Úřad pro ochranu osobních údajů

Ochrana osobních údajů

Obor státní služby č. 60

Studijní texty ke zvláštní části úřednické zkoušky

Zpracováno ke dni 30. listopadu 2023

Zpracoval: Úřad pro ochranu osobních údajů

Úvod

Tato učební pomůcka byla vypracována pro potřebu oboru státní služby č. 60. Důraz je kladen na srozumitelnost a přehlednost a také na vysokou odbornost předloženého textu. Zároveň je však třeba poznamenat, že obsah studijního textu není zcela vyčerpávající, jeho cílem je poskytnout čtenáři (z velké většiny se bude jednat o žadatele o vykonání úřednické zkoušky) základní orientaci v problematice oboru služby Ochrana osobních údajů. Nemůže proto být považován za systematický výklad obecného nařízení o ochraně osobních údajů, zákona o zpracování osobních údajů, směrnice 680/2016 či jakéhokoli jiného právního předpisu či jejich plnohodnotnou náhradu. Na druhé straně u několika témat zahrnuje seznámení s vnitrostátní legislativou, která příslušné otázky pro potřeby celé státní správy nebo její určité části podrobněji zpracovává a umožňuje hlouběji porozumět systému práva ochrany osobních údajů v právním řádu Evropské unie a České republiky. Pomůcka zahrnuje rovněž základní výklad k nejdůležitějším aplikačním problémům trestněprávní směrnice. Znalost úpravy tematických okruhů, které jsou vyznačeny tučným pravým ohraničením a které se nacházejí v poznámkách pod čarou, není u zkoušky z oboru státní služby č. 60 vyžadována, neboť se nejedná o požadovaný rozsah znalostí vymezený ve vyhlášce č. 162/2015 Sb., o podrobnostech úřednické zkoušky, u oboru služby Ochrana osobních údajů, ale představují žádoucí doplnění a rozšíření požadovaných znalostí. Učební pomůcka vychází z právního stavu ke dni 30. listopadu 2023.

Vymezení ochrany osobních údajů

Ochrana osobních údajů je oborem provádějícím nejen v rámci státní služby jedno ze základních práv. V České republice je toto právo zakotveno ústavně, v článku 10 odst. 3 Listiny základních práv, vyhlášené pod č. 2/1993 Sb.: *Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.*[1]

Obsah současné právní úpravy i aplikačních požadavků a zvyklostí se ovšem opírá o článek 8 Charty základních práv Evropské unie, který zakotvuje tři základní komponenty práva na ochranu osobních údajů – subjektivní právo každé fyzické osoby, povinnosti všech, kdo s osobními údaji jiných lidí nějakým způsobem nakládají a existenci dozorového orgánu.

[1] Čl. 10 Listiny základních práv (č. 2/1993 Sb.)
(1) Každý má právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno.
(2) Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.
(3) Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.

Článek 8 ***Ochrana údajů osobního charakteru***

1. Každý člověk má právo na ochranu údajů osobního charakteru, které se ho týkají.

2. S těmito údaji musí být nakládáno čestně, pouze k přesně danému účelu a na základě souhlasu dotyčné osoby či na základě jiného legitimního opodstatnění uvedeného v zákoně.

Každý člověk má právo na přístup k údajům sebraným o jeho osobě a na jejich zpřesnění.

3. Respektování těchto pravidel podléhá kontrole nezávislé moci.

Je to tedy samostatné právo, byť s přesahem do dalších práv, z nichž se ve vztahu k osobním údajům nejvýrazněji uplatňuje právo obecně označované jako právo na ochranu soukromí. V Listině základních práv a svobod je postulováno jako právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života, v Chartě základních práv EU jako právo na respektování soukromého a rodinného života, obydlí a korespondence či jiných druhů komunikace. Jistý překryv existuje ovšem i s právem na svobodu projevu, které zahrnuje svobodu zastávat názory a přijímat či šířit informace bez zásahu státní moci a bez ohledu na hranice státu, jež je v České republice jako prvním politické právo zakotveno v čl. 17 Listiny základních práv a svobod[2].

Místo a rozsah zpracování osobních údajů ve veřejné správě moderního státu

Význam a dosah ochrany osobních údajů do života obyvatel a podnikatelských subjektů je dán objemem zpracování osobních údajů, na nichž je výkon veřejné správy v současném státě postaven, nebo které pouze využívá. Některá zpracování jsou kmenovou činností – např. vedení matrik, evidence občanských průkazů, cestovních dokladů, další nedílnou součástí činností kmenových – sem patří všechny úřední rejstříky (registry) a evidence. Je obtížné představit si, že je udržován a provozován nějaký informační systém veřejné správy, v němž nejsou zpracovávány žádné osobní údaje. Řada informačních systémů je přitom v souvislosti se zapojením České republiky do mezinárodních vazeb napojena na nadnárodní informační systémy, zejména informační systémy Evropské unie.

[2] Čl. 17 Listiny základních práv (č. 2/1993 Sb.)
(1) Svoboda projevu a právo na informace jsou zaručeny.
(2) Každý má právo vyjadřovat své názory slovem, písmem, tiskem, obrazem nebo jiným způsobem, jakož i svobodně vyhledávat, přijímat a rozšiřovat ideje a informace bez ohledu na hranice státu.
(3) Cenzura je nepřípustná.
(4) Svobodu projevu a právo vyhledávat a šířit informace lze omezit zákonem, jde-li o opatření v demokratické společnosti nezbytná pro ochranu práv a svobod druhých, bezpečnost státu, veřejnou bezpečnost, ochranu veřejného zdraví a mravnosti.
(5) Státní orgány a orgány územní samosprávy jsou povinny přiměřeným způsobem poskytovat informace o své činnosti. Podmínky a provedení stanoví zákon.

Zkušební otázky ke zvláštní části úřednické zkoušky pro obor státní služby č. 60

Seznam použitých zkratek

AIFO	Agendový identifikátor fyzické osoby
BCR	Binding Corporate Rules (Závazná vnitropodniková pravidla)
EDPB / Sbor	European Data Protection Board (Evropský sbor pro ochranu osobních údajů)
EHP	Evropský hospodářský prostor
EU	Evropská unie
GDPR / Obecné nařízení / Nařízení (EU) 2016/679	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)
ISZR	Informační systém základních registrů
SDEU	Soudní dvůr Evropské unie
ÚOOÚ / Úřad	Úřad pro ochranu osobních údajů
ZIFO	Zdrojový identifikátor fyzické osoby
Zákon č. 106/1999 Sb.	Zákon č. 106/1999 Sb., o svobodném přístupu k informacím
Zákon č. 273/2008 Sb.	Zákon č. 273/2008 Sb., o Policii České republiky
Zákon č. 111/2009 Sb.	Zákon č. 111/2009 Sb., o základních registrech
Zákon č. 110/2019 Sb.	Zákon č. 110/2019 Sb., o zpracování osobních údajů

1. Základní pojmy ochrany osobních údajů podle obecného nařízení o ochraně osobních údajů

Obecné nařízení o ochraně osobních údajů[3] (dále jen „obecné nařízení“) definuje 26 pojmů; všechny definice jsou v článku 4 obecného nařízení. Pro aplikační potřebu v jakékoli oblasti nejsou všechny z nich stejně významné. Za základní je s ohledem na prováděné základní právo[4] a nejrozšířenější aplikační potřeby třeba považovat osobní údaj(e), zpracování, evidenci, správce, zpracovatele, příjemce, třetí stranu, porušení zabezpečení osobních údajů, podnik, dozorový úřad a přeshraniční zpracování. Z praktických důvodů je na místě považovat za základní pojem rovněž *subjekt údajů*, i když je definován pouze jako jeden z parametrů osobního údaje. Pojem subjektu údajů je definován také v § 3 zákona o zpracování osobních údajů, a to jako fyzická osoba, k níž se osobní údaje vztahují.[5] Obecně jsou pojmy definované v čl. 4 obecného nařízení používány v původním významu i v českých právních předpisech.

Osobní údaj a zpracování

Osobními údaji se rozumí 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. Text za středníkem je podle smyslu i účelu vymezením (definicí) subjektu údajů, nikoli osobního údaje. Preambule obecného nařízení výslovně stanoví, že zásady ochrany osobních údajů by se měly uplatňovat na všechny informace týkající se identifikovatelné nebo identifikované osoby a neměly by se vztahovat na anonymní informace, jimiž se rozumí informace, které se netýkají identifikované či identifikovatelné fyzické osoby[6]. Současně není rozhodná vypovídací schopnost daného údaje; ta musí být zvažována v rozhodování o nakládání s osobním údajem, včetně jeho zpracování. Do jisté míry se tak děje v samotném obecném nařízení, zejm. požadavky na zpracování zvláštních kategorií osobních údajů.

[3] 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).

[4] Ochrana fyzických osob v souvislosti se zpracováním osobních údajů je základním právem. Ustanovení čl. 8 odst. 1 Listiny základních práv Evropské unie (dále jen „Listina“) a čl. 16 odst. 1 Smlouvy o fungování Evropské unie (dále jen „Smlouva o fungování EU“) přiznávají každému právo na ochranu osobních údajů, které se jej týkají. Recital (1) k obecnému nařízení.

[5] § 3 zák. č.110/2019 Sb., o zpracování osobních údajů

[6] Recital (26) obecného nařízení.

Správné pochopení pojmu osobní údaj vychází ze zjištění a uznání spojení mezi reálnou fyzickou osobou a hodnotou určitého údaje bez ohledu na to, zda je vyjádřena nominálně, číselně nebo jinak či méně strukturovanou formou. Tam, kde taková vazba existuje (je přítomna), tam se jedná o osobní údaj. To se často označuje jako objektivní povaha nebo objektivní pojetí osobního údaje. Proti tomu je stavěno subjektivní pojetí, vycházející ze subjektivně pragmatického přístupu omezujícího se situačně. Nejen že je subjektivní přístup nesprávný, ale v praktickém životě může vést k postihu za neoprávněné nakládání s osobními údaji jiného nebo k nedodržení povinností při zpracování osobních údajů podle kteréhokoli z platných právních předpisů. Není přitom rozhodné, zda ten, kdo používá jiný údaj než jedinečný identifikátor fyzické osoby, má aktuálně k dispozici technické nebo organizační prostředky k tomu, aby k údajům, jimiž disponuje, připojil nějaký obecně uznávaný a používaný identifikátor[7], nebo údaje, jimiž aktuálně disponuje, použil sám k identifikaci („nepřímé") jiného.

Osobní údaje používané ve veřejné správě jsou z velké části formalizovány; značná míra formalizace je typická pro údaje zpracovávané automatizovaně v informačních systémech určených ze zákona k výkonu působnosti taxativně určených orgánů veřejné moci (agendové informační systémy). Vysoce formalizované jsou i osobní údaje zpracovávané v informačních systémech standardně používaných soukromoprávními správci (zákaznické systémy (systémy CRM), docházkové a přístupové systémy).

Informace vztahující se k identifikované nebo identifikovatelné zemřelé osobě jsou osobními údaji. Obecné nařízení se na zpracování takových osobních údajů nevztahuje. Členské státy mohou stanovit pravidla týkající se zpracování osobních údajů zesnulých osob a děje se tak standardně. V České republice upravuje nakládání s osobními údaji zemřelých několik zákonů, především občanský zákoník, zákon o zdravotních službách, zákon o matrikách, jménu a příjmení, zákon o archivnictví a spisové službě a zákon o pohřebnictví[8].

Zpracováním je jakákoliv 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.

Výčet operací je příkladný a nové technologie zpracování osobních údajů přinášejí i nové operace. Po elektronických adresách (účastnická čísla, e-mail, datová schránka) soubor obvyklých a široce používaných osobních údajů rozšířily transakční údaje komunikačních a sociálních sítí (např. i nicky). Osobní údaje vznikají dále snímáním z technických zařízení

[7] Vizte též kap 2 této učební pomůcky.
[8] Zák. č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), zák. č. 256/2001 Sb., o pohřebnictví a o změně některých zákonů

v dispozici subjektu údajů i v dispozici toho, kdo s nimi dále nakládá nebo je zpracovává (nebo interpretace příkazu v hlasových asistentech). Za formu shromažďování (sběru) osobních údajů je třeba považovat jejich technicky podmíněné vytváření (odpozorované údaje).

Jako operace zpracování osobních údajů je v obecném nařízení definována jejich pseudonymizace.

Pseudonymizací se rozumí zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací; tyto dodatečné informace musí být uchovávány odděleně a musí se na ně vztahovat technická a organizační opatření, bránící přiřazení identifikované či identifikovatelné fyzické osobě. Tato operace má v obecném nařízení zvláštní postavení – je výslovně postulována jako vhodná záruka (např. při zpracování pro jiný než původní účel – čl. 6, odst. 4, písm. e) obecného nařízení nebo jako vhodné technické a organizační opatření – čl. 25 odst. 1 a čl. 32 odst. 1, písm. a) nebo čl. 89 odst. 1 obecného nařízení). Vychází se z předpokladu, že použití pseudonymizace osobních údajů může omezit rizika pro dotčené subjekty údajů a napomoci správcům a zpracovatelům splnit jejich povinnosti týkající se ochrany práv a svobod fyzických osob v souvislosti se zpracováním osobních údajů. Doporučována je zejména co nejrychlejší pseudonymizace.[9] Výslovné zavedení „pseudonymizace“ v tomto nařízení nemá za cíl předem vyloučit jakákoliv další opatření sledující zajištění ochrany osobních údajů.[10]

Evidencí je jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska; tj. bez ohledu na to, jaké pořádací (soupisné) nebo selekční údaje jsou v něm používány. Použití automatizovaných postupů není rozhodné. Evidencí jsou všechny úřední registry, rejstříky, ale i veřejné seznamy, pokud obsahují osobní údaje, stejně tak jako jakékoli spisové kartotéky, pokud jsou soupisným znakem osobní údaje, tedy i zdravotnické kartotéky.

Správce, zpracovatel, příjemce a třetí strana

Správce je definován jako fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem EU nebo členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení.

Zpracovatelem je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce. Zpracovatelem není fyzická osoba

[9] Recital (78) obecného nařízení.
[10] Recital (28) a (29) obecného nařízení.

reprezentující správce a vykonávající některé nebo veškeré operace zpracování, včetně vnitřně stanovené odpovědnosti za ně.

Důležitými pojmy v kontextu modelu ochrany osobních údajů stanoveného obecným nařízením jsou dále příjemce osobních údajů a třetí strana. Příjemcem je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli. Za příjemce nelze považovat orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem členského státu; zpracování přijatých osobních údajů těmito orgány veřejné moci v rámci jejich zvláštních oprávnění musí být v souladu s použitelnými pravidly ochrany údajů pro dané účely zpracování. To má přímé důsledky pro rozsah povinnosti poskytnout subjektu údajů informace o zpracování podle čl. 13–15 obecného nařízení. Třetí stranou je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, která je oprávněna ke zpracování osobních údajů; je to tedy někdo, kdo stojí mimo institucionální nebo funkční model příslušného zpracování osobních údajů, např. agendového informačního systému.

Podnikem je jakákoli fyzická nebo právnická osoba vykonávající hospodářskou činnost bez ohledu na její právní formu, včetně osobních společností nebo sdružení, která běžně vykonávají hospodářskou činnost. Definovat podnik jako základní pojem ochrany osobních údajů je významné proto, že povinnosti správců, kteří jsou podniky, se v určitých ohledech odlišují od správců nebo zpracovatelů, kteří jsou veřejnými subjekty; veřejné subjekty mají zpravidla zákonem speciálně upraveny povinnosti, směřující k naplňování jednotlivých práv subjektů údajů. V aplikační praxi dozorových úřadů, včetně českého, se používá často po vzoru soudní praxe termín „společnost“.

Porušení zabezpečení osobních údajů

Porušení zabezpečení osobních údajů je specifický pojem ochrany osobních údajů, byť má podle smyslu významný obsahový překryv s pojmem *narušení bezpečnosti* z kybernetické a informační bezpečnosti. Porušením zabezpečení osobních údajů se rozumí porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů. Porušením zabezpečení tedy není zásah, který k některému z výše uvedených účinků nevede.

Narušení bezpečnosti není ekvivalentem porušení zabezpečení osobních údajů a není ani samostatně definováno. Naopak, je použito jako definiční parametr v definici dvou základních pojmů kybernetické a informační bezpečnosti. Zákon o kybernetické bezpečnosti definuje za jeho použití *kybernetickou bezpečnostní událost* (událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací) a *kybernetický bezpečnostní incident* (narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události)[11]. Jedním ze základních pojmů tohoto zákona je *bezpečnost informací.* Rozumí se jí zajištění důvěrnosti, integrity a dostupnosti informací a dat, tedy složky zabezpečení osobních údajů podle čl. 32 obecného nařízení.

Přeshraniční zpracování

Přeshraničním zpracováním je zpracování osobních údajů, které buď probíhá v souvislosti s činnostmi provozoven ve více než jednom členském státě správce či zpracovatele v Unii, je-li tento správce či zpracovatel usazen ve více než jednom členském státě; nebo probíhá v souvislosti s činnostmi jediné provozovny správce či zpracovatele v Unii, ale kterým jsou nebo pravděpodobně budou podstatně dotčeny subjekty údajů ve více než jednom členském státě. Pojem je klíčový pro určení působnosti dozorových úřadů působících v členských státech EU nebo v některé ze zemí Evropského hospodářského prostoru.

Dozorový úřad

Dozorovým úřadem se rozumí nezávislý orgán veřejné moci zřízený členským státem, který je pověřen monitorováním uplatňování obecného nařízení a směrnice 2016/680 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů a o volném pohybu těchto údajů (dále jen „trestněprávní směrnice“), s cílem chránit základní práva a svobody fyzických osob v souvislosti se zpracováním jejich osobních údajů a usnadnit volný pohyb osobních údajů uvnitř Unie.

Kritéria nezávislosti dozorového vymezuje obecné nařízení v čl. 52–54 a trestněprávní směrnice obdobně v čl. 42–44 jako požadavek na provedení vnitrostátním právem členského státu EU.

Počet nezávislých orgánů veřejné moci, které jsou monitorováním uplatňování obecného nařízení s cílem chránit základní práva a svobody fyzických osob v souvislosti se zpracováním jejich osobních údajů a usnadnit volný pohyb osobních údajů uvnitř Unie v jednotlivých členských státech pověřeny, není omezen. Každý dozorový úřad však musí přispívat k jednotnému uplatňování obecného nařízení v celé Unii. Dozorové úřady za tímto účelem spolupracují mezi sebou a s Komisí. Dozorové úřady jsou zřizovány zákony členských států.

[11] § 7 zákona č. 181/2014 Sb., o kybernetické bezpečnosti.

2. Rodné číslo, zdrojové a agendové identifikátory podle obecného nařízení, zákona o evidenci obyvatel a zákona o základních registrech

Identifikátory a identifikační čísla

Definice osobního údaje jako prvního ze základních pojmů obecného nařízení výslovně uvádí ve výčtové části identifikační číslo určité fyzické osoby:

„*Osobními údaji*“ [se rozumí] *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 /…/.*

Zřejmý důraz na identifikátory obecně a identifikační čísla jako jeden z druhů identifikátorů odráží společenské poměry – všudypřítomné používání jmenných identifikátorů. Jedinečnost identifikátorů musí být zaručena jeho konstrukcí a pravidly používání. Nakládání s obecnými identifikátory upravují zákony (např. jména) nebo technické standardy.

Občanský zákoník, který chrání jméno člověka, rovněž stanoví soubor obvyklých identifikátorů, z nichž ani jeden není z podstaty věci jedinečný: *Údaji, podle nichž lze člověka zjistit, jsou zejména jméno, bydliště a datum narození, popřípadě identifikující údaj podle jiného právního předpisu. Identifikujícím údajem právnické osoby nebo podnikatele je identifikační číslo osoby, bylo-li jim přiděleno*.[12]

I v kontextu ochrany osobních údajů je zvýšená pozornost věnována jedinečným identifikátorům fyzických osob. Obecné nařízení v čl. 87 stanoví, že *členské státy mohou […] stanovit zvláštní podmínky pro zpracování národních identifikačních čísel nebo jakýchkoliv jiných všeobecně uplatňovaných identifikátorů. V takovém případě se národní identifikační číslo nebo jakýkoliv jiný všeobecně uplatňovaný identifikátor použije pouze v závislosti na vhodných zárukách práv a svobod daného subjektu údajů podle tohoto nařízení.*

Některé z jedinečných identifikátorů fyzické osoby, a tedy subjektu údajů, a jejich zpracování upravuje v České republice několik zákonů. Všeobecné uplatnění má zákon o platebním styku; *jedinečný identifikátor* definuje jako kombinaci písmen, číslic nebo symbolů, kterými se podle určení poskytovatele identifikuje uživatel nebo jeho účet při provádění platebních transakcí.[13] V návaznosti na tento zákon např. občanský soudní řád upravuje využívání údajů o peněžních

[12] § 3019 zák. č. 89/2012 Sb., občanský zákoník.
[13] Zák. č. 370/2017 Sb., o platebním styku.

ústavech, u nichž mají účastníci, předvolaní nebo oprávnění účty a čísel účtů nebo jiných jedinečných identifikátorů.[14]

Takové jedinečné identifikátory však nejsou považovány za národní (vnitrostátní). Jimi jsou pouze a právě ty, které jsou konvenčně označovány jako národní identifikační čísla. I ona jsou – jako např. rodné číslo – v České a republice a ve Slovenské republice velmi rozšířena a používají se jak ve veřejné, tak v soukromé sféře. Jejich status umocňuje využitelnost v nejrůznějších situacích a pro různé účely.

Např. daňový řád upravuje jak používání jedinečného identifikátoru ve významu stanoveném zákonem o platebním styku, tak i rodného čísla, které je ovšem pouze prvkem jiného jedinečného identifikátoru fyzické osoby – daňového identifikačního čísla. Daňové identifikační číslo přidělí správce daně daňovému subjektu. Daňové identifikační číslo obsahuje kód „CZ“ a kmenovou část, kterou tvoří obecný identifikátor, jímž je u fyzické osoby rodné číslo, popřípadě jiný obecný identifikátor, stanoví-li tak zákon, a u právnické osoby identifikační číslo.[15]

Nejrozšířenějšími národními obecně používanými identifikátory jsou v současné době v ČR rodná čísla („RČ“) a zdrojové („ZIFO") a agendové („AIFO“) identifikátory. Rodná čísla vznikla za dob listinných evidencí, zdrojové a agendové identifikátory jsou produktem digitalizace veřejné správy. Rodná čísla jsou využívána prakticky všeobecně, zdrojové a agendové identifikátory byly zavedeny pro používání v informačních systémech veřejné správy, které slouží k výkonu agendy jako zákonem stanovené působnosti taxativně určených orgánů veřejné moci, využívání elektronických formulářů nebo elektronické identifikaci. Jako další identifikátory se využívají klientské[16] a stykové identifikátory[17] fyzické osoby.

[14] §§ 260, 260e a 261 zák. č. 99/1963 Sb., občanský soudní řád.

[15] § 130 zákona č. 280/2009 Sb., daňový řád.

[16] Klientský identifikátor fyzické osoby („KIFO“) je definován a vytvářen v rámci konkrétního resortu na základě jeho resortního právního předpisu a slouží k identifikaci osoby při komunikaci se soukromoprávními subjekty, spadající pod výkon působnosti tohoto rezortu. Tento identifikátor je z principu veřejný a může být tedy uváděn na nejrůznějších veřejných dokumentech a listinách např. výpisech z evidencí, různých průkazech, zdravotních záznamech, finančních a účetních dokladech atp. Příklady: bezvýznamový klientský identifikátor insolvenčního rejstříku (BKIIS) - podle § 420 odst. 4 insolvenčního zákona a podle článku CLXXXIII písm. f) DEPO s účinností od 1. ledna 2022 přiděluje soud; identifikátor pacienta (IP) podle § 2 odst. 2 zákona č. 325/2021 Sb., o elektronizaci zdravotnictví, který podle § 13–15 s účinností od 1. ledna 2023 přiděluje Ministerstvo zdravotnictví a identifikátor zdravotnického pracovníka (IZP) podle § 2 odst. 3 zákona č. 325/2021 Sb., o elektronizaci zdravotnictví, který podle § 13–15 s účinností od 1. ledna 2023 přiděluje Ministerstvo zdravotnictví.

[17] Stykový identifikátor fyzické osoby („SIFO“) je takový identifikátor, který je naopak fyzickým osobám vydáván plošně a centrálně a slouží zpravidla k prokázání jejich totožnosti. Jedná se tedy typicky o číslo identifikačního dokladu (například číslo občanského průkazu nebo cestovního pasu). Tento identifikátor je také veřejný a v odůvodněných případech se může vyskytovat na dokumentech či podáních, je-li to nutné vzhledem k povaze příslušného dokumentu či listiny.

Rodné číslo

Rodné číslo[18] upravuje zákon o evidenci obyvatel a rodných číslech[19] a definuje ho v § 13 jako *identifikátor fyzické osoby, která splňuje podmínky pro jeho přidělení.* Rodná čísla přiděluje Ministerstvo vnitra. Rodné číslo je desetimístné číslo, které je dělitelné jedenácti beze zbytku. První dvojčíslí vyjadřuje poslední dvě číslice roku narození, druhé dvojčíslí vyjadřuje měsíc narození, u žen zvýšené o 50, třetí dvojčíslí vyjadřuje den narození. Čtyřmístná koncovka je rozlišujícím znakem fyzických osob narozených v tomtéž kalendářním dnu. Rodná čísla přidělená fyzickým osobám narozeným před 1. lednem 1954 mají stejnou strukturu, jsou však devítimístná s třímístnou koncovkou a nesplňují podmínku dělitelnosti jedenácti. V případě, že jsou vyčerpána veškerá určená rodná čísla určená pro daný kalendářní den v příslušném kalendářním roce, určí Ministerstvo vnitra pro tento den dodatečnou sestavu rodných čísel, kde první dvojčíslí vyjadřuje poslední dvě číslice roku narození, druhé dvojčíslí měsíc narození, u mužů zvýšené o 20 a u žen o 70, třetí dvojčíslí vyjadřuje den narození. Čtyřmístná koncovka je rozlišujícím znakem fyzických osob narozených v tomtéž kalendářním dnu.

Jedinečnost rodného čísla jako národního identifikačního čísla je právně zajištěna ustanoveními, že totéž rodné číslo nesmí být přiděleno více fyzickým osobám a že jedna fyzická osoba je (může být) nositelem nejvýše jednoho rodného čísla.

Statut rodného čísla jako národního identifikačního čísla potvrzují a umocňují četné zákony, které výslovně nařizují nebo umožňují nakládání s rodným číslem jiných lidí. Základní rámec přístupu k rodným číslům poskytuje zákon o evidenci obyvatel a rodných číslech. Rodné číslo

[18] Identifikace fyzických osob byla dříve založena na ztotožňování (dohledávání) osob podle přirozených identifikátorů, jako je jméno, příjmení a bydliště. Protože přirozené identifikátory nemusejí v mnoha případech vyhovovat, zejména u velkých datových sad, bylo potřeba pro agendy z oblasti sociální, pro výpočet důchodů atd., identifikovat klienty jednoznačným identifikátorem, který by přiděloval stát ideálně při narození, bylo v 50. letech 20. století zavedeno rodné číslo (zákonem č. 29/1946 Sb., kterým se zavádějí pracovní průkazy, zaveden univerzální identifikátor. Vyhláškou Ministerstva národní bezpečnosti č. 240/1953 Ú. l., kterou se vydávají podrobnější předpisy o občanských průkazech, byl oddělen identifikátor dokladu, kterým se stalo jeho výrobní číslo, od rodného čísla), které postupně začalo plnit roli všeobecného a jednoznačného identifikátoru fyzické osoby pro více agend veřejné (tehdy státní) správy. Za tím účelem byl tento údaj postupně doplněn na osobní doklady sloužící jako průkazy totožnosti, jako je občanský průkaz, cestovní pas a řidičský průkaz. Na to následně začaly reagovat i veřejné služby, jako byly například pojišťovny, pošta včetně Sdruženého inkasa plateb obyvatelstva (SIPO), spořitelní služby atd. Po roce 1989 se přidaly i další soukromoprávní služby energetických, vodohospodářských, telekomunikačních, cestovních či zprostředkovatelských společností. Současně se s přidáváním veřejnoprávních agend postupovalo vždy tak, že nová agenda ve svém datovém fondu udržovala vždy zejména údaj o rodném čísle, aby bylo možné konkrétního člověka, který se dostavil na přepážku, spolehlivě a rychle identifikovat. Rodné číslo se tedy začalo používat jako základní a klíčový identifikátor pro nalezení záznamů o konkrétní fyzické osobě tak, že v zásadě nebylo nutné zadávat k rodnému číslu žádné další údaje. Tomu technicky nahrával i fakt, že u desetimístných rodných čísel, přidělovaných od 1. ledna 1954, je zadání rodného čísla z principu odolné vůči chybnému zadání, protože poslední 10. číslice obsahuje zbytek po celočíselném dělení číslem 11 (tzv. modulo 11 mechanismus). Pokud by byla zadána nesprávná kombinace, která nevyhovuje modulo 11, upozorní zadavatele na chybné rodné číslo.
Díky výše zmíněným vlastnostem se rodné číslo stalo během několika desítek let klíčovým údajem pro identifikaci a je možné jej tak dnes najít v informačních systémech drtivé většiny agend.

[19] Zák. č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů

je oprávněna užívat nebo rozhodovat o jeho využívání v mezích stanovených zákonem ("nakládat s rodným číslem") výlučně fyzická osoba, které bylo rodné číslo přiděleno ("nositel rodného čísla"), nebo její zákonný zástupce; jinak lze rodné číslo využívat jen:

a) jde-li o činnost ministerstev, jiných správních úřadů, orgánů pověřených výkonem státní správy, soudů, vyplývající z jejich zákonem stanovené působnosti, nebo notářů pro potřebu vedení Centrální evidence závětí,
b) stanoví-li tak zvláštní zákon,
c) pokud je to nezbytné pro vymáhání soukromoprávních nároků nebo pro předcházení vzniku nesplácených pohledávek, jsou-li přijata konkrétní opatření k ochraně práv a svobod subjektu údajů, která odpovídají stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i různě pravděpodobným a závažným rizikům pro práva a svobody fyzických osob, nebo
d) se souhlasem nositele rodného čísla nebo jeho zákonného zástupce.

Využíváním rodných čísel se rozumí využití jakékoliv kombinace čísel vyjadřující den, měsíc, rok narození a třímístnou nebo čtyřmístnou koncovku rodného čísla, z níž je možné dovodit identifikaci fyzické osoby.

Obecné zmocnění širokého okruhu institucí uvedených pod písm. a) bývá omezeno zvláštní právní úpravou výkonu určité působnosti jinak obecně oprávněné instituce. Nedostatečně určitá a současně svazující je s ohledem na vymezení konkrétních opatření k ochraně práv a svobod subjektu údajů podmínka uvedená pod písm. c). Není zřejmé, kdo a za splnění jakých podmínek může reálně využívat rodná čísla pouze na jejím základě. Zákon obecně stanoví, že konkrétní opatření vyžadovaná pro podmínku pod písm. c) (tedy konkrétní opatření k ochraně práv a svobod subjektu údajů) jsou vymezena otevřeným seznamem: mohou zahrnovat zejména a) technická a organizační opatření zaměřená na důsledné uplatnění povinnosti podle čl. 5 odst. 1 písm. c) obecného nařízení, b) pořizování záznamů alespoň o všech operacích shromáždění, vložení, pozměnění a výmazu osobních údajů, které umožní určit a ověřit totožnost osoby provádějící operaci, a uchovávání těchto záznamů nejméně po dobu 2 let od provedení operace, c) informování osob zpracovávajících osobní údaje o povinnostech v oblasti ochrany osobních údajů, d) jmenování pověřence pro ochranu osobních údajů, e) zvláštní omezení přístupu k osobním údajům v rámci správce nebo zpracovatele, f) pseudonymizaci osobních údajů, g) šifrování osobních údajů, h) opatření k zajištění trvalé důvěrnosti, integrity, dostupnosti a odolnosti systémů a služeb zpracování, i) opatření umožňující obnovení dostupnosti osobních údajů a včasný přístup k těmto údajům v případě incidentů, j) proces pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování, nebo k) zvláštní omezení přenosu osobních údajů do třetí země.

Kromě těchto podmínek ovšem nakládání s rodným číslem umožňuje a usnadňuje např. povinné uvádění rodného čísla v občanském průkazu. Rodné číslo obsahují všechny občanské průkazy vydané podle předchozího zákona a dále v občanském průkazu vydaném podle nového zákona do časově ohraničené doby, a to v podobě bezprostředně čitelné nebo vnímatelné člověkem a rovněž ve strojově čitelné podobě v nosiči dat[20].

Na základě výše uvedené „všudypřítomnosti“ údaje o rodném čísle, kterému nepomáhá jeho plošné použití v čísle pojištěnce zdravotního pojištění, stejně jako jeho použití jako daňové identifikační číslo (DIČ) u podnikajících fyzických osob, je možné při schopnostech výpočetní techniky doplněné propojením jednotlivých zařízení globální datovou sítí, datové fondy nekontrolovaně spojovat a výsledné informace využívat k nejrůznějším komerčním, marketingovým či jiným účelům v neprospěch osoby jeho držitele. To je z pohledu ochrany osobních údajů fyzických osob zcela nežádoucí stav a nelze se mu účinně bránit, protože v okamžiku nekontrolovaného rozšíření či dokonce zveřejnění tohoto údaje není, vyjma zcela mimořádných případů, možné jej běžným způsobem změnit.

Z tohoto důvodu je usilováno o útlum používání rodného čísla a nahrazení jinými identifikátory, přesněji o omezení jeho používání na nejnižší možnou míru, danou ideálně pouze agendou matrik a souvisejících veřejných listin, které souvisí s jejím provozem. Cílem útlumu používání rodných čísel je návrat k přirozenosti, posílení lidské důstojnosti odstraněním čísla nahrazující jméno a lepší prevence krádeže a zneužití identity.

Zdrojové a agendové identifikátory

V roce 2009 byl přijetím zákona č. 111/2009 Sb., o základních registrech, učiněn první významný krok k ochraně osobních údajů fyzických osob bez omezení efektivity výkonu veřejné správy. Výše popsaný model využívání jednotného a nezměnitelného identifikačního údaje (RČ) o fyzické osobě měl být v plné šíři nahrazen modelem využívání zdrojového identifikátoru fyzické osoby a mnoha agendových identifikátorů fyzické osoby. Systém základních registrů a agendových identifikátorů byl spuštěn v roce 2012 a postupně mnoho agendových systémů prošlo procedurou ztotožnění svých klientů. Tím došlo k doplnění údaje o agendovém identifikátoru do datového fondu konkrétní agendy, čímž veřejná správa již v roce 2012 naplnila základní požadavky na ochranu osobních údajů fyzických osob se zabráněním neoprávněného slučování údajů (tzv. profilování) o jedné osobě.

Základním právním předpisem pro zpracování zdrojových a agendových identifikátorů je tedy zákon č. 111/2009 Sb., o základních registrech. Ten zejména stanoví, že zdrojový identifikátor fyzické osoby je neveřejným identifikátorem. Zákon také stanoví, že ze zdrojového identifikátoru fyzické osoby nelze dovodit osobní ani jiné údaje o fyzické osobě, jíž byl přiřazen. Zdrojové

[20] § 72 odst. 10 zák. č. 269/2021 Sb., o občanských průkazech, do 31. prosince 2024.

identifikátory fyzických osob vytváří a jejich seznam vede Úřad pro ochranu osobních údajů. Reálně je zdrojový identifikátor generován informačním systémem a není komunikován navenek. Zdrojový identifikátor fyzické osoby používá výhradně Úřad, a to pro vytváření agendových identifikátorů fyzických osob a jejich převod.

Agendový identifikátor fyzické osoby je rovněž neveřejným identifikátorem a je jednoznačně přiřazen záznamu o fyzické osobě v agendovém informačním systému nebo základním registru v rámci příslušné agendy. Je odvozen ze zdrojového identifikátoru fyzické osoby a kódu agendy a je užíván výlučně k jednoznačnému určení fyzické osoby pro účely výkonu agendy, pro kterou byl přidělen. Z agendového identifikátoru fyzické osoby nelze odvodit zdrojový identifikátor fyzické osoby a nelze z něj ani dovodit osobní nebo jiné údaje o fyzické osobě, jíž byl přiřazen.

Fyzická osoba může být identifikována v jednotlivé agendě, která je podporována právě jedním agendovým informačním systémem, jehož správcem je vždy nějaký orgán veřejné moci, pouze jedním agendovým identifikátorem fyzické osoby. Tento identifikátor nesmí být přidělen více fyzickým osobám a nelze jej měnit.

Rovněž agendové identifikátory fyzických osob vytváří a jejich seznamy vede Úřad. Na základě zákonného požadavku zajišťuje převod agendového identifikátoru fyzické osoby v agendě na agendový identifikátor této fyzické osoby v jiné agendě.

Každý správce agendového informačního systému zajišťuje realizaci vazby mezi agendovým informačním systémem a informačním systémem základních registrů a mezi vlastním agendovým informačním systémem a jinými agendovými informačními systémy; komunikace se uskutečňuje prostřednictvím informačního systému základních registrů nebo informačního systému sdílené služby za účelem využívání údajů.

