MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

MVCRX03QQDV4
prvotní identifikátor

Č. j. MV-135322-2/AS-2017

Ochrana osobních údajů při výkonu spisové služby, zejména v informačních systémech spravujících dokumenty u veřejnoprávních původců[1]

(informace ke dni 4. prosince 2017)

Obsah:

Nařízení Evropského parlamentu a Rady (EU) 2016/679 z 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, dále jen „GDPR“) a stávající zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, stanovují rozsah ochrany osobních údajů, který musí být promítnut, v případě původce povinného výkonem spisové služby podle ustanovení § 3

[1] Veřejnoprávní původce ve smyslu § 3 odst. 1 zákona č. 499/2004 Sb.

odst. 1 zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „AZ"), také do oblasti spisové služby[2].

Každý původce, který vede ve smyslu ustanovení § 63 AZ povinně spisovou službu, proto musí dodržovat všechny tyto požadavky, tedy musí zabezpečit jejich realizaci prostřednictvím vnitřních opatření. Dnem 25. května 2018 se však jeho úloha v oblasti ochrany osobních údajů rozšiřuje. Původce jako správce osobních údajů musí zajistit realizaci požadavků plynoucích z GDPR v oblasti zpracování osobních údajů (tedy jakéhokoli systematické nakládání s nimi) a také plnit své povinnosti vůči subjektu údajů (fyzické osobě, jejíž osobní údaje jsou zpracovávány). Vzhledem k rozsahu nových požadavků v oblasti ochrany osobních údajů musí být upraveny všechny informační systémy spravující dokumenty (dále jen „ISSD"), tedy elektronické systémy spisové služby, samostatné evidence dokumentů a také další informační systémy (databáze a jakékoliv soubory informací obsahující osobní údaje žijících osob). Každému původci se doporučuje, aby provedl s dostatečným časovým předstihem sám kontrolu nebo si nechal provést audit se zaměřením na zpracovávání osobních údajů.

1. Informační zdroje

1.1. Příslušné právní předpisy

Právní předpisy

- Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.[3]
- Nařízení Evropského parlamentu a Rady (EU) 2016/679 z 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).
- Zákon č. 499/2004 Sb., o archivnictví a spisové službě ve znění pozdějších předpisů.
- Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby, ve znění pozdějších předpisů.

Směrnice 95/46/ES

V roce 1995 nabyla účinnosti směrnice 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. O pět let později byl vydán zákon č. 101/2000 Sb., který nabyl účinnosti k 1. červnu 2000, resp. k 1. prosinci 2000 (viz ustanovení § 51 zákona č. 101/2000 Sb.). Oba předpisy vytvořily právní prostředí pro nakládání

[2] GDPR stanoví povinnosti i pro subjekty, které dle zákona č. 499/2004 Sb. nejsou povinny vést spisovou službu. Nelze tedy připustit výklad, že se původců bez povinností výkonu spisové služby GDPR netýká.

[3] V souvislosti s GDPR je připravován nový zákon o zpracování osobních údajů.

s osobními údaji, resp. pro jejich zpracovávání[4]. Původci dokumentů jsou od té doby povinni zpracovávat osobní údaje v rozsahu a dle pravidel stanovených uvedenými právními předpisy. Rozsah ochrany osobních údajů je doplněn **GDPR**, **které nabývá účinnost 25. května 2018**.[5]

Účinnost GDPR

Původce je nutné upozornit, že GDPR je závazné v celém rozsahu a je přímo použitelné ve všech členských státech. Má proto úplný přímý účinek i bez přímé implementace do českého práva prostřednictvím jiného právního předpisu a nadto **má přednost před právními předpisy České republiky**[6]. Dnem nabytí účinnosti GDPR se zrušuje směrnice 95/46/ES, jejíž roli nařízení převezme. GDPR současně nahradí díky svému přímému účinku v některých částech ustanovení zákona č. 101/2000 Sb.

V současné době Ministerstvo vnitra připravuje nový zákon o zpracování osobních údajů, u kterého probíhá vypořádání připomínek z meziresortního připomínkového řízení

Zesnulé osoby jako subjekt údajů

GDPR se nevztahuje na údaje zesnulých osob!

1.2. Další metodické materiály

Úplné elektronické podání a eFaktura

Problematika zpracování osobních údajů v případě elektronických faktur je popsána v samostatném metodickém materiálu „Elektronická fakturace u veřejnoprávních subjektů“. Obdobně bude řešena v rámci metodického materiálu „Úplné elektronické podání“. Oba materiály budou po dokončení zveřejněny na webových stránkách Ministerstva vnitra.

