosti upravuje směrnice 2016/680, která je provedená do českého práva zákonem č. 110/2019 Sb., o zpracování osobních údajů.
3) Zcela jsou z režimu ochrany osobních údajů vyňaty případy, kdy zpracování osobních údajů provádí fyzická osoba v průběhu „*výlučně osobních či domácích činností*“ (viz čl. 2 odst. 2 písm. c) Obecného nařízení). Tuto výjimku je třeba vykládat velice úzce. Příkladem výlučně osobní či domácí činnosti tak může být vedení osobního seznamu telefonních čísel a dalších kontaktů, vytvoření domácí bibliotéky, nebo kamera na zvonku zobrazující kdo zvoní na dveře (záznam z takové kamery by však nesměl být ukládán a kamera by nesměla mířit na veřejně dostupné prostranství, protože v takových případech by již tuto domácí výjimku nebylo možné použít).

Místní působnost

Při zpracování osobních údajů obecně příliš nehraje roli, kde se fyzicky daná data nachází, tedy kde leží server systému, který je pro zpracování použit.[1] Místní působnost se určuje podle toho, kde má správce údajů svoji provozovnu. Provozovnou se myslí soubor statků, které jsou svázány s územím daného státu a které slouží ke zpracování osobních údajů. Zároveň není vůbec podstatné, zda se zpracovávané osobní údaje týkají osob žijících na území států Evropské unie. Kupříkladu, v rozhodnutí ve věci Google Spain[2] Soudní dvůr Evropské unie rozhodl, že společnost Google Spain, dceřiná společnost Google sídlící ve Španělsku, je správce osobních údajů, které Google zpracovával při poskytování vyhledávacích služeb, protože určovala způsob jejich zpracování v kontextu nabízené reklamy. Druhým příkladem pak může být rozhodnutí ve věci Weltimmo,[3] ve kterém Soudní dvůr Evropské unie určil, že slovenský správce osobních údajů má v Maďarsku svoji provozovnu, když tam má otevřený bankovní účet, webové stránky v maďarštině a stálé právní zastoupení. Hranice toho, kdy je možné považovat, že má správce provozovnu v daném státě je tak poměrně nízká. V praxi to pak znamená, že úřady daného státu mohou vymáhat porušení práv ochrany osobních údajů, pokud v něm má správce svoji provozovnu.[4]

> *Příklad 4: ABC Security má sídlo v Olomouci. Vzhledem k tomu, že se jedná o poměrně úspěšnou společnost, tak má zákazníky z celého světa, včetně Spojených států amerických, Jižní Koreji a Austrálie. Pro fungování svých služeb používá servery umístěné v Irsku a Švédsku. Krom toho má ve Francii pobočku, která se zabývá poskytováním služeb místním obyvatelům. Místně příslušný pro řešení případných problémů zpracování společnosti ABC Security bude český Úřad pro ochranu osobních údajů a rovněž jeho francouzská obdoba Commission nationale de l'informatique et des libertés (CNIL).*

Obecné nařízení přineslo zajímavou novinku v podobě silného přeshraničního přesahu své aplikace. Čl. 3 odst. 2 totiž stanoví, že se Obecné nařízení vztahuje i na zpracování osobních údajů správcem nebo zpracovatelem, který vůbec nemá v Unii provozovnu, pokud zpracování osobních údajů souvisí s nabídkou zboží nebo služeb nebo monitorováním chování subjektů údajů, kteří se nachází v Evropské Unii. Můžeme si tak představit společnost, která sídlí například v Arizoně a cílí své služby na evropské zákazníky, ačkoli není v Unii nijak přítomná, tedy nemá tam provozovnu. I přes to se na ni v takovém případě vztahují pravidla Obecného nařízení. To je samozřejmě velice problematické z hlediska vymáhání práva, protože případné porušení ochrany osobních údajů takovou arizonskou společností pravděpodobně zůstane nepotrestáno z toho důvodu, že na ni žádný evropský úřad pro ochranu osobních údajů „nedosáhne".

2.2 Zásady zpracování

Právní úprava ochrany osobních údajů spočívá na několika zásadách, které jsou vyjmenovány v čl. 5 Obecného nařízení, a které se promítají do každého zpracování osobních údajů. Jejich znalost je důležitá, protože tyto zásady umožňují dovodit, jak má správce osobních údajů v konkrétní situaci postupovat. Obecné nařízení je v kontextu jiných právních předpisů poněkud atypické, protože nenabízí jasný seznam („check-list") úkolů, které musí správce údajů splnit, aby dostál svým

[1] Právě uvedené platí, pokud jsou servery na území Evropské unie a Evropského hospodářského prostoru. V případě, že by se nacházely mimo toto území je situace komplikovanější, protože by se jednalo o předávání osobních údajů do zahraničí, což podléhá specifické regulaci, jejíž vysvětlení přesahuje tato skripta. Více viz čl. 44 – 50 Obecného nařízení.

[2] Rozsudek Soudního dvora Evropské unie ze dne 13. 5. 2014 ve věci C-131/12 - Google Spain.

[3] Rozsudek Soudního dvora Evropské unie ze dne 1. 10. 2015 ve věci C-230/14 - Weltimmo.

[4] V případě, že má správce více provozoven v různých státech EU, je určena tzv. hlavní provozovna. Jde o takovou provozovnu, která slouží jako administrativní centrum.

povinnostem a nehrozila mu sankce. Naopak, Obecné nařízení od správce vyžaduje, aby se před každým zpracováním zamyslel nad tím, jaké údaje, za jakými účely a jakým způsobem bude zpracovávat, zvážil rizikovost takové činnosti a tomu své zpracování přizpůsobil. Tento způsob regulace (tzv. „performativní regulace“, protože není zadána konkrétní povinnost, ale cíl, kterého má být dosaženo) je nesmírně efektivní zejména v technologických oblastech práva. Vychází z úvahy, že povinné subjekty (správci údajů) samy nejlépe ví, jak jejich konkrétní proces zpracování vypadá a vzhledem k tomu dokáží správně nastavit všechny podmínky celého procesu, jako je například technické a organizační zajištění, jak dlouho konkrétně mají být údaje uloženy atd. Na druhou stranu ovšem tento způsob regulace klade na správce údajů poměrně vysoké nároky v tom, že musí být schopni posoudit svoji situaci a správně se v kontextu právní úpravy osobních údajů rozhodnout, jak své zpracování nastavit. A právě k tomu je nezbytné znát základní zásady, protože při jejich použití je dosažení správného výsledku snazší.