Neveřejnost základního identifikátoru fyzické osoby zákon o základních registrech neupravuje za použití pojmů ochrany osobních údajů. Upravuje však přístupnost tím, že stanoví, že *k zabránění neoprávněnému přístupu k osobním údajům vedeným v základních registrech a v jiných informačních systémech veřejné správy používají orgány veřejné moci při komunikaci základních registrů navzájem a základních registrů s agendovými informačními systémy kód agendy a agendový identifikátor fyzické osoby.* Fakticky tím obecně stanoví nepřístupnost základního identifikátoru fyzické osoby.

Zpřístupnění údajů vedených v základních registrech a údajů vedených v agendových informačních systémech, jejichž prostřednictvím se zapisují údaje do základních registrů, v rozsahu oprávnění vedených v registru práv a povinností prostřednictvím služeb informačního systému základních registrů, zajišťuje Správa základních registrů. Ta také vydá na žádost osoby, o níž se vedou údaje v agendových informačních systémech, záznam o využívání těchto údajů. Záznam vydává rovněž v podobě ověřeného výstupu z informačního systému veřejné správy. Použije se přitom výslovná zvláštní úprava každého ze základních registrů.

§ 58 Poskytování údajů z registru obyvatel a registru práv a povinností

(1) Fyzické osobě (dále jen „subjekt údajů“) se poskytnou referenční nebo provozní údaje, které jsou k ní vedeny v registru obyvatel a registru práv a povinností, na základě žádosti podané:

- *a) elektronicky,*
- *b) v listinné podobě, nebo*
- *c) osobně.*

(2) Elektronicky lze podat žádost na elektronickém formuláři zpřístupněném Ministerstvem vnitra dálkovým přístupem.

(3) Žádost o poskytnutí údajů z registru obyvatel a registru práv a povinností může subjekt údajů zaslat také v listinné podobě kterémukoliv obecnímu úřadu obce s rozšířenou působností, krajskému úřadu a v případě údajů z registru obyvatel také Ministerstvu vnitra; žádost musí být opatřena úředně ověřeným podpisem. Úředně ověřený podpis se nevyžaduje, je-li žádost podepsána před zaměstnancem zařazeným ve správním orgánu, vůči kterému směřuje.

(4) Žádost o poskytnutí údajů podle odstavců 2 a 3 musí obsahovat:

- *a) jméno, popřípadě jména, a příjmení,*
- *b) datum a místo narození,*
- *c) číslo a druh identifikačního dokladu,*
- *d) adresu místa pobytu, popřípadě jinou kontaktní adresu,*
- *e) rozsah požadovaných údajů a formu jejich předání.*

(5) O poskytnutí údajů z registru obyvatel a registru práv a povinností může subjekt údajů požádat osobně u kontaktního místa veřejné správy, u kteréhokoli obecního úřadu obce s rozšířenou působností nebo krajského úřadu a v případě údajů z registru obyvatel také u Ministerstva vnitra; subjekt údajů sdělí rozsah požadovaných údajů. Subjekt údajů provede svoji identifikaci pomocí identifikačního dokladu.

(6) Údaje z registru obyvatel a registru práv a povinností poskytuje správní orgán, u kterého byla žádost podána.

(10) Za subjekt údajů může požádat o poskytnutí údajů zmocněnec na základě zvláštní plné moci s úředně ověřeným podpisem zmocnitele; údaje se poskytnou zmocněnci.

Údaj o agendovém identifikátoru fyzické osoby pro agendu evidence obyvatel, který je současně agendovým identifikátorem v registru obyvatel, se v současné době poskytuje pouze podle zákona o základních registrech, tj. není dáno právo na přístup samotnému subjektu údajů. Obdobně se údaje o agendovém identifikátoru fyzické osoby pro agendu cestovních dokladů a pro agendu diplomatických a služebních pasů se neposkytují, pokud tak nestanoví zvláštní právní předpis.[21]

Doplněním agendových identifikátorů došlo k vytvoření záruk pro pouze zákonem založené sdílení centrálního datového fondu a lidé tak již většině agendových správců nemusejí hlásit změny svých údajů, například změnu příjmení, místa trvalého pobytu, čísla identifikačního dokladu atd., protože eGovernment je nastaven tak, že agendové systémy se dozvědí o jejich změnách a následně si načtou jejich nové hodnoty ze základních registrů. Doplnění agendových identifikátorů však nezpůsobilo v širším měřítku upuštění od využívání rodného čísla v konkrétních agendách, protože je to zažité, technicky výhodné a relativně spolehlivé. S tím tedy bohužel přetrvává použití rodného čísla na dohledání občana při prezenčním styku s úřadem, často i při vyřizování písemného podání, na kterém bývá RČ často vyžadováno. Změna tohoto přístupu bude znamenat změny ve vyhledávacích dialozích mnoha informačních systémů veřejné správy, kde se místo zadávání RČ, typicky zadávaným opsáním z občanského průkazu, bude muset vyhledávat pomocí jiného unikátního údaje, ideálně čteného strojově. Jedním z doporučených řešení je čtení čísla občanského průkazu jednoduchou čtečkou čárového kódu. Zakódované číslo občanského průkazu je předmětem uvádění na občanském průkazu již mnoho let a jako takové se dá v prezenčních situacích začít používat okamžitě. Zadáním čísla dokladu dojde voláním služby ISZR k dohledání AIFO v dané agendě a s jeho znalostí je pak možné načíst jakékoliv další identifikační či agendové údaje.

Uvedený princip agendových identifikátorů funguje spolehlivě uvnitř veřejné správy, tj. v rámci agend vykonávaných vůči fyzické osobě orgány veřejné moci. Co se týká rozhraní veřejné a soukromé sféry koncept agendových identifikátorů, které jsou z definice v zákoně neveřejné, nemůže být použit, protože subjektům soukromého práva nesmí být neveřejné AIFO poskytnuto. Zejména proto se v některých situacích nadále setrvává na používání rodného čísla jako unikátního identifikátoru fyzické osoby. Aby se odstranil tento z pohledu ochrany osobních údajů nežádoucí stav, byl zákonodárcem od 1. července 2022 zaveden bezvýznamový směrový identifikátor („BSI"), který generuje správce národního bodu pro identifikaci a autentizaci, tedy Správa základních registrů.[22] BSI má soukromému sektoru sloužit jako plná náhrada rodného čísla a má pro něj tu výhodu, že poskytuje státem zaručenou lepší identifikaci jejich klientů bez ohledu na jakoukoliv změnu identifikátorů, včetně rodného čísla. Na rozdíl od rodného čísla však není BSI univerzální; je vázáno na konkrétního podnikatele. Lidé si BSI pamatovat nemusejí, dokonce se ho ani nedozvědí, protože vůči podnikateli (terminologií zákona poskytovateli služeb) se budou identifikovat přirozenými identifikátory a číslem dokladu, zejména občanského průkazu.

[21] § 30 zák. č. 329/1999 Sb.
[22] § 12a zákona č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů.

3. Zákonnost zpracování osobních údajů (právní důvody)

Právní základ zpracování

Jednou z klíčových zásad zpracování osobních údajů, kterou stanovuje obecné nařízení, je zákonnost zpracování zakotvená v jeho čl. 5 odst. 1 písm. a). Tato zásada je především promítnuta v čl. 6 a dále též např. v čl. 7, 8 či 9 obecného nařízení). Zmíněný čl. 6 stanoví, že 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 za účelem přijetí opatření před uzavřením smlouvy na žádost 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.

Každé zpracování osobních údajů se musí opírat o některý z uvedených právních důvodů zpracování osobních údajů (též označovaných jako právní základy či tituly). Jednotlivé právní důvody pak zároveň stanovují základní podmínky, za nichž je možné určité zpracování osobních údajů provádět.

Zároveň platí, že:

- žádný z těchto základů není nadřazen kterémukoli jinému,
- pořadí základů uvedených v obecném nařízení není rozhodné,
- žádný regulační nebo dozorový úřad není oprávněn stanovit nadřazenost nebo prioritu určitého právního základu,
- zákonnost zpracování vyjádřená odkazem (ze strany správce osobních údajů) na některý z právních důvodů musí být posuzována individuálně.

Obecné nařízení současně omezuje použitelnost právních důvodů pro zpracování: zpracování pro účely oprávněných zájmů (písm. f)) se nepoužije („netýká“) zpracování prováděného orgány veřejné moci při plnění jejich úkolů.

Pluralitě skutečně sledovaných účelů zpracování prováděných jako hlavní činnost, součást hlavní činnosti nebo jen činnost podpůrná odpovídá, že členské státy mohou zachovat nebo zavést konkrétnější ustanovení, aby přizpůsobily používání pravidel obecného nařízení pro zpracování ke splnění čl. 6 odst. 1 písm. c) a e) obecného nařízení tím, že přesněji určí konkrétní požadavky na zpracování a jiná opatření k zajištění zákonného a spravedlivého zpracování, a to i u jiných zvláštních situací, při nichž dochází ke zpracování, jak stanoví kapitola IX.

Právní důvod pro zpracování nezbytná pro splnění právní povinnosti, pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci musí být stanoven buď právem Unie, nebo právem členského státu, které se na správce vztahuje. Další podmínkou je, že účel zpracování musí vycházet z tohoto právního důvodu, nebo pokud jde o zpracování uvedené v čl. 6 odst. 1 písm. e) obecného nařízení, musí být toto zpracování nutné pro splnění úkolu prováděného ve veřejném zájmu či při výkonu veřejné moci, kterým je pověřen správce. Tento právní důvod může obsahovat konkrétní ustanovení pro přizpůsobení uplatňování pravidel tohoto nařízení, včetně obecných podmínek, kterými se řídí zákonnost zpracování správcem, typu osobních údajů, které mají být zpracovány, dotčených subjektů údajů, subjektů, kterým lze osobní údaje poskytnout, a účelu tohoto poskytování, účelového omezení, doby uložení a jednotlivých operací zpracování a postupů zpracování, jakož i dalších opatření k zajištění zákonného a spravedlivého zpracování, jako jsou opatření pro jiné zvláštní situace, při nichž dochází ke zpracování, jež stanoví kapitola IX. Právo Unie nebo členského státu musí splňovat cíl veřejného zájmu a musí být přiměřené sledovanému legitimnímu cíli.

V České republice se tak děje především v právních předpisech zakládajících nebo jinak upravujících jednotlivá zpracování osobních údajů. Obecně dále zákonnost zpracování založeného na těchto právních základech upravuje zákon o zpracování osobních údajů. Především obecně deklaruje splnění podmínek podle čl. 6 odst. 1 písm. c) a e):[23] správce je oprávněn zpracovávat osobní údaje, pokud je to nezbytné pro splnění povinnosti, která je tomuto správci uložena právním předpisem, nebo úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen. Toto ustanovení kompenzuje historickou neúplnost (fragmentárnost) právní úpravy pro správce působící v České republice obecně, nejen pro veřejnoprávní správce, a má podle důvodové zprávy k zákonu poskytnout ochranu před formalistickým výkladem:

[23] § 5 zák. č. 110/2019 Sb.

Přestože je nepochybné, že právní povinnost uvedenou v čl. 6(1)(c) stanoví pouze právní předpis, čl. 6(3) stejně vyžaduje, aby „základ pro zpracování" stanovil právní předpis. Proto je nutno počítat i s takovým, byť velmi formalistickým, výkladem, že právní předpis má stanovit samo oprávnění zpracovávat osobní údaje. Různé předpisy to ostatně činí již nyní. Ustanovení písm. a) tudíž poskytuje subsidiární titul pro zpracování, pokud jednoznačně neplyne z platných předpisů, a zajišťuje tak právní jistotu, neboť hovoří výslovně o oprávnění ke zpracování.

Vzhledem k obdobným obavám a tomu, že výklad čl. 6(3) je nejednoznačný mezi členskými státy v tom, zda vyžaduje i zákonné zakotvení „oprávnění ke zpracování" ve veřejném zájmu, písm. b) poskytuje právní jistotu i v těchto případech.

Pravomoci správců se nijak nerozšiřují, pouze se zajišťuje, že tam, kde plní úkoly na základě zákonné povinnosti nebo z důvodu veřejného zájmu, nejsou zbaveni možnosti zpracovávat osobní údaje. Jsou-li v platných předpisech omezení pro zpracování osobních údajů, nejsou dotčena, zpracování osobních údajů musí být v mezích těchto právních předpisů.

Předpokládá se, že s novelizací nebo jinou náhradou dřívější právní úpravy jednotlivých zákonem (byť implicitně) založených zpracováních bude použitelnost ustanovení § 5 zák. č.110/2019 Sb. postupně zanikat. Použitelnost ustanovení je podmíněna nezbytností zpracování osobních údajů – tedy stavem, kdy úkol nebo povinnost nelze splnit bez zpracování osobních údajů.

Dále zákon o zpracování osobních údajů k provedení čl. 6 odst. opět obecně stanoví rámec posuzování jednotlivých zpracování osobních údajů prováděných pro novinářské účely nebo pro účely akademického, uměleckého nebo literárního projevu. V § 17 je stanoveno, že *osobní údaje lze zpracovávat také tehdy, slouží-li to přiměřeným způsobem pro novinářské účely nebo pro účely akademického, uměleckého nebo literárního projevu. Při posouzení přiměřenosti podle věty první se přihlédne také k tomu, jestli zpracování zahrnuje osobní údaje uvedené v čl. 9 odst. 1 nebo čl. 10 nařízení Evropského parlamentu a Rady (EU) 2016/679. Zpracování osobních údajů pro účely uvedené v odstavci 1 není podmíněno povolením nebo schválením Úřadu a požívá práva na ochranu zdroje a obsahu informací, a to i v případě zpracování osobních údajů způsobem umožňujícím dálkový přístup.*[24] Toto ustanovení tedy současně pouze velmi obecně zakotvuje požadavky na zákonnost a naproti tomu konkrétně omezuje dozorové pravomoci v oblasti ochrany osobních údajů.

Pro zpracování osobních údajů k zajišťování obranných a bezpečnostních zájmů České republiky, pokud jiný právní předpis nestanoví jinak, stanoví požadavky na právní základ § 43

[24] § 17 zák. č. 110/2019 Sb.

(Hlava IV) zákona o zpracování osobních údajů. Osobní údaje může k některému z těchto účelů správce zpracovávat pouze se souhlasem subjektu údajů; na tento souhlas se použije definice z obecného nařízení. Bez tohoto souhlasu může správce osobní údaje zpracovávat, jestliže:

a) provádí zpracování nezbytné pro dodržení povinnosti správce,
b) je zpracování nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro jednání o uzavření nebo změně smlouvy uskutečněné na návrh subjektu údajů,
c) je zpracování nezbytné k ochraně životně důležitých zájmů subjektu údajů; v tomto případě je třeba bez zbytečného odkladu získat jeho souhlas, jinak musí správce toto zpracování ukončit a údaje vymazat,
d) se jedná o oprávněně zveřejněné osobní údaje,
e) je zpracování nezbytné pro ochranu práv nebo právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby; takové zpracování osobních údajů však nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života,
f) poskytuje osobní údaje o veřejně činné osobě, funkcionáři nebo zaměstnanci orgánu veřejné správy, které vypovídají o jeho veřejné nebo úřední činnosti nebo funkčním nebo pracovním zařazení, nebo
g) se jedná o zpracování výlučně pro účely archivnictví.

Další požadavky na souhlas jsou uvedeny v kapitole 7.

Zpracování k jinému účelu („slučitelnost účelů“)

Při zpracování osobních údajů může vyvstat otázka, zda lze osobní údaje zpracovávat i pro jiný účel, než pro který byly shromážděny. Zájem nebo potřeba odchýlit se při zpracování od původního účelu zpravidla nastává s časovým odstupem od návrhu zpracování a jeho zahájení. Jakkoliv se s takovou situací právní úprava výslovně vyrovnává, je třeba dodržet všechny podmínky stanovené zákonnou úpravou (resp. úpravou obsaženou v obecném nařízení).

Předně takové zpracování může být založeno na souhlasu subjektu údajů, nebo být výslovně povoleno právním předpisem EU nebo členského státu. Typicky je v čl. 5 odst. 1 písm. b) obecného nařízení zakotveno zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého nebo historického výzkumu nebo účely statistické.

Výslovná a specifická právní úprava se odlišuje v podrobnostech. V ČR je další zpracování omezeno okruhem možných přejímajících správců (např. § 52 zák. č. 280/2009 Sb., daňový řád), případně v kombinaci s dalším omezením. Typickým příkladem jsou ustanovení zákona o evidenci obyvatel a rodných číslech, kladoucí na vykonavatele státní správy vůči evidenci obyvatel společně s oprávněním údaje využívat požadavek využívat tyto údaje, využívat, jen jsou-li nezbytné pro výkon jeho působnosti (§§ 4 a 5 zák. č. 133/2000 Sb.).

Samotné obecné nařízení stanoví ve svém čl. 6 odst. 4 podmínky, za nichž mohou osobní údaje zpracovávány pro jiný účel, než pro který byly osobní údaje shromážděny. Toto ustanovení říká:

Pokud zpracování pro jiný účel, než pro který byly osobní údaje shromážděny, není založeno na souhlasu subjektu údajů nebo na právu Unie či členského státu, který v demokratické společnosti představuje nutné a přiměřené opatření k zajištění cílů uvedených v čl. 23 odst. 1[25]*, zohlední správce v zájmu zjištění toho, zda je zpracování pro jiný účel slučitelné s účely, pro něž byly osobní údaje původně shromážděny, mimo jiné:*

- *jakoukoli vazbu mezi účely, kvůli nimž byly osobní údaje shromážděny, a účely zamýšleného dalšího zpracování;*
- *okolnosti, za nichž byly osobní údaje shromážděny, zejména pokud jde o vztah mezi subjekty údajů a správcem;*
- *povahu osobních údajů, zejména zda jsou zpracovávány zvláštní kategorie osobních údajů podle čl. 9 nebo osobní údaje týkající se rozsudků v trestních věcech a trestných činů podle čl. 10;*
- *možné důsledky zamýšleného dalšího zpracování pro subjekty údajů;*
- *existenci vhodných záruk, mezi něž může patřit šifrování nebo pseudonymizace.*

V rámci popsaného testu slučitelnosti musí tedy správce přihlédnout ke všem výše uvedeným aspektům a současně zvážit i další, pokud jsou v jeho situaci relevantní. Je zřejmé, že k řádnému splnění podmínek musí správce současně k dodržení zásady odpovědnosti podle čl. 5 odst. 2 obecná nařízení být schopen slučitelnost, resp. její kladné vyhodnocení, doložit.[26] Je třeba nicméně doplnit a zdůraznit, že pro zpracování pro dodatečné účely vůči těm, pro které byly původně shromážděny, je třeba stanovit relevantní právní důvod ve smyslu čl. 6 odst. 1 obecného nařízení.

Kromě toho zákon o zpracování osobních údajů zakotvuje obecnou výjimku z povinnosti posuzovat slučitelnost účelů, omezenou výhradou zvláštní právní úpravy: Nestanoví-li jiný právní předpis jinak, správce není povinen při zajišťování chráněného zájmu posuzovat před zpracováním osobních údajů k jinému účelu, než ke kterému byly shromážděny, slučitelnost těchto účelů, je-li toto zpracování nezbytné a přiměřené pro splnění povinnosti, která je správci uložena, nebo úkolu ve veřejném zájmu stanoveného právním předpisem nebo při výkonu veřejné moci, kterým je správce pověřen.

[25] Výčet cílů obsahuje kap. 19 těchto skript.
[26] Recital (50) obecného nařízení.

Chráněným zájmem se zde rozumí:

a) obranné nebo bezpečnostní zájmy České republiky,
b) veřejný pořádek a vnitřní bezpečnost, předcházení, vyhledávání nebo odhalování trestné činnosti, stíhání trestných činů, výkon trestů a ochranných opatření, zajišťování bezpečnosti České republiky nebo zajišťování veřejného pořádku a vnitřní bezpečnosti, včetně pátrání po osobách a věcech,
c) jiný důležitý cíl veřejného zájmu Evropské unie nebo členského státu Evropské unie, zejména důležitý hospodářský nebo finanční zájem Evropské unie nebo členského státu Evropské unie, včetně záležitostí měnových, peněžních, rozpočtových, daňových a finančního trhu, veřejného zdraví nebo sociálního zabezpečení,
d) ochrana nezávislosti soudů a soudců,
e) předcházení, vyhledávání, odhalování nebo stíhání porušování etických pravidel regulovaných povolání,
f) dohledové, kontrolní nebo regulační funkce spojené s výkonem veřejné moci v případech uvedených v písmenech a) až e),
g) ochrana práv a svobod osob, nebo
h) vymáhání soukromoprávních nároků.

Výhradním zdrojem pro správnou interpretaci chráněného zájmu je uznávaná judikatura, primárně pak judikatura Soudního dvora Evropské unie dostupná například zde.

4. Vztah zákona o zpracování osobních údajů a obecného nařízení o ochraně osobních údajů

V obecném vnímání ochrany osobních údajů nejen nejširší veřejnosti je platná předpisová základna omezena právě na obecné nařízení. To je správné pouze na určité úrovni obecnosti s oporou v tom, že samo toto nařízení obsahuje jednak přímo použitelná ustanovení, a tedy i práva subjektu údajů nebo povinností správců a zpracovatelů, jednak ustanovení vyžadující provedení buď právem EU, nebo právem některého z členských států, případně oběma. Provedení je buď umožněno (…. *Členské státy mohou* …), nebo vyžadováno (*Každý členský stát stanoví, že* …). Ustanovení umožňující logicky obsahují i normy, které jsou přímo použitelné bez provedení vnitrostátním předpisem.

Zákon o zpracování osobních údajů je často zúženě vnímán jako **adaptační** vnitrostátní předpis k obecnému nařízení. Není však pouze jím, ale současně zákonem **implementujícím** směrnici č. 2016/680 (transpozičním předpisem k ní) a Úmluvu č. 108 o ochraně osob se zřetelem na automatizované zpracování osobních dat. To – byť poněkud nepřesně – vyjadřuje § 1 zákona o zpracování osobních údajů; nepřesnost je dána jednak tím, že text není úplný bez dvou poznámek pod čarou, jednak odkazováním na striktně vzato v platné legislativě neexistujícím výslovně formulovaným právem na ochranu soukromí. Řádný rámec poskytuje § 1 pouze ve spojení s § 2:

*§ 1 **Předmět úpravy***

Tento zákon zapracovává příslušné předpisy Evropské unie[1)], zároveň navazuje na přímo použitelný předpis Evropské unie[2)] a k naplnění práva každého na ochranu soukromí upravuje práva a povinnosti při zpracování osobních údajů.

*§ 2 **Působnost zákona***

Tento zákon upravuje:

a) zpracování osobních údajů podle nařízení Evropského parlamentu a Rady (EU) 2016//679[2)],

b) zpracování osobních údajů příslušnými orgány za účelem předcházení, vyhledávání nebo odhalování trestné činnosti, stíhání trestných činů, výkonu trestů a ochranných opatření, zajišťování bezpečnosti České republiky nebo zajišťování veřejného pořádku a vnitřní bezpečnosti, včetně pátrání po osobách a věcech,

c) zpracování osobních údajů při zajišťování obranných a bezpečnostních zájmů České republiky,

d) další zpracování osobních údajů, které mají být nebo jsou zařazeny do evidence nebo jejichž zpracování probíhá zcela nebo částečně automatizovaně, ne-jde-li o zpracování osobních údajů fyzickou osobou v průběhu výlučně osobních nebo domácích činností, a

e) postavení a pravomoc Úřadu pro ochranu osobních údajů.

Poznámka pod čarou č. 1 odkazuje na Směrnici 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 (dále v tomto studijním textu též pouze „trestněprávní směrnice" nebo „směrnice č. 2016/680").

Poznámka pod čarou č. 2 odkazuje na 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).

Předmět a účel Úmluvy č. 108 je v ní samotné deklarován jako *zaručit na území každé smluvní strany každé fyzické osobě, ať je jakékoli národnosti nebo pobývá kdekoli, úctu k jejím právům a základním svobodám, a zejména k jejímu právu na soukromý život, se zřetelem k automatizovanému zpracování osobních údajů, které se k ní vztahují*.

Jinými slovy, zákon o zpracování osobních údajů implementuje do právního řádu České republiky dva sekundární právní předpisy Evropské unie. Protože však nařízení nepředpokládá a ani neumožnuje, aby se provedlo v rámci národní legislativy, pokud tak není v nařízení přímo umožněno, nelze do zákona přebírat pojmy a jiné součásti obecného nařízení. Zákon o zpracování osobních údajů tak musí být aplikován současně s obecným nařízením. Zákon obsahuje obecnou úpravu, doplněnou nebo modifikovanou zvláštními výjimkami a postupy v jiných zákonech.[27]

Vzhledem k tomu, že žádný z orgánů veřejné moci v České republice se nemůže řídit v otázkách ochrany osobních údajů pouze obecným nařízením a ustanoveními zákona o zpracování osobních údajů toto nařízení provádějícími, není vhodné, aby správní úřady používaly k označení kontaktních platforem pro subjekty údajů z řad vlastních zaměstnanců nebo specializované či obecné veřejnosti označení „gdpr".

V důsledku struktury a obsahu zákona je implementační část v užším slova smyslu omezena na to, co se označuje jako „neunijní" zpracování osobních údajů. Schematicky, tj. s nevyhnutelným zjednodušením, se za adaptační považují ustanovení hlavy II. Patří k nim ovšem i hlavy V. a VI. zákona, jejichž ustanovení ovšem nejsou pouze navazujícími na obecné nařízení.

[27] Důvodová zpráva k vládnímu návrhu zákona č. 110/2019 Sb.

Úvodní ustanovení zákona stanoví působnost zákona v členění na zpracování, na které dopadá obecné nařízení nebo jež do jeho působnosti vtahuje hlava II. To především znamená, že u justičních a policejních orgánů dochází k tzv. „smíšenému“ či „trestněprávnímu“ zpracování podle směrnice 2016/680, které je obsaženo zejména v hlavě III[28]. Hlava IV pokrývá zpracování osobních údajů, které je vyňato z působnosti práva EU a které se týká bezpečnosti a obrany ČR, tj. zpracování osobních údajů, k němuž dochází v rámci zpravodajských služeb, při některých zpracováních osobních údajů prováděných Národním bezpečnostním úřadem a Národním úřadem pro kybernetickou a informační bezpečnost. Naplňují se tu – v rozsahu stejném jako v předchozí právní úpravě ochrany osobních údajů ve vnitrostátním předpisu – závazky ČR vyplývající z ratifikace Úmluvy č. 108 v institucionálním rozsahu a do značné míry shodně s účely sledovanými takovými institucemi při zpracování osobních údajů účelu pro zpracování nepokrytá hlavami II a III. Hlava V. řeší postavení, úkoly a pravomoci nezávislého kontrolního úřadu, jehož zřízení je po členských státech požadováno jak obecným nařízením, tak směrnicí 2016/680[29]. Její ustanovení naplňují povinnost České republiky provést příslušná ustanovení obou předpisů.

Hlava VI. a část druhá zákona o zpracování osobních údajů obsahují část týkající se správního trestání[30] a nezbytná přechodná a závěrečná ustanovení. V rámci skutkových podstat přestupků jsou upravena jak porušení obecného nařízení, kde je vyhrazen prostor vnitrostátní úpravě, tak porušení, která se však také deklarují jako přestupky podle národní úpravy správního trestání (a tím této úpravě podřazují). Formulace skutkových podstat přestupků, které se odvíjejí od výslovné úpravy obecného nařízení, zohledňují zvláštní povahu předpisů evropského práva a principy tvorby právní úpravy přestupků[31].

V ustanoveních Hlavy II *Zpracování osobních údajů podle přímo použitelného předpisu Evropské unie* jsou využity možnosti členských států zachovat původní ustanovení nebo zavést konkrétnější. Takto jsou povoleny výjimky z povinnosti posuzovat slučitelnost účelů[32], povinnosti posoudit vliv zpracování na ochranu osobních údajů a povinnosti oznámit porušení zabezpečení osobních údajů subjektu údajů. Výjimka z povinnosti posoudit vliv zpracování na ochranu osobních údajů v případě, že právní předpis danému správci ukládá povinnost takové zpracování provést nebo provádět má odstranit pochybnosti o pokračujícím zpracování veřejnoprávních i soukromých správců, kteří ke dni nabytí účinnosti zákona o zpracování osobních údajů osobní údaje zpracovávali na základě právní úpravy, která nesplňovala všechny požadavky stanovené právě obecným nařízením.

---

[28] K omezení práv a povinností podle hlavy III vizte kap. 19.
[29] O Úřadu pro ochranu osobních údajů pojednává kapitola 18.
[30] O správním trestání pojednává kapitola 15.
[31] O správním trestání pojednává kapitola 15.
[32] Podrobněji vizte kap. 3.

Obecnou úpravou naopak nejsou adresovány další podmínky zpracování zvláštních kategorií osobních údajů podle čl. 9.

5. Věcná a místní působnost obecného nařízení o ochraně osobních údajů a zákona o zpracování osobních údajů

Věcná a místní[33] působnost obecného nařízení

Věcná působnost je stanovena v čl. 2: nařízení se vztahuje na zcela nebo částečně automatizované zpracování[34] osobních údajů a na neautomatizované zpracování těch osobních údajů, které jsou obsaženy v evidenci nebo do ní mají být zařazeny. V případě manuálního zpracování se tedy nařízení uplatní vždy, když jsou osobní údaje obsaženy v evidenci (např. v kartotéce) nebo do ní mají být zařazeny.

Z věcné působnosti stanoví nařízení v odst. 2 celkem 4 výjimky:

a) Nařízení se nevztahuje na zpracování osobních údajů prováděné při výkonu činností, které nespadají do oblasti působnosti práva Unie,
b) Nařízení se nevztahuje na zpracování osobních údajů prováděné členskými státy při výkonu činností, které spadají do oblasti působnosti hlavy V kapitoly 2 Smlouvy o EU,
c) Nařízení se nevztahuje na zpracování osobních údajů prováděné fyzickou osobou v průběhu výlučně osobních či domácích činností. Recitál 18 nařízení výslovně zmiňuje, že činnosti osobní povahy nebo činnosti prováděné výhradně v domácnosti musí být bez jakékoliv souvislosti s profesní nebo obchodní činností. Jako příklad takových činností uvádí korespondenci a vedení adresářů nebo využívání sociálních sítí a internetu v souvislosti s těmito činnostmi,
d) Nařízení se nevztahuje na zpracování osobních údajů prováděné příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů a za účelem výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení a také na zpracování osobních údajů prováděné orgány, institucemi a jinými subjekty Unie[35].

---

[33] K místní působnosti viz podrobněji Pokyny EDPB č. 3/2018 k místní působnosti nařízení.

[34] Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat (Úmluva 108) z roku 1981 definuje automatizované zpracování jako operace uskutečňované zcela nebo zčásti pomocí automatizovaných postupů: ukládání na nosiče dat, provádění logických a/nebo aritmetických operací s těmito daty, jejich změna, výmaz, vyhledávání nebo rozšiřování.

[35] Tato oblast je upravena Směrnicí Evropského parlamentu a Rady 2016/680 ze dne 27. 4. 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.

Místní působnost je stanovena v čl. 3[36], který definuje místní působnost nařízení na základě dvou hlavních kritérií: **(i) kritéria „provozovny"**[37], podle kterého se nařízení vztahuje na zpracování osobních údajů v souvislosti s činnostmi provozovny správce nebo zpracovatele v Unii bez ohledu na to, zda zpracování probíhá v Unii či mimo ni (čl. 3 odst. 1). **(ii) kritéria „zaměření"** (na jednotlivce v EU), buď tím, že jim je nabízeno zboží či služby, nebo že je monitorováno jejich chování. Nařízení se tedy vztahuje na zpracování osobních údajů subjektů údajů, které se nacházejí v Unii, správcem nebo zpracovatelem, který není usazen v Unii, pokud činnosti zpracování souvisejí: a) *s nabídkou zboží nebo služeb těmto subjektům údajů v Unii, bez ohledu na to, zda je od subjektů údajů požadována platba, nebo b) s monitorováním jejich chování, pokud k němu dochází v rámci Unie* (čl. 3 odst. 2).

A konečně se nařízení vztahuje na zpracování osobních údajů správcem, který není usazen v Unii, ale na místě, kde se právo členského státu uplatňuje na základě mezinárodního práva veřejného (čl. 3 odst.3).

Správci nebo zpracovatelé, na které se vztahuje nařízení na základě čl. 3 odst. 2, jsou povinni jmenovat zástupce v EU dle čl. 27 nařízení např. na základě smlouvy o poskytování služeb. Funkce zástupce není slučitelný s funkcí externího pověřence.

To vše je reakcí na hospodářskou a sociální integraci vyplývající z fungování vnitřního trhu, jehož logickým důsledkem je mimo jiné nárůst přeshraničních toků osobních údajů. Takto vymezená působnost zajišťuje, že ochrana poskytovaná tímto nařízením by se měla týkat zpracování osobních údajů fyzických osob bez ohledu na jejich státní příslušnost nebo bydliště.[38]

Věcná a místní působnost zákona o zpracování osobních údajů

Poznámka: k působnosti zákona se významně vztahuje kapitola 4 této učební pomůcky.

Věcná a místní působnost zákona č. 110/2019 Sb. je upravena v § 2. Zahrnuje:

a) zpracování osobních údajů podle obecného nařízení,
b) zpracování osobních údajů příslušnými orgány za účelem předcházení, vyhledávání nebo odhalování trestné činnosti, stíhání trestných činů, výkonu trestů a ochranných opatření, zajišťování bezpečnosti České republiky nebo zajišťování veřejného pořádku a vnitřní bezpečnosti, včetně pátrání po osobách a věcech,
c) zpracování osobních údajů při zajišťování obranných a bezpečnostních zájmů České republiky,

[36] Místní působnost je velmi úzce provázána s předávání osobních údajů do třetích zemí podle kap. V. nařízení (otázka č. 17). K tomu viz Pokyny EDPB 5/2021 ke vztahu mezi čl. 3 a kap. 5 nařízení.
[37] Pojem provozovna zahrnuje jakoukoliv efektivní a skutečnou činnost, i minimální, vykonávanou prostřednictvím stálého zařízení. Právní forma provozovny není rozhodující (recitál 22).
[38] Recital (14).

d) další zpracování osobních údajů, které mají být nebo jsou zařazeny do evidence nebo jejichž zpracování probíhá zcela nebo částečně automatizovaně, ne-jde-li o zpracování osobních údajů fyzickou osobou v průběhu výlučně osobních nebo domácích činností,
e) postavení a pravomoc Úřadu pro ochranu osobních údajů (dále v textu též jen „Úřad").

V zájmu zachování stejné věcné působnosti se opakuje část vymezení působnosti obecného nařízení o ochraně osobních údajů v rozsahu vyloučení zpracování, které provádí fyzická osoba v průběhu výlučně osobních nebo domácích činností. Tato zpracování se tudíž nebudou řídit obecným nařízením a tímto zákonem, ale občanským zákoníkem.[39]

[39] Důvodová zpráva k zák. č. 110/2019 Sb.

6. Ohlašovací a oznamovací povinnosti správců a spravujících orgánů vůči Úřadu pro ochranu osobních údajů, subjektům údajů a příjemcům

Ohlašovací a oznamovací povinnosti správců upravuje obecné nařízení a zákon o zpracování osobních údajů a doplňkově zvláštní zákony, povinnosti spravujícího orgánu upravuje zákon o zpracování osobních údajů a také zvláštní zákony.[40]

Povinnosti správců

Správce má ohlašovací a oznamovací povinnost v souvislosti se zjištěním porušení zabezpečení osobních údajů. Ohlašovací povinnost[41] směřuje k Úřadu pro ochranu osobních údajů, oznamovací[42] vůči subjektům údajů.

Obsahem ohlašovací povinnosti správce je ohlásit místně příslušnému dozorovému úřadu skutečnosti týkající se jím zjištěného porušení zabezpečení osobních údajů. Povinnost není absolutní – je vázána na skutečnost, že postižený správce zjistí, že jím nastavené a používané zabezpečení osobních údajů bylo porušeno a současně je zmírněna nízkou nebo zanedbatelnou rizikovostí zjištěného porušení.

Obecně je správce povinen bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásit dozorovému úřadu jakékoli porušení zabezpečení osobních údajů, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Pokud není ohlášení dozorovému úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění. Pokud porušení zjistí zpracovatel, je povinen to ohlásit bez zbytečného odkladu správci.

Ohlášení[43] musí obsahovat přinejmenším:

a) popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů,
b) jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace,
c) popis pravděpodobných důsledků porušení zabezpečení osobních údajů,

[40] Příklady dále v této kapitole.

[41] Čl. 33 obecného nařízení

[42] Čl. 34 obecného nařízení

[43] Čl. 33 odst. 3 obecného nařízení

d) popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Informace, které nebylo možné uvést v prvotním ohlášení, lze ohlašovat postupně, samozřejmě opět bez zbytečného odkladu. V souladu se zásadou odpovědnosti správce podle čl. 5 odst. 2 obecného nařízení má správce povinnost dokumentovat případy porušení zabezpečení osobních údajů; tato dokumentace musí zahrnovat skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření.

Pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí správce porušení bez zbytečného odkladu subjektu údajů. V oznámení určeném subjektu údajů správce popíše za použití jasných a jednoduchých jazykových prostředků povahu porušení a uvede alespoň jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, popis pravděpodobných důsledků porušení zabezpečení osobních údajů a popis opatření, která přijal nebo navrhl k přijetí s cílem vyřešit dané porušení, včetně případných opatření ke zmírnění možných nepříznivých následků.[44]

Rovněž v této povinnosti je promítnuta rizikovost pro práva dotčených subjektů údajů, a to tak, že oznámení subjektu údajů se nevyžaduje, je-li splněna kterákoli z těchto podmínek:

a) správce zavedl náležitá technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup, jako například šifrování,
b) správce přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů se již pravděpodobně neprojeví,
c) vyžadovalo by to nepřiměřené úsilí. V takovém případě musí být subjekty údajů informovány stejně účinným způsobem veřejným oznámením nebo podobně.

Do okamžiku oznámení subjektům údajů může dozorový úřad po posouzení pravděpodobnosti toho, že dané porušení bude mít za následek vysoké riziko, požadovat, aby tak správce učinil, nebo může rozhodnout, že je splněna některá z liberačních podmínek[45].

[44] Obsah oznámení dle čl. 34 odst. 2 obecného nařízení

[45] Pojem „liberační podmínky“ v daném kontextu znamená výčet situací, v nichž je správce zproštěn oznamovací povinnosti vůči dotčeným subjektům údajů, viz čl. 34 odst. 3 obecného nařízení.

Bez ohledu na to, zda má správce povinnost jmenovat pověřence, tak pokud tak učiní, musí jeho/její kontaktní údaje oznámit dozorovému úřadu.[46]

Povinnosti spravujícího orgánu

Také spravující orgán[47] má ohlašovací a oznamovací povinnost v souvislosti se zjištěním porušení zabezpečení osobních údajů.

Ohlašování porušení zabezpečení osobních údajů Úřadu je pro spravující orgán stanoveno v § 41 zákona o zpracování osobních údajů a není shodné s povinností správců. Spravující orgán je povinen ohlásit bez zbytečného odkladu porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů, ledaže je riziko neoprávněného zásahu do práv a svobod subjektu údajů nízké. Pokud spravující orgán provede ohlášení po více než 72 hodinách od okamžiku, kdy se o něm dozvěděl, připojí odůvodnění prodlení.

V ohlášení spravující orgán uvede[48], pokud jsou mu tyto údaje známy, alespoň:

a) popis povahy porušení zabezpečení osobních údajů,
b) kategorie a přibližný počet subjektů údajů a záznamů osobních údajů, kterých se porušení zabezpečení týká,
c) jméno a kontaktní údaje pověřence nebo jiného pracoviště, které poskytne bližší informace k porušení zabezpečení osobních údajů,
d) popis pravděpodobných důsledků porušení zabezpečení osobních údajů,
e) popis opatření přijatých nebo navržených spravujícím orgánem k nápravě nebo zmírnění újmy způsobené porušením zabezpečení osobních údajů.

Skutečnosti, které mu nebyly v době ohlášení známy, doplní spravující orgán bez zbytečného odkladu poté, co se o nich dozví.

Spravujícímu orgánu je dále stanovena povinnost ohlášení vůči jinému spravujícímu orgánu České republiky nebo orgánu jiného členského státu EU, který osobní údaje poskytl, nebo obdržel.[49]

Spravující orgán vede o každém porušení zabezpečení osobních údajů, jeho důsledcích a přijatých nápravných opatřeních dokumentaci, kterou uchovává nejméně 3 roky.[50]

---

[46] Čl. 37 odst. 7 obecného nařízení

[47] Podle § 24 odst. 3 zákona o zpracování osobních údajů se spravujícím orgánem rozumí orgán veřejné moci příslušný k plnění úkolu a výkonu veřejné moci za účelem předcházení, vyhledávání a odhalování trestné činnosti, stíhání trestných činů, výkonu trestů a ochranných opatření, zajišťování bezpečnosti České republiky nebo zajišťování veřejného pořádku a vnitřní bezpečnosti, včetně pátrání po osobách a věcech, který není zpravodajskou službou nebo obecní policií.

[48] § 41 odst. 3. zákona o zpracování osobních údajů

[49] § 41 odst. 5 zákona o zpracování osobních údajů

[50] § 41 odst. 6 zákona o zpracování osobních údajů

Bez zbytečného odkladu oznámí[51] spravující orgán porušení zabezpečení osobních údajů subjektu údajů, pokud je riziko neoprávněného zásahu do práv a svobod subjektu údajů plynoucí z tohoto porušení vysoké. V oznámení spravující orgán uvede alespoň údaje uvedené v § 41 odst. 3 písm. a) a c) až e). Pokud by oznámení subjektu údajů vyžadovalo nepřiměřené úsilí, spravující orgán oznámení vhodným způsobem zveřejní. Ani spravující orgán není povinen porušení zabezpečení osobních údajů oznámit, pokud provedená technická a organizační opatření zajišťují, že dotčené osobní údaje nelze zneužít, nebo následná opatření spravujícího orgánu významně snížila riziko neoprávněného zásahu do práv a svobod subjektu údajů.

Zvláštní specifickou záruku pro práva subjektu údajů představuje ustanovení § 42 odst. 5, podle něhož o existenci vysokého rizika neoprávněného zásahu do práv a svobod subjektu údajů nebo o splnění podmínek podle odstavce 4 může rozhodnout také Úřad pro ochranu osobních údajů.

Zákon zakotvil rovněž omezení oznamovací povinnosti; spravující orgán porušení zabezpečení osobních údajů neoznámí, popř. oznámí pouze částečně, pokud by oznámením došlo k ohrožení:

a) plnění úkolu v oblasti předcházení, vyhledávání a odhalování trestné činnosti, stíhání trestných činů, výkonu trestů a ochranných opatření, zajišťování bezpečnosti České republiky nebo zajišťování veřejného pořádku a vnitřní bezpečnosti, včetně pátrání po osobách a věcech,
b) průběhu řízení o přestupku, kázeňském přestupku nebo jednání, které má znaky přestupku,
c) ochrany utajovaných informací, nebo
d) oprávněných zájmů třetí osoby.

Pro oznamovací povinnost vůči subjektu údajů stanoví zákon o zpracování osobních údajů formu zveřejnění způsobem umožňujícím dálkový přístup. Takto je spravující orgán povinen zveřejnit informace o:

a) svém názvu a kontaktních údajích,
b) kontaktních údajích pověřence pro ochranu osobních údajů (dále jen „pověřenec“),
c) účelu zpracování osobních údajů,
d) právu podat stížnost k Úřadu a kontaktních údajích Úřadu,
e) právu na přístup k osobním údajům, jejich opravu, omezení zpracování nebo výmaz.[52]

Povinnost sdělit kontaktní údaje pověřence Úřadu spravující orgány nemají. Podle zákona o mezinárodní justiční spolupráci ve věcech trestních má ohlašovací povinnost vůči Úřadu

[51] § 42 zákona o zpracování osobních údajů

[52] § 27 zákona o zpracování osobních údajů

orgán České republiky při předání osobních údajů do jiného státu, který není členským státem nebo přidruženým státem, nebo mezinárodním organizacím. Orgán ČR může za v tomto zákoně stanovených podmínek i bez žádosti předat osobní údaje příslušnému orgánu státu, který není členským státem nebo přidruženým státem, nebo mezinárodní organizaci, je-li to nezbytné pro předcházení, vyhledávání a odhalování trestné činnosti, trestní řízení nebo zajišťování veřejného pořádku a bezpečnosti. Pokud byla nezbytná opatření pro zajištění ochrany osobních údajů ve státě nebo mezinárodní organizaci, kterým mají být předány osobní údaje, přijata jiným způsobem než právním předpisem nebo formou mezinárodní smlouvy, orgán ČR informuje Úřad o kategoriích předání a uchová informace o čase, příjemci a důvodech předání, jakož i o dotčených osobních údajích.[53]

[53] § 18 zákona č. 104/2013 Sb.

7. Souhlas subjektu údajů

Souhlas se zpracováním

Souhlas subjektu údajů je jedním z právních základů zpracování osobních údajů stanovených v čl. 6 obecného nařízení. Souhlas je definován obecným nařízením,[54] které rovněž stanoví požadavky pro jeho použití. Právní rámec ochrany osobních údajů uplatňuje ve vztahu k souhlasu koncept nerovnováhy plynoucí z nerovného vztahu mezi správcem a subjektem údajů. Z tohoto důvodu je nepravděpodobné, že by například orgány veřejné moci mohly spoléhat na souhlas subjektu údajů se zpracováním, neboť v takovém vztahu je mezi správcem a subjektem údajů je zřejmá nerovnováha sil, totéž platí např. pro vztah mezi zaměstnancem a zaměstnavatelem.[55] Obecně platí, že korektní použití souhlasu jako právního základu omezené na situace, kdy je postavení nositele správce a zpracovatele rovnocenné.

Obecně může být souhlas odpovídajícím právním základem pouze tehdy, pokud má subjekt údajů možnost kontroly a skutečné volby mezi přijetím nebo odmítnutím nabízených podmínek či jejich odmítnutím, aniž by byl poškozen. Když správce žádá o souhlas, má povinnost posoudit, zda bude splňovat všechny požadavky na získání platného souhlasu. Byl-li souhlas získán v plném souladu s obecným nařízením o ochraně osobních údajů, je nástrojem, který subjektům údajů poskytuje kontrolu nad tím, zda budou jejich osobní údaje zpracovány, nebo nikoli. Pokud tímto způsobem získán nebyl, kontrola ze strany subjektu údajů je pouze iluzorní a souhlas bude neplatným základem pro zpracování, čímž se takové zpracování stává protiprávním (Pokyny (EDPB) č. 05/2020 k souhlasu podle nařízení 2016/679) ze dne 4. 5. 2020, bod 3.

Obecné nařízení definuje 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.[56] Z této definice lze odvodit požadavky, které musí souhlas splňovat. Správce musí být přitom schopen doložit, že subjekt údajů mu udělil souhlas se zpracováním svých osobních údajů.[57] Běžné může být uchovávání písemného nebo (zaznamenaného) ústního prohlášení.

[54] Čl. 4 odst. 11 obecného nařízení o ochraně osobních údajů
[55] Bod 43 pokyny
[56] Čl. 4 odst. 11 obecného nařízení o ochraně osobních údajů.
[57] Čl. 7 odst. 1 obecného nařízení o ochraně osobních údajů.

V úvahu připadá několik různých formátů udělení souhlasu, např. zaškrtnutí volného políčka, výběr určitých parametrů („nastavení“) nebo postup, který jednoznačně vyjadřuje svolení subjektu údajů; naopak mlčení, využití předem zaškrtnutého políčka, pouhé pokračování v používání služby nebo jinou nečinnost na straně subjektu údajů, nelze považovat za projev volby.

Pokud je souhlas subjektu údajů vyjádřen písemným prohlášením, které se týká rovněž jiných skutečností, musí být žádost o vyjádření souhlasu jasně odlišitelná, vyjádřená srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků. Jakákoli část tohoto prohlášení, která porušuje obecné nařízení o ochraně osobních údajů, není závazná.[58] Při posuzování toho, zda je souhlas svobodný, musí být důsledně zohledněna skutečnost, zda je mimo jiné plnění smlouvy, včetně poskytnutí služby, podmíněno souhlasem se zpracováním osobních údajů, které není pro plnění dané smlouvy nutné.[59]

Jedním z významných požadavků na souhlas subjektu údajů, který musí správce zohlednit, je jeho odvolatelnost. Odvolatelnost souhlasu garantuje, že na straně subjektu údajů zůstává určitá míra kontroly nad jeho osobními údaji.[60] Subjekt údajů má právo svůj souhlas kdykoli odvolat. Odvoláním souhlasu není dotčena zákonnost zpracování vycházejícího ze souhlasu, který byl dán před jeho odvoláním.[61] Před udělením souhlasu musí být subjekt údajů o možnosti odvolat souhlas informován. Dalším požadavkem je, že odvolat souhlas má být stejně snadné jako jej poskytnout.[62] Byl-li souhlas získán elektronicky pouhým jedním kliknutí myší, přejetím prstem po displeji nebo stiskem klávesy, musí být pro subjekt údajů stejně jednoduché souhlas odvolat. Subjekt údajů musí mít možnost svůj souhlas odvolat bez jakékoliv újmy.

Souhlas lze udělit pro jeden nebo více specifických stanovených účelů zpracování.[63]

Výslovný souhlas

V systému ochrany osobních údajů se rozlišuje pojem souhlas a výslovný souhlas. Výslovný souhlas se vyžaduje v situacích, kdy dochází k závažnému riziku ve vztahu ke zpracování osobních údajů, a tudíž je považováno za vhodné zajistit vysokou úroveň kontroly jednotlivce nad osobními údaji. Výslovný souhlas se uplatňuje zejména při zpracování zvláštních kategorií osobních údajů,[64] pří předávání osobních údajů do třetích zemí nebo mezinárodním

[58] Čl. 7 odst. 2 obecného nařízení o ochraně osobních údajů.
[59] Čl. 7 odst. 4 obecného nařízení o ochraně osobních údajů.
[60] Bod 10 pokyny EDPB 5/2020 k souhlasu podle nařízení 2016/679.
[61] Čl. 7 odst. 3 obecného nařízení o ochraně osobních údajů.
[62] Čl. 7 odst. 3 obecného nařízení na ochranu osobních údajů.
[63] Čl. 6 odst. 1 písm. a) obecného nařízení na ochranu osobních údajů.
[64] Čl. 9 odst. 2 písm. a) obecného nařízení na ochranu osobních údajů

organizacím za podmínek čl. 49 obecného nařízení a u automatizovaného individuálního rozhodování, včetně profilování.

Výslovný souhlas subjektu údajů podle čl. 9 odst. 2 písm. a) obecného nařízení není na rozdíl od souhlasu podle čl. 6 odst. 1 písm. a) samostatným právním důvodem pro zpracování osobních údajů, ale dodatečnou právem vyžadovanou zárukou ochrany práv subjektu údajů dotčeného zpracováním jeho údajů vyžadujících zvýšenou ochranu.[65] Totéž platí pro výslovný souhlas subjektu údajů podle čl. 49; zde je výslovný souhlas jednou ze záruk vyžadovaných obecným nařízením za situace, kdy neexistuje rozhodnutí o odpovídající ochraně ani jiné záruky pro předání osobních údajů do třetí země nebo mezinárodní organizaci.[66]

Pojem *výslovný* odkazuje na způsob vyjádření souhlasu. Ve vhodných případech by správce mohl získat písemné prohlášení podepsané subjektem údajů. V digitálním nebo on-line kontextu může být výslovný souhlas udělen vyplněním elektronického formuláře, zasláním emailu, nahráním naskenovaného dokumentu opatřeného podpisem subjektu údajů včetně podpisu elektronického. Teoreticky není vyloučeno ani ústní prohlášení.

Souhlas nezletilé osoby (dítěte)

Obecně platí, že právní rámec ochrany dat je založen na východisku, že děti zasluhují zvláštní ochranu osobních údajů, protože si mohou být méně vědomy dotčených rizik, důsledků a záruk a svých práv v souvislosti se zpracováním osobních údajů.[67]

Obecné nařízení o ochraně osobních údajů klade výslovné požadavky na souhlas dítěte, jímž se rozumí obecně nezletilá osoba, v souvislosti se službami informační společnosti.[68] Pro souhlas nezletilé osoby se použijí vedle podmínek stanovených výslovně obecným nařízením o ochraně osobních údajů rovněž vnitrostátní předpisy. V České republice se jedná o příslušná ustanovení občanského zákoníku.

Obecné nařízení o ochraně osobních údajů považuje, za situace, kdy se jedná o zpracování osobních údajů v souvislosti s nabídkou služeb informační společnosti přímo dítěti, zpracování osobních údajů dítěte za zákonné, je-li dítě ve věku nejméně 16 let. Je-li dítě mladší, je zpracování zákonné pouze tehdy a do té míry, pokud byl souhlas vyjádřen nebo schválen osobou, která vykonává rodičovskou zodpovědnost k dítěti. Na správce se vztahuje povinnost vyvinout přiměřené úsilí s ohledem na dostupnou technologii, aby ověřil, že souhlas udělila nebo schválila osoba vykonávající rodičovskou zodpovědnost. Souhlas rodiče nebo

[65] K tomu viz též kap. 9 této učební pomůcky.
[66] K tomu podrobněji vizte kap. 17 této učební pomůcky.
[67] Bod 38 preambule obecného nařízení o ochraně osobních údajů.
[68] Čl. 8 obecného nařízení o ochraně osobních údajů.

zákonného zástupce pro zpracování však není nutný v případě preventivních či poradenských služeb nabízených přímo dětem.[69]

Zmocnění pro členské státy stanovit nižší věk, ne však nižší než třináct let, využila Česká republika. V § 7 zákona o zpracování osobních údajů se stanoví, že dítě nabývá způsobilosti k udělení souhlasu se zpracováním osobních údajů v souvislosti s nabídkou služeb informační společnosti přímo jemu dovršením patnáctého roku věku, jedná se o tzv. digitální věk.

Souhlas pro „neunijní zpracování“

V České republice je souhlas subjektu údajů základním právním důvodem pro zpracování osobních údajů k zajišťování obranných a bezpečnostních zájmů České republiky, pokud jiný právní předpis nestanoví jinak. Tyto požadavky na právní základ stanoví § 43 (Hlava IV) zákona o zpracování osobních údajů. Osobní údaje může k některému z těchto účelů správce zpracovávat pouze se souhlasem subjektu údajů, na který se uplatní definice z obecného nařízení[70]. Bez tohoto souhlasu může správce osobní údaje zpracovávat, jestliže mu svědčí některá z výjimek.[71] Na souhlas pro takové zpracování klade zákon požadavek, aby subjekt údajů byl před udělením souhlasu informován o tom, pro jaký účel zpracování osobních údajů a k jakým osobním údajům souhlas dává, jakému správci a na jaké období. Souhlas subjektu údajů musí být správce schopen prokázat po celou dobu jejich zpracování.

[69] Bod 150 pokynů EDPB č. 5/2020 k souhlasu podle nařízení 2016/679.
[70] Vizte též kapitola 7.
[71] Výjimky vizte kap. 6.

8. Práva subjektu údajů a odpovídající povinnosti správce a zpracovatele

Práva subjektů údajů jsou důležitým prvkem celého systému ochrany dat, který byl obecným nařízením významně posílen a zpřísněn, ačkoli tato práva byla již před jeho účinností součástí právního rámce ochrany dat. Práva subjektu údajů jsou upravena v kapitole III (čl. 12 až 23) obecného nařízení o ochraně osobních údajů, případně v dalších článcích, zejm. čl. 34 a 49. Kapitola III obecného nařízení vychází z čl. 8 Listiny základních práv EU, zejména je provedením druhé věty odst. 2: *Každý má právo na přístup k údajům, které o něm byly shromážděny, a má právo na jejich opravu.*[72]

Právo subjektu údajů na přístup

Právo na přístup k osobním údajům je jedním z práv subjektu údajů upravených v kapitole III obecného nařízení mezi dalšími právy, jako je například právo na opravu, právo na výmaz, právo na omezení zpracování, právo na přenositelnost, právo vznést námitku proti zpracování a právo nebýt předmětem automatizovaného rozhodnutí včetně profilování.[73]

Právo na přístup se v pojetí obecného nařízení skládá ze tří složek, kterými se rozumí: 1. právo na potvrzení, zda jsou osobní údaje zpracovávány či nikoliv, 2. přístup k nim a 3. informace o samotném zpracování. Obsahem práva na přístup je, že subjekt údajů má právo získat od správce potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, má právo získat přístup k těmto osobním údajům a k informacím o zpracování Subjekt údajů má právo, aby mu správce tyto údaje a informace sdělil.

Jedná se přitom o následující údaje a informace:

a) účely zpracování,
b) kategorie dotčených osobních údajů,
c) příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny, zejména příjemci ve třetích zemích nebo v mezinárodních organizacích,
d) plánovaná doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá ke stanovení této doby,
e) existence práva požadovat opravu nebo výmaz osobních údajů, práva na omezení zpracování a práva vznést námitku proti zpracování,
f) právo podat stížnost u dozorového úřadu,
g) veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů,

[72] Viz Úvod této učební pomůcky.
[73] Články 16, 17, 18, 20, 21 a 22 obecného nařízení na ochranu osobních údajů.

h) skutečnost, že dochází k automatizovanému rozhodování, včetně profilování a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, významu a předpokládaných důsledků takového zpracování pro subjekt údajů.[74]

Pokud se osobní údaje předávají do třetí země nebo mezinárodní organizaci má subjekt údajů právo být informován o vhodných zárukách podle čl. 46 obecného nařízení, které se vztahují na předání.[75]

Právo na přístup zahrnuje povinnost správce poskytnout kopii zpracovávaných osobních údajů. Za případné další kopie na žádost subjektu údajů může správce účtovat přiměřený poplatek na základě administrativních nákladů.[76] Jestliže subjekt údajů podá žádost v elektronické formě, informace mu jsou poskytnuty také v elektronické formě, která se běžně používá, pokud subjekt údajů nepožádá o jiný způsob.[77] Právo na přístup podléhá omezení, které vyplývá z čl. 15 odst. 4 obecného nařízení, kdy právem získat kopii nesmějí být nepříznivě dotčena práva a svobody jiných osob. O takovou situaci se může jednat, pokud kopie osobních údajů obsahuje kromě osobních údajů žádajícího subjektu údajů také údaje jiných osob, např. u videozáznamu nebo obrazového či zvukového záznamu.

Právo na opravu a právo na výmaz

Dalšími dvěma samostatnými právy subjektů údajů, které vycházejí z čl. 8 Listiny základních práv EU a jsou provedeny v obecném nařízení o ochraně osobních údajů, jsou právo na opravu a právo na výmaz, označované též jako „právo být zapomenut“.[78]

Obsahem práva na opravu je právo subjektu údajů na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se ho týkají. Subjekt údajů má rovněž – s přihlédnutím k účelům zpracování – právo na doplnění neúplných osobních údajů, a to i poskytnutím dodatečného prohlášení.[79]

Podle práva na výmaz[80] má subjekt údajů právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají, a povinnost osobní údaje bez zbytečného odkladu vymazat, pokud je splněn jeden z taxativním výčtem uvedených důvodů

[74] Čl. 15 odst. 1 obecného nařízení o ochraně osobních údajů.
[75] Čl. 15 odst. 2 obecného nařízení o ochraně osobních údajů.
[76] Čl. 15 odst. 3 věta druhá obecného nařízení na ochranu osobních údajů.
[77] Článek 15 odst. 3 obecného nařízení na ochranu osobních údajů.
[78] Rozsudek SD EU ve věci C-131/12 ve věci Google Spain.
[79] Čl. 16 obecného nařízení na ochranu osobních údajů.
[80] Čl. 17 obecného nařízení na ochranu osobních údajů.

a za podmínky, že zpracování je prováděno jako nezbytné pro jeden z následujících šesti důvodů:

a) osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány,
b) subjekt údajů odvolá souhlas, na jehož základě byly zpracovány, a neexistuje žádný další právní důvod pro zpracování,
c) subjekt údajů vznese námitky proti zpracování podle čl. 21 odst. 1 a neexistují žádné převažující oprávněné důvody pro zpracování nebo subjekt údajů vznese námitky proti zpracování podle čl. 21 odst. 2,
d) osobní údaje byly zpracovány protiprávně,
e) osobní údaje musí být vymazány ke splnění právní povinnosti stanovené v právu Unie nebo členského státu, které se na správce vztahuje,
f) osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle čl. 8 odst. 1 obecného nařízení.[81]

Jestliže správce osobní údaje zveřejnil a je povinen je vymazat, přijme s ohledem na dostupnou technologii a náklady na provedení přiměřené kroky, včetně technických opatření, aby informoval správce, kteří tyto osobní údaje zpracovávají, že je subjekt údajů žádá, aby vymazali veškeré odkazy na tyto osobní údaje, jejich kopie či replikace.[82]

Výše uvedené se neuplatní, pokud je zpracování nezbytné:

a) pro výkon práva na svobodu projevu a informace,
b) pro splnění právní povinnosti, jež vyžaduje zpracování podle práva Unie nebo členského státu, které se na správce vztahuje, nebo pro splnění úkolu provedeného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen,
c) z důvodů veřejného zájmu v oblasti veřejného zdraví v souladu s čl. 9 odst. 2 písm. h) a i) a čl. 9 odst. 3,
d) pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu či pro statistické účely v souladu s čl. 89 odst. 1, pokud je pravděpodobné, že by právo uvedené v odstavci 1 znemožnilo nebo vážně ohrozilo splnění cílů uvedeného zpracování,
e) pro určení, výkon nebo obhajobu právních nároků.[83]

Dalším právem subjektů údajů je právo na omezení zpracování, jehož obsahem je právo subjektu údajů na to, aby správce omezil zpracování, v kterémkoli z těchto případů:

[81] Čl. 17 odst. 1 obecného nařízení o ochraně osobních údajů.
[82] Čl. 17 odst. 3 obecného nařízení na ochranu osobních údajů.
[83] Čl. 17 odst. 3 obecného nařízení na ochranu osobních údajů.

a) subjekt údajů popírá přesnost osobních údajů, a to na dobu potřebnou k tomu, aby správce mohl přesnost osobních údajů ověřit,
b) zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití,
c) správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků,
d) subjekt údajů vznesl námitku proti zpracování podle čl. 21 odst. 1, dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody subjektu údajů.[84]

Pokud bylo zpracování omezeno, mohou být tyto osobní údaje, s výjimkou jejich uložení, zpracovány pouze se souhlasem subjektu údajů, nebo z důvodu určení, výkonu nebo obhajoby právních nároků, z důvodu ochrany práv jiné fyzické nebo právnické osoby nebo z důvodů důležitého veřejného zájmu Unie nebo některého členského státu.[85] Subjekt údajů, který dosáhl omezení zpracování, je správcem předem upozorněn na to, že bude omezení zpracování zrušeno.[86]

Následující práva subjektu údajů jsou vázána (omezena) na určitý právní základ, na němž je zpracování založeno.

Právo na přenositelnost

Právo na přenositelnost je novým právem upraveným v článku 20 obecného nařízení, které souvisí s právem na přístup k osobním údajům, ale zároveň se od něj liší. Umožňuje subjektu údajů získat osobní údaje, které poskytl správci údajů, a to ve strukturovaném, běžně používaném a strojově čitelném formátu, a předat tyto údaje jinému správci údajů. Účelem tohoto nového práva je dát subjektu údajů větší kontrolu nad osobními údaji, které se ho týkají.

Právo na přenositelnost údajů svědčí subjektu údajů tehdy, když je zpracování založeno na souhlasu podle čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a), nebo na smlouvě podle čl. 6 odst. 1 písm. b), a zpracování provádí automatizovaně. Pouze v takovém případě má subjekt údajů právo získat osobní údaje, které se ho týkají a které poskytl správci, a předat je jinému správci, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil. Rozsah práva je tedy omezen na údaje, které subjekt údajů sám správci poskytl. Osobní údaje musí být poskytnuty ve strukturovaném, běžně používaném a strojově čitelném formátu, je-li to technicky proveditelné, přičemž tyto osobní údaje předá přímo jeden správce druhému správci.[87]

[84] Čl. 18 odst. 1 obecného nařízení na ochranu osobních údajů.
[85] Čl. 18 odst. 2 obecného nařízení na ochranu osobních údajů.
[86] Čl. 18 odst. 3 obecného nařízení na ochranu osobních údajů.
[87] Čl. 20 odst. 1 a 2 obecného nařízení na ochranu osobních údajů.

Podobně jako u práva na přístup platí, že naplněním práva žádajícího subjektu údajů nemohou být nepříznivě dotčena práva a svobody jiných osob.[88]

Právo vznést námitku

Právo vznést námitku je rovněž omezené, pokud jde o právní základ zpracování podle čl. 6. Subjekt údajů má z důvodů týkajících se jeho konkrétní situace právo kdykoli vznést námitku proti zpracování osobních údajů, které se jej týkají, pouze pokud je zpracování založeno na právním důvodu podle čl. 6 odst. 1 písm. e) nebo f), a to včetně profilování. Nastane-li taková situace, správce osobní údaje dále nezpracovává, pokud neprokáže závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků, tedy pokud se nepoužije jedna ze dvou podmínek.[89]

Pokud se osobní údaje zpracovávají pro účely přímého marketingu, má subjekt údajů právo vznést kdykoli námitku proti zpracování osobních údajů pro tento marketing, což zahrnuje i profilování, pokud se týká tohoto přímého marketingu. V takovém případě nelze osobní údaje pro tyto účely již dále zpracovávat.[90]

Subjekt údajů je třeba na toto právo výslovně upozornit a právo uvést zřetelně a odděleně od jakýchkoli jiných informací, a to nejpozději v okamžiku první komunikace se subjektem údajů.[91]

V souvislosti s využíváním služeb informační společnosti může subjekt údajů uplatnit své právo vznést námitku automatizovanými prostředky pomocí technických specifikací.[92]

Ve vztahu ke zpracování pro účely vědeckého nebo historického výzkumu nebo pro statistické účely podle čl. 89 odst. 1, je právo vznést námitku proti zpracování omezeno na situace, kdy zpracování není nezbytné pro splnění úkolu prováděného z důvodů veřejného zájmu.[93]

Právo nebýt předmětem rozhodnutí založeného výhradně na automatizovaném zpracování

Subjekt údajů má právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká, Jde o nejstarší právo ze současných práv subjektů údajů, k němuž se členské státy Evropského hospodářského společenství hlásily ještě před tím,

[88] Čl. 20 odst. 4 obecného nařízení na ochranu osobních údajů.
[89] Čl. 21 odst. 1 obecného nařízení na ochranu osobních údajů.
[90] Čl. 21 odst. 2 a 3 obecného nařízení na ochranu osobních údajů.
[91] Čl. 21 odst. 4 obecného nařízení n
[92] Čl. 21 odst. 5 obecného nařízení o ochraně osobních údajů.
[93] Čl. 21 odst. 6 obecného nařízení o ochraně osobních údajů.

než nabyla účinnosti směrnice 95/46/ES94, předchůdkyně obecného nařízení o ochraně osobních údajů. V obecném nařízení o ochraně osobních údajů je upraveno v čl. 22; nelze se ho dovolávat, pokud je rozhodnutí:

a) nezbytné k uzavření nebo plnění smlouvy mezi subjektem údajů a správcem údajů,
b) povoleno právem Unie nebo členského státu, které stanoví vhodná opatření zajišťující ochranu práv a svobod a oprávněných zájmů subjektu údajů,
c) založeno na výslovném souhlasu subjektu údajů.[95]

V případech podle písm. a) a c) provede správce údajů vhodná opatření na ochranu práv a svobod a oprávněných zájmů subjektu údajů, alespoň práva na lidský zásah ze strany správce, práva vyjádřit svůj názor a práva napadnout rozhodnutí.[96]

Žádné z výhradně automatizovaných rozhodnutí uvedená se nemůže opírat o zvláštní kategorie osobních údajů, s výjimkou rozhodování s výslovným souhlasem subjektu údajů a v rámci zpracování nezbytné pro významný veřejný zájem, a to za dodržení všech podmínek podle čl. 9 a používání vhodných opatření pro zajištění práv a svobod a oprávněných zájmů subjektu údajů.[97]

Povinnosti správce

Nutným předpokladem naplňování všech uvedených práv subjektu údajů je uložení odpovídajících konkrétních povinností správcům. Kromě těch, které jsou formulovány jako fakticky neoddělitelná součást základní formulace každého z práv, jsou takové povinnosti uložené v čl. 12 až 14 a čl. 19 obecného nařízení o ochraně osobních údajů. Svým obsahem naplňují zásady obecného nařízení, zejména zásadu zákonnosti, korektnosti a transparentnosti ve vztahu k subjektu údajů a vytvářejí předpoklady pro to, aby subjekt údajů měl stejnou pozici vůči kterémukoli ze správců, vůči němuž se domáhá svých práv.

Obecné požadavky uložené správci jsou upraveny v čl. 12 obecného nařízení. Od správce se požaduje, aby poskytl subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků veškeré informace uvedené v čl. 13 a 14 a učinil veškerá sdělení podle čl. 15 až 22 a 34 obecného nařízení o zpracování, zejména pokud se jedná o informace určené konkrétně dítěti. Informace poskytne písemně nebo jinými prostředky, včetně ve vhodných případech v elektronické

[94] Toto právo bylo upraveno v čl. 15 této směrnice a v návaznosti na to v § 11 odst. 6 zákona o ochraně osobních údajů.
[95] Čl. 22 odst. 2 obecného nařízení o ochraně osobních údajů.
[96] Čl. 22 odst. 3 obecného nařízení o ochraně osobních údajů.
[97] Čl. 22 odst. 4 obecného nařízení o ochraně osobních údajů.

formě. Pokud si to subjekt údajů vyžádá, mohou být informace poskytnuty ústně, za předpokladu, že je prokázána totožnost subjektu údajů.[98]

Dalším požadavkem na správce je, aby usnadňoval výkon práv subjektu údajů podle čl. 15 až 22. Informace na žádost subjektu údajů správce poskytne bez zbytečného odkladu a v každém případě do jednoho měsíce od obdržení žádosti. Lhůtu je možné prodloužit o dva měsíce v případě potřeby a s ohledem na složitost a počet žádostí. O prodloužení lhůty správce informuje subjekt údajů do jednoho měsíce od obdržení žádosti spolu s důvody pro odklad. Jestliže subjekt údajů podá žádost v elektronické formě, poskytnou se informace také v elektronické formě, je-li to možné a pokud subjekt údajů nepožádá o jiný způsob. Pokud správce žádosti subjektu údajů nevyhoví, informuje ho bezodkladně a nejpozději do jednoho měsíce od přijetí žádosti o důvodech a o možnosti podat stížnost u dozorového úřadu a žádat o soudní ochranu.[99]

Informace podle čl. 13 a 14 a veškerá sdělení a veškeré úkony podle čl. 15 až 22 a 34 se poskytují a činí bezplatně. Nicméně, jsou-li žádosti subjektu údajů zjevně nedůvodné nebo nepřiměřené, zejména protože se opakují, může správce buď uložit přiměřený poplatek zohledňující administrativní náklady spojené s poskytnutím požadovaných informací nebo sdělení nebo s učiněním požadovaných úkonů, nebo odmítnout žádosti vyhovět. Doložit zjevnou nedůvodnost nebo nepřiměřenost žádosti je na správci.[100]

Pokud má správce důvodné pochybnosti o totožnosti fyzické osoby, která podává žádost, může požádat o poskytnutí dodatečných informací nezbytných k potvrzení totožnosti subjektu údajů.[101]

Informace, které mají být subjektům údajů poskytnuty, mohou být doplněny standardizovanými ikonami s cílem poskytnout snadno viditelným, srozumitelným a jasným způsobem přehled o zamýšleném zpracování. Pokud jsou ikony prezentovány v elektronické formě, musí být strojově čitelné.[102]

Komise má pravomoc přijímat k ikonám akty v přenesené pravomoci. Dosud se tak nestalo a není připravován žádný návrh; jedním z důvodů je, že obecná známost standardizovaných ikon je napříč všemi členskými státy EU omezena na ikonografiku veřejných prostranství a objektů a dopravní značky. [103]

[98] Čl. 12 odst. 1 obecného nařízení na ochranu osobních údajů.
[99] Čl. 12 odst. 2,3 a 4 obecného nařízení na ochranu osobních údajů.
[100] Čl. 12 odst. 5 obecného nařízení na ochranu osobních údajů.
[101] Čl. 12 odst. 6 obecného nařízení o ochraně osobních údajů.
[102] Čl. 12 odst. 7 obecného nařízení na ochranu osobních údajů.
[103] Čl. 12 odst. 8 obecného nařízení na ochranu osobních údajů.

Specifické postupy a rozsah informací, které je správce povinen poskytnout subjektu údajů, jsou stanoveny jednak pro situace, kdy se osobní údaje pro zpracování získávají přímo od subjektu údajů, tj. subjekt údajů je jejich výhradním zdrojem (čl. 13), a jednak pro situace, kdy osobní údaje získává správce z jakéhokoliv jiného zdroje (čl. 14).

Podle čl. 19 má správce oznamovací povinnost ohledně opravy, výmazu nebo omezení zpracování. Obsahem povinnosti je oznamování veškerých oprav a výmazů osobních údajů nebo omezení zpracování, s výjimkou případů, kdy se to ukáže jako nemožné nebo to vyžaduje nepřiměřené úsilí, jednotlivým příjemcům, jimž byly osobní údaje zpřístupněny. Pokud to subjekt údajů požaduje, informuje ho správce o těchto příjemcích.

Omezení některého z práv subjektu údajů jiným zákonem je věnována kapitola 19 této učební pomůcky, odpovědnosti správce vůči subjektu údajů kapitola 13.

