

SBÍRKA

INTERNÍCH AKTŮ ŘÍZENÍ
REKTORA POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Ročník: 2018

Praha 24. května 2018

Částka: 27

OBSAH

- Část I
2. Pokyn rektora Policejní akademie České republiky v Praze, kterým se vydává Směrnice rektora k ochraně a zpracování osobních údajů na Policejní akademii České republiky v Praze

2.
Pokyn
rektora Policejní akademie České republiky v Praze,
ze dne 24. května 2018,
kterým se vydává Směrnice rektora k ochraně a zpracování osobních
údajů na Policejní akademii České republiky v Praze

Tato směrnice vychází z nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „Nařízení“) a ze zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon o ochraně osobních údajů“), s tím, že doplňuje a rozpracovává některá jejich ustanovení pro úpravu vztahů v rámci Policejní akademie České republiky v Praze (dále jen „PA ČR“) a stanoví organizační řešení v rámci PA ČR zajišťující jejich realizaci.

Čl. 1
Předmět a účel úpravy

- (1) Tato směrnice stanoví zásady a pravidla při zpracování osobních údajů v rámci PA ČR. Stanoví odpovědnost a povinnosti osob zajišťujících ochranu osobních údajů na PA ČR, upravuje interní procesy zpracování osobních údajů zaměstnanců, studentů PA ČR při plnění jejich pracovních či studijních povinností, případně i dalších fyzických a právnických osob, které vystupují ve vztahu k PA ČR jako objednatelé služeb (např. celoživotních kurzů, expertních činností, ubytovacích, stravovacích a jiných služeb aj.). Dále upravuje vztahy s fyzickými a právnickými osobami, které zpracovávají pro PA ČR osobní údaje na základě smluv. V neposlední řadě se týká nakládání s osobními údaji v rámci ostrahy areálu PA ČR.
- (2) Předmětem úpravy této směrnice je zpracování osobních údajů realizovaná zaměstnanci a studenty PA ČR při realizaci jejich pracovních či studijních povinností, případně dalšími fyzickými a právnickými osobami, které zpracovávají osobní údaje na základě smluv s PA ČR.
- (3) Účelem směrnice je seznámit zaměstnance se základními principy řešení ochrany osobních údajů (dále jen „OÚ“) v rámci PA ČR s tím, že následně budou vydanými konkrétními normami, metodickými návody, pokyny apod. k jednotlivým agendám rozpracována potřebná organizační a technická opatření k zabezpečení ochrany OÚ.

Čl. 2
Definice vybraných pojmů a zkratk

- (1) OÚ jsou 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.

- (2) „Zpracováním OÚ“ se rozumí jakákoliv operace nebo soubor operací s OÚ nebo soubory OÚ, 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.
- (3) „Správcem OÚ“ se rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování OÚ; 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.
- (4) „Zpracovatelem OÚ“ se rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.
- (5) „Profilováním“ se rozumí jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu.
- (6) „Pseudoanonymizací OÚ“ se rozumí zpracování OÚ tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě.
- (7) „Evidencí OÚ“ se rozumí jakýkoliv strukturovaný soubor OÚ přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska.
- (8) „Příjemcem OÚ“ se rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou OÚ poskytnuty, ať už se jedná o třetí stranu, či nikoli. Orgány veřejné moci, které mohou získávat OÚ údaje v rámci zvláštního šetření v souladu s právem členského státu, se za příjemce nepovažují; zpracování těchto OÚ těmito orgány veřejné moci musí být v souladu s použitelnými pravidly ochrany OÚ pro dané účely zpracování.
- (9) „Třetí stranou“ se rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, jež je oprávněna ke zpracování OÚ.
- (10) „Souhlasem“ je jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle (jednání), kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých OÚ.
- (11) „Porušením zabezpečení OÚ“ je porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných OÚ.
- (12) „Genetickými údaji“ se rozumí OÚ týkající se zděděných nebo získaných genetických znaků fyzické osoby, které poskytují jedinečné informace o její

fyzilogii či zdraví a které vyplývají zejména z analýzy biologického vzorku dotčené fyzické osoby.

- (13) „Biometrickými údaji“ jsou OÚ 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.
- (14) „Údaji o zdravotním stavu“ jsou OÚ týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu.
- (15) Definice dalších pojmů užitých při zacházení a ochraně OÚ jsou uvedeny v čl. 4 Nařízení, případně v textu či přílohách této směrnice tam, kde je to účelné.