1.3. Užitečné webové odkazy

Webové odkazy

- GDPR
  - ✓ http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679&from=en
- vodítka/stanoviska ke GDPR
  - ✓ https://www.uoou.cz/pokyny-pracovni-skupiny-wp29/ds-4728/archiv=0&p1=3938
- pověřenec pro ochranu osobních údajů
  - ✓ http://www.mvcr.cz/odk2/
  - ✓ http://www.mvcr.cz/sluzba/clanek/ministerstvo-vnitra-zverejnuje-metodicke-doporuceni-k-problematice-poverencu-pro-ochranu-osobnich-udaju.aspx

[4] Zpracováváním se rozumí jakákoliv operace nebo soustava operací, kterou provádí původce dokumentů systematicky s osobními údaji ať již automatizovaně nebo jinými prostředky; zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace; srovnej ustanovení § 4 písm. e) zákona č. 101/2000.

[5] Čl. 99 GDPR – „Toto nařízení se použije ode dne 25. května 2018“.

[6] Nařízení – právně závazné v celém rozsahu EU a přímo použitelné.

- ✓ https://www.uoou.cz/pracovni-skupina-wp29-vydala-tri-dokumenty-k-obecnemu-narizeni-o-ochrane-osobnich-udaju/d-21750
- informace, metodiky, časté dotazy
  - ✓ http://www.mvcr.cz/clanek/ochrana-osobnich-udaju-ochrana-osobnich-udaju.aspx
  - ✓ https://www.uoou.cz/gdpr/ds-3938/p1=3938

1.4. Základní pojmy

Subjekt údajů

Subjekt údajů – identifikovaná nebo identifikovatelná fyzická osoba; 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.

Správce

Správce – 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 Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení;

Zpracovatel

Zpracovatel – fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.

Původce

Původce – každý, z jehož činnosti dokument vznikl; za dokument vzniklý z činnosti původce se považuje rovněž dokument, který byl původci doručen nebo jinak předán;

Osobní údaj

Osobní údaj – veškeré informace o subjektu údajů.

Zpracování osobních údajů

Zpracování osobních údajů – 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.

2. Požadavky v oblasti ochrany osobních údajů vůči ISSD a dalším informačním systémům původce

Základní zásady GDPR

GDPR stanovuje sedm základních zásad pro práci s osobními údaji žijících identifikovaných nebo identifikovatelných osob[7]:

- zásada zákonnosti, korektnosti a transparentnosti,
- zásada účelového omezení,
- zásada minimalizace údajů,

[7] Čl. 5 a 6 GDPR

- zásada přesnosti,
- zásada omezení uložení,
- zásada integrity a důvěrnosti,
- zásada odpovědnosti.

Při posuzování kvality zpracovávání osobních údajů musí být posouzeno dodržování všech uvedených zásad. Výsledkem posouzení pak musí být okruhy informací o dodržování všech zásad souvisejících s osobními údaji nebo sadami osobních údajů, popsaných v následujících kapitolách. V souvislosti se zásadou minimalizace zpracovávaných údajů je vhodné upozornit, že v případě zpracování osobních údajů, které nejsou uvedeny výčtem v právním předpisu, se jedná o zpracování na základě souhlasu a to i v případě plnění právní povinnosti.

2.1. Osobní údaje jsou zpracovávány zákonným a transparentním způsobem s definovaným účelem

Účel, rozsah, zákonnost a transparentnost zpracování

Předmětem posouzení zpracovávání osobních údajů je ověření zákonnosti zpracování (naplňuje jeden ze sedmi důvodů specifikovaných v rámci nařízení)[8], zda jeho rozsah a způsob realizace odpovídá stanovenému účelu a osobní údaje jsou zpracovávány korektním a transparentním způsobem.

Bude-li výsledek posouzení skutečně konkrétní, původce bude poté schopen doložit, že osobní údaje zpracovává vždy a pouze na základě ověřitelného důvodu, tedy na základě příslušného právního předpisu nebo z jiného oprávněného důvodu (tzv. „zákonnost zpracování“). Výčet oprávněných důvodů, na jejichž základě je oprávněn zpracovávat osobní údaje, si může původce snadno ověřit podle čl. 6 GDPR. Je to především zpracování při plnění příslušné povinnosti s oporou v právních předpisech, zpracování je však možné také na základě souhlasu dotčené fyzické osoby, v souvislosti s plněním smlouvy, při ochraně životně důležitých zájmů a ve veřejném zájmu (souvislost s výkonem veřejné moci). Obdobně původce ověří rozsah, transparentnost a další podmínky pro správu a zpracování osobních údajů podle GDPR.