Informace poskytované subjektu údajů

Pokud se osobní údaje týkající se subjektu údajů získávají od subjektu údajů, poskytne správce v okamžiku získání osobních údajů subjektu údajů informace:

a) totožnost a kontaktní údaje správce a jeho případného zástupce,
b) případně kontaktní údaje případného pověřence pro ochranu osobních údajů,
c) účely zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování,
d) oprávněné zájmy správce nebo třetí strany v případě, že je zpracování založeno na čl. 6 odst. 1 písm. f),
e) případné příjemce nebo kategorie příjemců osobních údajů,
f) úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci a (ne)existenci rozhodnutí Komise o odpovídající ochraně nebo, v případech předání podle čl. 46, 47 nebo čl. 49 odst. 1 druhém pododstavci, odkaz na vhodné záruky a prostředky k získání kopie těchto údajů nebo informace o tom, kde byly tyto údaje zpřístupněny.[104]

Kromě toho správce poskytne subjektu údajů v okamžiku získání osobních údajů tyto další informace, jsou-li nezbytné pro zajištění spravedlivého a transparentního zpracování:

a) doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby,
b) existence práva požadovat od správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování, a vznést námitku proti zpracování, jakož i práva na přenositelnost údajů,

[104] Čl. 13 odst. 1 obecného nařízení na ochranu osobních údajů.

c) pokud je zpracování založeno na čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a), existence práva odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním,
d) existence práva podat stížnost u dozorového úřadu,
e) skutečnost, zda poskytování osobních údajů je zákonným či smluvním požadavkem, nebo požadavkem, který je nutné uvést do smlouvy, a zda má subjekt údajů povinnost osobní údaje poskytnout, a ohledně možných důsledků neposkytnutí těchto údajů,
f) skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, uvedenému v čl. 22 odst. 1 a 4, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.[105]

Pokud správce hodlá osobní údaje dále zpracovávat pro jiný účel, než pro který byly shromážděny, poskytne subjektu údajů ještě před dalším zpracováním informace o tomto jiném účelu a příslušné další informace.[106]

Jestliže osobní údaje nebyly získány od subjektu údajů, tj. že jejich zdrojem je někdo jiný než subjekt údajů sám, poskytne správce subjektu údajů informace:

a) totožnost a kontaktní údaje správce a jeho případného zástupce,
b) případně kontaktní údaje případného pověřence pro ochranu osobních údajů,
c) účely zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování,
d) kategorie dotčených osobních údajů,
e) případné příjemce nebo kategorie příjemců osobních údajů,
f) případný záměr správce předat osobní údaje příjemci ve třetí zemi nebo mezinárodní organizaci a o existence či neexistence rozhodnutí Komise o odpovídající ochraně nebo, v případech předání uvedených v čl. 46 nebo 47 nebo v čl. 49 odst. 1 druhém pododstavci, odkaz na vhodné záruky a prostředky k získání kopie těchto údajů nebo informace o tom, kde byly tyto údaje zpřístupněny.[107]

Dále správce poskytne další informace, jsou-li nezbytné pro zajištění spravedlivého a transparentního zpracování ve vztahu k subjektu údajů. Takovými informacemi jsou:

a) doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby,

[105] Čl. 13 odst. 2 obecného nařízení na ochranu osobních údajů.
[106] Čl. 13 odst. 3 obecného nařízení o ochraně osobních údajů.
[107] Čl. 14 odst. 1 obecného nařízení o ochraně osobních údajů.

b) oprávněné zájmy správce nebo třetí strany v případě, že je zpracování založeno na čl. 6 odst. 1 písm. f),
c) existence práva požadovat od správce přístup k osobním údajům, jejich opravu nebo výmaz anebo omezení zpracování a práva vznést námitku proti zpracování, jakož i práva na přenositelnost údajů,
d) pokud je zpracování založeno na čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a), existence práva odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním,
e) existence práva podat stížnost u dozorového úřadu,
f) zdroj, ze kterého osobní údaje pocházejí, a případně informace o tom, zda údaje pocházejí z veřejně dostupných zdrojů,
g) skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, uvedenému v čl. 22 odst. 1 a 4, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.[108]

Informace správce poskytne v přiměřené lhůtě po získání osobních údajů, ale nejpozději do jednoho měsíce, s ohledem na konkrétní okolnosti, za nichž jsou osobní údaje zpracovávány; nejpozději v okamžiku, kdy poprvé dojde ke komunikaci se subjektem údajů, mají-li být osobní údaje použity pro účely této komunikace; nebo nejpozději při prvním zpřístupnění osobních údajů, pokud je má v úmyslu zpřístupnit jinému příjemci.[109]

Pokud správce hodlá osobní údaje dále zpracovat pro jiný účel, než pro který byly získány, poskytne subjektu údajů ještě před uvedeným dalším zpracováním informace o tomto jiném účelu a příslušné další informace.[110]

Bez ohledu na zdroj osobních údajů vstupujících do zpracování nemá správce povinnost informace poskytnout, pokud subjekt údajů již uvedené informace má, a do té míry, v níž je má. Za situace, kdy jsou osobní údaje získávány od někoho jiného, než je subjekt údajů, nemá správce povinnost informace podle čl. 14 poskytnout, pokud:

- se ukáže, že poskytnutí takových informací není možné nebo by vyžadovalo nepřiměřené úsilí; to platí zejména v případě zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely s výhradou podmínek a záruk uvedených v čl. 89 odst. 1, nebo pokud je pravděpodobné, že uplatnění povinnosti uvedené v odstavci 1 tohoto článku by

[108] Čl. 14 odst. 2 obecného nařízení o ochraně osobních údajů.
[109] Čl. 14 odst. 3 obecného nařízení o ochraně osobních údajů.

[110] Čl. 14 odst. 4 obecného nařízení o ochraně osobních údajů.

znemožnilo nebo výrazně ztížilo dosažení cílů uvedeného zpracování. V takových případech přijme správce vhodná opatření na ochranu práv, svobod a oprávněných zájmů subjektu údajů, včetně zpřístupnění daných informací veřejnosti,

- je získávání nebo zpřístupnění výslovně stanoveno právem Unie nebo členského státu, které se na správce vztahuje a v němž jsou stanovena vhodná opatření na ochranu oprávněných zájmů subjektu údajů,
- osobní údaje musí zůstat důvěrné s ohledem na povinnost zachovávat služební tajemství upravenou právem Unie nebo členského státu, včetně zákonné povinnosti mlčenlivosti.[111]

Povinnosti spravujícího orgánu

Zákon o zpracování osobních údajů upravuje povinnosti spojené s právy subjektu údajů jednak jako obecnější oznamovací a informační povinnosti vůči subjektu údajů a podmínky, jednak specificky pro jednotlivá práva subjektu údajů. Spravující orgán je povinen zveřejnit způsobem umožňujícím dálkový přístup informace o svém názvu a kontaktních údajích, kontaktních údajích pověřence pro ochranu osobních údajů, účelu zpracování osobních údajů, právu podat stížnost k Úřadu a kontaktních údajích Úřadu a právu na přístup k osobním údajům, jejich opravu, omezení zpracování nebo výmaz.[112]

Pokud subjekt údajů podá žádost k naplnění práva na přístup k osobním údajům, spravující orgán mu sdělí, zda zpracovává osobní údaje vztahující se k jeho osobě. Jestliže takové údaje zpracovává, předá je subjektu údajů a sdělí mu informace o účelu zpracování, právních předpisech, na jejichž základě údaje převážně zpracovává, příjemcích, popř. kategoriích příjemců, předpokládané době uchování nebo způsobu jejího určení, dále o právu požádat o opravu, omezení zpracování nebo výmaz osobních údajů a zdroji těchto údajů. Na této úpravě stojí z pohledu subjektu údajů za pozornost jednak to, že příjemce je definován shodně jako v obecném nařízení o ochraně osobních údajů, což má důsledky pro obsah informací, které lze subjektu údajů poskytnout, jednak to, že u právních předpisů se nepodává úplný výčet.

Další omezení rozsahu práva na přístup stanoví zákon jako podmínky, za nichž spravující orgán žádosti subjektu údajů nevyhoví, popř. vyhoví pouze částečně. Tato podmínka se použije, pokud by vyhověním došlo k ohrožení plnění úkolu v oblasti předcházení, vyhledávání a odhalování trestné činnosti, stíhání trestných činů, výkonu trestů a ochranných opatření, zajišťování bezpečnosti České republiky nebo zajišťování veřejného pořádku a vnitřní bezpečnosti, včetně pátrání po osobách a věcech, nebo průběhu řízení o přestupku,

[111] Čl. 14 odst. 5 obecného nařízení o ochraně osobních údajů.
[112] § 27 zák. č. 110/219 Sb.

kázeňském přestupku nebo jednání, které má znaky přestupku, ochrany utajovaných informací, nebo oprávněných zájmů třetí osoby.

Pokud spravující orgán shledá ohrožení kteréhokoli z úkolů spravujícího orgánu při vyhovění žádosti nebo sdělením, že žádosti nevyhovuje, informuje spravující orgán subjekt údajů stejně jako ty žadatele, jejichž osobní údaje nezpracovává. V takovém případě je důležitá formulace sdělení doručeného subjektu údajů, neboť sdělení nesmí být nepravdivé, tj. zejména nelze sdělovat, že příslušný spravující orgán osobní údaje žadatele nezpracovává, pokud tomu tak není.

O důvodech omezení sdělovaných údajů vede spravující orgán dokumentaci, kterou uchovává nejméně 3 roky.[113]

Úprava práva na opravu, omezení zpracování nebo výmaz osobních údajů podle hlavy III zákona o zpracování osobních údajů již vykazuje menší rozdíly oproti úpravě obsažené v obecném nařízení o ochraně osobních údajů. Spravující orgán na žádost subjektu údajů zásadně provede opravu nebo doplnění osobních údajů a vyžaduje-li to účel zpracování, může místo opravy osobní údaje doplnit nebo k nim připojit dodatečné prohlášení, které má v informačních systémech obvykle standardizovanou formu, zahrnující používání ikon (např. *).

Základní reakcí spravujícího orgánu na žádost subjektu údajů o výmaz je, že výmaz osobních údajů se provede, pokud spravující orgán porušil zásady zpracování osobních údajů podle § 25 zákona o zpracování osobních údajů, tj. porušil zásady zpracování osobních údajů, nebo porušil zásady zpracování osobních údajů jiného právního předpisu nebo omezení zpracování některých kategorií osobních údajů, nebo pokud má spravující orgán povinnost tyto údaje vymazat. Také v tomto případě může spravující orgán namísto opravy nebo výmazu osobních údajů omezit zpracování zvláštním označením osobních údajů. Takto se postupuje, popírá-li subjekt údajů jejich přesnost, přičemž nelze zjistit, zda jsou tyto údaje přesné, nebo musí být uchovány pro účely dokazování.

Před zrušením omezení spravující orgán informuje subjekt údajů; stejně postupuje, pokud má omezení být zrušeno na základě rozhodnutí Úřadu nebo soudu. Žádosti subjektu údajů spravující orgán nevyhoví, nebo vyhoví částečně, pokud by vyhověním došlo k ohrožení podle § 28 odst. 2; za takové situace spravující orgán žadatele informuje tak, aby takovému ohrožení předcházel. I v tomto případě se dokumentace uchovává nejméně 3 roky.[114]

Lhůta pro vyřízení žádosti subjektu údajů je stanovena jako bez zbytečného odkladu, nejdéle však do 60 dnů ode dne jejího podání. Žádosti lze nevyhovět, pokud spravující orgán doloží, že je zjevně nedůvodná nebo nepřiměřená, zejména proto, že se v krátké době v téže věci

[113] § 28 zák. č. 110/2019 Sb.
[114] § 28 zák. č. 110/2019 Sb.

opakuje. Oznamovací povinnost spravujícího orgánu zahrnují informování subjektu údajů o možnosti požádat o ověření zákonnosti zpracování osobních údajů prostřednictvím Úřadu a o kontaktních údajích Úřadu, možnosti podat stížnost Úřadu[115] a žádat o soudní ochranu.

Informace o vyřízení žádosti musí být písemná a obsahovat odůvodnění, s výjimkou případu, kdy se žádosti vyhovuje v plném rozsahu. Je-li subjekt údajů zastoupen, může spravující orgán požadovat, aby byl podpis na písemné plné moci úředně ověřen; úřední ověření není třeba, pokud byla plná moc udělena před spravujícím orgánem.

Soud a státní zastupitelství neinformují subjekt údajů o možnostech obrátit se na Úřad pro ochranu osobních údajů.

[115] K postupu Úřadu při ověření zákonnosti zpracování osobních údajů vizte kap. 18 této učební pomůcky.

9. Zvláštní kategorie osobních údajů

Zvláštní kategorie v obecném nařízení

Osobní údaje lidí mají rozdílnou vypovídací hodnotu a zejména se vztahují k různým sférám života lidí a společnosti. Vypovídací hodnota některých je rozlišována i obecnou veřejností a subjektivně vnímána jako *(zvýšená) citlivost*. Právní úprava založená na obecném nařízení i Úmluvě č. 108[116] vymezuje některé z těchto údajů a označuje je jako osobní údaje patřící do zvláštní kategorie nebo představujících takovou kategorii. V obecném nařízení jsou vymezeny kombinací taxativního výčtu kategorií a přímým definováním tří z nich.

Zvláštními kategoriemi osobních údajů jsou osobní 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. Tento taxativní seznam neurčitě vymezených osobních údajů a jejich možných seskupení je výsledkem shody zákonodárců.

Přímo v obecném nařízení jsou definovány genetické údaje, biometrické údaje a údaje o zdravotním stavu: genetickými údaji jsou osobní údaje týkající se zděděných nebo získaných genetických znaků fyzické osoby, které poskytují jedinečné informace o její fyziologii či zdraví a které vyplývají zejména z analýzy biologického vzorku dotčené fyzické osoby; biometrickými údaji osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje; „údaji o zdravotním stavu“ osobní údaje týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytování zdravotních služeb, které vypovídají o jejím zdravotním stavu.

Aniž je to v oficiálních odůvodněních kteréhokoli z platných předpisů výslovně uvedeno, platí, že všechny uvedené kategorie zahrnují osobní údaje, které vykazují zvýšenou náchylnost k použití v neprospěch subjektu údajů, popř. k jeho diskriminaci. Proto je základní situací pro jejich zpracování zákaz, doplněný deseti výjimkami. Ty pokrývají stav, kdy:

a) subjekt údajů udělil výslovný souhlas se zpracováním určitých osobních údajů pro jeden nebo více stanovených účelů, s výjimkou případů, kdy právo Unie nebo členského státu stanoví, že zákaz nemůže být subjektem údajů zrušen,
b) zpracování je nezbytné pro účely plnění povinností a výkon zvláštních práv správce nebo subjektu údajů v oblasti pracovního práva a práva v oblasti sociálního

[116] Čl. 8 Úmluvy č. 108.

zabezpečení a sociální ochrany, pokud je povoleno právem Unie nebo členského státu nebo kolektivní dohodou podle práva členského státu,
v němž se stanoví vhodné záruky týkající se základních práv a zájmů subjektu údajů,

c) zpracování je nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas,
d) zpracování provádí v rámci svých oprávněných činností a s vhodnými zárukami nadace, sdružení nebo jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle, a za podmínky, že se zpracování vztahuje pouze na současné nebo bývalé členy tohoto subjektu nebo na osoby, které s ním udržují pravidelné styky související s jeho cíli, a že tyto osobní údaje nejsou bez souhlasu subjektu údajů zpřístupňovány mimo tento subjekt,
e) zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů,
f) zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků, nebo pokud soudy jednají v rámci svých soudních pravomocí,
g) zpracování je nezbytné z důvodu významného veřejného zájmu na základě práva Unie nebo členského státu, které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů,
h) zpracování je nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče či léčby nebo řízení systémů a služeb zdravotní nebo sociální péče na základě práva Unie nebo členského státu nebo podle smlouvy se zdravotnickým pracovníkem a při splnění podmínek a záruk uvedených v odstavci 4,
i) zpracování je nezbytné z důvodů veřejného zájmu v oblasti veřejného zdraví, jako je ochrana před vážnými přeshraničními zdravotními hrozbami nebo zajištění přísných norem kvality a bezpečnosti zdravotní péče a léčivých přípravků nebo zdravotnických prostředků, na základě práva Unie nebo členského státu, které stanoví odpovídající a zvláštní opatření pro zajištění práv a svobod subjektu údajů, zejména služebního tajemství,
j) zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely v souladu s čl. 89 odst. 1 na základě práva Unie nebo členského státu, které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů.

Naplnění některé z výše uvedených liberačních podmínek[117] nepředstavuje samostatný právní základ pro zpracování; naopak platí, že správce je může využít pouze, pokud pro stanovený účel zpracování mu svědčí některý z právních základů podle čl. 6 obecného nařízení

Vnitrostátní úprava

Zpracování pro účely preventivního nebo pracovního lékařství, pro posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče či léčby nebo řízení systémů a služeb zdravotní nebo sociální péče je i v ČR upraveno několika zákony, které vesměs splňují požadavek obecného nařízení o ochraně osobních údajů, aby osobní údaje patřící do zvláštní kategorie nebo ji představující byly zpracovávány podle stanovených pravidel osobami vázanými služebním tajemstvím nebo na jejich odpovědnost. Patří mezi ně i zákoník práce, který současně upravuje zpracování pro účely podle písm. b)[118]. Ustanovení § 30, že *zaměstnavatel smí vyžadovat v souvislosti s jednáním před vznikem pracovního poměru od fyzické osoby, která se u něj uchází o práci, nebo od jiných osob jen údaje, které bezprostředně souvisejí s uzavřením pracovní smlouvy* je nedostatečně určité; na rozdíl od ustanovení, které platí pro zpracování pro účely podle písm. h), že v *případech stanovených zvláštním právním předpisem je zaměstnavatel povinen zajistit, aby se fyzická osoba před vznikem pracovního poměru podrobila vstupní lékařské prohlídce,* a ustanovení o lékařských posudcích v průběhu zaměstnání a při jeho skončení. Základním předpisem pro posouzení pracovní schopnosti zaměstnance je zákon č. 373/2011 Sb., o specifických zdravotních službách. Jeho ustanovení o posudkové péči se použijí i pro státní zaměstnance.[119]

> Zákon č. 361/2003 Sb., o služebním poměru příslušníků bezpečnostních sborů speciálně upravuje posuzování zdravotní, osobnostní a fyzické způsobilosti, přičemž stanoví, že pro posuzování zdravotní způsobilosti příslušníka se použije rovněž zákon o specifických zdravotních službách.

Členské státy mohou zachovat nebo zavést další podmínky, včetně omezení, pokud jde o zpracování genetických údajů, biometrických údajů či údajů o zdravotním stavu.

Nejrozsáhlejší a současně nejméně přehledná je právní úprava zpracování osobních údajů, které vypovídají o zdravotním stavu žijící fyzické osoby. Situaci navíc neusnadňuje, že termín *údaje, které vypovídají o zdravotním stavu*, není pro potřeby práva dostatečně určitý. V ČR upravuje zpracování údajů o zdravotním stavu celá řada právních předpisů, včetně výše

[117] Pojem „liberační podmínky" v tomto kontextu lze chápat jako výjimky z obecně platného zákazu zpracování zvláštních kategorií osobních údajů.

[118] Zákon č. 262/2006 Sb.

[119] § 28 odst. 5 a § 61 odst. 2 zákona č. 234/2014 Sb.

uvedených a řada z nich v návaznosti na právní předpis EU. Zpracování genetických údajů lidí výslovně upravuje zákon o lidských tkáních a buňkách.[120] Tento zákon splňuje požadavek, aby zpracování bylo obligatorně podmíněno specifickými a účinnými zárukami. Stávající úpravu lze pro obě skupiny těchto zvláštních kategorií považovat za zachovávající podmínky čl. 9 obecného nařízení a naplňujících dílčí podmínky a požadavky tam uvedené.

Výrazně odlišná je situace ve vztahu ke zpracování biometrických osobních údajů, splňujících definiční kritéria pojmu podle čl. 4 bod 14 obecného nařízení. ČR dosud nevyužila možnost zavést další podmínky, včetně omezení, obecně. Např. v návaznosti na předpisy EU upravuje zákon o cestovních dokladech biometrické pasy, tj. cestovní pasy s digitálním biometrickým zobrazením obličeje a otisků prstů nositele pasu.[121]

Řadu let platí úprava vyžadující biometrickou identifikaci a autorizaci[122] při zacházení s jaderným materiálem. V § 11 odst. 2 současné vyhlášky o zabezpečení jaderného zařízení a jaderného materiálu[123] je stanoveno, že pro kontrolu vstupu fyzických osob musí být nejméně při vstupu do vnitřního nebo životně důležitého prostoru použita biometrická identifikace a aktuální databáze vstupů musí být dostupná nejméně 1 měsíc a musí být zajištěno její trvalé uchovávání.

Zákon o platebním styku stanoví mj. podmínky pro použití silného ověření uživatele, což zahrnuje použití alespoň dvou z těchto prvků: údaje, který je znám pouze uživateli, věci, kterou má uživatel ve své moci a biometrických údajů uživatele[124].

Pro využívání biometriky v jiných oblastech a pro jiné účely není platná jiná právní úprava než právě v obecném nařízení. To v praxi znamená, že podmínky stanovené v čl. 9 obecného nařízení jsou s ohledem na potřebnou specifikaci záruk na vnitrostátní úrovni imperfektní, tzn. neúplné, chybí vnitrostátní speciální právní úprava. Za situace, kdy je používání lidské biometriky běžné přinejmenším v prostředí osobních elektronických přístrojů a zařízení a také

[120] Mj. § 3 zákon č. 296/2008 Sb.

[121] Zákon č. 329/1999 Sb. a prováděcí vyhláška č. 415/2006 Sb., kterou se stanoví technické podmínky a postup při pořizování a dalším zpracovávání biometrických údajů obsažených v nosiči dat cestovního dokladu navazuje na ustanovení nařízení (EU)2019/1157 o posílení zabezpečení průkazů totožnosti občanů Unie a povolení k pobytu vydávaných občanům Unie a jejich rodinným příslušníkům, kteří vykonávají své právo volného pohybu, které stanoví, že průkazy totožnosti vydávané členskými státy se vyhotovují ve formátu ID-1 a obsahují strojově čitelnou zónu. Tyto průkazy totožnosti vycházejí ze specifikací a minimálních bezpečnostních norem stanovených v dokumentu ICAO 9303 a musí splňovat požadavky stanovené v písmenech c), d), f) a g) přílohy nařízení (ES) č. 1030/2002, ve znění nařízení (EU) 2017/1954.

[122] Identifikace (synonymum k autentizaci) **je operace, při které zjišťujeme totožnost subjektu údajů, jeho identitu. Autorizace je operace, při které zjišťujeme, jestli je subjekt oprávněn k nějaké činnosti**, např. přístup k objektu. Logicky tedy autentizace (identifikace) předchází autorizaci.

[123] Vyhláška č. 361/2016 Sb., o zabezpečení jaderného zařízení a jaderného materiálu

[124] § 223 zákon č. 370/2017 Sb., o platebním styku

pro účely kontroly přístupu do určitých prostor, nejméně pro účely bezpečnostní autorizace, založeno právě na využívání jedné nebo několika biometrických charakteristik, absence specifické právní úpravy znamená, že každý budoucí správce musí provádět vyhodnocování a přípravné práce v míře, která neodpovídá stavu, kdy používání biometriky v souvislosti s autentizací vyžadují nebo výslovně předpokládají technické předpisy a standardy a na trhu jsou volně dostupná různě složitá plně standardizovaná řešení (aplikace).

Zvláštním kategoriím se blíží (z důvodů reálných i možných důsledků pro dotčené subjekty údajů) osobní údaje týkající se rozsudků v trestních věcech a trestných činů. Podmínky pro jejich zpracování jsou také stanoveny doplňkově jako dodatečné záruky pro subjekty údajů k právnímu základu podle čl. 6 obecného nařízení, ale jsou definovány pozitivně: zpracování osobních údajů týkajících se rozsudků v trestních věcech a trestných činů či souvisejících bezpečnostních opatření na základě čl. 6 odst. 1 tohoto nařízení se může provádět pouze pod dozorem orgánu veřejné moci, nebo pokud je oprávněné podle práva Unie nebo členského státu poskytujícího vhodné záruky, pokud jde o práva a svobody subjektů údajů. Jakýkoli souhrnný rejstřík trestů může být veden pouze pod dozorem orgánu veřejné moci. Takovým rejstříkem je v ČR rejstřík trestů upraveny zákonem, který obsahuje rovněž specifické a účinné záruky (mj. pro vydávání výpisů a opisů).[125]

[125] Zákon č. 269/1994 Sb.

10. Zásady ochrany osobních údajů, přístup založený na riziku a záměrná a standardní ochrana v obecném nařízení o ochraně osobních údajů a v zákoně o zpracování osobních údajů

Současné zásady ochrany osobních údajů nejsou absolutní novinkou, kterou by přineslo obecné nařízení. Zachována je kontinuita s dřívější mezinárodní právní úpravou, a to jak v zásadách, tak v klíčových instrumentech. Reakcí na vývoj prostředí, zejména na rozvoj informačních technologií pro zpracování osobních údajů a globalizaci, je zásada panevropského (EU) dosahu. Obecné nařízení naplňuje sedm zásad ochrany osobních údajů: práva subjektů údajů, povinnosti správců a zpracovatelů, záměrnou a standardní ochranu, přístup založený na riziku, panevropský (EU) dosah, nezávislý dozor a vymahatelnost. V souladu s charakterem obecného nařízení jako právní úpravy zohledňující prováděné činnosti jsou jednotlivé zásady jednak rozvíjeny v dedikovaných částech obecného nařízení, jednak prostupují některými dalšími částmi.

Zásady zpracování osobních údajů

Obecné nařízení obsahuje vedle toho také zásady samotného zpracování osobních údajů. Sedm zásad je zakotveno v čl. 5 obecného nařízení.

Zásada zákonnosti, korektnosti a transparentnosti ve vztahu k subjektu údajů zní: Osobní údaje musí být ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem. Vyjadřuje v prvé řadě požadavek, aby jakékoli zpracování osobních údajů bylo prováděno zákonným a spravedlivým způsobem. To zahrnuje splnění podmínky, aby konkrétní účely, pro které jsou osobní údaje zpracovávány, byly jednoznačné a legitimní v obecném významu tohoto slova a aby byly stanoveny k okamžiku shromažďování osobních údajů. Transparentnost bývá v aplikační praxi vnímána a posuzována také samostatně. Její obsah daný výkladovým ustanovením obecného nařízení do značné míry předjímá obsah informačních povinností správce vůči subjektu údajů (čl. 12–14 obecného nařízení): mělo by pro ně být transparentní, že jejich osobní údaje, jsou zpracovávány a v jakém rozsahu tomu tak bude. Zásada transparentnosti vyžaduje, aby všechny informace a všechna sdělení jich se týkající byly snadno přístupné a srozumitelné a podávané za použití jasných a jednoduchých jazykových prostředků; platí to pro informování subjektů údajů o totožnosti správce a účelech zpracování a o dalších záležitostech v zájmu zajištění spravedlivého a transparentního zpracování a práva subjektu na sdělení zpracovávaných osobních údajů, které se jich týkají. Fyzické osoby by měly být upozorněny na to, jaká rizika, pravidla, záruky a práva existují v souvislosti se zpracováním jejich osobních údajů a jak mají uplatňovat svá práva.

Zásada účelového omezení byla dříve v České republice známa jako povinnost stanovit účel zpracování. Současným obsahem zásady je, aby osobní údaje byly pro určité, výslovně vyjádřené a legitimní účely a současně nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný. Za neslučitelné s původními účely se nepovažují účely archivace ve veřejném zájmu, vědecký nebo historický výzkum nebo statistické účely podle čl. 89 odst. 1 obecného nařízení; vždy však jde o další zpracování osobních údajů, pro něž byl při shromáždění stanoven jiný specifický účel.

Navazující zásada minimalizace údajů vyžaduje, aby zpracovávané osobní údaje byly přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány; rozvedena je dále v čl. 25 obecného nařízení.

Zásada přesnosti požaduje, aby zpracovávané osobní údaje byly přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny. Podrobnosti k této zásadě jsou uvedeny jako součást povinností správce podle čl. 16 až 19 obecného nařízení.

Zásada omezení uložení vyžaduje, aby zpracovávané osobní údaje byly uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány. Výjimka, tj. možnost uložení po delší dobu, je vázána na výhradní zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely podle čl. 89 odst. 1 obecného nařízení, za předpokladu provedení příslušných technických a organizačních opatření požadovaných obecným nařízením s cílem zaručit práva a svobody subjektu údajů. Na tuto zásadu je přímo navázána povinnost správce podle čl. 25 odst. 2 obecného nařízení.

Zásada integrity a důvěrnosti je svým obsahem společná se zásadami kybernetické a informační bezpečnosti; osobní údaje musí být zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením. Zásada je dále promítnuta v povinnostech správce a zpracovatele podle čl. 24–25 a 32 obecného nařízení.

Podle zásady odpovědnosti správce odpovídá za dodržení předchozích zásad a musí být schopen toto dodržení souladu doložit. Tím je mj. naplňována zásada vymahatelnosti ochrany osobních údajů. Zásada je precizována výslovně v čl. 24 a 25 obecného nařízení, konkludentně např. též v čl. 28 a 82 obecného nařízení.

V trestněprávní směrnici jsou tyto zásady „převzaty“ a doplňuje je zásada zpracování pro jiný účel podle práva EU/ČS, nezbytného a přiměřeného v souladu s právem, a naopak součástí zásad není transparentnost vůči subjektu údajů. Čl. 4 směrnice požaduje po členských státech, aby zajistily, že osobní údaje mohou být zpracovávány pouze:

a) zákonným a korektním způsobem,
b) shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nebyly zpracovávány způsobem, který je s těmito účely neslučitelný,
c) přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelům, pro které jsou zpracovávány,
d) přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření zajišťující, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny,
e) uchovávány ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány,
f) zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením.

Zpracování stejným nebo jiným správcem pro kterýkoli účel uvedený v čl. 1 odst. 1 směrnice jiný než účel, pro nějž byly osobní údaje shromážděny, je přípustné, pokud je správce oprávněn zpracovávat takové osobní údaje pro takový účel v souladu s právem Unie či členského státu a zpracování pro tento jiný účel je nezbytné a přiměřené v souladu s právem Unie či členského státu. Zpracování stejným nebo jiným správcem může zahrnovat archivaci ve veřejném zájmu či vědecké, statistické nebo historické použití pro účely uvedené v čl. 1 odst. 1 směrnice, s výhradou vhodných záruk pro práva a svobody subjektů údajů.

Záměrná a standardní ochrana

Záměrnou a standardní ochranou se v obecném nařízení rozumí povinnost správce zavést s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k pravděpodobným rizikům pro práva a svobody fyzických osob, jež s sebou zpracování nese, vhodná technická a organizační opatření. Povinnost pokrývá okamžik určení prostředků pro zpracování, tak dobu zpracování samotného. Jejím účelem je provádět zásady ochrany údajů účinným způsobem a začlenit do zpracování nezbytné záruky, tak aby splnil požadavky tohoto nařízení a ochránil práva subjektů údajů. Jako vhodná technická a organizační opatření jsou uznávány – za předpokladu, že mohou být účinně použity pro dané zpracování osobních údajů – minimalizace zpracování osobních údajů, co nejrychlejší pseudonymizace osobních údajů, transparentnost s ohledem na funkce a zpracování osobních údajů, umožnění subjektům údajů monitorovat zpracování osobních údajů a umožnění správcům vytvářet a zlepšovat bezpečnostní prvky (vztahuje se na zhotovitele produktů, služeb a aplikací).

Ideu záměrné a standardní ochrany naplňují dále povinnost posuzovat vliv jednotlivých zpracování a vyžádat si předběžnou konzultaci u dozorového úřadu a povinnost posouzení pro systematické a rozsáhlé vyhodnocování osobních aspektů, na němž se zakládají rozhodnutí s právními účinky, pro rozsáhlé systematické monitorování veřejně přístupných prostorů a rozsáhlé zpracování citlivých údajů.

Přístup založený na riziku

Přístup založený na riziku se promítá v řadě ustanovení obecného nařízení a to tak, že každý, kdo navrhuje nebo jinak připravuje zpracování či významnější změny v něm, má za povinnost řádně vyhodnotit rizikovost a podle toho postupovat dále. Rizikovost je logicky dovozována z rozsahu zpracování, zpracovávaných osobních údajů (příslušnosti ke zvláštním kategoriím nebo jinak založené citlivosti) a používaných technologií. Takto chápaná rizikovost je v samotném obecném nařízení klíčem k nastavování povinností.

Povinnost zabezpečení osobních údajů podle čl. 32 obecného nařízení a začlenění nezbytných záruk je formulována se zohledněním mj. různě pravděpodobných a různě závažných rizik pro práva a svobody. Při posuzování úrovně bezpečnosti se zohlední zejména rizika ze zpracování (náhodné/protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění osobních údajů, neoprávněný přístup). Obdobně je tomu při ohlašování a oznamování porušení zabezpečení osobních údajů podle čl. 33 a 34.[126] Také povinnost posoudit vliv zamýšlených operací zpracování na ochranu osobních údajů podle čl. 35 obecného nařízení a předchozí konzultace podle čl. 36 obecného nařízení jsou založeny na rizikovosti.[127]

Přístup založený na riziku se dále promítá v požadavcích na jmenování pověřence pro ochranu osobních údajů podle čl. 37 až 39 obecného nařízení a podmínkách a nárocích na předávání osobních údajů do třetích zemí a mezinárodním organizacím podle kapitoly V obecného nařízení.

Výjimečně podmíněné je vyrovnání se s rizikem pro povinnost vést záznamy o činnostech zpracování podle čl. 30 obecného nařízení, podle něhož povinnost vést záznamy o činnostech zpracování se nepoužije *pro podnik nebo organizaci zaměstnávající méně než 250 osob, ledaže zpracování, které provádí, pravděpodobně představuje riziko pro práva a svobody subjektů údajů, zpracování není příležitostné, nebo zahrnuje zpracování zvláštních kategorií údajů uvedených v čl. 9 odst. 1 nebo osobních údajů týkajících se rozsudků v trestních věcech*

[126] Podrobněji vizte kap. 6 a 16 této učební pomůcky.
[127] Podrobněji vizte kap. 11 této učební pomůcky.

a trestných činů uvedených v čl. 10. Úskalí formulace nízké rizikovosti je v pojmech *riziko pro práva a svobody subjektů údajů* a *příležitostný charakter*. Dosud jsou obecně chápány výhradně subjektivně a rizikovost je často až úzkostlivě spatřována v každém zpracování. Ze znění liberační podmínky je přitom zřejmé, že mají existovat zpracování, na něž se povinnost nevztahuje.

Ještě jinak se přístup založený na riziku promítá v pseudonymizaci.[128]

Přístup založený na riziku v zákoně o zpracování osobních údajů

Zákon o zpracování osobních údajů ctí přístup založený na riziku podle obecného nařízení. Výslovně se to promítá v §§ 10 (Výjimka z povinnosti posouzení vlivu zpracování osobních údajů na ochranu osobních údajů), 16 (Zpracování osobních údajů za účelem vědeckého nebo historického výzkumu nebo pro statistické účely a 17 (zpracování osobních údajů prováděné pro novinářské účely nebo pro účely akademického, uměleckého nebo literárního projevu).

V implementaci trestněprávní směrnice v zákoně o zpracování osobních údajů naplňuje přístup založený na rizikovosti zpracování zejména v §§ 32 a 36 až 42, jejichž obsah je paralelou k uchopení rizikovosti podle obecného nařízení. Formulační odchylkou a potvrzením, že rizikovost je přiměřeně vyhodnocena a kompenzována, je § 36 Automatizované pořizování záznamů[129].

(1) Provádí-li spravující orgán automatizované zpracování osobních údajů, pořizuje záznamy alespoň
o operacích shromáždění, vložení, pozměnění, kombinování, nahlédnutí, předání, sdělení a výmazu osobních údajů.

(2) Záznamy o operacích shromáždění, vložení, nahlédnutí nebo sdělení podle odstavce 1 umožňují určit a ověřit důvod a čas těchto operací, totožnost osoby provádějící operaci a totožnost příjemce, ledaže zjištění totožnosti těchto osob není z technických důvodů možné.

(3) Záznamy podle odstavce 1 lze využít pouze pro účely trestního řízení, ověření zákonnosti zpracování osobních údajů, zajištění neporušenosti zabezpečení osobních údajů a zajištění plnění úkolů spravujícího orgánu nebo zpracovatele a povinností osob, kterým se poskytuje přístup k osobním údajům.

(4) Záznamy podle odstavce 1 jsou uchovávány po dobu 3 let od výmazu osobních údajů, ke kterým se vztahují.

[128] Podrobněji vizte kap. 1 této učební pomůcky.
[129] Provedení čl. 25 trestněprávní směrnice.

(5) Povinnosti spravujícího orgánu stanovené v odstavcích 1 až 4 platí pro zpracovatele obdobně.

Pro zpracování osobních údajů prováděná podle hlavy IV zákona o zpracování osobních údajů, tj. při zajišťování obranných a bezpečnostních zájmů České republiky je relevantnost přístupu založeného na riziku potvrzena v § 46 (Povinnosti osob při zabezpečení osobních údajů).

11. Povinnosti správce před započetím zpracování osobních údajů

Na toho, kdo je (resp. bude) při zpracování osobních údajů připravovaného zpracování v postavení správce, dopadá několik povinností. Bez ohledu na to, zda jednotlivé články obecného nařízení výslovně předpisují písemnou (dokumentovou) formu, vyplývá správci z čl. 5 odst. 2 povinnost být schopen dodržení souladu doložit a k tomu vede cesta primárně skrze vypracování odpovídající dokumentace. Pořadí započetí prací na jednotlivých povinnostech není dáno důsledně systematikou obecného nařízení, ale je spoluurčováno specifickými parametry připravovaného zpracování.

Stanovení účelu zpracování a návrh zpracování

První a výchozí povinností správce je stanovit přiměřeně specifický účel[130]. Po stanovení účelu musí správce stanovit k tomuto účelu odpovídající právní důvod chystaného zpracování osobních údajů. Obecně musí právní základ zpracování odpovídat stanovenému účelu zpracování osobních údajů. Jedno a totéž zpracování může sledovat více než jeden účel a na straně druhé může správce zpracovávat osobní tytéž osobní údaje k rozdílným účelům, opírajícím se o rozdílné právní základy.