Čl. 3

Odpovědnost PA ČR a stanovení osob odpovědných za zajištění ochrany OÚ

- (1) PA ČR je subjektem odpovědným za zpracování OÚ uvedených v čl. 1 odst. 2. Dle konkrétních případů může PA ČR vystupovat jak v roli správce, v některých případech i v roli zpracovatele. Za účelem naplňování ochrany OÚ tak, jak je požadováno Nařízením a zákonem o ochraně OÚ, jsou v této směrnici stanoveny osoby odpovědné za zajišťování výše uvedeného účelu.
- (2) Rektor - postavení rektora je dáno zákonem č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů a Statutem PA ČR. Rektor jedná jako statutární orgán PA ČR odpovědný za dodržování zásad, pravidel a postupů při zpracování OÚ vně i dovnitř PA ČR.
- (3) Kvestor - odpovídá rektorovi za dodržování zásad, pravidel a postupů při zpracování OÚ realizovaných v oblasti své působnosti dané Organizačním řádem PA ČR a pověřením kvestora rektorem.
- (4) Kancléř - odpovídá rektorovi za dodržování zásad, pravidel a postupů při zpracování OÚ realizovaných v rámci oblasti své působnosti dané Organizačním řádem PA ČR a pověřením kancléře rektorem.
- (5) Prorektorů - odpovídají rektorovi za dodržování zásad, pravidel a postupů při zpracování OÚ realizovaných v rámci oblasti jejich činnosti a působností daných Organizačním řádem PA ČR a pověřením konkrétního prorektora rektorem.
- (6) Děkaní jednotlivých fakult - odpovídají rektorovi za dodržování zásad, pravidel a postupů při zpracování OÚ realizovaných jim podřízenými zaměstnanci fakulty při plnění jejich pracovních povinností, případně dalšími fyzickými či právníckými osobami, které zpracovávají OÚ na základě smlouvy ve věcech jim svěřených Organizačním řádem PA ČR.
- (7) Interní auditor, Bezpečnostní ředitel, vedoucí všech jiných pracovišť PA ČR odpovídají rektorovi PA ČR za dodržování zásad, pravidel a postupů při zpracování OÚ realizovaných jim podřízenými zaměstnanci při plnění jejich pracovních povinností, případně dalšími fyzickými či právníckými osobami, které zpracovávají OÚ na základě smlouvy ve věcech jim svěřených Organizačním řádem PA ČR, případně na základě pověření těchto pracovníků rektorem.

Čl. 4

Koordinátor zpracování OÚ

- (1) Koordinátor zpracování OÚ (dále jen „koordinátor“) odpovídá za koordinaci procesů a výstupů podle směrnice, Nařízení a dalších relevantních obecně závazných právních předpisů za součást PA ČR, za kterou byl ustanoven.
- (2) Koordinátorem zpracování osobních údajů je stanoven na fakultách vedoucí kanceláře děkana fakulty, na součástech zpravidla ekonom součásti. Na rektorátu se tato pozice neustanovuje.
- (3) V případech, kdy není ustanovena osoba koordinátora dle odst. 2, vykonává působnost Koordinátora osoba uvedená v čl. 3 směrnice, přičemž je o této skutečnosti povinna písemně informovat pověřence pro ochranu osobních údajů, a to bez zbytečného odkladu.

Čl. 5

Garanti zpracování OÚ

- (1) Za účelem zajištění ochrany OÚ a jejich zpracování v souladu s Nařízením jsou pro jednotlivé případy, či oblasti zpracování, ustanoveni garanti zpracování OÚ (dále jen „garant“).
- (2) Garanty ustanovuje do funkce rektor. Návrh na ustanovení osoby garantem předkládají prorektor, kvestor, děkani, bezpečnostní ředitel, interní auditor, vedoucí jiných pracovišť a účelových zařízení a kancléř, za agendy/oblast/činnost, kterou přímo řídí. Při návrhu na ustavení garanta se zohlední ustanovení odst. 7 tohoto článku.
- (3) Návrh na ustanovení osoby garantem předkládají rektorovi všichni povinní dle Čl. 5 bodu (2) nejpozději ke dni nabytí účinnosti Nařízení.
- (4) Garant je osoba přímo odpovědná za dodržování zásad, pravidel a postupů (uvedených v této směrnici, Nařízení a dalších relevantních obecně závazných právních předpisech) při zpracování OÚ realizovaných v jemu svěřené agendě/činnosti. O činnosti spojené s výkonem funkce garanta bude upravena jeho pracovní náplň. Garant odpovídá za uvedené činnosti od data svého ustanovení až po ukončení činnosti, a to včetně zajištění bezpečné archivace dat.
- (5) Garant poskytuje aktivní a včasnou součinnost při vyřizování žádosti subjektu údajů.
- (6) Garant je dále povinen poskytovat veškerou nutnou součinnost všem osobám, které zajišťují nebo se jinak podílejí na ochraně osobních údajů.
- (7) Garanty pro jednotlivé případy/oblasti/činnosti zpravidla jsou:
 - a) na fakultách – vedoucí kanceláře děkana, vedoucí studijního oddělení, vedoucí příslušného referátu nebo oddělení děkanátu; není-li takový vedoucí ustanoven, stává se garantem koordinátor.
 - b) na součástech - vedoucí příslušného oddělení, není-li takový vedoucí ustanoven, stává se garantem koordinátor zpracování osobních údajů;
 - c) na rektorátu – vedoucí jednotlivých odborů a oddělení, v případě referátu podřízeného prorektorovi vykonává působnost garanta zpravidla tento prorektor.