Zásada zákonnosti, korektnosti a transparentnosti

První zásada zpracování osobních údajů stanoví, že osobní údaje musí být zpracovávány korektně a zákonným a transparentním způsobem. To předně znamená, že zpracování musí probíhat za účelem, který je v souladu s právem. Z definice správce osobních údajů vyplývá, že jeho základní povinností je stanovit účel zpracování. Ten může být obecně jakýkoli, pokud neporušuje zákony.

> *Příklad 5: ABC Security na základě svých bezpečnostních auditů a penetračního testování vede databázi lidí, o kterých ví, že mají slabé zabezpečení. Tuto databázi chce prodat na černém trhu. Tento způsob zpracování osobních údajů je zjevně protiprávní, a proto nesmí takto probíhat.*

Zásada zákonnosti vedle toho dále znamená, že správce osobních údajů musí disponovat právním titulem, který zpracování umožňuje. Právní tituly najdeme vyjmenované v čl. 6 odst. 1 Obecného nařízení a blíže se jim věnuje třetí část této kapitoly.

Zásady korektnosti a transparentnosti by se jednoduše daly shrnout do požadavku, že správce osobních údajů má údaje zpracovávat férově (korektně). Důležité proto je, aby zpracování neprobíhalo skrytě, tedy aby měl subjekt údajů vždy možnost zjistit, kdo jeho údaje zpracovává. Tato znalost je totiž naprosto klíčová, aby subjekt údajů mohl vykonávat kontrolu nad probíhajícím zpracováním a tím realizovat své právo na informační sebeurčení. Jinými slovy, zásada korektnosti a transparentnosti zaručuje, že se subjekt údajů může bránit proti škodlivému zpracování osobních údajů. Pokud totiž neví, že zpracování probíhá, bránit se nemůže.

Zásada omezení účelem

Zásada omezení účelem stanoví, že osobní údaje musí být zpracovávány za určitým, výslovně vyjádřeným a legitimním účelem a nesmí být zpracovávány způsobem, který by byl s tímto účelem neslučitelný. Obecně tedy platí, že až na naprosté výjimky v podobě následného vědeckého, historického nebo statistického využití je možné osobní údaje zpracovávat za jiným účelem, než pro který byly shromážděny (tzv. „další zpracování“), pouze pokud je tento nový účel se starým slučitelný. Otázku slučitelnosti pak musíme vykládat velice úzce, aby nedošlo k nepřiměřenému zásahu do práv subjektů údajů. Více problematiku dalšího zpracování upravuje čl. 6 odst. 4 Obecného nařízení. Ten stanoví, že správce může další zpracování vykonávat na základě souhlasu subjektu údajů, případně pokud zvláštní právní předpis takovou možnost výslovně umožní. Zároveň uvádí několik aspektů, které je třeba zvážit při hodnocení, zda je účel dalšího zpracování slučitelný s účelem původním. Jde zejména o míru možného očekávání ze strany subjektu údajů (zde se tedy ptáme, zda subjekt údajů mohl v době původního zpracování očekávat zpracování nové za novým účelem), riziko, které nové zpracování představuje pro práva a svobody subjektů údajů a míru zabezpečení osobních údajů v rámci nového zpracování.

Účel zpracování a jeho určení jsou pro správce údajů a hodnocení zákonnosti zpracování naprosto klíčové, protože dle účelu se poměřuje celá řada dalších povinností správce. Účel proto musí být stanoven dostatečně určitě, aby ověření správného plnění povinností vyplývajících z Obecného nařízení bylo možné. Zároveň je však vhodné, aby účel nebyl až příliš úzce vymezen, protože by taková situace vedla k přílišnému svázání správce údajů v ohledu toho, jak může s osobními údaji nakládat. Účel je možné stanovit obecněji a pak jej dílčím způsobem konkretizovat pro specifické procesy zpracování údajů. Důležité však je v souladu se zásadou transparentnosti a korektnosti řádně informovat subjekty údajů o tom, za jakými účely zpracování osobních údajů probíhá.

> *Příklad 6: Společnost ABC Security zpracovává osobní údaje hned za několika různými účely, přičemž typově stejné osobní údaje mohou být zpracovávány za rozdílnými účely, pokud je to tak stanoveno od počátku zpracování. Jde například o následující:*
>
> 1. *Poskytování služeb svým zákazníkům v souvislosti s poskytováním kyberbezpečnostních řešení (IP adresy, logy, síťový provoz…).*
> 2. *Prodej zboží a nabízení služeb (osobní údaje zákazníků a jejich využití přímo nezbytné pro uskutečnění prodeje nebo poskytnutí služby).*
> 3. *Marketingové účely v podobě zasílání nabídek na nové zboží a služby (osobní údajů zákazníků a dalších fyzických osob, které projevily zájem o zasílání takových obchodních sdělení).*
> 4. *Zajištění bezpečnosti a ochrany majetku a zdraví v prodejnách a na pracovišti (kamerové záznamy).*
> 5. *Personalistika a pracovněprávní vztahy (osobní údaje zaměstnanců nezbytné pro pracovněprávní vztah).*
>
> *Společnost ABC Security po čase zjistí, že osobní údaje sesbírané za účelem č. 1 může technicky využít dvěma novými způsoby, které zahrnují dva nové účely: I) Komplexní analýza dat za účelem vytvoření vzorců kyberbezpečnostních incidentů a jejich zahrnutí do nových preventivních nástrojů; II) vytvoření profilů svých klientů na základě jejich online činnosti a následné nabízení cílené reklamy na zboží a služby třetích stran. První nový účel je dostatečně slučitelný s účelem původním a společnost ABC Security takové zpracování může provádět. Druhý nový účel je však již neslučitelný a takové zpracování osobních údajů by bylo protiprávní. Pokud by jej správce údajů chtěl využít, musel by získat od subjektů údajů souhlasy s tímto procesem.*