2.2. Osobní údaje jsou uchovávány pouze po dobu nezbytnou, odpovídající účelu zpracování

Spisový řád – přehled všech evidencí původce

Každý původce musí podle požadavků AZ vydat spisový řád se spisovým a skartačním plánem[9]. Ve spisovém řádu uvede kromě popisu oběhu dokumentů ve spisové službě také všechny samostatné evidence dokumentů vedené v analogové nebo elektronické podobě. Ve spisovém a skartační plánu pak musí

[8] Např. zákonné zmocnění, kdy není potřeba souhlas.
[9] § 66 AZ.

stanovit pro všechny druhy dokumentů skartační lhůty[10] (případně skartační lhůty se spouštěcí událostí[11]).

Spisový a skartační plán

Doporučuje se, aby původce provedl revizi spisového a skartačního plánu, zejména pak skartačních lhůt. Prověří, zda skartační lhůty odpovídají lhůtám uvedeným v právních předpisech, jsou-li pro konkrétní typy dokumentů lhůty stanoveny, a zda ostatním typům dokumentů stanovil přiměřené skartační lhůty, které budou odpovídat požadavkům na délku uchovávání dokumentů po jejich vyřízení pro úřední potřebu a současně požadavkům veřejného zájmu.

Skartační lhůty

Pro tyto účely je možné využít metodiku vydanou MV a obsahující vybrané právní předpisy, stanovující dobu ukládání vybraných typů dokumentů. Při zpracovávání spisového a skartačního plánu se doporučuje využít konzultací s příslušným archivem, který u původce provádí dohled nad výkonem spisové služby[12].

Skartační řízení dokumentů s osobními údaji

V této souvislosti je vhodné připomenout, že již s ohledem na současnou právní úpravu zákona č. 101/2000 Sb., je zavedena povinnost podle § 20 tohoto zákona po uplynutí účelu zpracování osobních údajů tyto likvidovat[13]. Na druhou stranu ustanovení § 20 zákona č. 101/2000 Sb. se aplikuje až bezprostředně po ukončeném výběru dokumentů v rámci skartačního řízení[14], neboť do této doby je účel zpracování dán zákonným požadavkem pro uchování a umožnění výběru archiválií.

Po pravomocném ukončení výběru archiválií **původce:**

1) **dokumenty určené ke zničení a část jejich metadat zničí[15],**
2) **vybrané dokumenty s osobními údaji a jejich metadata předá k uložení do příslušného archivu[16],**
3) **po potvrzení příslušného archivu o převzetí vybraných dokumentů k trvalému uložení zničí jejich repliky v ISSD včetně části jejich metadat.**

U analogových evidencí se postupuje obdobně.

Důrazně upozorňujeme všechny původce, že povinnost řádného vyřazování dokumentů ve skartačním nebo mimo skartační řízení podle AZ[17] není GDPR dotčena. Zničení dokumentu bez provedení výběru archiválií naplňuje skutkovou podstatu přestupku a je sankcionováno[18].

---

[10] Délku skartační lhůty nelze „legalizovat“ odkazem na „ukládání (osobních údajů) pro archivní účely“. K „archivnímu“ uložení a čerpání výjimky dle GDPR je oprávněn pouze archiv jako zařízení ve smyslu AZ.

[11] Spouštěcí událost – okamžik, který je rozhodný pro počátek běhu skartační lhůty (§15 odst. 4 vyhlášky č. 259/2012 Sb.).

[12] Určení původci zasílají spisový a skartační plán příslušnému archivu bezodkladně po jeho vydání nebo změně (§ 66 odst. 2 AZ).

[13] Za likvidaci odpovídá vždy původce (srovnej rozsudek Nejvyššího správního soudu 3 As 121/2014-35).

[14] Srovnej § 7 až 12 AZ.

[15] Požadavek 6.3.10 až 6.3.16 Národního standardu pro elektronické systémy spisové služby VMV čá 57/2017.

[16] Další uchovávání osobních údajů je podle GDPR zákonné (mj. čl. 17 odst. 3 písm. b)).

[17] § 3 a související ustanovení zákona č. 499/2004 Sb.

[18] § 74 zákona č. 499/2004 Sb.