- (8) V případech již existujících systémů zpracování osobních údajů je garant ustanoven dnem účinnosti této směrnice. U nových systémů bude garant určen před zahájením zpracování údajů.
- (9) Garant provádí v jemu svěřené agendě posouzení vlivu nově zamýšlených operací zpracování na ochranu OÚ, je-li tak podle čl. 35 Nařízení třeba. Za tímto účelem si následně vyžádá posudek pověřence pro ochranu OÚ.

Čl. 6

Další oprávněné osoby

- (1) S OÚ mohou přicházet do styku:
 - a) osoby, které jsou podle charakteristiky příslušného zpracování údajů pověřeny sběrem a dalším zpracováním OÚ v listinné podobě nebo vkládáním do elektronických informačních systémů,
 - b) osoby, které jsou nadřizeny osobám uvedeným v písm. a) po organizační či metodické linii;
 - c) osoby, které zabezpečují organizační, funkční a technickou správu příslušného zpracování údajů (zpravidla analytici, programátoři, správci systémů, sítí, referenti na jednotlivých útvarech apod.);
 - d) další osoby v jiných agendách (např. právních), které jsou podle charakteristiky příslušného zpracování údajů pověřeny, aby tyto OÚ využívaly k plnění svých úkolů,
 - e) garanti,
 - f) pověřenec pro ochranu OÚ.
- (2) Garant vede seznamy oprávněných osob. V případě přijetí či přeřazení osob na místa s pověřením přicházet do styku s OÚ dle odstavce 1 je nezbytné jejich předchozí průkazné seznámení s touto směrnicí, Nařízením a dalšími relevantními obecně závaznými právními předpisy. Za splnění této podmínky je odpovědný garant.
- (3) Osoby uvedené v odstavci 1 jsou povinny zpracovávat OÚ vždy jen v rozsahu nezbytném pro zabezpečení agendy při plném respektování zákonnosti zpracování a sledování oprávněných zájmů subjektu údajů dle OÚ dle čl. 6. Nařízení.
- (4) Osoby uvedené v odstavci 1 jsou povinny zachovávat mlčenlivost o OÚ a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení OÚ. Povinnost mlčenlivosti trvá i po ukončení pracovního poměru, studia nebo výkonu příslušných prací. Osoby uvedené v odst. 1 písm. a) až e) jsou povinny podrobit se uzavření Dohody o mlčenlivosti.

Čl. 7

Závěrečné a jiné práce studentů, účastníků CŽV a realizace projektů

V případech, kdy by u závěrečných prací studentů (bakalářské, magisterské, rigorózní a disertační, případně odborné práce účastníků CŽV) byly zpracovávány OÚ, je vedoucí práce/školitel povinen seznámit zpracovatele s povinnostmi dle Nařízení

a této směrnice a zajistit případné další kroky v souladu s touto směrnicí. Obecně se tato povinnost týká i jiných případů, kdy osoba v rámci svých studijních či pracovních povinností realizuje projekt či jinou činnost, v rámci níž jsou zpracovávány OÚ.