Zásada minimalizace údajů

Zásada minimalizace údajů úzce souvisí s prevenční povahou právní úpravy ochrany osobních údajů a spočívá v tom, že správce může zpracovávat jen ty údaje, které jsou striktně nezbytné pro účel, který si pro dané zpracování osobních údajů stanovil. Správce údajů tak nesmí sbírat a uchovávat osobní údaje „pro jistotu“, kdyby se mu někdy v budoucnu náhodou hodily. Z vymezeného účelu tak musí být jasné, jaké údaje správce bude pro dané zpracování potřebovat, a proč tomu tak je. Se zásadou minimalizace údajů souvisí povinnost správce zpracovávat osobní údaje v souladu s principy záměrné a standardní ochrany osobních údajů („*data protection by design*“ a „*data protection by default*“) upravené v čl. 25 Obecného nařízení. První ze jmenovaných stanoví, že správce má již při navrhování svých činností myslet na to, že bude zpracovávat osobní údaje, a tomu dané činnosti přizpůsobit tak, aby zpracování osobních údajů nezasahovalo do práv

a svobod subjektu údajů. Druhá ze jmenovaných stanoví, že v základním nastavení mají být služby a aplikace poskytovány koncovému uživateli tak, aby byly jeho osobní údaje co nejvíce chráněny.

> *Příklad 7: Mobilní mapová aplikace „Kam na oběd?" nabízí přehled restaurací v okolí uživatele. Účelem zpracování osobních údajů je poskytování této služby a nezbytně zpracovávané osobní údaje pro tento účel jsou lokace uživatele a případně též osobní jídelní preference, pokud si je uživatel navolí. Pokud by aplikace zaznamenávala další údaje z uživatelova telefonu (např. jeho kontakty, nebo i lokační data v době, kdy uživatel službu nepoužívá), jednalo by se o porušení zásady minimalizace a takové zpracování by bylo protiprávní.*

Zásada přesnosti

Zásada přesnosti stanoví, že zpracovávané osobní údaje mají být přesné, a v případě potřeby aktualizované. Z toho vyplývá, že každý správce osobních údajů musí dbát na to, aby přizpůsobil proces zpracování a zajistil, že nebude zpracovávat nepřesné nebo chybné osobní údaje. Na druhou stranu je třeba říci, že pokud nepřesnost údajů pochází například již přímo od subjektu údajů, nemůže za takovou situaci správce údajů nést odpovědnost. Otázka toho, jak moc musí správce údajů dbát na kontrolu a aktualizaci údajů přímo vyplývá z účelu zpracování a z míry rizika pro práva a svobody subjektů údajů, které zpracování představuje. Pokud například na základě zpracování osobních údajů dochází k rozhodování o právech a povinnostech subjektu údajů, je naprosto zásadní, aby zpracovávané údaje byly přesné a aktuální. Takovým případem je například zpracování osobních údajů za účelem hodnocení úvěruschopnosti v bance, na jehož základě se pak rozhoduje o tom, zda subjekt údajů získá úvěr, nebo ne, případně v jaké úrokové výši. Na druhou stranu zpracování údajů za statistickými účely tak vysokou míru kontroly vyžadovat nebude. V souladu se zásadou přesnosti je rovněž právo subjektu údajů požadovat opravu nebo aktualizaci chybných nebo neaktuálních osobních údajů, případně omezení jejich zpracování do doby, než k opravě dojde.

Zásada omezení uložení

Zásada omezení uložení stanoví, že osobní údaje mohou být uchovávány jen po takovou dobu, která je nezbytná vzhledem k účelu, pro který jsou zpracovávány. Otázka „jak dlouho můžeme mít data uložená" je jednou z nejčestnějších praktických otázek, které se v průběhu nastavování procesů zpracování osobních údajů objevují. Odpověď na ni není možné jednoznačně dopředu určit konkrétním datem (den, týden, měsíc…), ale je závislá na konkrétní situaci konkrétního účelu a způsobu zpracování osobních údajů. Jako v jiných případech, vzhledem k prevenční povaze systému ochrany osobních údajů, je otázku nezbytnosti nutné vykládat úzce. Nezbytnost ve smyslu této zásady představuje faktickou nezbytnost doby uložení, bez které by zpracování osobních údajů bylo vzhledem ke svému účelu nerealizovatelné. Otázka toho, jak dlouho je možné osobní údaje zpracovávat se odvíjí i od rizika, jaké toto zpracování představuje z hlediska možnosti zásahu do práv a svobod subjektu údajů. Nezbytnou dobu zpracování pak může správce údajů odůvodnit v dokumentaci ke zpracování.

Správce údajů má povinnost určit nezbytnou dobu uložení, když zahajuje proces zpracování osobních údajů. Doba může být vyjádřena jak absolutně (měsíc, dva roky…), tak relativně („*po dobu poskytování služby*", nebo „*do odvolání souhlasu*"). I v tomto případě tedy platí, že není možné osobní údaje uchovávat na základě pouhé technické možnosti a „protože by se mohly někdy hodit".

Výjimku ze striktní zásady omezení uložení má zpracování osobních údajů za účelem vědeckého či historického výzkumu či pro statistické účely. V těchto případech je (pochopitelně vzhledem k jejich povaze) možné uchovávat osobní údaje po velice dlouhou dobu. Další možností, jak zajistit

dlouhodobou využitelnost informační hodnoty, kterou dané osobní údaje mají, je jejich anonymizace. Pro připomenutí, v případě, že jsou údaje anonymizované, již nejsou osobními údaji.

> *Příklad 8: Společnost ABC Security uchovává osobní údaje získané při analýze síťového provozu (účelem zpracování je zajištění kybernetické bezpečnosti) po devět měsíců od sběru dat, protože na základě dřívějších analýz síťového provozu zjistila, že právě devět měsíců je průměrná doba, během které je možné v jejích službách určitě vzorce síťového provozu a incidentů. Osobní údaje svých klientů uchovává jen po dobu trvání poskytování služby, následně pak uchovává jen jejich elektronické adresy za účelem nabízení dalších služeb a zboží, ledaže klient dá najevo, že si takové zpracování osobních údajů nepřeje. Kamerové záznamy (účelem zpracování je ochrana zdraví zaměstnanců a majetku společnosti) jsou uchovávány po dobu pěti dnů, protože taková doba je zcela dostatečná pro to, aby v případě odhalené bezpečnostní události bylo možné zjistit, jak k ní došlo. Po delší dobu může uchovávat údaje o klientech například za účelem zajištění ochrany a vymáhání pohledávek z právních vztahů; v takovém případě bude vhodná délka odpovídat promlčecí lhůtě v kontextu daného právního vztahu.*