Pokud bude zpracování prováděno v souladu se zákonnou povinností, která se na správce vztahuje, nebo pokud je zpracování nezbytné ke splnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci, měl by mít právní předpis EU nebo členského státu stanovit kromě jiného také účel zpracování.

Účel zpracování by měl být formulován přesně a uváděn konzistentně shodně, tj. jak v dokumentech určených subjektům údajů, tak v záznamech o činnostech zpracování podle čl. 30 obecného nařízení.

Na stanovení nebo ujasnění účelu zpracování navazuje stanovení (návrh) jednotlivých parametrů zpracování, počínaje osobními údaji, které budou shromažďovány od subjektu údajů, z jiného externího zdroje, nebo generovány vlastní činností správce na základě odpozorování projevů učiněných subjektem údajů a operacemi s osobními údaji, které mají být prováděny. Určování a vyhodnocování jednotlivých parametrů by mělo respektovat rizikovost pro práva a svobody subjektů údajů.

Posouzení důsledků připravovaného zpracování pro subjekt údajů

Po ujasnění tohoto je na místě posouzení důsledků takto koncipovaného zpracování pro subjekt údajů. To je absolutní povinnost. Bez jejího splnění totiž není možné rozhodnout, zda se

[130] K účelu vizte též kap. 3 této učební pomůcky.

na správce, resp. příslušné zpracování, vztahuje povinnost podle čl. 35 obecného nařízení, totiž provést posouzení vlivu na ochranu osobních údajů. Pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude mít s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování za následek vysoké riziko pro práva a svobody fyzických osob, má správce před zpracováním povinnost posoudit vlivu zamýšlených operací zpracování na ochranu osobních údajů. Obecné nařízení umožňuje, aby *pro soubor podobných operací zpracování, které představují podobné riziko*, bylo provedeno pouze jedno posouzení. Úskalím je neurčitost pojmu „podobné riziko", proto je na místě provést posouzení důkladně a relativně samostatně pro každé z identifikovaných nebo předpokládaných rizik pro práva a svobody subjektů údajů.

Povinnost provést takové posouzení se vztahuje na:

a) systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad,
b) rozsáhlé zpracování zvláštních kategorií údajů uvedených v čl. 9 odst. 1 nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v čl. 10,
c) rozsáhlé systematické monitorování veřejně přístupných prostorů.

Rozhodování správce usnadňují seznamy zveřejňované dozorovým úřadem, v ČR Úřadem pro ochranu osobních údajů. Povinně Úřad zveřejňuje seznam druhů operací zpracování, které podléhají požadavku na posouzení vlivu na ochranu osobních údajů. *Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů (Verze 1.0)* je trvale dostupný na webových stránkách úřadu.[131] Úřad dále využil možnosti sestavit a zveřejnit seznam druhů operací zpracování, u nichž není posouzení vlivu na ochranu osobních údajů nutné. Také *Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů (Verze 1.0)* je trvale dostupný.

Na každého, kdo má zahájit zpracování osobních údajů podle čl. 6 odst. 1 písm. c) nebo e), tj. jako nezbytné pro splnění právní povinnosti, která se na něho vztahuje, nebo nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, je-li tento správce výkonem přímo pověřen, se vztahuje § 10 zákona o zpracování osobních údajů. Správce nemusí provádět posouzení vlivu zpracování na ochranu osobních údajů před jeho zahájením, pokud mu právní předpis stanoví povinnost takové zpracování osobních údajů provést nebo provádět. Jediným předpokladem v této situaci je, že se správce ujistí, že platný

[131] https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=38940

právní předpis mu dané zpracování osobních údajů ukládá. K tomu je však nutné dodat, že právním předpisem uložené zpracování osobních údajů musí být jednoznačně určitě stanoveno tak, aby vylučovalo více možností provést dané zpracování osobních údajů. V opačném případě (tedy v případě, že by například ustanovení právního předpisu pouze deklarovalo cíl, kterého má být zpracováním osobních údajů dosaženo) by nebylo možné užít výjimku stanovenou v § 10 zákona o zpracování osobních údajů.

Posouzení vlivu prováděné před započetím zpracování správcem obsahuje alespoň:

a) systematický popis zamýšlených operací zpracování a účely zpracování, případně včetně oprávněných zájmů správce,
b) posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů,
c) posouzení rizik pro práva a svobody subjektů údajů,
d) plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s obecným nařízením, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob.

Při posuzování vlivu na ochranu osobních údajů si správce vyžádá posudek pověřence pro ochranu osobních údajů. Povinnost posouzení vlivu připravovaného zpracování osobních údajů na subjekt údajů zahrnuje také získání stanoviska subjektů údajů nebo jejich zástupců ve vhodných případech a přezkum, zda je zpracování prováděno v souladu s posouzením vlivu na ochranu osobních údajů alespoň v případech, kdy dojde ke změně rizika, jež operace zpracování představují.

Pokud z posouzení vlivu vyplyne, že by dané zpracování mělo za následek vysoké riziko v případě, že by správce nepřijal opatření ke zmírnění rizika, je správce povinen konzultovat před zahájením zpracování s dozorovým úřadem, tj. s Úřadem pro ochranu osobních údajů, podle čl. 36 obecného nařízení. Uvedené se nicméně vztahuje na situace, kdy by i v případě přijetí opatření k řešení rizik pro práva a svobody subjektů údajů správcem zůstávala tato rizika vysoká. Povinnost mají pouze správci, kteří podléhají dozorové působnosti Úřadu.

Pro konzultaci musí správce poskytnout dozorovému úřadu informace o:

a) ve vhodných případech rozdělení odpovědnosti správce, společných správců a zpracovatelů, zejména v případě zpracování v rámci skupiny podniků,
b) účelech a způsobech zamýšleného zpracování,
c) opatřeních a zárukách poskytnutých za účelem ochrany práv a svobod subjektů údajů podle obecného nařízení,
d) kontaktní údaje pověřence pro ochranu osobních údajů,
e) samotné posouzení vlivu na ochranu osobních údajů podle čl. 35,

f) veškeré další informace, o které dozorový úřad požádá.

Dosud nebyl přijat zákon, který by od určitých správců vyžadoval, aby s Úřadem konzultovali a získali povolení pro zpracování prováděné pro plnění úkolu ve veřejném zájmu.

K posouzení vlivu na ochranu osobních údajů je nutné doplnit, že (jak vyplývá z čl. 35 odst. 11 obecného nařízení) správce případně provede přezkum s cílem posoudit, zda je zpracování prováděno v souladu s posouzením vlivu na ochranu osobních údajů alespoň v případech, kdy dojde ke změně rizika, jež představují operace zpracování. Posouzení vlivu na ochranu osobních údajů je tedy živý dokument, který musí být neustále aktuální.

Příprava provozní dokumentace a dokumentů určených subjektům údajů

Další činnosti, které obecně směřují k plnění povinnosti správce podle čl. 5 odst. 2 a čl. 24 obecného nařízení být schopen doložit dodržení souladu, budou prováděny zpravidla souběžně. Na projektovou a provozní dokumentaci nekladou nařízení a zákon o zpracování osobních údajů specifické formální požadavky; vychází se tedy z obecných požadavků např. podle technických standardů ISO, popř. ze speciálních sektorových požadavků.

Správci, kteří jsou orgány veřejné moci nebo orgány veřejné správy v ČR, jsou povinni dodržovat v závislosti na kategorizaci jimi prováděných zpracování osobních údajů v rámci informačních systémů veřejné správy – tedy jsou správci nebo provozovateli informačního systému kritické informační infrastruktury, nebo významného informačního systému[132] povinnosti podle zákona o kybernetické bezpečnosti[133].

Na všechny informační systémy veřejné správy spravované státními orgány nebo orgány územních samosprávných celků se vztahují povinnosti podle zákona o informačních systémech veřejné správy, včetně např. povinnosti vytvářet a vydávat provozní dokumentaci k jednotlivým informačním systémům veřejné správy, uplatňovat ji v praxi a vyhodnocovat její dodržování[134]. Strukturu a náležitosti provozní dokumentace stanoví prováděcí právní předpis; vyhláška o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace

[132] Významným informačním systémem je informační systém, jehož správcem je orgán veřejné moci, který je organizační složkou státu, krajem nebo hlavním městem Praha, využívaný při výkonu působnosti orgánu veřejné moci k zajištění a) elektronické pošty, je-li určena k použití v rámci výkonu veřejné moci, b) kontrolní nebo inspekční činnosti anebo státního dozoru, c) výkonu veřejné moci při přípravě na krizové situace a jejich řešení, d) výkonu spisové služby, e) vedení úřední desky způsobem umožňujícím dálkový přístup,
f) mezinárodní spolupráce, nebo g) zadávání veřejných zakázek (Vyhl. č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích).
[133] Zák. č. 181/2014 Sb.
[134] Zák. č. 365/2000 Sb.

a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy kromě jiného stanoví strukturu a obsah provozní dokumentace[135].

Každý správce by měl nicméně dbát na to, aby se v této dokumentaci řádně promítla záměrná a standardní ochrana podle čl. 25 obecného nařízení. Dokumentace („opatření") musí být podle potřeby revidována a aktualizována i v částech., které nepodléhají povinnostem podle zákona o informačních systémech veřejné správy.

Požadavky na obsah a některé formální náležitosti dokumentů určených subjektům údajů jak pro fáze shromažďování osobních údajů, tak pro další operace zpracování, a dále pro naplňování práv subjektů údajů podle čl. 12 až 22 obecného nařízení, stanoví obecné nařízení naopak v souladu s jeho smyslem výslovně.

Poznámka: K požadavkům na provozní dokumentaci vizte dále zejm. kap. 16, k dokumentům určeným subjektům údajů vizte kap. 8.

Záznamy o činnostech zpracování podle čl. 30 obecného nařízení

Před započetím zpracování osobních údajů by měly být vypracovány také záznamy o činnostech zpracování. Povinnost takové záznamy vést má každý správce a jeho případný zástupce[136]. Záznamy obsahují všechny tyto informace:

a) jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů,
b) účely zpracování,
c) popis kategorií subjektů údajů a kategorií osobních údajů,
d) kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích,
e) informace o předání osobních údajů do třetí země nebo mezinárodní organizaci, v případě předání podle čl. 49 odst. 1 druhého pododstavce obecného nařízení doložení vhodných záruk,
f) je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů,
g) je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v čl. 32 odst. 1 obecného nařízení.

---

[135] Vyhl. č. 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace
a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy (vyhláška o dlouhodobém řízení informačních systémů veřejné správy)

[136] Zástupcem je podle čl. 4 bod 17) jakákoli fyzická nebo právnická osoba usazená v Unii, která je správcem nebo zpracovatelem určena písemně podle čl. 27 obecného nařízení k tomu, aby správce nebo zpracovatele zastupovala, pokud jde o příslušné povinnosti správce nebo zpracovatele ve smyslu tohoto nařízení;

Rovněž každý zpracovatel a jeho zástupce vedou záznamy o všech kategoriích činností zpracování prováděných pro správce. Ty musí obsahovat: a) jméno a kontaktní údaje zpracovatele nebo zpracovatelů a každého správce, pro něhož zpracovatel jedná, a případného zástupce správce nebo zpracovatele a pověřence pro ochranu osobních údajů; b) kategorie zpracování prováděného pro každého ze správců; c) informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a v případě předání podle čl. 49 odst. 1 druhého pododstavce obecného nařízení doložení vhodných záruk a d) je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v čl. 32 odst. 1 obecného nařízení.

Záznamy o činnostech zpracování jsou určeny pro vnitřní potřebu správce a zpracovatele, včetně pověřence pro ochranu osobních údajů, a musí být poskytnuty dozorovému úřadu na vyžádání. Naproti tomu nejsou určeny subjektům údajů a neposkytují se tedy v rámci výkonu jejich práv.

K uvedenému je třeba dodat, že čl. 30 odst. 5 obecného nařízení zakotvuje výjimku z povinnosti vést záznamy o činnostech zpracování, která stanovuje, že *Povinnosti uvedené v odstavcích 1 a 2* [čl. 30 obecného nařízení] *se nepoužijí pro podnik nebo organizaci zaměstnávající méně než 250 osob, ledaže zpracování, které provádí, pravděpodobně představuje riziko pro práva a svobody subjektů údajů, zpracování není příležitostné, nebo zahrnuje zpracování zvláštních kategorií údajů uvedených v čl. 9 odst. 1 nebo osobních údajů týkajících se odsouzení v trestních věcech a trestných činů uvedených v článku 10.*

12. Povinnosti správce v průběhu zpracování prováděného jeho jménem

Po zahájení zpracování má správce v jeho průběhu na základě obecného nařízení o ochraně osobních údajů řadu povinností, které je třeba plnit průběžně, a to buď kontinuálně, nebo na základě rozhodné události. Plnění některých povinností směřuje vůči subjektu údajů nebo k příslušnému dozorovému úřadu, ale většina jsou povinnosti, jejichž plnění nemá jiného adresáta než samotného správce, případně správci tyto povinnosti vyplývají ze zapojení zpracovatele do zpracování.

Základní povinnosti

Za nejdůležitější z povinností správce, jíž je třeba plnit po celou dobu, po kterou zpracování osobních údajů probíhá, lze považovat povinnost aktivně postupovat a případně přijímat další opatření tak, aby dosáhl souladu s relevantními požadavky, které pro něho vyplývají z obecného nařízení o ochraně osobních údajů, případně z jiných právních předpisů, které se na něho vztahují. S tím bezprostředně souvisí úkol udržovat veškerou projektovou a provozní dokumentaci v aktuálním stavu. Změny v dokumentaci, jíž zejména dokládá splnění požadavků vyplývajících ze zásady odpovědnosti podle čl. 5 odst. 2 a čl. 24 odst. 1 obecného nařízení, kde je povinnost přijatá opatření podle potřeby revidovat a aktualizovat. Splnění nebo plnění této povinnosti předpokládá průběžné vyhodnocování dříve zavedených opatření. Jiným impulsem ke změně může, popř. by měla, být změna v rizicích identifikovaná vně správce; ta může být navozena jednak změnou požadavků stanovených správci právním předpisem, jednak vývojem obecného informačního prostředí, zejm. v kybernetické a informační bezpečnosti.[137] V návaznosti na změny ve vlastním zpracování, nebo v právní úpravě, jíž se zpracování osobních údajů u správce (včetně orgánů veřejné správy) řídí, se potřeba přiměřené aktualizace vztahuje i na záznamy o činnostech zpracování.

Další povinností pro určité správce – a pro orgány veřejné správy bez výjimky – je jmenovat pověřence pro ochranu osobních údajů a vytvářet pro jeho působení odpovídající podmínky.[138]

Pokud si správce najal na všechny nebo některé operace zpracování zpracovatele, začínají jeho povinnosti výběrem zpracovatele a klíčovou povinností je uzavřít se zpracovatelem smlouvu o zpracování osobních údajů. Správce může využívat pouze zpracovatele, kteří poskytují dostatečné záruky zavedení vhodných technických a organizačních opatření a za podmínky, že byla zajištěna ochrana práv subjektu údajů.

[137] Vizte též kap. 10 a 16 této učební pomůcky.
[138] Vizte kap. 14 této učební pomůcky.

Zpracovatel se při zpracování prováděném jménem správce řídí smlouvou nebo jiným právním aktem podle práva Unie nebo členského státu, které zpracovatele zavazují vůči správci a v nichž je stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce. Smlouva nebo jiný právní akt zejména stanoví, že zpracovatel:

a) zpracovává osobní údaje pouze na základě doložených pokynů správce, včetně v otázkách předání osobních údajů do třetí země nebo mezinárodní organizaci, pokud mu toto zpracování již neukládají právo Unie nebo členského státu, které se na správce vztahuje; v takovém případě zpracovatel správce informuje o tomto právním požadavku před zpracováním, ledaže by tyto právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu,
b) zajišťuje, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti, nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti,
c) přijme všechna opatření požadovaná k zabezpečení osobních údajů,
d) dodržuje podmínky pro zapojení dalšího zpracovatele,
e) zohledňuje povahu zpracování, je správci nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, pro splnění správcovy povinnosti reagovat na žádosti o výkon práv subjektu údajů,
f) je správci nápomocen při zajišťování souladu s povinnostmi podle čl. 32 až 36, a to při zohlednění povahy zpracování a informací, které má zpracovatel k dispozici,
g) v souladu s rozhodnutím správce všechny osobní údaje buď vymaže, nebo je po ukončení poskytování služeb spojených se zpracováním vrátí správci a vymaže existující kopie, pokud právo Unie nebo členského státu nepožaduje uložení jím zpracovávaných osobních údajů;
h) poskytne správci veškeré informace potřebné k doložení toho, že byly splněny povinnosti spojené s jeho působením, a umožní audity, včetně kontrol, prováděných správcem nebo auditorem, kterého správce pověřil, a k těmto auditům a kontrolám poskytne součinnost (přispěje).

Pokud zpracovatel dospěje k závěru, že podle jeho názoru určitý pokyn porušuje toto nařízení nebo jiné předpisy Unie nebo členského státu o ochraně osobních údajů, neprodleně správce informuje.

Dostatečné záruky lze doložit tím, že zpracovatel dodržuje schválený kodex chování nebo schválený mechanismus pro vydávání osvědčení[139]. Smlouvy nebo jiné právní akty mohou být

[139] Podrobněji vizte kap. 20 této učební pomůcky.

založeny zcela nebo částečně na standardních smluvních doložkách[140]. Smlouva nebo jiný právní akt podle odstavců 3 a 4 musí být vyhotoveny písemně[141].

Povinnost uzavřít se zpracovatelem smlouvu o zpracování osobních údajů stanoví § 44 zákona o zpracování osobních údajů správci, který osobní údaje zpracovává podle hlavy IV tohoto zákona. Smlouva musí mít písemnou formu, musí v ní být zejména výslovně uvedeno, v jakém rozsahu, za jakým účelem a na jakou dobu se uzavírá, a musí obsahovat záruky zpracovatele o přijetí a dodržování technických a organizačních opatření k zajištění bezpečnosti a ochrany osobních údajů. V návaznosti na to má zpracovatel uloženu v § 45 povinnost v případě, že zjistí, že správce porušuje povinnosti stanovené tímto zákonem nebo jiným právním předpisem. V takové situaci je povinen správce na to neprodleně upozornit a ukončit zpracování osobních údajů. Pokud tak neučiní, odpovídá za škodu společně a nerozdílně se správcem.

Rozhodnou událostí je podmíněn vznik povinnosti aktualizovat nebo nově vypracovat posouzení vlivu zpracování osobních údajů, v němž má dojít v návaznosti na technologickou změnu, spočívající nejen v zavedení nové informační technologie, ale také v rozšíření souboru zpracovávaných osobních údajů, nebo i ve sledovaných účelech zpracování, případně i externě nově zjištěným významným rizikem pro práva svobody lidí[142].

Povinnosti vůči subjektu údajů

Povinnosti správce vůči subjektu údajů zahrnují poskytování stanovených informací z vlastní iniciativy správce i na žádost subjektu údajů[143]. Doplňuje je oznamovací povinnost vůči subjektu údajů.[144]

Povinnosti vůči dozorovému úřadu (Úřadu pro ochranu osobních údajů)

Podle čl. 31 správce spolupracuje na požádání s dozorovým úřadem při plnění úkolů tohoto úřadu. Dále má vůči němu ohlašovací povinnost podle čl. 33[145] a podmíněnou povinnost požádat o předběžnou konzultaci podle čl. 36[146].

Povinnosti zpracovatele

Zpracovatel má v průběhu zpracování kromě smluvních závazků na základě smlouvy se správcem, který ho určitými operacemi zpracování osobních údajů pověřil, také další povinnosti, jež mu ukládá přímo obecné nařízení o ochraně osobních údajů nad rámec této

---

[140] Podrobněji vizte kap. 17 této učební pomůcky.
[141] Čl. 28 GDPR.
[142] Vizte kap. 11, oddíl věnovaný posouzení vlivu.
[143] K tomu podrobněji vizte kap. 8 této učební pomůcky.
[144] K ní podrobněji vizte kap. 16 této učební pomůcky.
[145] K tomu vizte kap. 6 této učební pomůcky.
[146] K tomu vizte kap. 11 této učební pomůcky.

smlouvy. Shodně jako správce má povinnost spolupracovat na požádání s dozorovým úřadem při plnění úkolů tohoto úřadu.

Pokud zpracovatel jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, může tyto osobní údaje zpracovávat pouze na pokyn správce, ledaže mu jejich zpracování ukládá právo Unie nebo členského státu. Stejná povinnost platí pro každou osobu, která takto jedná z pověření zpracovatele.

Zpracovatel zejména nezapojí do zpracování žádného dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení správce. V případě obecného písemného povolení zpracovatel informuje správce o všech zamýšlených změnách ohledně dalších zpracovatelů a poskytne správci příležitost vyslovit vůči změnám námitky. Pokud dalšího zpracovatele zapojí, aby jménem správce provedl určité činnosti zpracování, musí být i tomuto dalšímu zpracovateli uloženy na základě smlouvy nebo jiného právního aktu podle práva Unie nebo členského státu stejné povinnosti, jaké jsou uvedeny ve smlouvě nebo jiném právním aktu mezi správcem a zpracovatelem, a to zejména poskytnutí dostatečných záruk, pokud jde o vhodná technická a organizační opatření. Neplní-li další zpracovatel své povinnosti v oblasti ochrany údajů, odpovídá správci za plnění povinností dotčeného dalšího zpracovatele i nadále plně prvotní zpracovatel.

Je-li role zpracovatele svěřena určitému subjektu zákonem, pak ten může nad rámec pověřením z rozhodnutí správce, mít explicitně uloženy určité povinnosti.

Tak zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu zakládá oprávněním Finančně analytického úřadu žádat v rozsahu potřebném pro šetření podezřelého obchodu a výkon správního dozoru od zpracovatele nebo správce evidence poskytnutí informací z taxativně určených zpracování osobních údajů (označených jako registr nebo informační systém). Týž zákon dále stanoví, že zpracovatel nebo správce evidence poskytne informace bezplatně, nestanoví-li jiný právní předpis jinak a že dožádaný je povinen žádosti bez zbytečného odkladu vyhovět.
Tato úprava je prozatím výjimečná; její rozsah je nesporně ovlivněn tím, že byla přijata k provedení úpravy přijaté na úrovni EU a v návaznosti na ni. Obvykle však zákon v ČR zpravidla pouze suše konstatuje, že určitý subjekt je zpracovatelem vůči týmž zákonem upraveného zpracování („registru“): tak tomu je např. u registru uchazečů o vzdělávání v oborech vzdělání se stanovenou jednotnou zkouškou podle školského zákona[147], nebo dokonce pouze stanoví, že orgán veřejné správy, jemuž je zákonem uložen úkol spočívající v podstatné míře ve zpracování osobních údajů, může přenést část zpracování na pověřenou osobu, která se stává zpracovatelem osobních údajů.

[147] § 60b zák. č. 561/2004 Sb.

Např. zákon o cestovních dokladech stanoví, že zpracovatelem údajů v evidenci cestovních dokladů je pro Ministerstvo vnitra orgán příslušný k vydání cestovního dokladu s výjimkou diplomatických a služebních pasů. Zpracovatelem taxativně určených údajů je samo Ministerstvo vnitra, zpracovatelem některých dalších údajů zastupitelský úřad.[148]

Zákon o sociálních službách stanoví, že krajský úřad vede registr poskytovatelů sociálních služeb, že registr je veden v listinné a elektronické podobě a že krajský úřad je správcem listinné podoby registru a zpracovatelem elektronické podoby registru.[149] Za takové situace má zpracovatel pouze a právě povinnosti stanovené v obecném nařízení o ochraně osobních údajů.

Významné je, že pokud zpracovatel poruší obecné nařízení o ochraně osobních údajů tím, že určí účely a prostředky zpracování, považuje se ve vztahu k takovému zpracování za správce, se všemi z toho vyplývajícími důsledky.

[148] § 30 zák. č. 329/1999 Sb.
[149] § 85 zák. č.108/2006 Sb.

13. Správce, zpracovatel, jejich odpovědnost a vztahy mezi nimi

Správce je definován jako fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem EU nebo členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení.[150] Zpracovatelem je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.[151]

Pojem správce a jeho interakce s pojmem zpracovatele hrají zásadní úlohu při uplatňování GDPR, neboť určují, kdo je odpovědný za dodržování různých pravidel pro ochranu osobních údajů, a způsob, jakým mohou subjekty údajů uplatňovat svá práva v praxi. Obecné nařízení výslovně zavádí zásadu odpovědnosti, tj. správce je odpovědný za dodržování zásad týkajících se zpracování osobních údajů uvedených v článku 5 a je s to toto dodržování doložit. Obecné nařízení navíc zpřesnilo vztah správce a zpracovatele.[152]

Pokud jde o vztah správce a zpracovatele, obecné nařízení nově obsahuje ustanovení, které ukládají povinnosti přímo zpracovatelům. Zpracovatel musí například zajistit, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k zachování mlčenlivosti (čl. 28 odst. 3); musí vést záznamy o všech kategoriích činností zpracování (čl. 30 odst. 2) a musí zavést vhodná technická a organizační opatření (článek 32). Zpracovatel musí za určitých podmínek rovněž jmenovat pověřence pro ochranu osobních údajů (článek 37) a má povinnost informovat správce bez zbytečného odkladu, jakmile zjistí porušení zabezpečení osobních údajů (čl. 33 odst. 2). Kromě toho se na zpracovatele i na správce vztahují pravidla pro předávání osobních údajů do třetích zemí (kapitola V). V tomto ohledu se EDPB domnívá, že čl. 28 odst. 3 GDPR, který zadává konkrétní obsah pro nezbytnou smlouvu mezi správcem a zpracovatelem, ukládá zpracovatelům přímé povinnosti, včetně povinnosti být nápomocen správci při zajišťování souladu.[153]Pokud jde o volbu zpracovatele, správce má povinnost využívat „pouze ty zpracovatele“, kteří poskytují dostatečné záruky zavedení vhodných technických a organizačních opatření“, aby zpracování splňovalo požadavky obecného nařízení, včetně požadavků na bezpečnost zpracování, a aby zajišťovalo ochranu práv subjektu údajů.[154]

---

[150] Čl. 4 odst. 7 obecného nařízení o ochraně osobních údajů.
[151] Čl. 4 odst. 8 obecného nařízení o ochraně osobních údajů.
[152] Pokyny EDPB č. 7/2020 k pojmům správce a zpracovatele v GDPR, bod 2.
[153] Pokyny EDPB č. 7/2020 k pojmům správce a zpracovatele v GDPR, bod 93.
[154] Čl. 28 odst. 1 a čl. bod 81odůvodnění obecného nařízení na ochranu osobních údajů. Pokyny EDPB č. 7/2020 k pojmům správce a zpracovatele v GDPR, bod 94.

Záruky „poskytnuté“ zpracovatelem jsou záruky, které je zpracovatel schopen správci uspokojivě prokázat, neboť jsou jediné, které správce může účinně zohlednit při posuzování souladu s jeho povinnostmi. Často to bude vyžadovat výměnu příslušné dokumentace (např. zásad ochrany soukromí, servisních podmínek, záznamů o činnostech zpracování, zásad správy záznamů, zásad bezpečnosti informací, zpráv o externích auditech ochrany údajů a uznávaných mezinárodních osvědčení.[155]

Veškeré zpracování osobních údajů zpracovatelem se musí podle čl. 28 odst. 3 obecného nařízení řídit smlouvou nebo jiným právním aktem mezi správcem a zpracovatelem podle práva EU nebo členského státu. Smlouva zavazuje zpracovatele vůči správci a stanoví předmět a dobu trvání zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce. Tato smlouva nebo jiný akt zejména stanoví, že zpracovatel:

a) zpracovává osobní údaje pouze na základě doložených pokynů správce, včetně v otázkách předání osobních údajů do třetí země nebo mezinárodní organizaci, pokud mu toto zpracování již neukládá právo Unie nebo právo členského státu, které se na zpracovatele vztahuje; v takovém případě zpracovatel správce informuje o tomto právním požadavku před zpracováním, ledaže by tyto právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu,
b) zajišťuje, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k důvěrnosti nebo aby se na ně vztahovala zákonná povinnost důvěrnosti,
c) přijme všechna opatření požadovaná podle článku 32,
d) dodržuje podmínky pro zapojení dalšího zpracovatele uvedené v odstavcích 2 a 4,
e) zohledňuje povahu zpracování, je správci nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, pro splnění správcovy povinnosti reagovat na žádosti o výkon práv subjektu údajů stanovených v kapitole III,
f) je správci nápomocen při zajišťování souladu s povinnostmi podle článků 32 až 36, a to při zohlednění povahy zpracování a informací, jež má zpracovatel k dispozici,
g) v souladu s rozhodnutím správce všechny osobní údaje buď vymaže, nebo je vrátí správci po ukončení poskytování služeb spojených se zpracováním, a vymaže existující kopie, pokud právo Unie nebo členského státu nepožaduje uložení daných osobních údajů,
h) poskytne správci veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené v tomto článku, a umožní audity, včetně inspekcí, prováděné správcem nebo jiným auditorem, kterého správce pověřil, a k těmto auditům přispěje.[156]

[155] Pokyny EDPB č. 7/2020 k pojmům správce a zpracovatele v GDPR, bod 95.

[156] Čl. 28 odst. 3 obecného nařízení o ochraně osobních údajů.

Pokud zpracovatel zapojí dalšího zpracovatele, aby jménem správce provedl určité činnosti zpracování, musí být tomuto dalšímu zpracovateli uloženy na základě smlouvy nebo jiného právního aktu podle práva Unie nebo členského státu stejné povinnosti na ochranu údajů, jaké jsou uvedeny ve smlouvě nebo jiném právním aktu mezi správcem a zpracovatelem podle odstavce 3, a to zejména poskytnutí dostatečných záruk, pokud jde o zavedení vhodných technických a organizačních opatření tak, aby zpracování splňovalo požadavky tohoto nařízení. Neplní-li uvedený další zpracovatel své povinnosti v oblasti ochrany údajů, odpovídá správci za plnění povinností dotčeného dalšího zpracovatele i nadále plně prvotní zpracovatel.[157]

Zpracovatel a jakákoliv osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, může tyto osobní údaje zpracovávat pouze na pokyn správce, ledaže jí jejich zpracování ukládá právo Unie nebo členského státu.[158]

Správce či zpracovatele může přímo určit zákon. Např. zákon o cestovních dokladech stanoví, že Ministerstvo vnitra je správcem evidence cestovních dokladů a zpracovatelem údajů v této evidenci je pro ministerstvo orgán příslušný k vydání cestovního dokladu s výjimkou diplomatických a služebních pasů. Školský zákon stanoví, že Ministerstvo školství, mládeže a tělovýchovy je správcem registru uchazečů o vzdělávání v oborech vzdělání se stanovenou jednotnou zkouškou; Centrum pro zjišťování výsledků vzdělávání je zpracovatelem tohoto registru. Zpracovatelem není fyzická osoba reprezentující správce a vykonávající některé nebo veškeré operace zpracování, včetně vnitřně stanovené odpovědnosti za ně.

Správce a zpracovatel jsou za zpracování osobních údajů odpovědni jak vůči subjektům údajů, tak vůči dozorovým úřadům a soudům. Obecné nařízení jim ukládá povinnosti zejména v kapitolách II. – IV. Jejich právní odpovědnost vůči subjektům údajům je upravena v kapitole VIII. obecného nařízení o ochraně osobních údajů.

Odpovědnost správce a zpracovatele vůči subjektu údajů

Odpovědnost správce a zpracovatele je upravena v čl. 82 obecného nařízení o ochraně osobních údajů. Její rozsah vymezuje ustanovení, že kdokoli, kdo v důsledku porušení tohoto nařízení utrpěl hmotnou či nehmotnou újmu, má právo obdržet od správce nebo zpracovatele náhradu této újmy.[159]

Rozhraničení odpovědnosti mezi správcem a zpracovatelem je nastaveno jednoznačně: správce je odpovědný za újmu, kterou způsobí zpracováním, porušujícím obecné nařízení

[157] Čl. 28 odst. 4 obecného nařízení na ochranu osobních údajů.
[158] Čl. 29 obecného nařízení na pchranu osobních údajů
[159] Čl. 82 odst. 1 obecného nařízení na ochranu osobních údajů.

o ochraně osobních údajů. Zpracovatel je za újmu způsobenou zpracováním odpovědný pouze v případě, že nesplnil povinnosti stanovené tímto nařízením konkrétně pro zpracovatele nebo že jednal nad rámec zákonných pokynů správce nebo v rozporu s nimi.[160]

Správce nebo zpracovatel jsou odpovědnosti zproštěni, pokud prokáží, že nenesou odpovědnost za událost, která ke vzniku újmy vedla.[161]

Je-li do téhož zpracování zapojen více než jeden správce nebo zpracovatel, nebo správce i zpracovatel, a nesou-li odpovědnost za škodu způsobenou daným zpracováním, nese každý správce nebo zpracovatel odpovědnost za celou újmu, tak, aby byla zajištěna účinná náhrada újmy subjektu údajů.

[162]Správce nebo zpracovatel, který zaplatil plnou náhradu způsobené újmy, má právo žádat od ostatních správců nebo zpracovatelů zapojených do téhož zpracování vrácení části náhrady, která odpovídá jejich podílu na odpovědnosti za újmu. Soudní řízení o výkonu práva na náhradu újmy se zahajují u soudů členského státu, v němž má daný správce nebo zpracovatel provozovnu. Řízení se může popřípadě zahájit i u soudů členského státu, kde má subjekt údajů své obvyklé bydliště, s výjimkou případů, kdy je správce nebo zpracovatel orgánem veřejné moci některého členského státu, který jedná v rámci výkonu veřejné moci.[163]

Zpracovatel, který zpracovává osobní údaje podle hlavy IV zákona o zpracování osobních údajů, má podle § 45 téhož zákona v případě, že zjistí, že správce porušuje povinnosti stanovené tímto zákonem nebo jiným právním předpisem, povinnost správce na tuto situaci neprodleně upozornit a ukončit zpracování osobních údajů. Pokud tak neučiní, odpovídá za škodu společně a nerozdílně se správcem.

[160] Čl. 82 odst. 2 obecného nařízení na ochranu osobních údajů.
[161] Čl. 82 odst. 3 obecného nařízení o ochranu osobních údajů.
[162] Čl. 82 odst. 4 obecného nařízení na ochranu osobních údajů.
[163] Čl. 82 odst. 5 a 6 obecného nařízení na ochranu osobních údajů.

14. Pověřenec pro ochranu osobních údajů

Úkoly a postavení pověřence podle obecného nařízení

Ačkoli praxe v průběhu let rozvinula jmenování pověřence pro ochranu osobních údajů v některých členských státech již před účinností obecného nařízení,[164] teprve po přijetí nařízení se stal pověřenec pro ochranu osobních údajů klíčovým hráčem v novém systému ochrany osobních údajů v EU. Pověřenci jsou „základním kamenem odpovědnosti“, protože usnadňují soulad s předpisy, a současně také vystupují jako prostředníci mezi dozorovými úřady, subjekty údajů a organizací, která je jmenovala.[165] Koncept pověřence je založen na ideji, že při zajištění souladu s právním předpisem, zejm. obecným nařízením o ochraně osobních údajů, může správci nebo zpracovateli účinně napomáhat osoba s odbornými znalostmi v oblasti právních předpisů a postupů týkajících se ochrany osobních údajů. Potřebná úroveň odborných znalostí by se měla určit zejména podle prováděných operací zpracování a podle ochrany, která se vyžaduje pro zpracovávané osobní údaje. Pověřenci by, bez ohledu na to, zda se jedná o zaměstnance správce, měli být schopni plnit své povinnosti a úkoly nezávislým způsobem.[166]

Je-li pověřenec pro ochranu osobních údajů jmenován, pak bez ohledu na to, zda se jednalo o splnění povinnosti nebo dobrovolnou aktivitu subjektu odpovědného za zpracování osobních údajů (správce), má pověřenec plnit alespoň tyto úkoly:

a) poskytování informací a poradenství správcům nebo zpracovatelům a zaměstnancům, kteří provádějí zpracování, o jejich povinnostech v ochraně osobních údajů,
b) monitorování souladu s obecným nařízením, dalšími předpisy Unie nebo členských států a s koncepcemi správce nebo zpracovatele v ochraně osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do zpracování a souvisejících auditů,
c) poskytování poradenství na požádání, včetně posouzení vlivu na ochranu osobních údajů a monitorování jeho uplatňování podle čl. 35,
d) spolupráce s dozorovým úřadem a působení jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování, včetně předchozí konzultace podle čl. 36, a vedení konzultací v jiných záležitostech.[167]

Pověřenec bere při plnění svých úkolů patřičný ohled na riziko spojené s operacemi zpracování a současně přihlíží k povaze, rozsahu, kontextu a účelům zpracování. Povinnost jmenovat

[164] Pokyny WP 29 týkající se pověřenců pro ochranu osobních údajů ze dne 5. 4. 2017.
[165] Příručka evropského práva v oblasti ochrany osobních údajů. FRA 2018. Str. 177.
[166] Bod 97 preambule obecného nařízení o ochraně osobních údajů.
[167] Čl. 39 odst. 1 obecného nařízení o ochraně osobních údajů.

pověřence je v obecném nařízení promítnutím přístupu založeného na riziku. To znamená, že povinnost vzniká tam, kde je rutinně prováděné zpracování spojeno se zvýšeným nebo velkým rizikem pro práva a svobody subjektů údajů takovým zpracováním dotčené. Tato povinnost proto vzniká vždy, když:

a) zpracování provádí orgán veřejné moci či veřejný subjekt, s výjimkou soudů jednajících v rámci svých soudních pravomocí,
b) hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů,
c) hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.[168]

U orgánů veřejné moci a veřejných subjektů je dána nerovnováha mezi správcem a subjekty údajů mj. i proto, že zákon, podle kterého se správce řídí, může stanovit omezení některých práv subjektu údajů. Pro vznik povinnosti jmenovat pověřence podle písm. b) jsou rozhodné všechny tam uvedené podmínky současně, tj. rozsáhlé pravidelné a systematické monitorování subjektů údajů je hlavní činností nebo jednou z hlavních činností správce nebo zpracovatele. Obdobně právě rozsáhlé zpracování zvláštních kategorií osobních údajů a údajů týkajících se rozsudků v trestních věcech a trestných činů jako hlavní činnost správce nebo zpracovatele zakládá povinnost jmenovat pověřence.