Oprávněné zničení[19] dokumentů se prokazuje protokolem o provedeném skartačním řízení nebo protokolem o provedeném výběru archiválií mimo skartační řízení. Archivy jsou oprávněny ukládat trvale dokumenty vybrané za archiválie, včetně archiválií obsahujících osobní údaje žijících osob, což vyplývá mj. z čl. 17 a čl. 89 GDPR.[20]

2.3. Používaný ISSD je schopen splňovat kromě jiného všechny nároky na ochranu osobních údajů

Původci jsou povinni zabezpečit dokumenty obsahující osobní údaje proti přístupu neoprávněných osob, a to včetně vlastních zaměstnanců. Musí proto využívat zejména nástroje pro omezení přístupu k dokumentům a jejich metadatům obsahujícím osobní údaje pouze pro oprávněné osoby, a to při všech operacích s takovými dokumenty a metadaty, a zaznamenávání historie nahlížení do dokumentů a metadat obsahujících osobní údaje.

Možnosti řešení:

- Vztah zaměstnance k zaměstnavateli je dán pracovním/služebním poměrem. Konkrétní způsob zařazení zaměstnance ve struktuře zaměstnavatele stanovuje mj. popis služebního místa (státní zaměstnanec) či popis pracovní činnosti (zaměstnanec podle zákoníku práce). V něm musí být uvedeno, že zaměstnanec je oprávněn zpracovávat osobní údaje v souvislosti s výkonem jeho práce podle zařazení, v tomto konkrétním případu v souvislosti s plněním úkolů prostřednictvím ISSD a dalších evidencí. Totéž se musí promítnout také do opatření zaměstnavatele, vydaného k úpravě režimu zpracování a ochrany osobních údajů (vnitřní předpis, interní akt řízení atp.). — Smlouvy se zaměstnanci
- GDPR zavádí tzv. záměrnou a standardní ochranu, kdy hlavním cílem je minimalizace rizik souvisejících se zpracováním. Záměrná ochrana musí být nastavena **již ve fázi návrhu** zpracování a vychází z principu „privacy by design“ – např. neukládání osobních údajů decentralizovaně, protože ochrana osobních údajů je pak obtížná. — Privacy by design
- Možným nástrojem je využívání jmenných rejstříků[21], do nichž lze nahlížení umožnit menší skupině uživatelů, než do celého ISSD[22]. S tím souvisí i interní stanovení struktura pole „věc“ tak, aby osobní — Jmenné rejstříky

[19] Zničení ve smyslu § 21 odst. 8 vyhlášky č. 259/2012 Sb. – „znehodnotí do podoby znemožňující jejich rekonstrukci a identifikaci obsahu“.
[20] Srovnej s kapitolou 2.5 tohoto materiálu.
[21] § 64 odst. 4 a 5 zákona č. 499/2004 Sb.
[22] § 25 odst. 3 vyhlášky č. 259/2012 Sb., „Veřejnoprávní původce určí fyzické osoby oprávněné k přístupu do jmenného rejstříku.“

údaje byly v obecně dostupných, z hlediska nahlížení nelogovaných[23], uživatelských informacích v ISSD minimalizovány.

- V některých případech lze použít pseudonymizaci nebo anonymizaci osobních údajů. Při pseudonymizaci (náhrada osobních údajů identifikující osobu bezvýznamovým identifikátorem a omezení přístupu k identifikačním klíčům) i anonymizaci (úplné odstranění osobních údajů identifikujících osobu) je třeba zajistit, aby nedošlo k nevratnému poškození originálu dokumentu.

Pseudonymizace a anonymizace

- Další možností ochrany osobních údajů je omezení řetězcového a fulltextového vyhledávání v ISSD podle přístupových práv uživatelů ISSD.

Omezení vyhledávání

- Využívá-li původce k zabezpečení výkonu spisové služby či obecně ke správě dokumentů ISSD, musí do smlouvy s osobou zajišťující technickou podporu tohoto systému nebo jeho outsourcing vložit upozornění na skutečnost, že při těchto činnostech se seznamuje s osobními údaji (zpracovává je) a je povinována mlčenlivostí. Dále příslušný smluvní vztah musí podle GDPR jasně definovat roli správce nebo zpracovatele osobních údajů.[24] V případě outsourcingu ISSD je třeba dále přesně definovat, kde jsou ukládány osobní údaje (pozor na prostor mimo Evropský hospodářský prostor [dále jen „EHS“] a mezinárodní organizace) a jakým způsobem jsou zabezpečeny. Smlouvy též musí obsahovat záruky jednotlivých stran za zpracování osobních údajů a dále pak odpovědnost za případné škody, které po 25. květnu 2018 mohou nabývat velmi vysokých částek. Od 25. května 2018 je též vhodné upozornit všechny zpracovatele, že mohou zpracovávat osobní údaje pouze na základě předchozích pokynů správce (nelze tedy, aby například dodavatel prováděl jakékoliv zpracování bez přímého pokynu správce, toto se týká činností v souvislosti s údržbou systému).