Zásada integrity a důvěrnosti

Zásada integrity a důvěrnosti určuje povinnosti správce údajů zabezpečit proces zpracování tak, aby osobní údaje náležitě zabezpečil před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením. Účelem této zásady je, aby správce údajů minimalizoval riziko zásahu do práv a svobod subjektu údajů. Za tímto cílem může správce zapojit řadu technických a organizačních opatření. Technickým prostředkem je například šifrování, uchovávání osobních údajů na oddělených serverech nebo vyžadování několika faktorové autentizace při přístupu k osobním údajům. Organizační opatření je například vnitřní nastavení procesů ve společnosti tak, aby k osobním údajům měli přístup opravdu jen ti lidé, kteří to nezbytně potřebují vzhledem k výkonu své práce (např. k údajům o zaměstnancích má přístup jen personální oddělení atd.). To, jaké konkrétní prostředky a opatření v daném procesu zpracování využije, pak záleží na konkrétním účelu zpracování a na míře rizika, které zpracování představuje pro práva a svobody subjektů údajů. Platí přitom, že čím rizikovější zpracování je (protože například využívá nových technologií, dochází při něm k profilování nebo automatizovanému rozhodování o právech a povinnostech subjektu údajů), tím intenzivněji musí správce zpracovávané údaje chránit.

Zásada odpovědnosti správce

Zásada odpovědnosti správce (anglický ekvivalent zní „*accountability*“) je nová zásada, kterou zákonodárce výslovně zakotvil v Obecném nařízení, a která ve staré směrnici 95/46/ES a zákoně 101/2000 Sb. nebyla přítomná. Tato zásada stanoví, že správce musí při zpracování přijmout vhodná opatření, aby splnil všechny požadavky vyplývající z předchozích zásad a zároveň musí být schopen přijetí takových opatření doložit. V praxi to pak znamená, že správce údajů musí prostředky a způsob, jakými zpracování osobních údajů provádí, přizpůsobit účelu, riziku a dalším okolnostem daného zpracování. Čím větší riziko dané zpracování osobních údajů představuje, tím více povinností má a tím důkladněji je musí plnit. A naopak, čím je zpracování méně rizikové, tím snazší práci správce údajů má.

V tomto spočívá hlavní nesnáz při aplikaci Obecného nařízení. Správce osobních údajů se musí před zahájením zpracování zamyslet, jaké údaje a za jakým účelem potřebuje zpracovávat, a podle toho si nastaví prostředky a způsoby zpracování tak, aby co nejméně zasahoval do práv subjektům údajů.

Prokázání splnění svých povinností správce údajů může provést tím, že bude řádně vést dokumentaci (záznamy o zpracování, viz čl. 30 Obecného nařízení), ve kterých popíše dané zpracování, jeho účely, způsoby a opatření.

Pokud správce údajů povinnosti vyplývající z Obecného nařízení nesplní, hrozí mu pokuta v maximální výši 20 000 000 EUR, nebo 4 % celosvětového obratu, dle toho, která hodnota je vyšší. Správní úřady (např. Úřad pro ochranu osobních údajů) však při udělování pokut musí postupovat přiměřeně, takže takto vysoké sankce můžeme očekávat jen v případě nejzávažnějších a nejvíce rizikových zpracování, jako je profilování, nebo zneužití osobních údajů provozovateli sociálních sítí.

3. Povinnosti správce

Základní povinnosti správce osobních údajů, které při jejich zpracování musí dodržovat, vyplývají přímo ze základních zásad zpracování. Jde například o povinnost nést odpovědnost za zpracování (viz čl. 24 Obecného nařízení). Tím se míní povinnost zavést s přihlédnutím k povaze, rozsahu, kontextu, účelům a rizikům zpracování vhodná technická a organizační opatření, aby správce zajistil a byl schopen doložit, že zpracování je prováděno v souladu s Obecným nařízením. Dále pak již zmiňovaná povinnost nastavit proces zpracování osobních údajů tak, aby splňovalo požadavky záměrné a standardní ochrany osobních údajů (čl. 25 Obecného nařízení), nebo povinnost vést záznamy o zpracování (čl. 30 Obecného nařízení). Dále má správce údajů řadu povinností odpovídajících právům subjektů údajů, jako je například poskytnou na základě žádosti vybrané údaje (viz dále, část 4 této kapitoly).

Povinnosti správce vyplývají z konkrétního zpracování osobních údajů a jeho požadavků. Například, pokud správce zpracovává zvláštní kategorie osobních údajů ve smyslu čl. 9 Obecného nařízení, musí nad rámec dalších povinností splnit požadavky, které jsou v tomto článku uvedené.

Jednou z hlavních povinností správce nicméně je zajistit, aby každé zpracování osobních údajů bylo podloženo právním titulem pro zpracování.

Pokud můžeme o účelu zpracování uvažovat jako o základním kameni každého zpracování, dle kterého se poměřují ostatní povinnosti správce, tak právní titul je klíč, bez kterého není možné zpracování provádět.

3.1 Právní tituly pro zpracování osobních údajů

Právní tituly jsou upraveny v čl. 6 odst. 1 Obecného nařízení takto:

> *„1. Zpracování je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu:*
>
> *a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;*
> *b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;*
> *c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;*
> *d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;*
> *e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;*
> *f) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní*

práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.“

Jako první právní titul je sice uveden souhlas subjektu údajů, v praxi však ve většině případů zpracování souhlas není potřeba. Obecně platí, že pokud se správce může spolehnout na kterýkoli z dále jmenovaných právních titulů, je takové řešení vhodnější než požadovat po subjektu údajů souhlas. Souhlasu se však pro jeho specifičnost tento text věnuje detailněji dále.

Pod písmenem b) je uveden právní titul, který umožňuje zpracování osobních údajů, pokud je nezbytné pro splnění smlouvy subjektu údajů se správcem. Opět, jako v jiných případech, je pojem „nezbytné“ nutné chápat úzce ve smyslu „opravdu nezbytné“.