Jeden a týž pověřenec může současně působit u více než jednoho správce nebo zpracovatele: jediného pověřence může jmenovat skupina podniků, za podmínky, že je snadno dosažitelný z každého podniku. Jeden pověřenec může rovněž být jmenován pro několik orgánů veřejné moci nebo veřejných subjektů.[169]

Obecné nařízení předpokládá, že právo EU nebo členského státu může stanovit povinnost jmenovat pověřence i pro další správce a zpracovatele, ale také pro sdružení a jiné subjekty zastupující kategorie správců či zpracovatelů. Pověřenec pro ochranu osobních údajů pak může jednat ve prospěch sdružení a jiných subjektů zastupujících správce nebo zpracovatele. Pověřenec může být pracovníkem správce či zpracovatele, nebo plnit úkoly na základě smlouvy o poskytování služeb.[170]

[168] Čl. 37 odst. 1 obecného nařízení o ochraně osobních údajů.
[169] Čl. 37 odst. 2 a 3 obecného nařízení na ochranu osobních údajů.
[170] Čl. 37 odst. 4 obecného nařízení o ochraně osobních údajů.

Podle obecného nařízení o ochraně osobních údajů pověřenec musí být jmenován na základě svých profesních kvalit, zejména na základě svých odborných znalostí práva a praxe v oblasti ochrany údajů a své schopnosti plnit stanovené úkoly.[171]

Podmínky působení pověřence

Na jmenování pověřence navazuje plnění podmínek pro řádný výkon funkce a průběžné dosahování cílů, které působení pověřence u určitého správce, zpracovatele nebo jiného subjektu sleduje.

Ten, kdo pověřence jmenoval, má povinnost zajistit, aby pověřenec byl náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů. Pověřenci musí správce nebo zpracovatel poskytnout zdroje nezbytné k plnění těchto úkolů, k přístupu k osobním údajům a operacím zpracování a k udržování jeho odborných znalostí.[172]

Další povinností správce a zpracovatele je, aby pověřenec nedostával žádné pokyny týkající se výkonu těchto úkolů. Obecné nařízení výslovně stanoví, že pověřenec nemůže být propuštěn nebo sankcionován v souvislosti s plněním svých úkolů a že je přímo podřízen vrcholovým řídícím pracovníkům správce nebo zpracovatele.[173] Současně však může pověřenec plnit i jiné úkoly a povinnosti, správce nebo zpracovatel v takovém případě zajistí, aby žádné z těchto úkolů a povinností nevedly ke střetu zájmů. [174]

Pověřenec pro ochranu osobních údajů je v souvislosti s výkonem svých úkolů vázán tajemstvím nebo důvěrností, v souladu s právem Unie nebo členského státu.[175]

Subjekty údajů se mohou obracet na pověřence ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv podle obecného nařízení o ochraně osobních údajů.[176]

Povinnost jmenovat pověřence podle vnitrostátních předpisů v ČR

Pro zpracování v působnosti obecného nařízení o ochraně osobních údajů stanoví zákon o zpracování osobních údajů v § 14, že povinnost jmenovat pověřence mají kromě orgánů veřejné moci také orgány zřízené zákonem, které plní zákonem stanovené úkoly ve veřejném zájmu. To je třeba interpretovat tak, že ustanovení vyjasňuje okruh povinných správců. Zatímco skupina „orgánů veřejné moci" je poměrně jasná, odpovídající recitál obecného nařízení 97 hovoří jen o nich a pojem „veřejné subjekty" nerozvádí. Pojem veřejný subjekt současně není odborným pojmem ochrany osobních údajů a v zákoně o zpracování osobních údajů není

[171] Čl. 37 odst. 5 obecného nařízení o ochraně osobních údajů.
[172] Čl. 38 odst. 1 obecného nařízení o ochraně osobních údajů.
[173] Čl. 38 odst. 3 obecného nařízení o ochraně osobních údajů.
[174] Čl. 38 odst. 6 obecného nařízení o ochraně osobních údajů.
[175] Čl. 38 odst. 5 obecného nařízení o ochraně osobních údajů.
[176] Čl. 38 odst. 4 obecného nařízení o ochraně osobních údajů.

možné jej definovat, nebo vykládat v rozsahu daném zájmy např. svobodného přístupu k informacím. [177]

Povinnost zřídit funkci pověřence se upřesňuje tak, že dopadá na subjekty blížící se svou povahou orgánům veřejné moci, které plní veřejnoprávní funkce státu, aniž nutně autoritativně rozhodují o právech a povinnostech. Mezi veřejné subjekty patří Česká národní banka a Všeobecná zdravotní pojišťovna, ne však jiné zdravotní pojišťovny. Povinnost nedopadá na příspěvkové organizace a jiné pomocné instituce, protože v případech, kdy taková instituce provádí zpracování, jež vyžaduje nasazení pověřence, bude pokryta ustanoveními čl. 37 odst. 1 písm. b) nebo c) obecného nařízení (například zdravotnická nebo pečovatelská zařízení, protože provádějí systematický monitoring subjektů údajů nebo rozsáhlé zpracování citlivých údajů). Naopak pokud takové zpracování příspěvková organizace nebo jiná pomocné instituce orgánů veřejné moci nebo veřejné správy neprovádí, ani není ve zvláštním vztahu k subjektům údajů, bylo by zavádění pověřenců zbytečnou administrativní zátěží.

Zákon vychází z toho, že někteří správci, tradičně řazení spíše do veřejného sektoru, nevykazují podobný vztah se subjekty údajů jako orgány veřejné moci. Pokud však takový správce provádí jako svou hlavní činnost zpracování zahrnující rozsáhlé a systematické monitorování nebo rozsáhlé zpracování citlivých údajů nebo údajů o rozsudcích v trestních věcech a trestných činech, pověřence stejně jmenovat musí.[178] Příkladem jsou notáři a exekutoři, jejichž postupy jsou striktně vymezeny zákonem. Podobně jako u orgánů státní správy nemá subjekt údajů reálnou možnost ovlivnit, zda a jak budou jeho osobní údaje zpracovávány. Zakotvením povinnosti notáře a exekutora mít pověřence poskytuje dodatečnou ochranu subjektu údajů za situace, kdy notářské a exekutorské úřady jsou zřizovány zákonem a plní zákonem stanovené úkoly ve veřejném zájmu (např. vedení exekučního řízení, ověřování listin a podpisů atp.) a vzhledem k procesní úpravě je zpracování osobních údajů subjektu údajů nevyhnutelné.[179]

Pokud je k provedení trestněprávní směrnice povinnost jmenovat pověřence ukládána zákony, obecně upravujícími úkoly příslušných skupin spravujících orgánů, pak je povinnost oznámit kontaktní údaje pověřence Úřadu zakomponována do úkolu pověřence spolupracovat s Úřadem.

Podle zákona o Policii České republiky policejní prezident jmenuje pověřencem policistu nebo zaměstnance policie, který je odborně připraven k plnění úkolů:

a) poskytovat v policii informace a poradenství o povinnostech v oblasti ochrany osobních údajů,

[177] Důvodová zpráva k zák. č. 110/2019 Sb.
[178] § 14 zák. č. 110/2019 Sb.
[179] Důvodová zpráva k zák. č. 110/2019 Sb.

b) kontrolovat s přihlédnutím k riziku, povaze a rozsahu činností zpracování plnění povinností v oblasti ochrany osobních údajů, včetně zpřístupňování údajů, dodržování podmínek přístupu využívajících orgánů České republiky k údajům jmenné evidence cestujících, činnost příslušníka nebo zaměstnance Celní správy České republiky, pokud se podílí na vymezených činnostech zpracování osobních údajů podle hlavy III zákona o zpracování osobních údajů,
c) přijímat stížnosti a žádosti subjektů údajů související se zpracováním osobních údajů policií a s výkonem jejich práv a být v záležitostech týkajících se zpracování osobních údajů kontaktním místem pro Úřad a spolupracovat s ním.[180]

Podobně pro Celní správu České republiky zákon stanoví, že pověřencem jmenuje generální ředitel celníka nebo občanského zaměstnance, který je odborně připraven pro plnění úkolů pověřence. Generální ředitel může jmenovat jednoho pověřence pro více orgánů celní správy. Pověřenec je informován o všech připravovaných a prováděných činnostech zpracování osobních údajů orgánem celní správy, poskytuje orgánu celní správy informace a poradenství v oblasti ochrany osobních údajů, prověřuje s přihlédnutím k rizikovosti, povaze a rozsahu činností zpracování osobních údajů plnění povinností orgánu celní správy v oblasti ochrany osobních údajů, přijímá podání subjektů údajů a je v záležitostech týkajících se zpracování osobních údajů kontaktním místem pro Úřad a spolupracuje s ním.[181]

U orgánů státní moci, které se při zpracování osobních údajů řídí při plnění některých úkolů zákony implementujícími trestněprávní směrnici a současně obecným nařízením o ochraně osobních údajů, je situace složitější: Tak pro státní zastupitelství stanoví zákon o státním zastupitelství, že nejvyšší státní zástupce jmenuje pověřence pro celou soustavu státního zastupitelství; úkoly tohoto pověřence může na základě písemné dohody státního zastupitelství a Ministerstva spravedlnosti vykonávat pověřenec pro ochranu osobních údajů ministerstva. Činnost tohoto pověřence nepokrývá zpracování osobních údajů státním zastupitelstvím, které jsou nezbytné pro výkon trestní působnosti státního zastupitelství, tedy podle hlavy III zákona o zpracování osobních údajů.[182] V souladu s tím jsou na webových stránkách jednotlivých státních zastupitelství uváděny kontaktní údaje pověřence pouze pro netrestní působnost.

U soudů se s ohledem na jejich vynětí z dozorové působnosti Úřadu pro ochranu osobních údajů na základě korektní implementace ustanovení čl. 55 odst. 3 obecného nařízení o ochraně osobních údajů podle zákona o soudech a soudcích a absenci povinnosti jmenovat pověřence podle nařízení o ochraně osobních údajů ve stejném rozsahu, je působnost

[180] § 79a zák. č. 273/2008 Sb.
[181] § 57 zák. č. 17/2012 Sb.
[182] § 12k zák. č. 283/1993 Sb.

pověřence vymezena negativně, tj. tak, že nevykonává činnost ve vztahu ke zpracovávání osobních údajů soudem, které jsou potřebné pro výkon působnosti soudu při předcházení, vyhledávání a odhalování trestné činnosti a stíhání trestných činů, výkonu trestů a ochranných opatření, zajišťování bezpečnosti České republiky, veřejného pořádku a vnitřní bezpečnosti, včetně pátrání po osobách a věcech, a za účelem projednávání a rozhodování sporů a jiných věcí a pro činnosti s tím nezbytně spojené patřící do jejich pravomoci podle zákonů o občanském soudním řízení, zákonů o soudním řízení správním a v dalších případech stanovených zákonem nebo mezinárodní smlouvou – tj. s výlukou pro zpracování osobních údajů v rámci tzv. „soudních pravomocí“. Soudy se mohou písemně dohodnout, že úkoly pověřence podle obecného nařízení o ochraně osobních údajů vykonává pověřenec určený určitým soudem. Soudy a Ministerstvo spravedlnosti se mohou písemně dohodnout, že tyto úkoly vykonává pověřenec určený ministerstvem.[183]

Kvalifikační požadavky na pověřence ve veřejné správě

V České republice jsou právním předpisem stanoveny požadavky na pověřence pro ochranu osobních údajů působící v orgánech státní správy. Ve služebních úřadech má být činnost pověřence vykonávána státními zaměstnanci ve služebním poměru na dobu neurčitou, kteří vykonali úřednickou zkoušku v oboru státní služby Ochrana osobních údajů. Podle nařízení vlády č. 302/2014 Sb., o katalogu správních činností mohou být zařazeni do 12., příp. 13. platové třídy a s ohledem na povahu činnosti, která může kromě konzultací zahrnovat m. j. kontrolní činnost a řešení stížností. Osoba, která tuto funkci vykonává, musí složit zkoušku. Pro služební úřady s výjimkou Ministerstva vnitra lze v tomto oboru vykonat právě v Úřadu pro ochranu osobních údajů, který je rovněž garantem oboru státní služby „ochrana osobních údajů“.

Rovněž pro obce a územně samosprávné celky vyplývá pro pověřence pro ochranu osobních údajů z nařízení vlády č. 222/2010 Sb., o katalogu prací ve veřejných službách a správě, že je-li pověřenec zaměstnancem obce, vyplývá pro něj povinnost dosáhnout požadovaného vzdělání nepřímo ze zařazení do příslušné platové třídy. Výkon funkce pověřence je v kapitole státní správa a samospráva přiřazen referentu správy osobních údajů.

[183] § 122c zák. č. 6/2002 Sb.

15. Sankce v oblasti ochrany osobních údajů

Sankce podle obecného nařízení

Obecné nařízení přímo upravuje pouze ukládání správních pokut, jimiž jsou v České republice přestupky. Zároveň však ukládá členským státům, aby stanovily pravidla pro jiné sankce, jež se mají ukládat za porušení obecného nařízení, zejména za porušení, na něž se nevztahují správní pokuty podle čl. 83 obecného nařízení, a učinily veškerá opatření nezbytná k zajištění jejich uplatňování. Tyto sankce musí být účinné, přiměřené a odrazující.

Podmínky pro ukládání správních pokut jsou stanoveny v čl. 83 obecného nařízení. Je zde stanovena povinnost jednotlivých dozorových úřadů zajistit, aby ukládání správních pokut za porušení tohoto nařízení bylo v každém jednotlivém případě účinné, přiměřené a odrazující. Správní pokuty se ukládají podle okolností každého jednotlivého případu kromě či namísto opatření ukládaných k nápravě zjištěných nedostatků. Při rozhodování o tom, zda uložit správní pokutu, a rozhodování o výši správní pokuty v jednotlivých případech se řádně zohlední tyto okolnosti:

a) povaha, závažnost a délka trvání porušení s přihlédnutím k povaze, rozsahu či účelu dotčeného zpracování, jakož i k počtu dotčených subjektů údajů a míře škody, jež jim byla způsobena,
b) zda k porušení došlo úmyslně nebo z nedbalosti,
c) kroky podniknuté správcem či zpracovatelem ke zmírnění škod způsobených subjektům údajů,
d) míra odpovědnosti správce či zpracovatele s přihlédnutím k jimi zavedeným technickým a organizačním opatřením,
e) veškerá relevantní předchozí porušení správcem či zpracovatelem,
f) míra spolupráce s dozorovým úřadem za účelem nápravy daného porušení a zmírnění jeho možných nežádoucích účinků,
g) kategorie osobních údajů dotčené daným porušením,
h) způsob, jakým se dozorový úřad dozvěděl o porušení, zejména zda správce či zpracovatel porušení oznámil, a pokud ano, v jaké míře,
i) v případě, že vůči danému správci nebo zpracovateli byla v souvislosti s týmž předmětem dříve nařízena nápravná opatření,
j) dodržování schválených kodexů chování nebo schváleného mechanismu pro vydávání osvědčení,
k) jakoukoliv jinou přitěžující nebo polehčující okolnost vztahující se na okolnosti daného případu, jako jsou získaný finanční prospěch či zamezení ztrátám, přímo či nepřímo vyplývající z porušení.

Pokud správce nebo zpracovatel úmyslně či z nedbalosti u stejných nebo souvisejících operací zpracování poruší více ustanovení tohoto nařízení, nesmí celková výše správní pokuty překročit výši stanovenou pro nejzávažnější porušení.

Správní pokuty až do výše 10 000 000 EUR, nebo jedná-li se o podnik, až do výše 2 % celkového ročního obratu celosvětově za předchozí finanční rok, podle toho, která hodnota je vyšší, se vztahují na porušení ustanovení:

a) povinnosti správce a zpracovatele podle čl. 8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42 a 43 obecného nařízení,
b) povinnosti subjektu pro vydávání osvědčení podle článků 42 a 43,
c) povinnosti subjektu pro monitorování souladu s kodexem chování podle čl. 41 odst. 4.

Správní pokuty až do výše 20 000 000 EUR, nebo jedná-li se o podnik, až do výše 4 % celkového ročního obratu celosvětově za předchozí finanční rok, podle toho, která hodnota je vyšší, se vztahují na porušení následujících ustanovení:

a) základní zásady pro zpracování, včetně podmínek týkajících se souhlasu podle čl. 5, 6, 7 a 9,
b) práva subjektů údajů podle čl. 12 až 22,
c) předání osobních údajů příjemci ve třetí zemi nebo mezinárodní organizaci podle čl. 44 až 49,
d) jakékoli povinnosti vyplývající z právních předpisů členského státu přijatých na základě kapitoly IX,
e) nesplnění příkazu nebo dočasné či trvalé omezení zpracování nebo přerušení toků údajů dozorovým úřadem nebo neposkytnutí přístupu v rozporu s čl. 58.

Na nesplnění příkazu dozorového úřadu podle čl. 58 odst. 2 obecného nařízení se vztahují správní pokuty až do výše 20 000 000 EUR, nebo jedná-li se o podnik, až do výše 4 % celkového ročního obratu celosvětově za předchozí rozpočtový rok, podle toho, co je vyšší. Dvě sazby horní hranice správních pokut odrážejí závažnost porušení a přímo či nepřímo reflektují míru zásahu do práv chráněných obecným nařízením o ochraně osobních údajů.

Ukládání správních pokut za porušení povinností stanovených správci v obecném nařízení v České republice je zajištěno zněním § 62 zákona o zpracování osobních údajů, které zaručuje, že každé z porušení uvedených v čl. 83 obecného nařízení, je považováno za přestupek, který projednává Úřad. Ten také pokutu vybírá. Procesním předpisem je zákon č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich. Podle právního řádu České republiky se posuzuje odpovědnost za přestupek, který byl spáchán na území České republiky.[184]

[184] § 3 zák. č. 250/2016 Sb.

Možnosti, že členský stát může stanovit, zda a do jaké míry je možno ukládat správní pokuty orgánům veřejné moci a veřejným subjektům usazeným v daném členském státě, Česká republika využila. Podle § 62 odst. 5 zákona o zpracování osobních údajů Úřad upustí od uložení správního trestu, jde-li o tyto subjekty, tedy o orgány veřejné moci a veřejné subjekty. Úřad může upustit od uložení správního trestu také tehdy, pokud:

a) uloží opatření subjektu pro vydávání osvědčení podle § 54 odst. 1 písm. e) zákona o zpracováno osobních údajů,
b) podle § 60 zákona o zpracování osobních údajů uloží opatření k odstranění zjištěných nedostatků a stanoví přiměřenou lhůtu pro jejich odstranění.

Neukládání správních pokut z důvodu, že se na určité subjekty správní pokuty nevztahují na základě vnitrostátního právního předpisu, má být kompenzováno: podle ustanovení čl. 84 obecného nařízení členské státy stanoví pravidla pro jiné sankce a učiní veškerá opatření nezbytná k zajištění jejich uplatňování[185]. Rovněž tyto sankce musí být účinné, přiměřené a odrazující.

Přestupky podle zákona o zpracování osobních údajů

Zákon o zpracování osobních údajů upravuje správní trestání v oblasti ochrany osobních údajů v hlavě VI. Skutkové podstaty jsou obsaženy v § 61, 62 a 63 zákona o zpracování osobních údajů, přičemž § 62 obsahuje skutkové podstaty týkající se porušení obecného nařízení, jak je uvedeno výše.

Ust. § 62 zákona o zpracování osobních údajů stanovuje skutkovou podstatu přestupku, jehož se dopustí fyzická osoba, právnická osoba nebo podnikající fyzická osoba tím, že poruší zákaz zveřejnění osobních údajů stanovený jiným právním předpisem[186]. Za tento přestupek lze uložit pokutu do a) 1 000 000 Kč, nebo b) 5 000 000 Kč, jde-li o přestupek spáchaný tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem.

Přestupky právnických osob vzniklé porušením některé z povinností stanovených v hlavě III zákona o zpracování osobních údajů upravuje § 63. Jedná se o přestupky spáchané na úseku ochrany osobních údajů při jejich zpracování za účelem předcházení, vyhledávání a odhalování trestné činnosti, stíhání trestných činů, výkonu trestů a ochranných opatření, zajišťování bezpečnosti České republiky nebo zajišťování veřejného pořádku a vnitřní bezpečnosti, včetně pátrání po osobách a věcech. Tyto přestupky může spáchat pouze tzv. spravující orgány, kterým se ve smyslu § 24 odst. 3 zákona o zpracování osobních údajů rozumí

[185] Příkladem takové jiné sankce je ust. 180 zákona č. 40/2009 Sb., trestní zákoník, jež zakotvuje trestný čin Neoprávněného nakládání s osobními údaji.
[186] Například § 8a, § 8b odst. 1 až 4 a § 8c zákona č. 141/1961 Sb., § 52 až 54 zákona č. 218/2003 Sb., o soudnictví ve věcech mládeže, ve znění pozdějších předpisů.

orgán veřejné moci příslušný k plnění úkolu uvedeného v § 24 odstavci 1 téhož zákona, který není zpravodajskou službou nebo obecní policií. Právnická osoba se dopustí přestupku tím, že při zpracování osobních údajů v rozporu s příslušným ustanovením:

a) nestanoví účel zpracování osobních údajů nebo stanoveným účelem zpracování osobních údajů poruší povinnost nebo překročí oprávnění vyplývající z jiného zákona,
b) nepřijme opatření zajišťující, aby osobní údaje byly přesné ve vztahu k povaze a účelu jejich zpracování, uchovává osobní údaje po dobu delší než nezbytnou k dosažení účelu jejich zpracování,
c) neposkytne subjektu údajů informace v rozsahu nebo zákonem stanoveným způsobem, nevyhoví žádosti subjektu údajů,
d) nepřijme technická a organizační opatření nebo nevede jejich dokumentaci, nevede písemné přehledy o všech typových činnostech zpracování osobních údajů, nepořizuje automatizované záznamy o operacích zpracování (logy) nebo tyto záznamy využije k jinému účelu,
e) neprovede posouzení vlivu na ochranu osobních údajů nebo nepožádá Úřad o projednání připravovaného zpracování osobních údajů,
f) zasáhne do práv a právem chráněných zájmů subjektu údajů nebo způsobí jiný obdobně závažný následek pro subjekt údajů,
g) nepřijme organizační a technická opatření k zajištění odpovídající úrovně zabezpečení osobních údajů, neohlásí porušení zabezpečení osobních údajů Úřadu, neoznámí porušení zabezpečení osobních údajů subjektu údajů,
h) neprovede uložené opatření k nápravě ve lhůtě stanovené Úřadem,
i) poruší omezení zpracování zvláštních kategorií osobních údajů podle jiného právního předpisu,
j) poruší povinnost jmenovat pověřence podle jiného právního předpisu[187],
k) poruší povinnost informovat o nesprávném předání nebo o předání nepřesných osobních údajů nebo poruší některou z podmínek podle jiného právního předpisu pro předání osobních údajů do mezinárodní organizace nebo státu, který neuplatňuje právní předpisy k provedení směrnice Evropského parlamentu a Rady (EU) 2016/680, nebo poruší povinnost prověřovat potřebnost dalšího zpracování nebo vymazat osobní údaje podle jiného právního předpisu.

Přestupku se dopustí ten, kdo při zpracování osobních údajů v rozporu s příslušnými povinnostmi:

a) nevede přehledy o všech typových činnostech zpracování osobních údajů,
b) neoznámí spravujícímu orgánu porušení zabezpečení osobních údajů,

[187] K této povinnosti vizte kap. 14 této učební pomůcky.

c) nezpracovává osobní údaje pouze podle pokynů spravujícího orgánu nebo podle zákona,
d) nepořizuje automatizované záznamy o operacích zpracování (logy) nebo tyto záznamy využije k jinému účelu,
e) nepřijme organizační a technická opatření k zajištění odpovídající úrovně zabezpečení osobních údajů,
f) neprovede uložené opatření k nápravě ve lhůtě stanovené Úřadem,
g) poruší omezení zpracování zvláštních kategorií osobních údajů podle jiného právního předpisu,
h) poruší povinnost jmenovat pověřence podle jiného právního předpisu,[188]
i) poruší povinnost informovat o nesprávném předání nebo o předání nepřesných osobních údajů, poruší některou z podmínek podle jiného právního předpisu pro předání osobních údajů do mezinárodní organizace nebo státu, který neuplatňuje právní předpisy k provedení směrnice Evropského parlamentu a Rady (EU) 2016/680,
j) poruší povinnost prověřovat potřebnost dalšího zpracování nebo vymazat osobní údaje podle jiného právního předpisu.

Za spáchání některého z těchto přestupků lze uložit pokutu do 10 000 000 Kč.

Úprava správního trestání v zákoně o zpracování osobních údajů zahrnuje rovněž zvláštní ustanovení o odložení věci. Podle § 65 může Úřad věc odložit věc porušení obecného nařízení o ochraně osobních údajů usnesením, jestliže je vzhledem k významu a míře porušení nebo ohrožení chráněného zájmu, který byl činem dotčen, způsobu provedení činu, jeho následku, okolnostem, za nichž byl čin spáchán, nebo vzhledem k chování podezřelého po spáchání činu zřejmé, že účelu, jehož by bylo možno dosáhnout provedením řízení o přestupku, bylo dosaženo nebo jej lze dosáhnout jinak. Ustanovení zákona upravujícího odpovědnost za přestupky a řízení o nich týkající se vyrozumění o odložené věci se v takovém případě nepoužije.

Přestupek v souvislosti se jmenováním pověřence

Porušení povinnosti správce nebo zpracovatele podle některého z čl. 37–39, tj. při jmenování pověřence, jeho zapojení do veškerých relevantních činností a vytvoření podmínek požadovaných obecným nařízením o ochraně osobních údajů je sankcionovatelné správními pokutami. V České republice však Úřad upustí od uložení správního trestu vždy, když zjistí porušení některé z těchto povinností správcem a zpracovatelem, kteří jsou buď orgánem veřejné moci, nebo veřejným subjektem usazených v České republice.

[188] K této povinnost vizte navazující text

Nicméně porušení povinnosti právnické osoby jmenovat pověřence podle jiného právního předpisu je přestupkem dle § 63 odst. 1 písm. t) zákona č. 110/2019 Sb., za který lze uložit pokutu do 10 000 000 Kč. Takovou povinnost shodně ukládají zákon č. 273/2008 Sb., o Policii České republiky, zákon č. 341/2011 Sb., o Generální inspekci bezpečnostních sborů a o změně souvisejících zákonů, zákon č. 300/2013 Sb., o Vojenské policii a o změně některých zákonů, zákon č. 257/2000 Sb., o Probační a mediační službě, zákon č. 269/1994 Sb., o Rejstříku trestů, zákon č. 555/1992 Sb., o Vězeňské službě a justiční stráži České republiky, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, zákon č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních, a zákon č. 17/2012 Sb., o Celní správě České republiky. Tato sankce se použije pouze v návaznosti na zpracování osobních údajů podle hlavy III zákona o zpracování osobních údajů a za situace, kdy souběžně s takovým zpracováním je prováděno zpracování podle hlavy II tohoto zákona, na které dopadá povinnost pověřence jmenovat. Sankcionování pochybení, které podléhá pouze obecnému nařízení o ochraně osobních údajů, případně s doplněním o zvláštní právní úpravu, se řídí podmínkami uvedenými na začátku tohoto oddílu.

Trestní sankce

Významu chráněného práva na ochranu osobních údajů odpovídá i existence trestních sankcí. Jsou jinými sankcemi podle č. 84 obecného nařízení o ochraně osobních údajů.

V České republice je trestným činem určité neoprávněné nakládání s osobními údaji. Je jedním z trestných činů proti právům na ochranu osobnosti, soukromí a listovního tajemství a je upraveno v § 180 zákona č.40/2009 Sb., trestní zákoník, tak, že je relevantní pro zpracování osobních údajů institucemi působícími ve veřejné správě.

§ 180 Neoprávněné nakládání s osobními údaji

(1) Kdo, byť i z nedbalosti, neoprávněně zveřejní, sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje, které byly o jiném shromážděné v souvislosti s výkonem veřejné moci, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají, bude potrestán odnětím svobody až na tři léta nebo zákazem činnosti.

(2) Stejně bude potrestán, kdo, byť i z nedbalosti, poruší státem uloženou nebo uznanou povinnost mlčenlivosti tím, že neoprávněně zveřejní, sdělí nebo zpřístupní třetí osobě osobní

údaje získané v souvislosti s výkonem svého povolání, zaměstnání nebo funkce, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají.

(3) Odnětím svobody na jeden rok až pět let, peněžitým trestem nebo zákazem činnosti bude pachatel potrestán:

a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny,

b)spáchá-li takový čin tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem,

c) způsobí-li takovým činem značnou škodu, nebo

d) spáchá-li takový čin v úmyslu získat pro sebe nebo pro jiného značný prospěch.

(4) Odnětím svobody na tři léta až osm let bude pachatel potrestán:

a) způsobí-li činem uvedeným v odstavci 1 nebo 2 škodu velkého rozsahu,

b) spáchá-li takový čin v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu.

16. Povinnosti související se zabezpečením osobních údajů

Povinnosti správce

Povinnosti správce a případného zpracovatele související se zabezpečením osobních údajů jsou prvkem současného systému ochrany osobních údajů, který pronikl do obecného povědomí. S tím souvisí i skutečnost, že je referováno o únicích osobních dat, a to i v případech, kdy „únik osobních údajů“, nejčastěji jejich zveřejnění nebo zjištěné disponování takovými údaji neoprávněným subjektem, nastal v důsledku porušení povinností při zpracování osobních údajů obecně. Únik osobních údajů je něčím, čeho se nejvíce obává také široká veřejnost. Skutečnému místu zabezpečení osobních údajů v systému jejich ochrany, a to i podle obecného nařízení, odpovídá systematika obecného nařízení– ochrana osobních údajů, jejichž zpracování již započalo. Zabezpečení osobních údajů v souladu s požadavky obecného nařízení je organizačně a technicky náročná a je významnou nákladovou položkou a současně je do značné míry společnou záležitostí s kybernetickou a informační bezpečností. U naprosté většiny správců zajišťují zabezpečení osobních údajů odborníci s kvalifikací právě v informačních technologiích a kybernetické bezpečnosti.

Povinnost řádného zabezpečení osobních údajů respektuje na jedné straně rizikovost zpracovávaných osobních údajů a operací prováděných s osobními údaji, na straně druhé integruje požadavky stanovené jinými právními předpisy, zejména těch, které upravují některé aspekty kybernetické a informační bezpečnosti (platí pro všechny správce a zpracovatele) a těch, které upravují některé procesní postupy v orgánech veřejné správy. Právní požadavky a technické standardy z oblasti informačních technologií[189] jsou uloženy zákonem pro správní orgány – provozovatele informačních systémů veřejné správy, v nichž se osobní údaje zpracovávají.

Podle § 4 vyhlášky o dlouhodobém řízení informačních systémů veřejné správy[190] stanoví orgán veřejné správy v informační koncepci dlouhodobé cíle v oblasti řízení bezpečnosti informačních systémů veřejné správy; těmito cíli jsou vždy a) bezpečnost dat, která jsou v těchto systémech zpracovávána, b) bezpečnost technických a programových prostředků a c) bezpečnost služeb, které jsou prostřednictvím těchto systémů poskytovány. Pro dosažení cílů orgán veřejné správy stanoví požadavky na bezpečnost informačních systémů veřejné správy a plán řízení bezpečnosti. Podle § 10 téže vyhlášky tvoří provozní

---

[189] Např. standardy ČSN ISO/IEC řady Informační technologie, Informační technika, Bezpečnost informací a další.

[190] vyhl. č. 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy (vyhláška o dlouhodobém řízení informačních systémů veřejné správy)

dokumentaci informačního systému veřejné správy: a) bezpečnostní dokumentace informačního systému veřejné správy, b) systémová příručka a c) uživatelská příručka.

Obecná povinnost podle čl. 32 obecného nařízení, jejímiž adresáty jsou každý správce a zpracovatel, zní: „s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:

a) pseudonymizace a šifrování osobních údajů,
b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování,
c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů,
d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.“

Vyhovět těmto požadavků lze pouze individuálním postupem vůči každému prováděnému zpracování.

Jako jeden z prvků, jimiž lze doložit soulad s požadavky na zabezpečení, uvádí obecné nařízení dodržování schváleného kodexu chování nebo uplatňování schváleného mechanismu pro vydávání osvědčení.

Dalším z povinných prvků řádného zabezpečení zpracovávaných osobních údajů je, aby správce a zpracovatel přijali opatření pro zajištění toho, aby jakákoliv fyzická osoba, která jedná z jejich pověření a má přístup k osobním údajům, zpracovávala osobní údaje pouze na pokyn správce, nebo na základě povinnosti uložené právem Unie nebo členského státu. Tato opatření jsou, resp. měla by být, určována místními poměry u správce a zpracovatele.

Mimořádně významným prvkem řádného zabezpečení zpracovávaných osobních údajů jsou ohlašovací a oznamovací povinnost týkající porušení zabezpečení, které správce nebo zpracovatel zjistí. Jejich rozsah a forma jsou naopak shodné pro všechny správce a zpracovatele.

Správce má podle čl. 33 obecného nařízení povinnost ohlásit porušení zabezpečení osobních údajů bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, příslušnému dozorovému úřadu; tuto povinnost nemá, jestliže je nepravděpodobné, že by právě toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Zpracovatel má povinnost, ohlásit jím zjištění porušení bez zbytečného odkladu správci.

Ohlášení musí přinejmenším obsahovat:

a) popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů,
b) jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace,
c) popis pravděpodobných důsledků porušení zabezpečení osobních údajů,
d) popis opatření, která správce přijal nebo navrhl s cílem vyřešit porušení zabezpečení, včetně opatření ke zmírnění možných nepříznivých dopadů.

Takový rozsah povinných náležitostí ohlášení má umožnit dozorovému úřadu správně reagovat v zájmu maximální ochrany subjektu údajů a jeho práv a v zájmu dosažení stavu, kdy ohlašující správce bude postupovat v plném souladu s požadavky obecného nařízení.

Pokud se z jakéhokoliv důvodu nepodaří podat ohlášení dozorovému úřadu do 72 hodin, musí se tak stát co nejdříve a ohlášení doplnit o důvody zpoždění. To však neznamená, že správce ohlášení odloží proto, že některé skutečnosti zatím nezjistil. V takovém případě podá ohlášení odpovídající stavu k okamžiku ohlášení a dodatečná zjištění ohlásí v doplňujícím sdělení.

Druhou povinností správce je podle čl. 34 obecného nařízení při zjištěném porušení zabezpečení jím nebo jeho jménem zpracovávaných osobních údajů sdělit určité informace dotčeným subjektům údajů. Povinnost se vztahuje pouze na situace, v nichž je pravděpodobné, že posuzované porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob. Je-li tomu tak, má správce povinnost oznámit toto porušení bez zbytečného odkladu subjektu údajů. I tato povinnost má taxativně určené náležitosti. Oznámení musí používat pouze jasné a jednoduché jazykové prostředky, musí v něm být popsána povaha porušení a být uvedeny přinejmenším jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace, popis pravděpodobných důsledků porušení zabezpečení osobních údajů a popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Oznámení subjektu údajů není podle obecného nařízení vyžadováno, je-li splněna kterákoli z těchto podmínek: správce zavedl náležitá technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup, jako je například šifrování, nebo správce přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů se již pravděpodobně neprojeví. Adresné oznámení dotčeným subjektům údajů není požadováno, pokud by to vyžadovalo nepřiměřené úsilí správce. Subjekty údajů pak musí být informovány stejně účinným způsobem, za který jsou považována pouze veřejná oznámení nebo podobné (nespecifikované) opatření. Do doby, než správce porušení zabezpečení osobních údajů dotčeným subjektům údajů oznámí z vlastního rozhodnutí, může dozorový úřad po posouzení rizika požadovat po správci, aby tak učinil, nebo může rozhodnout, že je splněna některá z liberačních podmínek.

Povinnosti spravujícího orgánu

Spravující orgán je podle § 40 zákona o zpracování osobních údajů povinen přijmout taková organizační a technická opatření, aby zajistil úroveň zabezpečení osobních údajů odpovídající povaze, rozsahu, okolnostem, účelu a riziku jejich zpracování.