Čl. 8 Pověřenec pro ochranu OÚ

- (1) Pověřenec pro ochranu OÚ na PA ČR (dále jen „pověřenec“) je jmenován rektorem. Rektor jej může také odvolat.
- (2) Pověřenec je zaměstnancem PA ČR a je při výkonu této činnosti přímo podřízen rektori. Pověřenec je jmenován v souladu Nařízením jakožto povinnost veřejného subjektu, kterou PA ČR má.
- (3) V případě nepřítomnosti pověřence jej zastupuje kancléř rektora (dále také jako „zástupce pověřence“). V takovém případě poskytne pověřenec zástupci pověřence součinnost nezbytnou pro plnění povinností pověřence zástupcem pověřence. Zástupce pověřence je povinen neprodleně informovat pověřence o všech krocích učiněných v jeho nepřítomnosti.
- (4) Pověřenec je zapojen do veškerých procesů a záležitostí souvisejících s ochranou a zpracováním OÚ na PA ČR.
- (5) Pověřenci je umožněn přístup k OÚ, operacím zpracování a k veškerým zdrojům potřebným pro plnění úkolů, uvedených čl. 11. Nařízení.
- (6) Pověřenec je v souvislosti s výkonem svých úkolů vázán mlčenlivostí.
- (7) Údaje o pověřenci, včetně kontaktu na něj, jsou uvedeny ve veřejné části internetových stránek PA ČR.
- (8) Pověřenec vykonává zejména tyto úkoly:
 - a) poskytuje informace a poradenství zaměstnancům a studentům PA ČR, kteří provádějí zpracování OÚ, o jejich povinnostech podle této směrnice, Nařízení a dalších obecně závazných právních předpisů v oblasti ochrany OÚ;
 - b) monitoruje soulad s touto směrnicí, Nařízením, dalšími obecně závaznými právními předpisy v oblasti ochrany OÚ a s koncepcemi PA ČR v oblasti ochrany OÚ, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů;
 - c) dohlíží nad realizací ochrany a zpracování OÚ,
 - d) poskytuje poradenství a odbornou pomoc, pokud jde o posouzení vlivu na ochranu OÚ, a monitoruje jeho uplatňování podle čl. 35 Nařízení;
 - e) po předchozí konzultaci s osobami uvedenými v čl. 3 této směrnice ohlašuje případy porušení zabezpečení OÚ dozorovému úřadu (čl. 33 Nařízení) a oznamuje případy porušení ochrany OÚ subjektu údajů (čl. 34 Nařízení);
 - f) spolupracuje a komunikuje s dozorovým úřadem;
 - g) působí jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování OÚ, včetně předchozí konzultace podle článku 36 Nařízení, a případně vede konzultace v jakékoli jiné věci;
 - h) přijímá od zaměstnanců PA ČR návrhy na zahájení nového, resp. změnu dosavadního zpracování OÚ a zaujímá k takovýmto návrhům stanoviska;

- i) komunikuje se subjekty údajů, kteří se na něj mohou obracet ve všech záležitostech souvisejících se zpracováním jejich OÚ a výkonem jejich práv dle této směrnice a Nařízení;
 - j) plní další úkoly vyplývající pro jeho pozici z Nařízení, zákona či jiných obecně závazných právních předpisů, či vyplývajících z této směrnice a ostatních předpisů PA ČR.
- (9) Pověřenec dohlíží na fungování Registru zpracování OÚ PA ČR podle čl. 10 této směrnice.
- (10) Pověřenec bere při plnění svých úkolů patřičný ohled na riziko spojené s činnostmi zpracování a současně přihlíží k povaze, rozsahu, kontextu a účelům zpracování.

Čl. 9

Působnost pověřence na PA ČR

- (1) Dozví-li se pověřenec, že hrozí porušení pravidel na ochranu OÚ vyplývajících z Nařízení, zákona o ochraně OÚ či této směrnice nebo je-li porušení zjištěno, je povinen na to upozornit garanta a písemně doporučit odstranění závadného či rizikového stavu. Garant je povinen v přiměřené lhůtě projednat s pověřencem stav, a pokud se se zjištěním pověřence ztotožnil, zdržet se dalšího závadného či rizikového chování. Garant je rovněž povinen přijmout veškerá opatření k tomu, aby se situace neopakovala. Nesouhlasí-li garant s doporučením pověřence, tak pověřenci písemně zdůvodní vytýkané chování a uvede důvody, proč se domnívá, že nedošlo, či nehrozí, že by mohlo dojít k porušení pravidel uvedených v první větě. V takovém případě pověřenec oznámí tuto skutečnost věcně příslušným osobám uvedeným v čl. 3 této směrnice a postoupí jim celou dokumentaci. Dále pověřenec za přítomnosti garanta a koordinátora projedná celou věc přímo s rektorem, který rozhodne o dalším postupu.
- (2) Hrozí-li porušení pravidel na ochranu OÚ vyplývajících z Nařízení, zákona o ochraně osobních údajů či této směrnice, nebo je-li porušení zjištěno a pro daný případ/oblast/činnost zpracování nebyl stanoven garant, je pověřenec povinen na to písemně upozornit věcně příslušné osoby uvedené v čl. 3 této směrnice.
- (3) Pověřenec je povinen dát podnět k přijetí obecných či individuálních opatření v oblasti ochrany OÚ osobám uvedeným v čl. 3 vždy, když:
- a) na základě svých zjištění dle odstavce 1 zjistí hrozbu porušení či porušení pravidel;
 - b) to bude vhodné v návaznosti na zobecňování praxe v oblasti ochrany OÚ.
- (4) Ustanoveními odstavců 1 až 3 není dotčena povinnost pověřence po předchozí konzultaci s osobami uvedenými v čl. 3 této směrnice ohlásit porušení zabezpečení OÚ dozorovému úřadu a subjektu údajů dle čl. 8 odst. 7 písm. e) této směrnice.