Smlouvy s dodavateli

- V souvislosti s případnými požadavky na zajištění úprav ISSD je vhodné analyzovat současný stav s ohledem na 17 let platný zákon o ochraně osobních údajů, neboť právní úprava č. 101/2000 Sb. obsahuje již řadu povinností a ne vše, co GDPR přináší, je nové. Proto je vhodné tuto analýzu provést i s ohledem na případné posouzení oprávněnosti nákladů souvisejících s úpravou ISSD. Navíc je pak vhodné připomenout, že od okamžiku vstupu České republiky do Evropské unie jsou i nařízení součástí našeho právního řádu.

[23] Např. systém není nastaven k zaznamenávání přístupů zaměstnance k evidenčním údajům spisu nebo dokumentu (obecně do metadat).

[24] Zpracovatel může zpracovávat osobní údaje pouze na základě přesných pokynů správce a odpovídá pouze za technickou stránku provedení daných pokynů, správce je naopak zcela odpovědný za celý proces zpracování osobních údajů a dopady na subjekty údajů.

2.4. Naplnění povinností původce vůči subjektu údajů

V rámci posouzení připravenosti na GDPR je vhodné ověřit, zda používaný ISSD a případné další evidence umožňují naplnit povinnosti původce jako správce údajů vůči subjektu údajů podle čl. 13, 14, 15, 16, 18, 19, 20 a 21, 34 GDPR ve lhůtách stanovených v čl. 12 GDPR. Podle čl. 16 GDPR má subjekt údajů právo na opravu nepřesného osobního údaje, který se ho týká. Podle čl. 18 má subjekt údajů za vyjmenovaných okolností právo, aby původce jako správce údajů omezil zpracování jeho osobních údajů. V čl. 19 GDPR se správci údajů ukládá oznamovací povinnost o opravě, výmazu nebo omezení zpracování v případě osob, kterým byly osobní údaje zpřístupněny.[25] Článkem 20 GDPR se upravuje právo na přenositelnost osobních údajů a článkem 21 GDPR právo vznést námitku.

Žádosti subjektu údajů dle GDPR

Každá fyzická osoba je oprávněna požádat původce podle čl. 15 GDPR o informaci, jaké údaje o něm v dokumentech zpracovává, pro jaký účel a v jakém rozsahu, na základě jakého titulu[26] je zpracovává a po jakou dobu budou uloženy. Původce také musí informovat subjekt údajů o případném úmyslu předat osobní údaje do třetí země (mimo prostor EHS a mimo státy se srovnatelnou zárukou ochrany osobních údajů) nebo mezinárodní organizaci (čl. 13 GDPR)[27]. Původce musí v tomto případě informovat subjekt údajů o účelu zpracovávání jejích osobních údajů, o všech konkrétních osobních údajích, které zpracovává, a o povaze automatizovaného zpracovávání v souvislosti s jejich následným využitím pro rozhodování, jehož výsledkem je zásah do jejího práva a oprávněných zájmů. Pokud je možné shromáždit požadované údaje automatizovaně (z ISSD nebo jiných informačních systémů), původce je povinen tak učinit.

Jedině pokud by shromáždění takových údajů bylo nemožné nebo by vyžadovalo nepřiměřené úsilí (např. prohledávání velkého množství listinných dokumentů ve spisovnách, k nimž nebyly pořízeny příslušné vyhledávací pomůcky atp.), oznámí tuto skutečnost bez sdělení požadovaných údajů. Údaje oznámí v rozsahu: počet dokumentů, jejich označení v ISSD nebo mimo tento systém a dále údaje podle ustanovení článku 15 odst. 1 písm. a) až h) GDPR. Pokud dokument obsahující osobní údaje subjektu údajů obsahuje osobní údaje také jiných subjektů údajů, musí být tyto osobní údaje třetích osob před

[25] S výjimkou situací, kdy je toto nemožné nebo to vyžaduje nepřiměřené úsilí.

[26] Viz článek 6 GDPR.