Při automatizovaném zpracování přijme spravující orgán nezbytná opatření k:

a) zabezpečení osobních údajů před neoprávněným přístupem, přenosem, změnou, zničením, ztrátou, odcizením, zneužitím nebo jiným neoprávněným zpracováním,
b) zajištění obnovitelnosti osobních údajů,
c) zajištění možnosti určit a ověřit osobu, která osobní údaje vložila nebo které byly prostřednictvím zařízení pro přenos údajů předány nebo zpřístupněny; k tomu se automatizovaně pořizují záznamy alespoň o operacích shromáždění, vložení, pozměnění, kombinování, nahlédnutí, předání, sdělení a výmazu osobních údajů, které umožňují určit a ověřit důvod a čas těchto operací, totožnost osoby provádějící operaci a totožnost příjemce, ledaže zjištění totožnosti těchto osob není z technických důvodů možné; tyto záznamy se uchovávají 3 roky od výmazu osobních údajů, ke kterým se vztahují,
d) zajištění bezpečnosti a spolehlivosti informačního systému s osobními údaji, včetně hlášení výskytu chyb,
e) zabránění v neoprávněném přístupu k nosiči osobních údajů nebo zařízení užívanému k jejich zpracování.

Povinnosti platí pro zpracovatele obdobně.

Zjištěné porušení zabezpečení osobních údajů ohlásí spravující orgán bez zbytečného odkladu Úřadu, ledaže je riziko neoprávněného zásahu do práv a svobod subjektu údajů nízké. Pokud spravující orgán provede ohlášení po více než 72 hodinách od okamžiku, kdy se o něm dozvěděl, připojí k němu odůvodnění tohoto prodlení. V ohlášení uvede, pokud jsou mu tyto údaje známy, alespoň a) popis povahy porušení zabezpečení osobních údajů, b) kategorie a přibližný počet subjektů údajů a záznamů osobních údajů, kterých se porušení zabezpečení týká, c) jméno a kontaktní údaje pověřence nebo jiného pracoviště, které poskytne bližší informace k porušení zabezpečení osobních údajů, d) popis pravděpodobných důsledků porušení zabezpečení osobních údajů a e) popis opatření přijatých nebo navržených spravujícím orgánem k nápravě nebo zmírnění újmy způsobené porušením zabezpečení osobních údajů.

Skutečnosti, které mu nebyly v době ohlášení známy, spravující orgán doplní bez zbytečného odkladu poté, co se o nich dozví.

Ohlašované skutečnosti sdělí spravující orgán též osobě nebo orgánu jiného členského státu Evropské unie, který osobní údaje poskytl nebo obdržel.

Obecné míře rizikovosti zpracování osobních údajů prováděného podle hlavy III zákona o zpracování osobních údajů odpovídá specifická povinnost spravujícího orgánu vést o každém porušení zabezpečení osobních údajů, jeho důsledcích a přijatých nápravných opatřeních dokumentaci a uchovávat evidenční záznam nejméně 3 roky.

Také spravující orgán má oznamovací povinnost vůči subjektům údajů dotčeným zjištěným porušením zabezpečení osobních údajů: oznámit bez zbytečného odkladu porušení zabezpečení osobních údajů subjektu údajů, pokud je riziko neoprávněného zásahu do práv a svobod subjektu údajů plynoucí z tohoto porušení vysoké. Pokud by oznámení subjektu údajů vyžadovalo nepřiměřené úsilí, spravující orgán oznámení vhodným způsobem zveřejní.

Spravující orgán není povinen porušení zabezpečení osobních údajů oznámit, pokud již provedená technická a organizační opatření zajišťují, že dotčené osobní údaje nelze zneužít, nebo následná opatření spravujícího orgánu významně snížila riziko neoprávněného zásahu do práv a svobod subjektu údajů.

O existenci vysokého rizika neoprávněného zásahu do práv a svobod subjektu údajů nebo o splnění podmínek může rozhodnout také Úřad.

Spravující orgán porušení zabezpečení subjektu údajů neoznámí, popřípadě oznámí pouze částečně, pokud jsou dány podmínky pro omezení práva subjektu údajů na přístup[191] a oznámením by došlo k ohrožení podle § 28 odst. 2 zákona o zpracování osobních údajů.

Povinnosti podle Hlavy IV zákona o zpracování osobních údajů

Také při zpracování při zpracování osobních údajů k zajišťování obranných a bezpečnostních zájmů České republiky, pokud jiný právní předpis nestanoví jinak, má správce povinnosti při zabezpečení jím zpracovávaných osobních údajů. Jsou stanoveny v §§ 46 s 47 zákona o zpracování osobních údajů. Obecně je správce je povinen přijmout taková technická a organizační opatření (dále v této kapitole též pouze *opatření*), aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení, ztrátě, neoprávněnému přenosu nebo jinému neoprávněnému zpracování nebo zneužití. Ustanovení, že *tato povinnost platí i po ukončení zpracování osobních údajů,* je třeba chápat tak, že se vztahuje na dobu prostého uchování např. pro archivní účely nebo uložení mimo režim aktivního zpracování.

Přijatá opatření k zajištění ochrany osobních údajů musí být v souladu s právními předpisy a správce o nich musí vést dokumentaci, kterou uchovává po dobu zpracování osobních údajů. Při jejich volbě správce posuzuje rizika týkající se plnění pokynů pro zpracování osobních údajů osobami, které mají bezprostřední přístup k osobním údajům, zabránění neoprávněným osobám přistupovat k osobním údajům a k prostředkům pro jejich zpracování, zabránění neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě nebo vymazání záznamů obsahujících osobní údaje a opatření, která umožní určit a ověřit, komu byly osobní údaje předány.

Stejně jako v předchozí právní úpravě platí při automatizovaném zpracování osobních údajů pro zajišťování obranných a bezpečnostních zájmů České republiky pro správce i zpracovatele povinnosti:

a) zajistit, aby systém pro automatizované zpracování osobních údajů používala pouze oprávněná fyzická osoba,
b) zajistit, aby oprávněná fyzická osoba měla přístup pouze k osobním údajům odpovídajícím jejímu oprávnění, a to na základě zvláštního uživatelského oprávnění zřízeného výlučně pro tuto osobu,
c) pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány,
d) zabránit neoprávněnému přístupu k datovým nosičům.

[191] Vizte § 28 odst. 2 zák. č. 110/2019 sb. a kap. 8 této učební pomůcky.

(Tyto povinnosti platí obdobně i pro zpracovatele).

Zaměstnanci a jiné osoby, které zpracovávají osobní údaje na základě smlouvy se správcem nebo zpracovatelem, nebo osoby, které v rámci plnění zákonem stanovených oprávnění a povinností přicházejí do styku s osobními údaji u správce nebo zpracovatele, jsou povinni zachovávat mlčenlivost o osobních údajích a o organizačních a technických opatřeních, jejichž zveřejnění by ohrozilo bezpečnost osobních údajů. Povinnost mlčenlivosti trvá i po skončení zaměstnání nebo příslušných prací.

17. Předávání osobních údajů do třetích zemí nebo mezinárodním organizacím

Hlavní zásady předávání

Mezinárodní toky osobních údajů se řídí zásadou zakotvenou v obecném nařízení (čl. 44) a sice, že úroveň ochrany osobních údajů předávaných do třetích zemí musí být srovnatelná s úrovní ochrany poskytované právem EU. Přiměřená úroveň ochrany ve třetí zemi je zajištěna buď rozhodnutím evropské Komise o odpovídající úrovni ochrany (čl. 45 obecného nařízení) nebo odpovídající úroveň ochrany zajistí sám správce/zpracovatel (vývozce) údajů přijetím vhodných záruk (čl. 46 a 47 obecného nařízení). Podrobněji viz dále. V rámci EU, resp. EHP (Evropského hospodářského prostoru) platí zásada volného pohybu osobních údajů.

Předávání jako operace zpracování

Předávání osobních údajů do třetí země je v prvé řadě součást zpracování osobních údajů, je to jedna z operací zpracování osobních údajů. Zjednodušeně lze říci, že předávání osobních údajů je **operace zpracování**, při níž osobní údaje opouštějí Evropskou unii, resp. EHP.

Specifický charakter této operace zpracování si proto vyžaduje zvláštní pozornost právní úpravy, která věnuje předávání osobních údajů do třetí země samostatnou kapitolu, konkrétně kapitolu V. (čl. 44–50) obecného nařízení.

Hlavním účelem kapitoly V. obecného nařízení je zajistit, aby úroveň ochrany zaručená obecným nařízením nebyla při předávání osobních údajů do třetích zemí nebo mezinárodním organizacím narušena čili zajistit trvalou ochranu osobních údajů poté, co byly předány do třetí země nebo mezinárodní organizaci. Základní podmínky pro jakýkoliv přenos osobních údajů jsou obsaženy v čl. 44 obecného nařízení, který je koncipován jako generální klauzule, a který vymezuje, že jakékoliv předávání údajů musí být v souladu s obecným nařízením.

V případě zpracování spadajících pod trestněprávní směrnici, je předávání upraveno v kapitole V. (čl. 35–40) této směrnice.

Definice předávání

Je řada situací, kdy nám právní úprava nedává sama o sobě jednoduchou odpověď na otázku, zda jde o předávání či nikoliv. Nabízejí se tak otázky typu: jde o předávání, když zpracovatel nebo nový správce ve třetí zemi má pouze přístup k osobním údajům? Jde o předávání při přenosu osobních údajů do třetí země správci nebo zpracovateli, který ve třetí zemi provádí zpracování podle čl. 3(2) podléhající obecnému nařízení? Jde o předávání, když se data přenáší mezi provozovnami jediného správce (nebo jediného zpracovatele) v rámci zpracování podléhajícímu čl. 3(1) obecného nařízení? Jde o předávání, když zaměstnanec na služební cestě v cizině používá služební notebook s firemním emailovou schránkou nebo jinými aplikacemi pracujícími s osobními údaji?

Těmito otázkami se zabývají Pokyny Sboru 5/2021 ke vzájemné souhře mezi čl. 3 obecného nařízení a ustanoveními o předávání osobních údajů kapitoly V. obecného nařízení, které podávají následující podrobnou upřesňující definici předávání o třech kritériích.

Předávání podle kapitoly V. je takový **přenos nebo zpřístupnění** údajů, kdy současně:

1) **vývozcem** údajů je **správce nebo zpracovatel podléhající obecnému nařízení podle čl. 3** (bez ohledu na to, zda je v EU/EHP nebo ve třetí zemi),
2) **dovozcem** údajů, kterému vývozce přenese nebo zpřístupní údaje v rámci svého zpracování, je **JINÝ správce nebo zpracovatel**, případně společný správce,
3) tento dovozce je **ve třetí zemi nebo je mezinárodní organizací**, a to bez ohledu na to, jestli tento dovozce pro dané zpracování podléhá nebo nepodléhá obecnému nařízení podle čl. 3.

První upřesnění spočívá v tom, že o předávání osobních údajů jde nejenom v případě přenosu dat, kdy data fyzicky opouštějí EU, resp. EHP a jsou přenesena na médium do třetí země, ale i v případě, kdy jsou data pouze zpřístupněna entitám ve třetí zemi, např. zpracovatelům, kteří zajišťují údržbu a servis databáze nebo jiného softwaru pracujícího s daty. Z hlediska předávání je „pouhé" zpřístupnění osobních údajů naprosto rovnocenné reálnému přenosu údajů. Předávání osobních údajů je tedy **jak fyzický přenos, tak i zpřístupnění osobních údajů** za hranice Evropské unie.

Druhé upřesnění spočívá v tom, že **právní prostor, ve kterém se uplatňuje evropská legislativa jako celek**, zahrnuje nejenom členské státy EU, ale také ty členské státy EHP, které nejsou součástí EU, ale které se smluvně připojili k uplatňování evropské legislativy včetně úpravy ochrany osobních údajů, což jsou konkrétně Norsko, Lichtenštejnsko a Island. Je třeba vzít na vědomí, že ačkoliv se v mnoha dokumentech píše zjednodušeně o předání údajů mimo EU, ve smyslu evropské legislativy ochrany osobních údajů tento právní prostor **zahrnuje vedle členských států EU i tři uvedené státy Norsko, Lichtenštejnsko a Island**.

Třetí upřesnění spočívá v tom, že vývozcem osobních údajů je jedině entita, která podléhá obecnému nařízení čili entita, která zpracovává osobní údaje jako správce nebo zpracovatel. Z tohoto upřesnění mj. vyplývá, že **situace, kdy samy subjekty údajů z EU poskytují své údaje správcům či zpracovatelům do třetí země, není předáváním** osobních údajů.

Čtvrté upřesnění spočívá v tom, že vývozcem osobních údajů jsou nejenom správci a zpracovatelé v EU, resp. v EHP, ale i správci a zpracovatelé ve třetích zemích, pokud zpracování údajů, které hodlají předat, podléhá obecnému nařízení podle čl. 3. Z tohoto upřesnění vyplývá, že **na údaje jednou předané podle kapitoly V. do třetí země se může opakovaně vztahovat kapitola V. při jejich dalším předání jiným entitám ve třetích zemích**. Např. údaje předané zpracovateli ve třetí zemi, který provádí zpracování související s nabízením služeb, a podléhá tedy obecnému nařízení podle čl. 3(2), mohou být předmětem dalších předání podléhajících kapitole V., např. když tyto údaje předá jinému dílčímu zpracovateli, který pravděpodobně bude také podléhat obecnému nařízení podle čl. 3(2), nebo jinému správci ve třetí zemi, který už bude mimo působnost obecného nařízení. Na všechna tato předání je třeba aplikovat požadavky kapitoly V. obecného nařízení.

Páté upřesnění spočívá v zásadě, že předání vyžaduje dvě oddělené entity, kdy jedna předává údaje druhé. Čili vedle vývozce zde musí být dovozce osobních údajů, který je správcem nebo zpracovatelem odlišným od vývozce. Z tohoto upřesnění vyplývá, že **zpřístupnění údajů zveřejněním není předáváním osobních údajů do třetích zemí**, protože zveřejnění nepředpokládá konkrétního dovozce údajů. Páté upřesnění rovněž zajišťuje, že **zpřístupnění osobních údajů do notebooku vlastnímu zaměstnanci, který je na zahraniční cestě, není předáním**, protože se děje v rámci jednoho správce osobních údajů. A konečně toto upřesnění také zajišťuje, že **přenos nebo zpřístupnění dat z jedné provozovny správce do jiné provozovny téhož správce podle čl. 3(1) obecného nařízení, byť sídlící ve třetí zemi, není předáváním podle kapitoly V**.

Na základě tří výše uvedených kritérií, resp. pěti výše uvedených upřesnění, lze tedy předávání osobních údajů vyčerpávajícím způsobem definovat následovně: **předávání je operace zpracování, spočívající v přenosu nebo zpřístupnění údajů ze strany správce nebo zpracovatele podléhajícího obecnému nařízení podle čl. 3 jinému správci nebo zpracovateli ve třetí zemi nebo mezinárodní organizaci.**

Podmínky legálního předávání

Základní podmínkou a zásadou danou čl. 44 obecného nařízení je podmínka, že předání lze realizovat jen v případě, když nedojde ke znehodnocení úrovně ochrany předaných osobních údajů. Jinými slovy předávání je možné jen tehdy, pokud je zajištěna ochrana osobních údajů „v zásadě srovnatelná“ (esentially equivalent) s ochranou poskytovanou osobním údajům v EU.

Právní důvody pro předávání dle obecného nařízení:

- (i) předávání založené na rozhodnutí evropské Komise o odpovídající úrovni ochrany,
- (ii) předávání založené na vhodných zárukách garantovaných správcem/vývozcem údajů,
- (iii) předávání založené na tzv. výjimkách tzn., pokud neexistuje ani rozhodnutí o přiměřenosti ani vhodné záruky.

(i) Rozhodnutí Komise o odpovídající úrovni ochrany osobních údajů (čl. 45 obecného nařízení)

Nejjednodušší je předání osobních údajů do těch třetích zemí (nebo mezinárodní organizaci, nebo určitému odvětví či oblasti v třetí zemi), které disponují rozhodnutím evropské Komise o odpovídající úrovni ochrany osobních údajů podle čl. 45 obecného nařízení. Platná rozhodnutí jsou zveřejněna v Úředním věstníku EU a na internetových stránkách Komise. V současné chvíli disponuje tímto rozhodnutím čtrnáct států a území; přičemž jejich posloupnost od nejstaršího rozhodnutí Komise k nejnovějšímu je následující: Švýcarsko, Kanada, Argentina, Guernsey, Ostrov Man, Jersey, Faerské ostrovy, Andorra, Izrael, Uruguay, Nový Zéland, Japonsko, Velká Británie a Jižní Korea.

Rozhodnutí Komise je zárukou, že tyto země jsou z hlediska ochrany osobních údajů bezpečné, takže je možné předávat osobní údaje do těchto zemí bez omezení stejně jako v rámci EU, resp. EHP.

Příkladem rozhodnutí Komise, které nepokrývaly celou zemi, ale jen určitý sektor dovozců, byla rozhodnutí Komise o odpovídající úrovni ochrany osobních údajů poskytované účastí dovozců ze Spojených států amerických v sebecertifikačním programu garantovaném americkými ministerstvy obchodu a dopravy, ať už to byl starší program Bezpečný přístav (Safe Harbor, 2000) nebo mladší Štít soukromí (Privacy Shield, 2016). Tato rozhodnutí Komise, která napadl svými žalobami rakouský aktivista Maximillian Schrems, zrušil Soudní dvůr Evropské unie v rozsudcích Schrems I (2015)[192] a Schrems II (2020)[193]. V obou případech SDEU v rozsudcích konstatoval, že Spojené státy na základě platné legislativy realizují plošný přístup státních orgánů US k osobním údajům a nezajišťují tak dostatečnou ochranu předávaným údajům (v zásadě rovnocennou úrovni v EU) ani účinnou právní ochranu subjektům údajů. Evropská Komise vyjednala v roce 2022 se zástupci Spojených států třetí variantu sebecertifikačního programu pro americké dovozce osobních údajů pod názvem Rámec ochrany soukromí (Data Privacy Framework). Dne 10. července 2023 přijala Evropská komise Prováděcí rozhodnutí ze dne 10. července 2023 podle Nařízení Evropského parlamentu a Rady (EU) 2016/679

[192] Rozhodnutí Soudního dvora Evropské unie (SDEU) ve věci C-362/14 Maximillian Schrems v. Data Protection Commissioner (tzv. Schrems I) ze dne 6. října 2015 prohlásil za neplatné rozhodnutí Komise 2000/520/ES ze dne 26. července 2000 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně poskytované podle zásad „bezpečného přístavu" a s tím souvisejících „často kladených otázek" vydaných Ministerstvem obchodu Spojených států amerických.

[193] Rozhodnutí Soudního dvora Evropské unie (SDEU) ve věci C-311/18 Data Protection Commissioner v. Facebook Ireland Limited a Maximillian Schrems (tzv. Schrems II) ze dne 16. července 2020. Toto rozhodnutí prohlásilo za neplatné Prováděcí rozhodnutí Komise ze dne 12. července 2016 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající úrovni ochrany poskytované štítem EU–USA na ochranu soukromí.

o odpovídající ochraně osobních údajů poskytované Rámcem ochrany soukromí mezi EU a USA. Komise rozhodla, že pro účely článku 45 obecného nařízení Spojené státy americké zajišťují odpovídající úroveň ochrany osobních údajů předávaných z EHP organizacím v USA, které jsou zapsány v „Seznamu Rámce ochrany soukromí“ vedeného a zveřejňovaného Ministerstvem obchodu USA.

(II) Vhodné záruky pro předávání přijaté vývozcem údajů (čl. 46, 47 obecného nařízení)

Vedle čtrnácti třetích zemí, které jsou uznány rozhodnutím Komise podle čl. 45 obecného nařízení za bezpečné, jsou všechny ostatní státy zeměmi s nedostatečnou úrovní ochrany osobních údajů. Do těchto zemí je předání osobních údajů obecně možné jen na základě vytvoření vhodných záruk podle čl. 46, 47 obecného nařízení.

Tyto vhodné záruky mohou být vytvořeny **standardními nástroji pro předávání**, vyjmenovanými v čl. 46(2) obecného nařízení (mezinárodní smlouvy, závazná podniková pravidla, standardní smluvní doložky, kodexy chování v kombinaci se závaznými a vymahatelnými závazky dovozce, certifikace v kombinaci se závaznými a vymahatelnými závazky dovozce). Pokud vývozce osobních údajů využije některý ze standardních nástrojů pro vytvoření vhodných záruk, může předání realizovat bez předchozího povolení Úřadu.

Bezesporu nejčastěji používaným nástrojem je smlouva, jejíž nedílnou součástí jsou **standardní smluvní doložky** podle rozhodnutí Komise. V současné době jsou k dispozici univerzální standardní smluvní doložky, které jsou přílohou Prováděcího rozhodnutí Komise 2021/914 ze dne 15. června 2021 o standardních smluvních doložkách pro předávání osobních údajů do třetích zemí podle nařízení 2016/679.

Tyto univerzální standardní smluvní doložky pokrývají všechny běžné scénáře předávání (předání správce-správci, správce-zpracovateli, zpracovatel-zpracovateli, zpracovatel-správci), a to tím způsobem, že vedle obecných doložek, které mají stejné ustanovení pro všechny scénáře, jsou zde modulární doložky, jejichž znění se pro jednotlivé scénáře liší, takže vývozce osobních údajů musí vybrat modul odpovídající jeho předávání.

Druhým nejčastěji používaným nástrojem jsou **závazná podniková pravidla** (Binding Corporate Rules, BCR), která jsou ideálním nástrojem pro přeshraniční předávání osobních údajů v rámci velkých nadnárodních korporací. Závazná podniková pravidla představují souhrn zásad zpracování osobních údajů přijatý skupinou podniků, který je právně závazný pro všechny členy skupiny včetně jejich zaměstnanců. Tento souhrn musí splňovat požadavky kladené na BCR článkem 47 obecného nařízení a Doporučením Sboru 1/2022, musí být schválen vedoucím dozorovým úřadem pro daná BCR, přičemž schválení je podmíněno pozitivním stanoviskem Sboru vydaným v rámci mechanismu jednotnosti podle čl. 63 obecného nařízení.

Rozlišujeme BCR pro správce, určená pro předávání osobních údajů, které jednotlivé členové skupiny zpracovávají jako správci, v rámci skupiny, a BCR pro zpracovatele, určená pro předávání v rámci skupiny, jejíž členové zpracovávají osobní údaje jako zpracovatelé pro obvykle větší množství externích správců. Seznam schválených závazných podnikových pravidel lze nalézt na internetových stránkách Sboru.

Kodexy chování a **certifikace** dovozců osobních údajů ve třetích zemích se jako nástroje pro předávání osobních údajů dosud neuplatnily, protože se teprve postupně vytvářejí podmínky a požadavky, které musejí splňovat. Tyto požadavky jsou formulovány v Pokynech Sboru 4/2021 ke kodexům chování jako nástroji pro předávání a v Pokynech Sboru 7/2022 k certifikacím jako nástroji pro předávání.

Vhodné záruky lze vytvořit i **nestandardními nástroji pro předávání**, vyjmenovanými v čl. 46(3) obecného nařízení (**nestandardní smluvní doložky**, **správní ujednání** mezi orgány veřejné moci nebo veřejnými institucemi). V jejich případě však vývozce údajů musí získat povolení, resp. schválení dozorového úřadu, jehož vydání je podmíněno pozitivním stanoviskem Sboru vydaným v rámci mechanismu jednotnosti podle čl. 63 obecného nařízení.

Článek 46 obecného nařízení o ochraně osobních údajů stanoví další vhodné záruky jako nástroje pro předávání údajů mezi veřejnými subjekty: (i) právně závazný a vymahatelný nástroj, čl. 46 odst. 2 písm. a) nebo (ii) ustanovení určená k vložení do správních ujednání, čl. 46 odst. 3 písm. b). Pokyny EDPB 2/2020[194] poskytují obecná doporučení, která mají pomoci zajistit, aby právně závazné a vymahatelné nástroje (mezinárodní smlouvy) nebo správní ujednání (memoranda o porozumění) mezi veřejnými subjekty byly v souladu s obecným nařízením o ochraně osobních údajů.

*POZOR: Rozsudek SDEU ve věci Schrems II však vnáší do předávání jeden důležitý aspekt. Použití standardních smluvních doložek případně dalších standardních nástrojů podmiňuje SDEU **testem přiměřenosti** přijatých opatření v závislosti na okolnostech předání a zemi dovozce údajů. Podle SDEU by tedy vývozce údajů při posuzování úrovně měl brát v úvahu i relevantní prvky právního řádu třetí země. Musí v konkrétním případě předávání vyhodnotit rizika, a posoudit, zda jím zvolený nástroj poskytuje dostatečné záruky, případně přijmout doplňková opatření podle Doporučení Sboru 1/2020.*

V uvedeném doporučení Sbor popisuje v několika krocích, jak má postupovat správce (příp. zpracovatel), který hodlá předávat osobní údaje do třetí země s nedostatečnou úrovní ochrany osobních údajů, aby zajistil předaným údajům ve třetí zemi úroveň ochrany „v zásadě

[194] Pokyny 2/2020 k čl. 46 odst. 2 písm. a) a čl. 46 odst. 3 písm. b) nařízení 2016/679 pro předávání osobních údajů mezi orgány veřejné moci a veřejnými subjekty v EHP a mimo EH

rovnocennou“ s unijní úrovní ochrany osobních údajů, jak ji vyžaduje ustanovení čl. 46 obecného nařízení vyložené rozhodnutím SDEU ve věci Schrems II:

1. Správce musí předně skutečně znát okolnosti svého předání a uplatnit na předání jako na samostatnou operaci zpracování všechny zásady definované čl. 5 obecného nařízení, tzn. správce musí především vědět komu a do kterých zemí hodlá data předat, musí určit účel předání osobních údajů a vymezit relevantní údaje, které je nezbytné pro naplnění stanoveného účelu předat do třetí země.

2. Správce musí zvolit jeden z nástrojů pro předání vyjmenovaných v čl. 46 obecného nařízení, přičemž, pokud správce není členem skupiny disponující schválenými závaznými podnikovými pravidly, je v současné době stále jedinou schůdnou cestou použití standardních smluvních doložek podle rozhodnutí Komise.

3. Správce musí v kontextu daného předání, nejlépe ve spolupráci s potenciálním dovozcem osobních údajů, zhodnotit, zda legislativa třetí země nenaruší úroveň ochrany předaných osobních údajů takovým způsobem, že ani použití zvoleného nástroje podle čl. 46 obecného nařízení samo o sobě nezajistí vhodné záruky ochrany předaných osobních údajů. Především se správce musí soustředit na zhodnocení otázky, zda právní řád třetí země umožňuje jejím orgánům veřejné moci přístup k předaným osobním údajům v rozsahu, který jde nad rámec toho, co je obvyklé v demokratické společnosti, v čemž mu mohou pomoci Doporučení Sboru 2/2020 k zásadním zárukám přiměřeného přístupu k osobním údajům.

4. V případě, že správce dojde k závěru, že pro dané předání do třetí země neposkytuje zvolený nástroj podle čl. 46 obecného nařízení dostatečné záruky pro zajištění „v zásadě rovnocenné“ ochrany předaných osobních údajů, musí správce, zpravidla ve spolupráci s dovozcem, přijmout doplňková opatření, která navýší záruky na požadovanou úroveň. V přílohách uvedeného Doporučení Sboru 1/2020 jsou uvedeny příklady možných technických, smluvních a organizačních opatření. Pokud správce nepřijme nebo nenalezne taková doplňková opatření, nezbude mu nic jiného než předání nerealizovat, resp. v případech již probíhajících předávání toto zastavit nebo oznámit danou skutečnost příslušnému dozorovému úřadu, který rozhodne o zastavení předávání.

5. Správce musí posléze ve vhodných intervalech znovu zhodnotit, zda v právním řádu dané třetí země nedošlo k nepříznivému vývoji vzhledem k úrovni ochrany předávaných údajů, a zda tedy není nutné nalézt a přijmout ještě jiná doplňková opatření.

(III) Výjimky pro specifické situace (čl. 49 obecného nařízení)

Ve specifických situacích, v nichž nelze předání do třetí země s nedostatečnou úrovní ochrany osobních údajů zajistit výše uvedenými vhodnými zárukami, lze předání osobních údajů realizovat na základě výjimek (tzv. derogations) podle čl. 49 obecného nařízení (výslovný souhlas, uzavření nebo plnění smlouvy se subjektem údajů, uzavření nebo plnění smlouvy v zájmu subjektu údajů, veřejný zájem, obhajoba právních nároků, ohrožení života subjektu údajů, zpřístupnění veřejného rejstříku). Aplikace těchto tzv. výjimek od zásady odpovídající úrovně ochrany pro jednotlivce v praxi defacto znamená, že jeho osobní údaje v přijímací zemi nebudou požívat ochrany, které mu jsou zaručeny obecným nařízením. Rozhodnutí o tom, zda lze v konkrétním případě uplatnit některou z výjimek, leží na samotném správci osobních údajů. Uplatnění výjimky však musí respektovat obecnou právní zásadu, podle níž musí být výjimky z obecného pravidla vykládány restriktivně, aby se výjimka nestala pravidlem. Tyto výjimky, především výjimky uzavření a plnění smlouvy a obhajoby právních nároků, lze proto aplikovat pouze příležitostně, neměly by se tedy ve vztahu k subjektu údajů uplatňovat systematicky. Bližší výklad poskytují Pokyny Sboru 2/2018 k výjimkám podle článku 49 nařízení 2016/679.

Správce by měl vždy při rozhodování, jaký nástroj pro předávání zvolí, upřednostňovat řešení, která poskytují subjektům údajů záruku, že po předání jejich údajů do třetí země budou dotčené subjekty i nadále požívat základní práva a ochranná opatření, která jsou jim garantována obecným nařízením, tzn. využít některý z výše uvedených standardizovaných nástrojů. Naopak k výjimkám by měl přistoupit pouze v případech, kdy jsou rizika pro subjekt údajů v souvislosti s předáváním jejich osobních údajů malá, nebo kdy nad právem subjektu údajů na soukromí převládají jiné zájmy (veřejné zájmy nebo zájmy samotného subjektu údajů).

18. Úřad pro ochranu osobních údajů a další dozorové orgány v ČR: postavení, působnost, úkoly a pravomoci

Úřad pro ochranu osobních údajů (dále v této kapitole pouze „Úřad“) je v České republice jediným dosud zřízeným dozorovým úřadem podle obecného nařízení o ochraně osobních údajů a je rovněž určeným úřadem podle trestněprávní směrnice. Je rovněž jediným dosud oznámeným dozorovým orgánem podle čl. Úmluvy č. 108; při ratifikaci Úmluvy bylo v souladu s článkem 13 Úmluvy učiněno oznámení České republiky, že pověřeným úřadem je Úřad.[195] Všechny mezinárodní předpisy kladou na státy, které k nim přistoupily, nebo se na ně vztahují na jiném principu, požadavek nezávislosti a nadání určitými pravomocemi. To znamená, že příslušný stát jednotlivá ustanovení implementuje ve vnitrostátním právu. V České republice je v současné době základním implementujícím předpisem zákon o zpracování osobních údajů.

Úřad je ústředním správním úřadem, se všem i z toho vyplývajícími institucionálními důsledky.[196]

Úřad a subjekty údajů

Cílům obecného nařízení o ochraně osobních údajů a povaze i obsahu prováděného základního práva odpovídá, že subjekt údajů je nadán právem obrátit se na příslušný dozorový úřad a podat mu podnět nebo stížnost. V České republice se podávání, přijímání a vyřizování podnětů a stížností řídí správním řádem.

§ 42 zák. č. 500/2004 Sb., správní řád

Přijímání podnětů k zahájení řízení

Správní orgán je povinen přijímat podněty, aby bylo zahájeno řízení z moci úřední. Pokud o to ten, kdo podal podnět, požádá, je správní orgán povinen sdělit mu ve lhůtě 30 dnů ode dne, kdy podnět obdržel, že řízení zahájil, nebo že neshledal důvody k zahájení řízení z moci úřední, popřípadě že podnět postoupil příslušnému správnímu orgánu. […]

Postup Úřadu v reakci na podnět podaný subjektem údajů nebo kýmkoli jiným odpovídá tomu, že v ČR není veřejné subjektivní právo na to, aby správní orgán zahájil z moci úřední nějaké řízení. Na podnět podaný podle obecného nařízení o ochraně osobních údajů lze použít kteroukoli z pravomocí Úřadu podle čl. 58.

Každý dozorový úřad má usnadňovat podávání stížností opatřeními, jako je poskytnutí formuláře pro podávání stížností, který lze vyplnit i v elektronické formě. Provádění úkolů

[195] Sdělení Ministerstva zahraničních věcí č. 115/2001 Sb. m. s. uvádělo jako sídlo Úřadu, Havelkova 22, 130 00 Praha 3; aktuální sídlo Úřadu je Pplk. Sochora 27, 170 00 Praha 7.
[196] Důvodová zpráva k zák. č. 110/2019 Sb.

dozorového úřadu je pro subjekty údajů bezplatné. Nicméně jestliže jsou požadavky zjevně nedůvodné nebo nepřiměřené, zejména protože se opakují, může dozorový úřad uložit přiměřený poplatek na základě svých administrativních nákladů nebo odmítnout žádosti vyhovět. Zjevnou nedůvodnost nebo nepřiměřenost žádosti dokládá úřad.

K provedení trestněprávní směrnice se ve vztahu k právům dotčeného subjektu údajů vzájemný vztah subjektu údajů a dozorového úřadu řídí § 31 zákona o zpracování osobních údajů. Subjekt údajů může podat podnět k ověření zákonnosti zpracování osobních údajů a Úřad může na jeho základě zákonnost zpracování osobních údajů ověřit. Podnětu Úřad nemusí vyhovět zejména, pokud doloží, že podnět je zjevně nedůvodný nebo nepřiměřený, například proto, že se v krátké době v téže věci opakuje. Do 4 měsíců ode dne podání podnětu o ověření zákonnosti zpracování osobních údajů Úřad informuje subjekt údajů, zda zákonnost ověřil a pokud tak neučinil, připojí k informaci odůvodnění svého postupu. I ve vztahu ke zpracování osobních údajů podle hlavy III zákona o zpracování osobních údajů Úřad rovněž informuje subjekt údajů také o možnosti žádat o soudní ochranu.

Úkoly a činnosti Úřadu

Ve vztahu ke zpracováním osobních údajů podle obecného nařízení o ochraně osobních údajů jsou úkoly stanoveny v čl. 57 a pravomoci v čl. 58 a provedeny v § 54 zákona o zpracování osobních údajů, kde jsou upraveny zejména procesní aspekty.

Základní úkoly dozorového úřadu jsou:

a) monitorovat a vymáhat uplatňování obecného nařízení,
b) zvyšovat povědomí veřejnosti o rizicích, pravidlech, zárukách a právech v souvislosti se zpracováním,
c) v souladu s právem členského státu poskytovat poradenství vnitrostátnímu parlamentu, vládě a dalším orgánům a institucím ohledně legislativních a správních opatření týkajících se ochrany práv a svobod fyzických osob v souvislosti se zpracováním osobních údajů,
d) podporovat povědomí správců a zpracovatelů o jejich povinnostech,
e) poskytovat na požádání všem subjektům údajů informace ohledně výkonu jejich práv podle obecného nařízení a případně spolupracovat s dozorovými úřady v jiných členských státech EU,
f) zabývat se stížnostmi, které mu podá subjekt údajů nebo jiný oprávněný subjekt, a ve vhodné míře prošetřit předmět stížnosti a v přiměřené lhůtě informovat stěžovatele o vývoji a výsledku šetření,
g) spolupracovat s dalšími dozorovými úřady, mimo jiné formou sdílení informací, a s těmito úřady si vzájemně poskytovat pomoc,
h) provádět šetření o uplatňování obecného nařízení,

i) monitorovat vývoj v relevantních oblastech, pokud má vliv na ochranu osobních údajů, zejména vývoj informačních a komunikačních technologií a obchodních praktik,
j) přijímat standardní smluvní doložky uvedené v čl. 28 odst. 8 a čl. 46 odst. 2 písm. d),
k) připravit a udržovat seznam v souvislosti s posouzením vlivu na ochranu osobních údajů podle čl. 35 odst. 4 a poskytovat poradenství o operacích zpracování uvedených v čl. 36 odst. 2,
l) podporovat vypracování kodexů chování podle čl. 40, vydávat stanoviska a schvalovat kodexy chování, které poskytují dostatečné záruky,
m) vybízet k zavedení mechanismů pro vydávání osvědčení o ochraně údajů a pečetí a známek dokládajících ochranu údajů podle čl. 42 odst. 1 a schvalovat kritéria pro vydávání osvědčení, popř. pravidelně přezkoumávat osvědčení vydaná v souladu s čl. 42 odst. 7,
n) navrhovat a zveřejňovat požadavky na akreditaci subjektu pro monitorování kodexů chování a subjektu pro vydávání osvědčení,
o) schvalovat subjekty pro monitorování kodexů chování a subjekty pro vydávání osvědčení,
p) schvalovat smluvní doložky a ustanovení uvedená v čl. 46 odst. 3 a závazná podniková pravidla podle čl. 47,
q) přispívat k činnostem Evropského sboru pro ochranu osobních údajů (EDPB),
r) vést interní záznamy o porušeních tohoto nařízení a o opatřeních přijatých podle čl. 58 odst. 2,
s) plnit veškeré další úkoly související s ochranou osobních údajů.