Čl. 10

Registr zpracování osobních údajů PA ČR

- (1) PA ČR je povinna vést záznamy o činnostech zpracování OÚ. Za účelem dosažení přehledu o zpracování OÚ na PA ČR se zřizuje v elektronické formě a listinné formě Registr činností zpracování OÚ na PA ČR (dále jen „Registr“). Registr v elektronické i listinné formě obsahuje záznamy o všech kategoriích činností stanovených v čl. 30 Nařízení, Registr v listinné podobě dále pak doplňuje vedené záznamy v podrobnostech průběžně zjištěných nebo potřebných pro zajištění opatření bezpečného nakládání s OÚ při vedení jednotlivých agend.
- (2) Provozem tohoto registru je pověřeno pracoviště PA ČR Oddělení informačních technologií (dále jen „OIT“). Odpovědným za provoz registru je vedoucí OIT.
- (3) Za vedení záznamů v obou Registrech odpovídá pověřenec. Záznamy o činnostech vedené v Registrech jsou průběžně aktualizovány ve vazbě na uvedení do souladu s požadavky zákona o ochraně OÚ, dle provozních potřeb, změn procesů apod.
- (4) Pracoviště PA ČR, které zpracovávají nebo nově chtějí zpracovávat OÚ chráněné touto směrnicí, a Registr neobsahuje záznam o činnostech zpracování těchto OÚ, resp. chtějí změnit dosavadní způsob zpracování OÚ, oznámí tuto skutečnost prostřednictvím garanta pověřenci a připraví podklady pro aktualizaci v Registru. Pověřenec pak následně zajistí aktualizaci záznamu v Registru.
- (5) Oznámení dle odst. 4 musí obsahovat úplnou charakteristiku příslušného zpracování osobních údajů. Rozsah stanoví Příloha č. 1 a Příloha č. 2 této směrnice.
- (6) V případě, že změna způsobu zpracování či procesu zpracování OÚ má dopad na rozsah zpracovávaných OÚ, změnu způsobu zpracování (jiné automatizované postupy) nebo dobu zpracování apod., je povinností garanta vždy před započítím vyžádat si od pověřence předchozí stanovisko k postupu realizace a nastavení typového řešení ochrany OÚ.
- (7) Změnu v dosavadním způsobu zpracování OÚ lze realizovat až poté, kdy garant od pověřence obdrží oficiální stanovisko na základě výsledku oznámení změny. Je-li stanovisko záporné, je celá věc konzultována s osobami uvedenými v čl. 3 této směrnice a rektorem, který rozhodne o dalším postupu.

Čl. 11

Zásady zpracování osobních údajů

- (1) Zásady zpracování OÚ jsou uvedeny v kapitole 2 Nařízení. V souladu s ním musí být OÚ:
 - a) ve vztahu k subjektu údajů zpracovány zákonným, korektním a transparentním způsobem;
 - b) shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný;
 - c) přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovány;

- d) přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby OÚ, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny;
 - e) uloženy 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 OÚ, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením.
- (2) Za dodržování zásad dle odstavce 1 odpovídají osoby uvedené v čl. 3 až 7 této směrnice a musí být rovněž schopny toto dodržení souladu doložit.

Čl. 12

Zákonnost zpracování

- (1) V souladu s čl. 6 Nařízení je zpracování zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu:
- a) subjekt údajů udělil souhlas se zpracováním svých OÚ pro jeden či více konkrétních účelů (Podmínky vyjádření souhlasu jsou podrobně uvedeny v čl. 7 a 8 Nařízení);
 - b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;
 - c) zpracování je v souladu s platnými obecně závaznými právními předpisy 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 v souladu s platnými obecně závaznými právními předpisy 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 OÚ, zejména pokud je subjektem údajů dítě.
- (2) Odstavec 1 písm. f) se netýká zpracování OÚ prováděného PA ČR v případech, kdy PA ČR vystupuje jako orgán veřejné moci ve věcech jí svěřených zákonem.
- (3) Pokud zpracování pro jiný účel, než pro který byly OÚ shromážděny, není založeno na souhlasu subjektu údajů nebo na platných obecně závazných právních předpisech, zohlední garant v zájmu zjištění toho, zda je zpracování pro jiný účel slučitelné s účely, pro něž byly OÚ původně shromážděny, mimo jiné:
- a) jakoukoli vazbu mezi účely, kvůli nimž byly OÚ shromážděny, a účely zamýšleného dalšího zpracování;

- b) okolnosti, za nichž byly OÚ shromážděny, zejména pokud jde o vztah mezi subjekty údajů a PA ČR;
- c) povahu OÚ, zejména zda jsou zpracovávány zvláštní kategorie OÚ podle čl. 9 Nařízení nebo OÚ týkající se rozsudků v trestních věcech a trestných činů podle čl. 10 Nařízení;
- d) možné důsledky zamýšleného dalšího zpracování pro subjekty údajů;
- e) existenci vhodných záruk, mezi něž může patřit šifrování nebo pseudoanonymizace.