> *Příklad 9: ABC Security na svém e-shopu prodává routery, které umožňují zabezpečené připojení k internetu. Pro jejich provoz není potřeba žádná registrace, zcela stačí, když si je uživatel doma zapojí a daná technologie funguje. Aby mohla společnost ABC Security dané zboží prodat a doručit (tj. splnit svoje závazky z kupní smlouvy uzavřené se zákazníkem), potřebuje k tomu zpracovávat osobní údaje v podobě adresy a fakturačních údajů zákazníka. Pro jejich zpracování za účelem prodeje daného zboží tak může použít právní titul uvedený v čl. 6 odst. 1 písm. b).*

Písm. c) a e) spolu úzce souvisí. Obě totiž umožňují zpracování osobních údajů, které vyplývá jako nutnost z některého právního předpisu. Liší se v tom, že zatímco písm. c) umožňuje zpracování osobních údajů tehdy, když je povinnost zpracovávat osobní údaje výslovně uvedena v právním předpise, písm. e) se použije tehdy, když zpracování osobních údajů implicitně vyplývá jako nezbytné z jinak určené povinnosti.

> *Příklad 10: Jako příklady zpracování osobních údajů, pro které je právním titulem čl. 6 odst. 1 písm. c) nebo e) Obecného nařízení je možné uvést následující:*
>
> - *Poskytování údajů včetně osobních údajů z katastru nemovitostí.*
> - *Zpracování osobních údajů, které provádí policista, když uděluje pokutu za rychlou jízdu.*
> - *Zpracování osobních údajů zaměstnavatelem, které je nezbytné pro splnění povinností, které mu vyplývají z pracovně právních předpisů.*

Písm. d) umožňuje zpracování osobních údajů, pokud to je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby. Jako v jiných případech je tuto nezbytnost nutné vykládat úzce. Tento právní titul tak představuje značnou výjimku a vztahuje se na specifické případy, jako například zjištění zdravotního stavu a krevní skupiny člověka, který po zranění akutně potřebuje krevní transfuzi.

Písm. f) umožňuje zpracování osobních údajů tehdy, když je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany. Detailněji se tomuto právnímu titulu věnujeme dále.

Zákon o zpracování osobních údajů (č. 110/2019 Sb.) zavedl ve svém § 17 ještě jeden právní titul, který se vztahuje na případy, kdy ke zpracování osobních údajů dochází pro novinářské účely nebo pro účely akademického, uměleckého nebo literárního projevu. Tento paragraf je velice podobný ustanovení čl. 6 odst. 1 písm. f), bude se nicméně pro případy novinařiny a v kontextu zajištění svobody projevu používat přednostně, protože jde o zvláštní právní úpravu.

Souhlas se zpracováním

Souhlas se zpracováním osobních údajů je možnost, jak může správce údajů založit zpracování osobních údajů, které by jinak na základě jiného právního titulu nebylo možné. Pokud taková situace nastane a správce údajů stále chce osobní údaje zpracovávat, nezbývá mu nic jiného než požádat subjekt údajů o jeho svolení. Je třeba hned zkraje zdůraznit, že souhlas se zpracováním osobních údajů může subjekt údajů kdykoli odvolat a zpracování tak musí skončit, pokud správce nemá jiný právní titul, kterým by ho odůvodnil.

Čl. 4 odst. 11 vymezuje souhlas subjektu údajů jako „*jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů*“. Požadavek svobodnosti znamená, že souhlas je platný pouze tehdy, pokud nebyl udělen pod nátlakem, ať už přímým nebo nepřímým. V praxi to znamená, že správce údajů nemůže pro případ neudělení souhlasu hrozit nějakou sankcí, nebo zhoršením situace subjektu údajů. Velmi problematické je tak udělování souhlasu v případě nerovného postavení správce a subjektu údajů, jako je například ve vztahu zaměstnavatele a zaměstnance. Požadavek konkrétnosti znamená, že účel zpracování, stejně jako jeho prostředky a doba uchovávání údajů jsou dostatečně přesně vymezené, aby mohl mít subjekt možnost si zvážit, zda chce takové zpracování údajů umožnit. S tím souvisí požadavek na informovanost subjektu údajů, bez které není možné naplnit požadavek konkrétnosti, protože pokud subjekt údajů přesně neví (nebo si nemůže zjistit) informace o chystaném zpracování, nemůže se svobodně a konkrétně rozhodnout zpracování umožnit. Konečně, požadavek jednoznačnosti znamená, že souhlas musí být vykonán takovým způsobem, aby nebylo pochyb o tom, že byl udělen. Pro příklad, pouhé setrvávání v oblasti monitorované kamerami není možné považovat za dostatečně udělený souhlas. Souhlas rovněž nesmí být součástí jiných dokumentů.

> *Příklad 11: Vyloženě chybnou a protiprávní praxí je zapojování souhlasu se zpracováním do textu smluv tak, že subjekt údajů má dojem, že podpisem smlouvy uděluje rovněž souhlas se zpracováním údajů. Pokud je zpracování údajů nezbytné pro plnění předmětné smlouvy, není již potřeba souhlas, protože je možné aplikovat právní titul čl. 6 odst. 1 písm. b). Pokud chce správce údajů zpracovávat i jiné údaje, nebo pro další účely, musí být souhlas uveden v rámci samostatného dokumentu, aby bylo subjektu údajů jasné, o co se jedná.*

Posledně uvedené je pro správce údajů důležité rovněž z toho důvodu, že jednou z jeho povinností vyplývajících ze zásady odpovědnosti, je nezbytnost být schopen prokázat, že disponuje platně udělenými souhlasy pro zpracování.

Zvláštní pravidlo souhlasu se zpracováním se týká případů, kdy dochází ke zpracování osobních údajů v kontextu poskytování služeb informační společnosti (jde o prakticky veškeré poskytování služeb v online prostředí), pokud je subjekt údajů mladší 15 let (tento údaj se liší v různých členských státech a pohybuje se od 13 do 16 let). V takovém případě je souhlas platný pouze pokud je udělen jeho zákonným zástupcem. I v tomto případě je však třeba upozornit na to, že se toto pravidlo týká opravdu jen udělení souhlasu se zpracováním a pokud jsou osobní údaje zpracovávány na základě jiných právních titulů (např. smlouvy), není takové svolení zákonného zástupce potřeba.