[27] O předávání osobních údajů do třetích zemí hovoříme tehdy, pokud jsou osobní údaje předávány mimo prostor EU, resp., mimo Evropský hospodářský prostor (dále EHP). Součástí EHP jsou i státy stojící mimo EU - Island, Lichtenštejnsko a Norsko, které jsou rovněž považovány za země poskytující odpovídající úroveň ochrany. Dále pak existují závazky - např. především podpis a ratifikace Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních údajů (Rada Evropy, ETS 108, 1981, dále jen „Úmluva 108“). Země, které podepsaly Úmluvu 108, případně její Dodatkový protokol č. 181 z 24. září 2004 jsou považovány v současné době za země, které poskytují odpovídající úroveň ochrany. Doposud přijala Komise rozhodnutí týkající se odpovídající úrovně ochrany osobních údajů v zemích: Argentina, Faerské ostrovy, Guernsey, Izrael, Jersey, Man, Švýcarsko, Kanada, Nový Zéland, Uruguayská východní republika.

poskytnutím kopie anonymizovány.[28]

Součástí informace, kterou je původce povinen oznámit tázajícímu se subjektu údajů, je rovněž doba, po kterou budou osobní údaje uloženy. Původce může dotazující subjekt údajů předně upozornit, že dokumenty obsahující jeho osobní údaje nejsou uloženy jen po dobu vyřizování, ale rovněž určitou dobu po jejich vyřízení, a to podle stanovené skartační lhůty. V tomto případě musí být schopen doložit pomocí příslušného právního předpisu, případně vlastním vnitřní předpisem,[29] oprávněnost délky skartační lhůty přidělené dokumentu.[30]

Pokud vše prokáže, splnil povinnost a dokumenty s osobními údaji uchovává oprávněně po celou dobu, kterou stanovil skartační lhůtou. Informace o poskytnutí informace o osobních údajích subjektu údajů se zaznamená u dokumentu nebo ve spisu, ve kterém je dokument založen.

Lhůty pro poskytnutí informací podle GDPR

Lhůty, formu pro poskytnutí informací a přijetí opatření upravuje čl. 12 GDPR. Pokud původce jako správce údajů poskytne informace na žádost dle čl. 15 až 22, poskytuje je bez zbytečného odkladu, nejdéle do 1 měsíce od obdržení žádosti. Lhůtu je možné prodloužit až o 2 měsíce, ale subjekt údajů musí být nejdéle do 1 měsíce od obdržení žádosti informován o prodloužení lhůty vyřízení, a to spolu s důvody pro odklad.

Nepřijme-li původce jako správce údajů subjektem údajů požadovaná opatření, musí původce subjekt údajů bezodkladně – nejpozději do jednoho měsíce – informovat o důvodech nepřijetí opatření, o možnosti podat stížnost Úřadu pro ochranu osobních údajů a o možnosti žádat o soudní ochranu.

Poplatky/ bezplatnost

Odmítnutí odpovědi

Dále platí, že informace podle čl. 13, 14, 15 až 22 a 34[31] GDPR se poskytují bezplatně. Zpoplatnit (při zohlednění administrativních nákladů) nebo odmítnout odpověď může původce jako správce údajů jen žádosti nedůvodné nebo nepřiměřené[32]. Nedůvodnost nebo nepřiměřenost musí doložit původce jako správce údajů.

2.5. Povinnost uchovávat dokumenty a umožnit výběr archiválií podle AZ versus „právo na výmaz/právo být zapomenut“ podle čl. 17 GDPR

Skartační řízení a právo být zapomenut

Zmocnění archivů

Žádá-li subjekt údajů o provedení výmazu osobních údajů podle čl. 17 GDPR, pak původce ve smyslu AZ musí zohlednit další povinnosti, které mu vyplývají z AZ (mj. povinnost uchovat dokument a umožnit výběr archiválií)[33]. Jsou-li dokumenty zpracovávány v ISSD (a dalších evidencích), žádající subjekt údajů upozorní, že **výmaz** z ISSD (nebo odstranění z dokumentů v analogové

[28] Např. u čl. 15 a 20 GDPR je výslovně uvedeno, že „nesmí být nepříznivě dotčena práva a svobody jiných osob.“.
[29] Vnitřní předpis stanoví skartační lhůty příslušných dokumentů.
[30] Srovnej s kapitolou 2.2. tohoto materiálu.
[31] Čl. 34 GDPR – oznamování případů porušení zabezpečení osobních údajů subjektu údajů
[32] Např. opakující se žádosti.
[33] Srovnej s kapitolou 2.2. tohoto materiálu.