Čl. 13

Zpracování zvláštních kategorií osobních údajů

- (1) Je zakázáno zpracování OÚ, 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 v případech, na které se nevztahuje odstavce (2) a (3).
- (2) Výjimky ze zákazu zpracování OÚ dle odstavce 1 jsou dány čl. 9 Nařízení.
- (3) Výjimkami ze zákazu v odstavci 1 jsou také údaje o:
 - a) zdravotním stavu v osobních evidencích zaměstnanců a studentů za předpokladu, že tyto údaje byly subjektem údajů do zmíněné evidence dobrovolně předány a jsou vedeny v jeho prospěch (např. mají vliv na přijetí ke studiu, poskytování služeb osobám se specifickými nároky, ubytování v ubytovacích zařízeních PA ČR nebo výpočet jeho daňové povinnosti či jiných zákonných dávek),
 - b) členství v odborových organizacích působící na PA ČR uvedené v osobních a mzdových evidencích zaměstnanců za předpokladu, že byly subjektem údajů do zmíněné evidence dobrovolně předány a slouží pro placení členských příspěvků či jiných dávek, včetně účtování o těchto platbách,
 - c) biometrické údaje, které umožňují přímou identifikaci nebo autentizaci subjektu údajů,
 - d) zvláštní kategorie OÚ zpracovávané pro účely projektů/výzkumu.
- (4) Zpracování údajů definovaných v odstavci 1 může probíhat pouze na základě výslovného souhlasu subjektu údajů. Tento souhlas musí být dán písemně, podepsán subjektem údajů a musí z něho být zřejmé, jakých údajů se týká, k jakému účelu, na jaké období a kdo jej poskytuje. Subjekt údajů svým podpisem také potvrzuje, že byl předem poučen o svých právech.
- (5) Zpracování údajů podle odstavce 3 písm. c) může být používáno pouze tehdy, pokud paralelně existuje možnost dosáhnout daného účelu užitím jiných identifikačních nebo autentizačních prostředků, které nebudou na biometrických údajích závislé, a subjekt údajů bude mít možnost volby mezi nimi.
- (6) Zpracování OÚ, které nevyžaduje identifikaci subjektu údajů, upravuje čl. 11 Nařízení.

Čl. 14

Informace poskytované subjektu údajů

- (1) PA ČR v roli správce poskytuje subjektu údajů v souladu s čl. 12 Nařízení stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků veškeré informace uvedené v čl. 13 a 14 Nařízení a učiní veškerá sdělení podle čl. 15 až 22 a 34 Nařízení o zpracování. Informace je subjektu údajů poskytována v elektronické formě na webových stránkách PA ČR a rovněž v informačních systémech PA ČR.
- (2) Subjekty údajů se mohou obracet ve všech záležitostech souvisejících se zpracováním jejich OÚ a výkonem jejich práv dle této směrnice a Nařízení na pověřence.

Čl. 15

Práva subjektu údajů

Právo subjektu údajů na:

- a) přístup k OÚ upravuje čl. 15 Nařízení;
- b) opravu OÚ upravuje čl. 16 a 19 Nařízení;
- c) výmaz OÚ upravuje čl. 17 a 19 Nařízení;
- d) omezení zpracování OÚ upravuje čl. 18 a 19 Nařízení;
- e) přenositelnost OÚ upravuje čl. 20 Nařízení;
- f) právo vznést námitku a ochrana proti automatizovanému individuálnímu rozhodování upravuje čl. 21 a 22 Nařízení.

Čl. 16

Zveřejňování OÚ

- (1) Zveřejněním OÚ se rozumí jejich zpřístupnění konkrétně určeným osobám či skupinám osob, zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu (např. ve veřejné části internetových stránek PA ČR).
- (2) OÚ zaměstnance PA ČR chráněné podle této směrnice lze zveřejňovat nejvýše v rozsahu:
 - a. jméno a příjmení;
 - b. tituly;
 - c. fotografie;
 - d. pracovní zařazení na PA ČR;
 - e. zařazení v organizační struktuře PA ČR;
 - f. zastávané funkce na PA ČR;
 - g. kontaktní údaje v souvislosti s PA ČR (adresy pracovišť, telefonní a faxová čísla, e-mailové adresy);
 - h. životopis;
 - i. průběh akademické kvalifikace;
 - j. podíl na jednotlivých formách tvůrčí činnosti PA ČR;

- k. informace o vydaných publikacích;
- l. výuka uskutečňovaná na PA ČR;
- m. akademické osobní www-stránky (tj. www-stránky zaměstnanců a studentů PA ČR související s jejich akademickým anebo studijním působením na PA ČR);
- n. případně další údaje, které si zde subjekt o sobě zveřejnil sám.