Oprávněný zájem správce nebo třetí osoby

Oprávněný zájem správce nebo třetí osoby je právní titul upravený v čl. 6 odst. 1 písm. f) Obecného nařízení. Fakticky to znamená, že pokud správci údajů, nebo třetí osobě, svědčí oprávněný zájem na tom, aby zpracování osobních údajů probíhalo, může se na tento právní titul spolehnout. Je zde však přítomná zcela zásadní limitace v podobě poměřování zásahu, které zpracování představuje pro práva a zájmy subjektů údajů. Správce údajů se totiž může na tento právní spolehnout pouze

tehdy, pokud zpracováním údajů do práv a zájmů subjektů údajů není nepřiměřeně zasaženo. V praxi proto musí před zahájením zpracování provést test proporcionality, ve kterém vůči sobě poměří svůj oprávněný zájem vůči právům a zájmům subjektu údajů. Pokud test dopadne ve prospěch těchto práv a zájmů, správce údaje zpracovávat nesmí, nebo musí využít jiný právní titul, například souhlasu. Na straně subjektu údajů pak leží nejen jeho právo na ochranu osobních údajů, ale také veškerá jeho další práva (ochrana soukromí a osobnosti, právo nebýt diskriminován, ochrana majetku…) a zájmy. Jde tedy o poměrně širokou kategorii.

> *Příklad 12: Společnost poskytující půjčky provádí před uzavřením smlouvy kontrolu toho, zda je budoucí klient schopný splácet. Tento proces zpracování bez pochyby může být zařazen pod oprávněný zájem této společnosti (ochrana majetku a právo podnikat) a pokud není prováděn se souhlasem subjektu údajů, je to jediný právní titul, na který se tento správce údajů může spolehnout. Rozhodnutí o tom, zda je danému subjektu poskytnuta půjčka zasahuje do jeho práv a povinností. V závislosti na tom, s jakými daty a jakým způsobem je zpracování prováděno, může dojít k zásahu do práva na soukromí a ochranu osobnosti (př. nežádoucí profilování) nebo k diskriminaci subjektu údajů (např. pokud na základě adresy správce zjistí, že subjekt údajů bydlí ve čtvrti většinově obydlenou některou z národnostních menšin a na základě toho subjektu vůbec úvěr neumožní, nebo mu nabídne výrazně horší úrokové sazby a podmínky splácení).*

Oprávněný zájem správce musí být reálný a skutečný. Nesmí být spekulativní. To znamená, že správce údajů musí mít v daném případě objektivní potřebu osobní údaje zpracovávat. Kategorie oprávněných zájmů je však obecně poměrně široká. Jde o takové činnosti, které jsou právem uznávány a nejsou jím zakázány. Při poměřování existence oprávněného zájmu může pro správce pozitivně působit fakt, že je tento zájem aktivně právně chráněn (např. kybernetická bezpečnost). Oprávněný zájem ale může být například rovněž ochrana zdraví a majetku (např. využití kamerových systémů), svoboda projevu a právo na informace (např. indexace osobních údajů v kontextu poskytování služeb internetového vyhledávače) nebo i komerční využití (např. nabízení reklamních sdělení) které obecně vyplývá ze základního práva mít majetek. Stejně tak je třeba vzít v potaz míru rizika, které zpracování představuje pro práva a svobody subjektů údajů. Čím je riziko menší, tím spíš bude oprávněný zájem správci svědčit, a naopak, čím je riziko vyšší, tím silněji bude muset správce existenci oprávněného zájmu prokázat. V souladu se zásadou odpovědnosti totiž správce musí být schopný prokázat, že zpracovává osobní údaje v souladu s Obecným nařízením. Důkazní břemeno proto bude spočívat na něm. Správce údajů však může konkrétním nastavením zpracování pomoci své pozici a pokud zavede takové prostředky, které sníží riziko zásahu do práv a svobod subjektu údajů (např. zavede zabezpečené ukládání dat, upraví kameru tak, aby snímala co nejméně veřejný prostor atd.), může hodnocení v rámci testu proporcionality vychýlit na svoji stranu. Vždy je však nezbytné provádět hodnocení každého testu proporcionality zvlášť v kontextu konkrétní situace.

> *Příklad 13: ABC Security zpracovává osobní údaje v podobě IP adres a komunikačních logů, které nasbírá při zajišťování kybernetické bezpečnosti chráněných systémů. Vzhledem k tomu, že se nemůže spolehnout na žádný jiný právní titul, ověřuje testem proporcionality, zda toto zpracování nezasahuje nepřiměřeně do práv a svobod subjektů údajů (zpracovává jen jejich IP adresy, časové známky a popis komunikace, jestli byla škodlivá nebo ne, případně jak). Na straně správce spočívá oprávněný zájem v podobě ochrany síťové infrastruktury (ochrana bezpečnosti a majetku). Rizika pro subjekty údajů však*

budou v tomto případě relativně nízká, vzhledem k silně pseudonymní povaze IP adres. Takové zpracování je tedy možné provádět.

Příklad 14: Dva dobré příklady na otázku oprávněného zájmu nabízí rozhodovací praxe českého Nejvyššího správního soudu (NSS). Prvním je rozhodnutí ve věci Ryneš (rozsudek Nejvyššího správního soudu ze dne 25. 2. 2015, č. j. 1 As 113/2012-133, č. 3222/2015 Sb. NSS). V něm NSS rozhodl, že stěžovateli svědčil právní titul oprávněného zájmu pro zpracování osobních údajů CCTV kamerovým systémem, kdy kamera mířila na veřejný prostor (ulice a vchod protějšího domu). Hlavním důvodem byl fakt, že správce údajů byl v minulosti již několikrát napaden a byl poničen jeho majetek. Byl zde proto na jeho straně silný a odůvodnitelný základ pro zpracování osobních údajů za účelem zajištění ochrany zdraví a majetku. Zároveň nebyl k dispozici žádný jiný způsob, kterým by bylo možné situaci řešit tak, aby ke zpracování osobních údajů nedocházelo.

Druhý příklad je podobný. Jedná se o rozhodnutí NSS ve věci ekolo.cz (rozsudek Nejvyššího správního soudu ze dne 8. 6. 2016 č. j. 3 As 118/2015-34). V tomto případě majitel obchodu, kterému zloděj ukradl elektrické kolo, vyvěsil jeho podobiznu na sociální síť s nápisem „zloděj". I přes to, že díky tomu byla daná osoba snadno dopadena Policií ČR, NSS rozhodl, že se jednalo o protiprávní zpracování osobních údajů, protože majiteli obchodu nesvědčil právní titul oprávněného zájmu. Předpokládaným a proporcionálním způsobem řešení takové situace je předání záznamu přímo Policii ČR a nikoli jeho zveřejnění na internetu.