podobě) ve smyslu ustanovení článku 17 odst. 3 GDPR **je možné provést teprve po uplynutí skartačních lhůt dokumentů a jejich zařazení do procesu výběru archiválií, a to pouze u těch dokumentů, které nebudou příslušným archivem vybrány jako archiválie**.

k uložení archiválií s osobními údaji

U veřejnoprávního původce nemají být dokumenty zpracovávány mimo ISSD.[34] Při výběru archiválií se posuzují všechny dokumenty, jimž uplynuly skartační lhůty, případně dokumenty nalezené apod. (viz ustanovení § 7 až § 12 AZ).

Výběr archiválií, ať již ve skartačním řízení nebo mimo skartační řízení, je ukončen protokolem vydaným příslušným archivem, v němž archiv stanoví, které dokumenty budou vybrány jako archiválie k trvalému uložení, a které dokumenty lze zničit. Obdobně i současná právní úprava dle zákona č. 101/2000 Sb. nařizuje povinnou likvidaci dokumentů v případech, kdy obsahují osobní údaje a pominul účel jejich zpracování. Povinnost zabezpečit takové dokumenty před zneužitím ponechává na příslušném původci.

Speciální způsob nakládání však dále vyžadují dokumenty, které sice nebyly vybrány jako archiválie, ale obsahují osobní údaje. Subjekt údajů má právo na jejich výmaz ve všech dokumentech, které nebyly vybrány jako archiválie. Takové dokumenty musí původce v souladu s požadavkem ustanovení § 20 odst. 1 zákona č. 101/2000 Sb. zničit.[35] Zničením se rozumí fyzické zničení nosičů osobních údajů, jejich fyzické vymazání nebo trvalé vyloučení z dalšího zpracování. Původce je povinen zabezpečit, aby současně s vymazáním dokumentů obsahujících osobní údaje vyřazených ve skartačním řízení byla vymazána rovněž všechna metadata včetně zálohovaných dat. Pokud nelze výmaz z periodických provozních záloh z technických důvodů provést (např. zálohy na magnetických páskách apod.), musí původce bezpodmínečně zabezpečit, aby v případě výpadku a následné obnovy dokumentů a metadat do produkčního prostředí ze zálohovaných dat nebyly obnoveny do produkčního prostředí rovněž dokumenty obsahující osobní údaje již vyřazené ve skartačním řízení, respektive provést jejich opakovaný výmaz. Dále musí zajistit, že s obsahem záloh se mohou seznámit výhradně osoby, které jsou pověřeny péčí o ně.

2.6. Neevidované dokumenty a GDPR

Osobní údaje v neevidovaných dokumentech

U neevidovaných dokumentů platí v oblasti ochrany osobních údajů GDPR naprosto stejně jako u evidovaných – vždy je důležitý účel zpracování a povaha dokumentů. Evidenční povinnost je dána pro všechny dokumenty, které jsou původci dokumentů doručeny, nebo které vznikly z jeho činnosti, s výjimkami uvedenými ve spisovém řádu.

Zpracování některých typů dokumentů (např. datasety v informačních

[34] Srovnej s povinnostmi podle §§ 63 a výše AZ a vyhláškou č. 259/2012 Sb., o podrobnostech výkonu spisové služby.

[35] „Správce nebo na základě jeho pokynu zpracovatel je povinen provést likvidaci osobních údajů, jakmile pomine účel, pro který byly osobní údaje zpracovány“.

systémech apod.) však neprochází všemi postupy spisové služby, jako je tomu u běžných dokumentů obvyklé. I takové dokumenty však musí být po uzavření/vyřízení ukládány a vyřazovány ve skartačním řízení nebo mimo skartační řízení. Pokud původce přijme dokumenty, které obsahují osobní údaje a které zároveň podle spisového řádu není povinen evidovat, doporučujeme původci, aby vzhledem k povinnostem vyplývajícím z GDPR tyto dokumenty zaevidoval a to nejpozději při uložení ve spisovně podle ustanovení § 19 odst. 3 vyhlášky č. 259/2012 Sb.

2.7. Předávání osobní údajů do třetích zemí, případně mezinárodním organizacím[36]

V souvislosti s GDPR je nutné pohlížet odlišně na zpracování, které probíhá uvnitř EHS, případně ve státech se srovnatelnou úrovní záruk,[37] a dále pak na zpracování, která probíhají při předání mezinárodním organizacím, případně do třetích států odlišných od výše uvedených. Je nutné zohlednit požadavky GDPR a být připraven v případě dotazu na zpracování od subjektu údajů na podrobnou odpověď, včetně popisu zajištění záruk pro zpracování atp.