Subjekt údajů má právo zvolit si konkrétní rozsah zveřejňovaných údajů uvedených pod písm. d), i), a n), případně tyto údaje nezveřejnit vůbec.

(3) OÚ studenta PA ČR chráněné podle této směrnice lze zveřejňovat nejvýše v rozsahu:

- a) jméno a příjmení;
- b) tituly;
- c) fotografie;
- d) studijní program /studijní obor na PA ČR, do něhož je/byl student zapsán;
- e) rok zahájení studia, ročník studia;
- f) rok ukončení studia, údaj o absolutoriu, případně o jiném způsobu ukončení studia;
- g) kontaktní údaje v souvislosti s PA ČR (e-mailová adresa);
- h) osobní www-stránky (tj. www-stránky studentů PA ČR související s jejich akademickým anebo studijním působením na PA ČR);
- i) případně další údaje, které si subjekt o sobě zveřejnil sám.

Subjekt údajů student má právo zvolit si konkrétní rozsah zveřejňovaných údajů uvedených pod písm. c), h), a i), případně tyto údaje nezveřejnit vůbec.

(4) Údaje uvedené v odstavci 2 lze zveřejňovat pouze o subjektech údajů, jež:

- a) jsou zaměstnanci PA ČR;
- b) jsou zaměstnanci či studenti PA ČR a aktuálně působí v samosprávných akademických či poradních orgánech PA ČR;

(5) Údaje uvedené v odstavci 3 lze zveřejňovat pouze o subjektech údajů, jež:

- a) jsou studenty PA ČR;
- b) jsou absolventy PA ČR;

(6) V případě akademických funkcionářů a vedoucích součástí PA ČR bude zveřejňování OÚ upravováno individuálně.

(7) V případě akademických funkcionářů a osob aktuálně působících v samosprávných akademických či poradních orgánech PA ČR, které nejsou v pracovním poměru k PA ČR, bude zveřejňování OÚ upravováno individuálně.

Čl. 17

Využití studijního informačního systému PA ČR

- (1) Pro účely správy studia a vedení elektronického výkazu o studiu využívá PA ČR studijní informační systém (dále jen „SIS“). Využití SIS k shora uvedeným účelům je pro zaměstnance PA ČR a studenty povinné.
- (2) K OÚ uvedeným v SIS mají přístup zaměstnanci PA ČR v rozsahu potřebném pro výkon jejich zaměstnání na PA ČR a dále subjekt údajů. Třetím osobám, studentům PA ČR, je zpřístupněn pouze údaj týkající se zařazení subjektu údajů do jednotlivých vyučovacích skupin v rámci studijních předmětů a konaných zkoušek a zápočtů, případně dalších způsobů ukončení jednotlivých studijních předmětů.
- (3) Zobrazení OÚ je možné pouze po ověření přihlášením do systému zadáním uživatelského jména a hesla.

Čl. 18

Poskytování OÚ třetím stranám

- (1) Poskytování OÚ třetím stranám mimo PA ČR se řídí touto směrnicí, Nařízením a platnými obecně závaznými právními předpisy.
- (2) O každém poskytnutí OÚ třetí straně mimo PA ČR musí být předem písemně informován pověřenec se sdělením rozsahu poskytnutých údajů, účelu poskytnutí a identifikací třetí strany.
- (3) Za dodržování správného postupu při poskytování OÚ třetím osobám mimo PA ČR v souladu s touto směrnicí, Nařízením a platnými obecně závaznými právními předpisy je odpovědný garant ustanovený pro daný případ/oblast zpracování. Není-li pro daný případ/oblast zpracování ustanoven garant, odpovídají za dodržování správného postupu při poskytování OÚ třetím osobám mimo PA ČR věcně příslušné osoby uvedené v čl. 3 této směrnice.

Čl. 19

Zabezpečení osobních údajů

- (1) Písemnosti a mobilní/externí/přenosné technické nosiče informací, jimiž disponuje PA ČR a které obsahují OÚ chráněné podle této směrnice, musí být uchovávány pouze v uzamykatelných skříních na pracovištích PA ČR, případně na jiných bezpečných místech určených charakteristikou příslušného zpracování údajů, nebo zabezpečeny šifrováním.
- (2) Pokud jsou zpracovávány OÚ, které se bezprostředně vztahují k činnostem vykonávaným na PA ČR (např. docházkové archy, odpovědní listy, testy, poznámkové bloky, prezenční listiny apod.), postupuje se při jejich zabezpečení obvyklým způsobem tak, aby se předcházelo riziku zneužití OÚ. Další povinnosti stanovené v tomto článku se na zpracování takových OÚ použijí pouze v takovém rozsahu, v jakém to odpovídá jejich povaze a okolnostem jejich obvyklého zpracování.