3.2 Další povinnosti správce údajů

Obecné nařízení obsahuje několik dalších povinností správce údajů, které mají přispět k tomu, že zpracování bude probíhat bezpečně a způsobem, který bude šetřit práva subjektů údajů. Obecně pak platí, že nové povinnosti bude správce údajů mít tehdy, když dané zpracování osobních údajů představuje vyšší riziko pro práva a svobody subjektu údajů. Jde například o následující povinnosti:

Posouzení vlivu na ochranu osobních údajů (čl. 35)

Pokud je z prvotního prozkoumání rizikovosti budoucího zpracování osobních údajů zřejmé, že by chystané zpracování mohlo znamenat vysoké riziko pro práva a svobody subjektů údajů (a dalších fyzických osob), musí správce údajů vypracovat posouzení vlivu na ochranu osobních údajů (tzv. „DPIA" z anglického „*Data Protection Impact Assessment*"). Jedná se o dokument, ve kterém jsou shrnuta rizika, která zpracování představuje a navržena řešení, jak tato rizika eliminovat, nebo alespoň snížit. Tato praxe má správci údajů napomoci při správném nastavení procesu zpracování údajů.

Správce osobních údajů musí posouzení vlivu provádět zejména v případech, že jsou při zpracování využívány nové technologie, dochází k rozsáhlému sledování subjektů údajů, nebo zpracování slouží jako podklad pro rozhodování o právech a povinnostech subjektů údajů.

Jmenování pověřence pro ochranu osobních údajů (čl. 37 a následující)

V případech, kdy je správce údajů orgán veřejné moci, nebo hlavní činnost správce spočívá ve zpracování osobních údajů vyžadující pravidelné a systematické monitorování subjektů údajů, nebo hlavní činnost správce spočívá ve zpracování zvláštních kategorií osobních údajů (citlivých osobních údajů), musí správce jmenovat pověřence pro ochranu osobních údajů. Pověřenec je osoba, která správci osobních údajů pomáhá při nastavování prostředků a metod zpracování a

slouží jako hlavní kontaktní bod pro subjekty údajů. Působí rovněž jako prostředník mezi správcem a Úřadem pro ochranu osobních údajů.

Důležité

Závěrem části věnované povinnostem správce údajů je třeba zdůraznit a zopakovat následující skutečnost. Každé zpracování je proces vymezený jeho účelem. Vůči tomuto účelu se poměřuje, jaký je vhodný právní titul pro zpracování, jaké osobní údaje mohou být zpracovávány, jak dlouho mohou být uchovávány a jak často musí být aktualizovány. Vzhledem k rizikovosti daného zpracování je pak nutné určit, jakými konkrétními technickými a organizačními prostředky má správce zpracování zabezpečit. V případě analýzy plánovaných procesů zpracování je vhodné postupovat tak, že se nejprve identifikují jednotlivé účely a vůči nim se pak určují všechny další povinnosti správce údajů.

4. Práva subjektu údajů

Obecné nařízení garantuje subjektům údajů subjektivní práva, kterých se mohou vůči správcům dovolávat, a ti pak mají odpovídající povinnosti chovat se tak, aby byla práva subjektu dodržena. Tato práva najdeme formulována v čl. 12-22 Obecného nařízení. Práva subjektu údajů hrají v systému ochrany osobních údajů zásadní roli, protože umožňují subjektům údajů vykonávat určitou míru kontroly nad zpracováním v celém jeho průběhu.

Čl. 12-14 garantují transparentnost zpracování. Správce údajů obecně musí subjekty údajů informovat o probíhajícím zpracování (ať probíhá na základě jakéhokoli právního titulu) a to obecně minimálně v rozsahu následujících otázek:

i. Kdo je správce údajů a jak je možné jej kontaktovat?
ii. Jaké jsou účely pro zpracování osobních údajů?
iii. Jaké právní tituly správci umožňují v kontextu těchto účelů údaje zpracovávat?
iv. Jak dlouho jsou údaje v kontextu těchto účelů uchovávány?
v. Budou údaje v kontextu zpracování za vymezenými účely předávány dalším osobám?
vi. Budou údaje v kontextu zpracování za vymezenými účely předávány do zemí mimo EU nebo Evropský hospodářský prostor?
vii. Hodlá správce zpracovávat údaje pro nějaký jiný účel?

Vedle toho musí správce subjekt údajů informovat o právech, které mu Obecné nařízení garantuje. Informace by měla být poskytnuta jednoznačně a pokud možno co nejvíce srozumitelně. Pokud správce údajů získává údaje přímo od subjektu údajů, měl by ho informovat v době získání těchto údajů. Pokud ale dochází ke sběru údajů z jiných zdrojů, musí dát správce údajů alespoň možnost subjektu údajů se s těmito informacemi seznámit (např. umístěním na webu). Transparentnost zpracování je naprosto klíčová, protože bez znalosti, že zpracování probíhá se subjekt proti němu nemůže případně bránit a využívat svá další práva.

> *Příklad 15: Společnost ABC Security informuje o zpracování různé subjekty údajů, jejichž údaje zpracovává za různými účely, různým adekvátním způsobem. V případě účelu poskytování jejích služeb je informace o zpracování k dispozici online na stránkách společnosti ve formě samostatného dokumentu, který je této problematice věnován a na který míří odkaz z objednávkového formuláře. V případě zpracování IP adres v souvislosti s monitorováním síťového provozu je informace o této činnosti zpracování rovněž přítomná na stránkách společnosti. V případě zpracování osobních údajů zaměstnanců by k předání mělo dojít v souvislosti s nástupem do zaměstnání, například formou vnitřního předpisu.*

Následující práva mají společné to, že subjektu údajů přímo umožňují určitým způsobem se svými osobními údaji nakládat, respektive může po správci údajů požadovat, aby s danými daty nakládat určitým způsobem. Jde o právo na přístup k osobním údajům (čl. 15), dle kterého se může subjekt údajů dotázat správce, jestli zpracovává jeho osobní údaje a pokud ano, může si vyžádat jejich kopii. Dále pak čl. 16 pak garantuje subjektu údajů právo na opravu chybných nebo nepřesných údajů. Často skloňované je právo na výmaz, známé též pod názvem „právo být zapomenut", které je upraveno v čl. 17. Dle něj může subjekt údajů požadovat vymazání osobních údajů, jejichž účel zpracování již pominul, u kterých není právní titul na zpracování, případně které jsou obecně zpracovávány protiprávně. Mezi další práva subjektu údajů pak patří právo na omezení zpracování (čl. 18), právo na přenositelnost údajů (čl. 20), právo vznést námitku proti probíhajícímu zpracování (čl. 21) a právo nebýt předmětem automatizovaného rozhodování (čl. 22).