Členské státy musí zajistit, že každý dozorový úřad má všechny taxativně určené vyšetřovací, nápravné, povolovací a poradní pravomoci. Toto rozdělení pravomocí je věcí evropského práva a nelze jej automaticky přenášet do práva vnitrostátního (např. sankce nejsou v ČR nápravnými opatřeními). Adaptační normy se naopak drží smyslu jednotlivých pravomocí a jejich koncepčního uchopení ve vnitrostátních předpisech. Úřad typicky postupuje podle správního řádu.[197]

Přímo z obecného nařízení má každý dozorový úřad, který je zřízen k plnění úkolů podle něho následující pravomoci.

1. Vyšetřovací pravomoci:

- nařídit správci a zpracovateli, případně zástupci správce nebo zpracovatele, aby mu poskytli veškeré informace, které potřebuje k plnění svých úkolů,

[197] Důvodová zpráva k zák. č. 110/2019 Sb.

- provádět vyšetřování formou auditů ochrany údajů[198],
- provádět přezkum osvědčení vydaných v souladu s čl. 42 odst. 7,
- ohlásit správci nebo zpracovateli údajné porušení tohoto nařízení,
- získat od správce a zpracovatele přístup ke všem osobním údajům a ke všem informacím, které potřebuje k výkonu svých úkolů,
- získat přístup do všech prostor, v nichž správce a zpracovatel působí, včetně přístupu k veškerému zařízení a prostředkům určeným ke zpracování údajů, v souladu s procesním právem Unie nebo členského státu.

2. Nápravné pravomoci:

- upozornit správce či zpracovatele, že zamýšlené operace zpracování pravděpodobně porušují toto nařízení,
- udělit napomenutí správci či zpracovateli, jehož operace zpracování porušily toto nařízení,
- nařídit správci nebo zpracovateli, aby vyhověli žádostem subjektu údajů o výkon jeho práv podle tohoto nařízení,
- nařídit správci či zpracovateli, aby uvedl operace zpracování do souladu s tímto nařízením, a to případně předepsaným způsobem a ve stanovené lhůtě,
- nařídit správci, aby subjektu údajů oznámil případy porušení zabezpečení osobních údajů,
- uložit dočasné nebo trvalé omezení zpracování, včetně jeho zákazu,
- nařídit opravu či výmaz osobních údajů nebo omezení zpracování podle čl. 16, 17 a 18 a ohlašování takových opatření příjemcům, jimž byly osobní údaje zpřístupněny podle čl. 17 odst. 2 a čl. 19;
- odebrat osvědčení nebo nařídit, aby subjekt pro vydávání osvědčení odebral osvědčení vydané podle čl. 42 a 43, nebo aby osvědčení nevydal, pokud požadavky na osvědčení plněny nejsou nebo již přestaly být plněny,
- uložit správní pokutu podle čl. 83 vedle či namísto opatření uvedených v tomto odstavci, podle okolností každého jednotlivého případu,
- nařídit přerušení toků údajů příjemci ve třetí zemi nebo toků údajů mezinárodní organizaci.

3. Povolovací a poradní pravomoci:

- poskytovat poradenství správci v souladu s postupem předchozí konzultace podle čl. 36,

[198] V současné době není provádění auditů ochrany údajů nijak standardizováno; v ČR je na místě používat termín *kontrola*.

- z vlastního podnětu nebo na požádání vydávat stanoviska určená vnitrostátnímu parlamentu, vládě členského státu nebo dalším institucím a subjektům, jakož i veřejnosti, ohledně otázek souvisejících s ochranou osobních údajů,
- povolovat zpracování uvedené v čl. 36 odst. 5, pokud právo členského státu takové předchozí povolení vyžaduje,
- vydávat stanoviska a schvalovat návrhy kodexů chování podle čl. 40 odst. 5,
- akreditovat subjekty pro vydávání osvědčení podle čl. 43,
- vydávat osvědčení a schvalovat kritéria pro vydávání osvědčení podle čl. 42 odst. 5,
- přijímat standardní doložky o ochraně údajů podle čl. 28 odst. 8 a čl. 46 odst. 2 písm. d),
- povolovat smluvní doložky podle čl. 46 odst. 3 písm. a),
- povolovat správní ujednání podle čl. 46 odst. 3 písm. b),
- schvalovat závazná podniková pravidla podle čl. 47.

Pro vyšetřovací pravomoci § 54 zákona o zpracování osobních údajů stanoví, že Úřad postupuje podle kontrolního řádu, který kromě jiného zaručuje oprávnění Úřadu podle posledních dvou vyšetřovacích pravomocí.

Další ustanovení zajišťují nápravné a povolovací a poradní pravomoci: Úřad může správce vyzvat k vyjasnění nebo nápravě, sdělením upozornit správce nebo zpracovatele, že zamýšleným zpracováním osobních údajů zřejmě poruší své povinnosti, stanovit vyhláškou kritéria nebo požadavky podle čl. 41 odst. 3, čl. 42 odst. 5 nebo čl. 43 odst. 1 písm. b) obecného nařízení, nařídit subjektu pro vydávání osvědčení, aby odebral osvědčení, které tento subjekt vydal podle čl. 42 a 43 obecného nařízení, schvaluje kodexy chování a zveřejňuje způsobem umožňujícím dálkový přístup standardní smluvní doložky přijaté podle čl. 28 odst. 8 nebo čl. 46 odst. 2 písm. d) obecného nařízení.

Ukládání nápravných opatření včetně omezení zpracování je upraveno v § 60 zákona o zpracování osobních údajů a platí pro všechny správce a spravující orgány, na něž se vztahuje dozorová působnost Úřadu. Ta nezahrnuje pouze soudy nebo státní zastupitelství, pokud postupují podle hlavy III tohoto zákona a zpravodajské služby.

Při zjištěném porušení povinnosti může Úřad uložit opatření k odstranění zjištěných nedostatků a stanovit přiměřenou lhůtu pro jejich odstranění. Ukládání správních pokut je věnována kap. 15 této učební pomůcky.

Ve vztahu ke zpracování osobních údajů podle hlavy III, nejde-li o zpracování osobních údajů prováděné soudy a státními zastupitelstvími, zákon o zpracování osobních údajů stanoví, že Úřad:

a) provádí dozor nad dodržováním povinností stanovených zákonem při zpracování osobních údajů,

b) ověřuje zákonnost zpracování osobních údajů na podnět subjektu údajů podle § 31,
c) přijímá podněty a stížnosti na porušení povinností stanovených zákonem při zpracování osobních údajů a informuje o jejich vyřízení,
d) projednává přestupky a ukládá pokuty,
e) poskytuje konzultace v oblasti ochrany osobních údajů,
f) informuje veřejnost o rizicích, pravidlech, zárukách a právech v souvislosti se zpracováním osobních údajů,
g) informuje správce a zpracovatele o jejich povinnostech v oblasti ochrany osobních údajů,
h) vykonává další působnost stanovenou mu zákonem.

Úřad dále každoročně vypracovává, Parlamentu ČR a vládě předkládá a veřejnosti zpřístupňuje výroční zprávu o své činnosti, zajišťuje plnění požadavků vyplývajících z mezinárodních smluv, jimiž je Česká republika vázána, a z přímo použitelných předpisů Evropské unie, a i bez žádosti poskytuje Parlamentu ČR vyjádření k návrhu právního předpisu, který upravuje zpracování osobních údajů.

Požadavek umožnit dozorovému úřadu obracet se na justiční orgány je saturován možností obrátit se na státní zastupitelství prostřednictvím podání trestního oznámení (v souvislosti se speciální skutkovou podstatou v § 180 trestního zákoníku.[199]

Úkolem Úřadu je rovněž podílet se na činnosti Evropského sboru pro ochranu osobních údajů, spolupracovat s obdobnými úřady jiných států, s orgány Evropské unie a s orgány mezinárodních organizací působícími v oblasti ochrany osobních údajů.

V souladu s tím, že členský stát EU může v právních předpisech stanovit, že jeho dozorový úřad má další pravomoci, jež však nesmí narušit účinné fungování vnitrounijní spolupráce a mechanismus jednotnosti, má Úřad dílčí působnost pro šíření obchodních sdělení podle zák. č. 480/2004 Sb., o některých službách informační společnosti.

Dílčí působnost v oblasti svobodného přístupu k informacím je stanovena zák. č. 106/1999 Sb. a působnost v základních registrech v zákonu o základních registrech.[200]
Některé zákony kromě toho výslovně stanoví působnost Úřadu v ochraně osobních údajů: zákon o elektronických komunikacích stanoví, že dozor nad dodržováním povinností při zpracování osobních údajů podle tohoto zákona vykonává Úřad; zákon o regulaci reklamy, že pro nevyžádanou reklamu šířenou elektronickými prostředky je Úřad orgánem příslušným k výkonu dozoru nad dodržováním tohoto zákona a konečně zákon o ochraně spotřebitele,

[199] Důvodová zpráva k zák. č. 110/2019; k § 180 trestního zákoníku vizte kap. 15 této učební pomůcky.
[200] K tomu blíže kap. 2 této učební pomůcky.

že dozor nad dodržováním povinností při zpracování osobních údajů stanovených v části páté tohoto zákona provádí Úřad.

Oprávnění Úřadu na přístup k informacím a mlčenlivost

Úřad je oprávněn seznamovat se se všemi informacemi nezbytnými pro plnění konkrétního úkolu. Pro informace chráněné povinností mlčenlivosti podle jiného právního předpisu platí podmínky tam stanovené. Např. kontrolující je povinen prokázat oprávnění k přístupu k utajované informaci.[201]

Výjimky stanoví zákon pro informace chráněné povinností mlčenlivosti podle zákona o advokacii a podle zákona o daňovém poradenství a Komoře daňových poradců České republiky. S nimi je Úřad oprávněn se seznamovat pouze za přítomnosti a se souhlasem zástupce České advokátní komory, resp. podle zákona o daňovém poradenství a Komoře daňových poradců České republiky, v režimu stanoveném zákonem o zpracování osobních údajů. V obou případech platí, že odmítne-li zástupce komory souhlas udělit, bezodkladně zajistí na písemnou žádost Úřadu důvěrnost a neporušenost informací podle věty první a bezodkladně předá kontrolní radě komory písemnou žádost Úřadu o nahrazení souhlasu zástupce komory rozhodnutím kontrolní rady komory. Nerozhodne-li kontrolní rada komory o žádosti Úřadu tak, že nahrazuje souhlas zástupce komory, ve lhůtě 30 dnů ode dne doručení žádosti zástupcem komory, lze souhlas zástupce komory nahradit na návrh Úřadu rozhodnutím soudu podle zákona o zvláštních řízeních soudních.

Úřad vyloučí z nahlížení do spisu informace, které jsou obchodním, bankovním nebo jiným obdobným zákonem chráněným tajemstvím, informace, které požívají autorskoprávní ochrany, a informace chráněné podle jiného předpisu. Úřad zpřístupní účastníkovi řízení informace vyloučené podle věty první, pokud jimi byl nebo bude proveden důkaz. Před zpřístupněním informace musí být účastník řízení nebo jeho zástupce poučen o ochraně, kterou informace požívá. Právo na přístup k takovým informacím nezahrnuje právo činit si výpisy nebo právo na pořízení kopií informací.

Místopředseda a zaměstnanci Úřadu jsou povinni zachovávat mlčenlivost o osobních údajích, o informacích podle § 58 odst. 4 zákona o zpracování osobních údajů, jakož i o organizačních a technických opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů, se kterými se seznámili při výkonu působnosti Úřadu nebo v souvislosti s ní. Tato povinnost trvá i po skončení služebního nebo pracovního poměru. Povinnosti zachovávat mlčenlivost může místopředsedu Úřadu a zaměstnance zprostit předseda Úřadu nebo jím pověřená osoba.

[201] Podle zák. č. 412/2005 Sb.

Povinnosti zachovávat mlčenlivost se nelze dovolávat vůči Úřadu. Vůči orgánu činnému v trestním řízení nebo soudu se jí lze dovolávat pouze tehdy, pokud by se povinnosti mlčenlivosti v daném případě mohl dovolávat ten, jemuž byla zákonem uložena a od něhož informace chráněná povinností mlčenlivosti pochází. Subjektu údajů lze osobní údaje sdělit, pouze pokud tímto sdělením nedojde k ohrožení chráněného zájmu uvedeného v § 6 odst. 2 zákona o zpracování osobních údajů.

19. Omezení práv a povinností podle čl. 23 obecného nařízení o ochraně osobních údajů a podle čl. 15 směrnice 680/2016 v zákoně o zpracování osobních údajů

Omezení podle čl. 23 obecného nařízení v zákoně o zpracování osobních údajů

Obecné nařízení o ochraně osobních údajů není uzavřeným předpisem. Předpokládá vydání několika prováděcích předpisů, k nimž zmocňuje Komisi[202]. Kromě toho přímo vtahuje do obsahu otevřenou množinu unijních a vnitrostátních (národních) právních předpisů.

V obecném nařízení se tak děje zejména, nikoli však výlučně, v čl. 23. Stejného účinku je dosahováno dalšími zmocňovacími ustanovení pro právo Unie nebo členského státu,[203] článek 23 je významný proto, že vymezuje obecný rámec pro výjimky z povinností správců a zpracovatelů a z práv subjektů údajů. Současně klade na takové výjimky – tedy omezení rozsahu konkrétní povinnosti nebo konkrétního práva subjektu údajů – formální požadavky na právní předpisy sahající od ústavnosti až taxativní výčet minimálních obsahových parametrů. Pro nositele veřejné moci v České republice má mimořádný dosah, protože výjimky nejsou neobvyklé. Tyto výjimky a omezení obsahují jak přímo proveditelné předpisy EU (např. čl. 7 nařízení EP a Rady (EU) 2021/953 o rámci pro vydávání, ověřování a uznávání interoperabilních certifikátů o očkování, o testu a o zotavení v souvislosti s onemocněním COVID-19 (digitální certifikát EU COVID) za účelem usnadnění volného pohybu během pandemie COVID-19 nebo čl. 31 a 32 nařízení EP a Rady (EU) 2021/2303 o zřízení Agentury Evropské unie pro otázky azylu), tak české zákony. Některé byly zavedeny současně s přijetím zákona o zpracování osobních údajů (např. § 59a daňového řádu, § 165 zákona o doplňkovém penzijním připojištění, § 22c zákona o kybernetické bezpečnosti, §§ 56a a 56b zákona o zdravotních službách), jiné již dříve nebo naopak později (např. § 63 zákona o občanských průkazech).

Takové předpisy mohou omezit výhradně rozsah povinností a práv uvedených v čl. 12 až 22 a v čl. 34, ale také v čl. 5, v rozsahu, v jakém ustanovení tohoto čl. odpovídají právě právům a povinnostem stanoveným v čl. 12 až 22. Základním požadavkem je, aby omezení respektovalo podstatu základních práv a svobod a současně představovalo nezbytné a přiměřené opatření v demokratické společnosti s cílem zajistit jeden z osmi cílů; poměrně významný aplikační problém představuje to, že cíl není v každé situaci možné ztotožnit s účelem sledovaným posuzovaným zpracováním osobních údajů. Výsledek a parametry posuzování se mění v čase

[202] Vizte např. kap. 17 a 20 této učební pomůcky.
[203] Zmocňující ustanovení společně s požadavky kladenými na vnitrostátní právní úpravu obsahují např. čl. 85 – 89. Dále k tomu vizte též kap. 3 této učební pomůcky, oddíl Zpracování k jinému účelu („slučitelnost účelů“).

a jak je v ochraně osobních údajů normou, je to vývoj poměrně dynamický. Stačí vzít za příklad přístup k nezbytnosti a přiměřenosti otisků prstů v identifikačních dokladech[204] – nařízení (EU) 2019/1157 o posílení zabezpečení průkazů totožnosti občanů Unie a povolení k pobytu vydávaných občanům Unie a jejich rodinným příslušníkům, kteří vykonávají své právo volného pohybu deklaruje v recitalu 46 cíl *zvýšení bezpečnosti a zjednodušení výkonu práva na volný pohyb občanů Unie a jejich rodinných příslušníků*, a konstatuje, že tohoto *cíle nemůže být dosaženo uspokojivě členskými státy, ale spíše jich z důvodu rozsahu a účinků může být lépe dosaženo na úrovni Unie a* […] že nařízení *nepřekračuje rámec toho, co je nezbytné pro dosažení těchto cílů.*

Povinnosti správců a zpracovatelů a práva subjektu údajů lze omezit pro kterýkoli z těchto cílů:

a) národní bezpečnost,
b) obranu,
c) veřejnou bezpečnost,
d) prevenci, vyšetřování, odhalování či stíhání trestných činů nebo výkon trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení,
e) jiné důležité cíle obecného veřejného zájmu Unie nebo členského státu, zejména důležitý hospodářský nebo finanční zájem Unie nebo členského státu, včetně peněžních, rozpočtových a daňových záležitostí, veřejného zdraví a sociálního zabezpečení,
f) ochranu nezávislosti soudnictví a soudních řízení,
g) prevenci, vyšetřování, odhalování a stíhání porušování etických pravidel regulovaných povolání,
h) monitorovací, inspekční nebo regulační funkci spojenou, i pouze příležitostně, s výkonem veřejné moci v případech uvedených v písmenech a), b), c), d), e) a g),
i) ochranu subjektu údajů nebo práv a svobod druhých,
j) vymáhání občanskoprávních nároků.

Na právní předpis je dále kladen požadavek, aby obsahoval, pokud je to relevantní, zejména konkrétní ustanovení vymezující alespoň účely zpracování nebo kategorie zpracování; kategorie osobních údajů; rozsah zavedených omezení; záruky proti zneužití údajů nebo protiprávnímu přístupu nebo předání; správce nebo kategorie správců; dobu uložení a platné záruky s ohledem na povahu, rozsah a účely zpracování nebo kategorie zpracování; rizika z hlediska práv a svobod subjektů údajů a právo subjektů údajů být informováni o daném omezení, pokud toto informování nemůže být na újmu účelu omezení.

[204] Zák. č.261/2021 Sb., nebo zák. č. 326/1999 Sb.

Omezení podle čl. 23 obecného nařízení o ochraně osobních údajů v dalších zákonech

Současná legislativní praxe v České republice standardně nevymezuje rizika v normativním textu, ale v důvodové zprávě (odůvodnění); normativní text má obsahovat záruky kompenzující nebo odstraňující rizika identifikovaná v části Zhodnocení současného stavu a dopadů navrhovaného řešení ve vztahu k ochraně soukromí a osobních údajů. Vše ostatní by měl obsahovat v normativní podobě vlastní právní předpis.

Např. daňový řád stanoví, že právo na přístup k osobním údajům zpracovávaným při správě daní uplatňuje daňový subjekt v rozsahu a způsobem stanoveným pro nahlížení do spisu nebo nahlížení do osobních daňových účtů; obdobně se postupuje při uplatnění práva třetí osoby na přístup k osobním údajům zpracovávaným při správě daní. Při uplatnění práva na námitku nebo jiného prostředku ochrany proti zpracování osobních údajů se použijí obdobně ustanovení o stížnosti.[205]

Podle zákona o kybernetické bezpečnosti pokud Národní úřad pro kybernetickou a informační bezpečnost nebo provozovatel národního CERT v rámci činnosti, na kterou se vztahuje obecné nařízení o ochraně osobních údajů obdrží při řešení kybernetického bezpečnostního incidentu nebo kybernetické bezpečnostní události anebo při prevenci kybernetických hrozeb nebo rizik osobní údaje, které zpracovává pouze za účelem plnění povinností podle tohoto zákona, pak po dobu plnění těchto povinností nemusí poskytovat subjektu údajů informace o opravách nebo výmazu osobních údajů nebo omezení zpracování, zajistit přístup subjektu údajů k osobním údajům, nebo opravit či doplnit osobní údaje na žádost subjektu údajů.[206]

Kromě toho zákon o zpracování osobních údajů stanoví v § 13 v přímé návaznosti na omezení některých práv subjektu údajů obecnou možnost osobní údaje dále předávat: *Pokud bylo zpracování osobních údajů omezeno podle čl. 18 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2016/679, není tím dotčena povinnost správce nebo zpracovatele tyto osobní údaje předat nebo zpřístupnit, je-li tato povinnost stanovena právním předpisem. Tyto údaje se při předání nebo zpřístupnění označí jako údaje uvedené v čl. 18 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2016/679.*

Omezení práv a povinností podle čl. 15 směrnice 680/2016 v zákoně o zpracování osobních údajů

Trestněprávní směrnice vytváří prostor pouze pro omezení jediného z práv subjektu údajů. V čl. 15 se členským státům umožňuje přijmout právní úpravu, která přístup subjektů údajů k informacím úplně nebo částečně omezuje, a to v takovém rozsahu a na takovou dobu, jak

[205] § 59a zák. č. 280/2009 Sb., daňový řád
[206] § 22c zák. 181/2014 Sb.

je to v demokratické společnosti s náležitým přihlédnutím k základním právům a oprávněným zájmům dotčené fyzické osoby nutné a přiměřené. Toto omezení musí sledovat výhradně některý z pěti cílů:

a) zabránit maření úředních nebo právních šetření, vyšetřování nebo postupů,
b) zabránit nepříznivému ovlivňování prevence, odhalování, vyšetřování či stíhání trestných činů nebo výkonu trestů,
c) chránit veřejnou bezpečnost,
d) chránit národní bezpečnost,
e) chránit práva a svobody druhých.

Tyto cíle se většinově překrývají s cíli pro výjimky a omezení podle obecného nařízení o ochraně osobních údajů; jediným unikátním cílem je cíl pod písm. b). Cíl pod písm. d) přesahuje působnost trestněprávní směrnice a nespadá ani do působnosti obecného nařízení o ochraně osobních údajů.[207]

Umožňující ustanovení pro členské státy připouští, aby omezení byla cílena na *kategorie zpracování*, aniž by byl tento pojem upřesněn. Zavedená omezení práva subjektu údajů musí být kompenzována jeho informováním o odmítnutí nebo omezení přístupu a o důvodech takového postupu. Tyto informace není třeba uvádět, pokud by jejich poskytnutí ohrožovalo některý z výše uvedených pěti účelů. Členské státy musí stanovit, že správce informuje subjekty údajů o možnosti podat stížnost u dozorového úřadu nebo žádat soudní ochranu. Správci má být uložena povinnost dokumentovat věcné či právní důvody, na nichž se rozhodnutí zakládá a tyto informace zpřístupnit dozorovým úřadům.

V České republice jsou tato ustanovení provedena v §§ 28 a 30 zákona o zpracování osobních údajů.

[207] Vizte kap. 5 této učební pomůcky.

20. Kodexy chování a vydávání osvědčení

Obecné nařízení zdůrazňuje větší odpovědnost správců a zpracovatelů za jimi prováděná zpracování osobních údajů. K zajištění tohoto účelu definovalo v rámci zajištění ochrany osobních údajů nepovinné nástroje, umožňující správcům nebo zpracovatelům zajistit nezávislé a nestranné vyhodnocení souladu jimi prováděných (operací) zpracování s obecným nařízením. Jedná se o kodexy chování a vydávání osvědčení o ochraně údajů.

Kodexy chování

Komu je kodex určen a kdo ho předkládá

Kodex chování je určen **skupině správců nebo zpracovatelů stejného typu** (např. cestovní kanceláře, zdravotnická zařízení, pojišťovny, banky, energetika apod.). Kodex spravuje (předkládá) určený subjekt (obchodní a zastupující sdružení, odvětvové organizace, akademické organizace, zájmové skupiny apod.) **tzv. držitel kodexu,** který musí prokázat, že je účinným zastupujícím orgánem (např. počet potencionálních členů kodexu). Měl by se zavázat i k jeho aktualizaci ve vztahu k vývoji legislativy, změnám postupů správců nebo zpracovatelů, případně i k vývoji informačních technologií. Teprve po jeho schválení Úřadem pro ochranu osobních údajů se k němu může přihlásit příslušný správce nebo zpracovatel.

Smyslem kodexu chování je usnadnit účinné uplatnění obecného nařízení v každodenním provozu správců a zpracovatelů. Kodex by neměl opakovat obecné normy nařízení ale poskytovat praktická řešení problémů, se kterými se správci či zpracovatelé budou setkávat ve svém oboru činnosti. S ohledem na nutnost schválení kodexů chování Úřadem nabývají do jisté míry normativní povahy v daném odvětví nebo pro danou skupinu správců či zpracovatelů. Jak je uvedeno v recitálu (98) obecného nařízení, kodexy by měly zejména upřesňovat povinnosti správců a zpracovatelů s přihlédnutím k riziku, které ze zpracování pravděpodobně vyplyne pro práva a svobody fyzických osob.

Evropský sbor pro ochranu osobních údajů přijal Pokyny Sboru 1/2019 týkající se kodexů chování a subjektů pro monitorování. Tyto pokyny představují významný zdroj informací pro subjekty uvažující o tvorbě kodexů chování.

Kodex chování je tedy stručně řečeno předem připravený text (upravující zásady a požadavky na zpracování osobních údajů) opatřený závazkem subjektu (správce nebo zpracovatele) k dodržování v kodexu popsaných postupů. Závazek zahrnuje rovněž zajištění monitorování dodržování kodexu (viz dále v textu).

Příklady zpracování pokryté kodexem chování

Z textu Pokynů Sboru 1/2019 vyplývají dvě možnosti zaměření kodexů chování, a to na **všechna** zpracování osobních údajů určité skupiny správců nebo zpracovatelů nebo pouze na j**edno** dílčí zpracování určité skupiny správců.

Kodex chování bude zpravidla vypracován pro (operace) zpracování osobních údajů:

1) prováděné správci nebo zpracovateli s obdobným charakterem činnosti (například v rámci provozování internetových obchodů nebo cestovních kanceláří nebo lékařských ordinací apod.), který může pokrývat veškeré zpracování osobních údajů prováděné takovou skupinou správců (například v případě cestovních kanceláří – personalistika, účetnictví, evidence zákazníků, objednávky, rezervace, zasílání obchodních sdělení apod.). V tomto případě se ověření dodržování kodexu týká kodexem upravených (operací) zpracování, tj. zpravidla všech operací zpracování prováděných stejným správcem,
2) prováděné správci nebo zpracovateli průřezově bez ohledu na charakter činnosti (například likvidace osobních údajů, přímý marketing, personalistika apod.).

Kodex se tedy nevztahuje na všechny (operace) zpracování prováděné stejným správcem.

Obsah kodexu chování

Kodexy by měly z praktického hlediska aplikovat pravidla obsažená v obecném nařízení do kontextů činností správců či zpracovatelů, pro něž je kodex tvořen. Zejména by předkladatel kodexu měl popsat:

- **Působnost a předmět kodexu** (účel kodexu, územní působnost kodexu (evropská či národní), věcná působnost kodexu (kodexem upravené operace zpracování), popis průběhu zpracování kodexu, včetně případné podpůrné dokumentace v příloze),
- **Zásady, požadavky a postupy (operací) zpracování osobních údajů** (upřesňují a rozpracovávají požadavky obecného nařízení, proto není možné v kodexu pouze opisovat ustanovení obecného nařízení, vždy musí být rozpracovány na specifické zásady, postupy a požadavky pro kodexem upravené (operace) zpracování),
- **Organizační zajištění kodexu chování** (definuje a upravuje zajištění kodexu vzhledem k jeho dlouhodobé udržitelnosti a dalšímu rozvoji, tj. určení řídícího orgánu, návrh monitorujících subjektů, které potom mohou být akreditovány Úřadem pro ochranu osobních údajů, členů kodexů a jejich činnosti, dokumentace, úrovně shody s kodexem, řešení stížností, zajištění financování apod.).

Ohledně náležitostí kodexu jsou důležitým vodítkem zejména pokyny Sboru 1/2019 ke kodexům chování a Metodická příručka Úřadu verze 2.0 ze dne 8. 10. 2019 dostupná na webových stránkách Úřadu.

Schvalování a zveřejnění kodexu

Návrh kodexu probíhá schvalovací procedurou v závislosti na tom, jaké území zasahuje. Pokud se kodex vztahuje pouze na subjekty v rámci jednoho členského státu (Česká republika), předloží zpracovatel jeho návrh Úřadu pro ochranu osobních údajů. Úřad vydá stanovisko, zda je nebo není kodex v souladu s obecným nařízením. Pokud kodex je v souladu s obecným nařízením, Úřad ho schválí, zaregistruje a zajistí jeho zveřejnění.

Pokud se kodex vztahuje na subjekty v rámci více členských států Evropské unie, předloží zpracovatel jeho návrh Úřadu v českém a anglickém jazyce. Ten ho dále pošle ke schválení Sboru na základě mechanismu jednotnosti podle čl. 63 obecného nařízení, který vydá stanovisko, zda je či není v souladu s obecným nařízením. Kladné stanovisko Sboru může být předloženo evropské Komisi, která může prostřednictvím prováděcích aktů rozhodnout, že schválený kodex chování má všeobecnou platnost v rámci EU.

Monitorování dodržování kodexu chování

Podle obecného nařízení musí být dodržování kodexu jednotlivými správci nebo zpracovateli pravidelně monitorováno nezávislým subjektem. S výjimkou kodexů, určených pro orgány veřejné moci nebo veřejné subjekty, provádí monitorování subjekt akreditovaný Úřadem pro ochranu osobních údajů na základě akreditačních požadavků. V praxi to tedy znamená, že každý subjekt, který se přihlásí k dodržování kodexu, se musí zároveň zavázat, že se podrobí monitorování shody ze strany buď dozorového úřadu nebo akreditovaného subjektu.

Podmínky získání akreditace

Akreditaci vydává Úřad pro ochranu osobních údajů všem subjektům, které splní akreditační požadavky. Akreditační požadavky schvaluje po vypracování a předložení Úřadem Evropský sbor. Subjekt, který usiluje o akreditaci musí Úřadu prokázat, že splňuje akreditační požadavky tzn. požadavky na odbornost, nezávislost, úpravu vztahů s monitorovaným subjektem, finanční zajištění, řešení stížností na porušování kodexů, absenci střetu zájmů apod. Akreditační požadavky byly schváleny Evropským sborem a jsou připraveny ke zveřejnění.

Úřad může akreditaci kdykoliv přezkoumat (např. na základě změny kodexu, na základě podstatné změny subjektu pro monitorování nebo na základě informací o nedostatcích monitorování) a může rozhodnout o jejím zrušení v případě, pokud subjekt přestane splňovat akreditační požadavky nebo jím prováděné monitorování neprobíhá v souladu s požadavky čl. 41. odst. 4 obecného nařízení.

Platnost akreditace je 5 let. Žádost o prodloužení akreditace musí subjekt pro monitorování podat nejméně tři měsíce před vypršením platnosti akreditace.

Akreditace se provádí pouze ve vztahu k jednomu kodexu. Subjekt pro monitorování může získat samostatně několik akreditaci na monitorování dodržování různých kodexů. Nelze ovšem provádět monitorování více kodexů na základě jedné akreditace.

Orgán oprávněný kontrolovat dodržování kodexu

Oprávněn kontrolovat dodržování kodexu ze strany jednotlivých správců nebo zpracovatelů, kteří se k dodržování kodexu zavázali je pouze subjekt akreditovaný Úřadem pro ochranu osobních údajů (subjekt pro monitorování kodexů chování). Pokud tento subjekt zjistí porušování kodexu, může přijmout vhodná opatření k nápravě, včetně vyloučení správce nebo zpracovatele z účasti na kodexu nebo pozastavení jejich účasti na kodexu. O tomto kroku akreditovaný subjekt musí informovat Úřad pro ochranu osobních údajů. Existence akreditovaného subjektu však neomezuje dozorové kompetence Úřadu pro ochranu osobních údajů. Úřad pro ochranu osobních údajů může akreditaci zrušit, pokud akreditovaný subjekt nesplňuje podmínky akreditace nebo jedná v rozporu s obecným nařízením.

Subjekt pro monitorování může být externí nebo interní. Externí subjekt pro monitorování musí být právnickou nebo fyzickou osobou podnikající. Interní subjekt pro monitorování musí být jasně vymezenou částí právnické osoby, která je schopna nést právní odpovědnost za všechny činnosti při monitorování kodexu; touto právnickou osobou nesmí být člen daného kodexu.

Vydávání osvědčení (certifikace) o ochraně údajů

Podobně jako kodexy chování je i osvědčení o ochraně údajů dobrovolnou možností, jak prokázat soulad (operací) zpracování s obecným nařízením. Osvědčení je dokument vydaný subjektem pro vydávání osvědčení (certifikačním orgánem), kterým subjekt (správce, zpracovatel) prokazuje zajištění souladu zpracování s požadavky obecného nařízení. Osvědčení mohou vydávat pouze subjekty pro vydávání osvědčení pro tuto činnost akreditované (viz dále) nebo vnitrostátní dozorový orgán.

Předmět hodnocení

Předmětem hodnocení za účelem vydání osvědčení (certifikátu) podle obecného nařízení mohou být:

- operace zpracování osobních údajů (tj. jednotlivé zpracování osobních údajů nebo celá řada operací zpracování),
- produkty, tedy HW a SW a služby, jsou-li spojeny a poskytovány společně s operacemi zpracování osobních údajů. Tedy samostatně poskytovaný HW, SW a služby, byť určené ke zpracování osobních údajů, nemohou být předmětem hodnocení.

Orgán oprávněný akreditovat

Udělit akreditaci (oprávnit k provádění vydávání osvědčení/certifikaci) mohou podle obecného nařízení:

- dozorový úřad (v ČR je to Úřad pro ochranu osobních údajů),
- vnitrostátní akreditační orgán určený v souladu s nařízením Evropského parlamentu a Rady č. 765/2008 (v ČR je to Český institut pro akreditaci – ČIA),
- dozorový úřad i vnitrostátní akreditační orgán zároveň.

V rámci České republiky akreditaci subjektů pro vydávání osvědčení provádí na základě požadavků pro akreditaci subjektů pro vydávání osvědčení Český institut pro akreditaci, o.p.s. v souladu s § 15 zákona č. 110/2019 Sb., o zpracování osobních údajů.

Český institut pro akreditaci, o.p.s. může akreditaci pro vydávání osvědčení subjektu zrušit (rovněž na základě podnětu Úřadu), pokud zjistí, že nejsou dodržovány podmínky akreditace nebo akreditovaný subjekt porušuje obecné nařízení.

Akreditace se vydává na dobu max. 5 let a lze ji obnovit za stejných podmínek, pokud daný subjekt splňuje příslušné požadavky.

Orgán oprávněný vydat osvědčení

Vydat osvědčení (certifikaci) může subjekt, který je akreditován vnitrostátním akreditačním orgánem státu Evropské unie určeným podle nařízení Evropského parlamentu a Rady (ES) č. 765/2008 (v ČR je to Český institut pro akreditaci).

Osvědčení může vydat i příslušný dozorový úřad (v ČR Úřad pro ochranu osobních údajů) na základě jim schválených kritérií nebo kritérií schválených Evropským sborem. V tom případě to může vést k vydání společného osvědčení, evropské pečeti ochrany údajů.

Subjekt pro vydávání osvědčení má povinnost předem sdělit Úřadu důvody pro vydání nebo odebrání osvědčení, aby umožnil případný výkon jeho pravomocí.

Osvědčení se vydává na dobu max. 3 let a lze ho prodloužit za stejných podmínek, pokud jsou i nadále plněny všechny požadavky.

Podmínky získání akreditace

Požadavky na akreditaci schvaluje po vypracování a předložení Úřadem pro ochranu osobních údajů Evropský sbor. Definují požadavky na subjekt pro vydávání osvědčení z hlediska odbornosti, úpravy vztahů se zákazníkem (správce nebo zpracovatel), finančního zajištění, řešení stížností apod. Základem je norma ČSN EN ISO/IEC 17065:2013 Posuzování shody – Požadavky na orgány certifikující produkty, procesy a služby doplněná o požadavky Evropského sboru pro ochranu osobních údajů (v rámci zajištění jednotnosti definované společně v Pokynech Evropského sboru 4/2018) a národními požadavky definovanými

Úřadem pro ochranu osobních údajů. Akreditační požadavky byly schváleny Evropským sborem a jsou připraveny ke zveřejnění.

Certifikační kritéria

Certifikační kritéria definují souhrn požadavků, jejichž dodržováním se prokazuje soulad s obecným nařízením. Certifikační požadavky schvaluje Úřad pro ochranu osobních údajů, a v případě certifikačních kritérií s širší územní působností je schvaluje též Evropský sbor. Certifikační kritéria mohou být obecného charakteru (uplatnitelná u všech nebo většího počtu (operací) zpracování nebo konkrétní pokrývající jen určitý druh (operací) zpracování (například umělá inteligence). Je zde jistá analogie s požadavky definovanými kodexem chování.

Je to ve výsledku subjekt pro vydávání osvědčení (certifikační orgán) akreditovaný ČIA, který, na základě certifikačních kritérií, vydává osvědčení (certifikát), kterým správce/zpracovatel prokazuje soulad hodnocených (operací) zpracování s certifikačními kritérii, resp. s obecným nařízením.

Rozeznáváme:

1) **národní certifikační kritéria** platná pro jeden členský stát,
2) **nadnárodní certifikační kritéria platná pro více států** (nemají status Evropské pečetě),
3) celoevropsky platná **certifikační kritéria pro Evropskou pečeť**, která jsou schválena rozhodnutím Sboru, přičemž o schválení Sborem žádá majitel schématu prostřednictvím kompetentního dozorového úřadu procedurou mechanismu jednotnosti podle **čl. 64(2)** (protože jde o záležitost, která se týká všech členských států).