Osobní údaje předávané třetím zemím a mezinárodním organizacím

2.8. Pověřenec pro ochranu osobních údajů

Nejpozději 26. května 2018 uvede veřejnoprávní původce kontaktní údaje „pověřence pro ochranu osobních údajů“, tj. zveřejní je.[38] K činnosti a ustanovení pověřence pro ochranu osobních údajů odkazujeme na „Metodické doporučení k činnosti obcí k organizačně-technickému zabezpečení funkce pověřence pro ochranu osobních údajů podle obecného nařízení o ochraně osobních údajů v podmínkách obcí podle právního stavu k 10. srpnu 2017“ a na text „Pověřenci ochrany osobních údajů ve služebních úřadech – metodické doporučení“ na webových stránkách Ministerstva vnitra, případně na „Pokyn týkající se pověřenců pro ochranu osobních údajů“ z 13. prosince 2016, zpracovaný pracovní skupinou WP 29 a publikovaný mj. na webových stránkách Úřadu pro ochranu osobních údajů.

Pověřenec pro ochranu osobních údajů

3. Co bych měl udělat?

3.1. Desatero závěrem:

1. Analýza činností původce souvisejících s informacemi (zejména pak s osobními údaji); zjištění agend a systémů, ve kterých se vyskytují osobní údaje (vedení seznamu o činnostech zpracování); možnost využít obdobnou analýzu provedenou v organizaci z důvodu zákona o kybernetické bezpečnosti.

Kde, co máme?

[36] Čl. 44 až 50 GDPR.
[37] Srovnej poznámku 27 v tomto materiálu.
[38] Čl. 37 odst. 7 GDPR.

2. Analýza právních předpisů, na základě jejichž zmocnění shromažďujeme údaje (případně souhlas subjektu údajů, smlouva, plnění veřejného zájmu atp.). Jakým právem?
3. Stanovení postupů a politiky ochrany – analýza přístupových oprávnění, bezpečnosti uložení (dokumentů, spisů, systémů, informací). Jak to chráníme?
4. Proškolení zaměstnanců: správná správa hesel, řádné návyky zaměstnanců, nastavení odpovědnosti, procesy při ukončení pracovního / služebního poměru, pracovní náplně odpovídající práci s osobními údaji atp. (GDPR se netýká „jen personalistů“!). Kdo to chrání?
5. Revize pracovních smluv se zaměstnanci, doplnění doložky o ochraně osobních údajů. Co si dále zkontroluji?
6. Revize spisového řádu (doplnit všechny evidence vedené u původce) a revize spisového a skartačního plánu (provést revizi skartačních lhůt z hlediska zákonného zmocnění a skutečné provozní potřebnosti).
7. Revize výkonu spisové služby, ISSD a dalších evidencí s osobními údaji a přijetí opatření. Nad čím se zamyslím?
8. Ověření správy dat a jejich záloh (v případě externího dodavatele prověření smluv a ošetření ochrany osobních údajů ve smlouvách). Co si prověřím?
9. Příprava procesů včetně šablon odpovědí a nastavení lhůt vyřízení podání, která přijdou podle GDPR (čl. 12 až 22 a 34 GDPR). Co si připravím?
10. Stanovení postupů pro detekování bezpečnostních incidentů a řešení porušení zabezpečení (kdo odpovídá za nahlášení incidentu, kam oznamuji, komu atp.).

3.2. Doporučujeme

11. U větších původců (ministerstva, centrální úřady) stanovení pracovního týmu/skupiny pro provedení analýz a návrhů řešení implementace GDPR do provozu úřadu (včetně ISSD a dalších informačních systémů), který provede výše uvedené analýzy včetně analýzy rozporů, konfliktních, rizikových míst, předloží návrhy řešení rozporů a návrhy postupů pro nově vzniklé agendy (čl. 13 až 22 a 34) a postupy pro kontrolu a ohlašovací povinnost v případě incidentu. Pracovní skupiny
12. Proškolení zaměstnanců na téma GDPR a s ním související činnosti a nové agendy. Školení zaměstnanců
13. Zavedení výstupů z analýz do praxe a zajištění jejich dlouhodobé udržitelnosti.

PhDr. Jiří Úlovec
ředitel