5. Závěrem

Tato kapitola velice stručně představila základní koncepty, které se vyskytují v právní úpravě ochrany osobních údajů, včetně povinností správce a práv subjektu údajů. Celá řada dalších otázek upravených v Obecném nařízení však zůstala vzhledem k jejich komplexnosti a možném rozsahu tohoto textu vynechána. Jedná se zejména o problematiku předávání osobních údajů do třetích zemí mimo EU a Evropský hospodářský prostor, možnosti certifikace zpracování osobních údajů a dále pak veškeré procesní otázky, stejně jako pravomoci dozorových úřadů a fungování Evropského sboru pro ochranu osobních údajů. K jejich bližšímu poznání je možné odkázat zejména na výborný Handbook on European data protection law (FRA), který je zdarma dostupný online.

6. Doporučená literatura

Knihy, komentáře, učebnice

European Union Agency for Fundamental Rights (FRA). *Handbook on European data protection law* [online]. Luxembourg: Publications Office of the European Union, 2018, 397 s. ISBN 978-92-9491-901-4. Dostupné z: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf

KASL, František. Osobnost, soukromí a osobní údaje v moderní společnosti. In: POLČÁK, Radim et al. *Právo informačních technologií*. Vydání první. Praha: Wolters Kluwer, 2018, s. 391-485. ISBN 978-80-7598-045-8.

LYNSKEY, Orla. *The foundations of EU data protection law*. First edition. Oxford, United Kingdom: Oxford University Press, 2015, 307 s. Oxford studies in European law. ISBN 978-0-19-871823-9.

NULÍČEK, Michal et al. GDPR - obecné nařízení o ochraně osobních údajů. Praha: Wolters Kluwer, 2017. ISBN 978-80-7552-765-3.

Články a kapitoly knih

HERT, Paul de. GUTWIRTH, Serge. Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. In: GUTWIRTH, Serge et al., eds. *Reinventing data protection?* Dordrecht: Springer, 2009, s. 3–44. ISBN 978-1-4020-9497-2.

MÍŠEK, Jakub. Souhlas se zpracováním osobních údajů za časů Internetu. *Revue pro právo a technologie*. 2014, roč. 5, č. 9, s. 3–74. ISSN 1805-2797.

NONNEMANN, František. Náležitosti souhlasu se zpracováním osobních údajů. *Správní právo*. 2011, roč. 44, č. 14, s. 520–522. ISSN 0139-6005.

NONNEMANN, František. Objektivní, či subjektivní pojetí osobních údajů? *Právní rozhledy*. 2015, roč. 23, č. 12, s. 425–431. ISSN 1210-6410.

OHM, Paul. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*. 2009, roč. 57, č. 6, s. 1701–1777. ISSN 0041-5650.

QUELLE, Claudia. The 'Risk Revolution' in EU Data Protection Law: We can't Have Our Cake and Eat it, Too. In: LEENES, Ronald et al., eds. *Data Protection and Privacy: (In)visibilities and Infrastructures*. Cham: Springer, 2017, s. 33-62. ISBN 978-1-5099-1934-5.

QUELLE, Claudia. Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability and Risk-based Approach. *European Journal of Risk Regulation* [online]. 2018, roč. 9, č. 3, s. 502–526. ISSN 2190-8249. Získáno z: doi:10.1017/err.2018.47

WAGNEROVÁ, Eliška. Kde má být svoboda, tam musí být soukromí. In: ŠIMÍČEK, Vojtěch, ed. *Právo na soukromí*. 1. vyd. Brno: Masarykova Univ., Mezinárodní Politologický Ústav, 2011, s. 49-62. ISBN 978-80-210-5449-3.

Soudní rozhodnutí

Rozsudek Evropského soudního dvora ze dne 6. 11. 2003 ve věci C-101/01 - Bodil Lindqvist, [dostupné z curia.europa.eu, vid. 20. 9. 2019].

Rozsudek Soudního dvora Evropské unie ze dne 13. 5. 2014 ve věci C-131/12 - Google Spain, [dostupné z curia.europa.eu, vid. 20. 9. 2019].

Rozsudek Soudního dvora Evropské unie ze dne 11. 12. 2014 ve věci C-212/13 - Ryneš, [dostupné z curia.europa.eu, vid. 20. 9. 2019].

Rozsudek Soudního dvora Evropské unie ze dne 1. 10. 2015 ve věci C-230/14 - Weltimmo, [dostupné z curia.europa.eu, vid. 20. 9. 2019].

Rozsudek Soudního dvora Evropské unie ze dne 19. 10. 2016 ve věci C-582/14 - Breyer, [dostupné z curia.europa.eu, vid. 20. 9. 2019].

Rozsudek Soudního dvora Evropské unie ze dne 5. 6. 2018 ve věci C-210/16 - Wirtschaftsakademie Schleswig-Holstein, [dostupné z curia.europa.eu, vid. 20. 9. 2019].

Rozsudek Soudního dvora Evropské unie ze dne 10. 7. 2018 ve věci C-25/17 - Jehovan todistajat, [dostupné z curia.europa.eu, vid. 20. 9. 2019].

Rozsudek Soudního dvora Evropské unie ze dne 29. 7. 2019 ve věci C-40/17 - Fashion ID, [dostupné z curia.europa.eu, vid. 20. 9. 2019].

Rozsudek Nejvyššího správního soudu ze dne 25. 2. 2015, č. j. 1 As 113/2012-133, č. 3222/2015 Sb.NSS, [dostupné z nssoud.cz, vid. 20. 9. 2019].

Rozsudek Nejvyššího správního soudu ze dne 8. 6. 2016 č. j. 3 As 118/2015-34, [dostupné z nssoud.cz, vid. 20. 9. 2019].