- (3) Počítače a další technické prostředky, na nichž jsou uložena data obsahující OÚ chráněné podle této směrnice, musí být zabezpečeny před volným přístupem neoprávněných osob, zpravidla přístupovými hesly, šifrováním či uzamčením.
- (4) Kopie OÚ chráněných podle této směrnice musí být pořizovány na technické nosiče informací podle provozních pravidel stanovených pro jednotlivá zpracování údajů a uchovávány v uzamykatelných skříních na pracovištích PA ČR, případně na jiných bezpečných místech určených charakteristikou příslušného zpracování údajů, nebo zabezpečeny šifrováním, musí být ukládány zásadně vždy v jiné místnosti než originální údaje.
- (5) Informační aktiva, která sloužila k uchovávání či přenosu osobních údajů a již nejsou dále potřebná nebo dosáhla konce svojí životnosti, musí být bezpečně zlikvidována a záznam o jejich likvidaci je uchován u garanta, který předá vždy na konci kalendářního roku souhrnnou zprávu o likvidaci pověřenci.
- (6) V případě, kdy garant, oprávněná osoba anebo zaměstnanec PA ČR zjistí nebo nabude podezření, že by mohlo dojít nebo že došlo k porušení zabezpečení OÚ, je povinen to neprodleně oznámit pověřenci a osobám uvedeným v čl. 3 této směrnice.
- (7) Ohlašování případů porušení zabezpečení OÚ dozorovému orgánu (čl. 33 Nařízení) a oznamování případů porušení ochrany OÚ subjektu údajů (čl. 34 Nařízení) provádí po předchozí konzultaci s osobami uvedenými v čl. 3 této směrnice pověřenec.

Čl. 20

Technická opatření k zajištění bezpečnosti OÚ v elektronické formě

- (1) Přístup k osobním údajům je přidělován zaměstnancům PA ČR jen v rozsahu nezbytně nutném pro výkon funkce. Za tímto účelem koordinátor ve spolupráci s garantem udržuje evidenci jednotlivých rolí týkajících se bezpečnosti IT, u nichž je jednoznačně stanovena rozsah přístupu k OÚ, zodpovědnost a pracovní náplň za účelem snížit rizika vyplývajících z lidského faktoru. Evidence je uložena u pověřence.
- (2) Pokud provoz IT, zpracování účetnictví či jiné externě zpracovávané agendy vyžadují přístup dodavatelů, musí být této přístup řešen smluvně, v souladu s bezpečnostní dokumentací tak, aby byla zajištěna bezpečnost osobních údajů uvnitř i vně společnosti zpracovávající OÚ. O přístupu dodavatele je nutno informovat pověřence a vyžádat si jeho stanovisko. V případě nesouhlasného stanoviska rozhodne o povolení přístupu rektor.
- (3) Externí zpracování OÚ povoluje rektor po předchozím vyjádření pověřence. Výběr potencionálních zpracovatelů OÚ pro PA ČR je podložen schopností uzavřít a dodržovat povinnosti stanovené zpracovatelskou smlouvou, dostatečným zabezpečením osobních údajů, dobrou pověstí dodavatele v rámci ochrany osobních údajů, relevantní certifikací ÚOOÚ nebo ochrany informací obecně, ev. dalšími relevantními faktory ve vztahu ke konkrétnímu účelu zpracování.
- (4) Je povoleno provozovat pouze schválený, legálně nabytý a evidovaný SW a HW ve shodě s licenčním ujednáním výrobce a způsobů využití. Tento SW a HW majetek je evidován a jejich nákup se řídí příslušnými platnými normami PA ČR.

- (5) Osobní a citlivé údaje nesmí opustit chráněné IT prostředí PA ČR. Pokud zaměstnanec potřebuje s OÚ pracovat mimo pracoviště PA ČR, je oprávněn tyto údaje z disků PA ČR nebo úložiště stáhnout na externí úložiště jen v nezbytně nutném rozsahu a po nezbytně nutnou dobu a po ukončení práce zajistit bezpečnou likvidaci těchto dat z externího zařízení.
- (6) Zaměstnanci a studenti jsou povinni používat pro pracovní či studijní účely oficiálně přidělené obecné či osobní e-mailové adresy se zakončením „@pacr.eu“. Výjimku schvaluje pověřenec.
- (7) Použití veřejných uložišť, služeb a nástrojů (Dropbox, Goggle Drive, uloz.to, uschovna.cz, torrents, P2P, Basecamp, Slack, apod.) bez uzavřené smlouvy mezi poskytovatelem služeb a PA ČR je zakázáno.

Čl. 21 Závěrečná ustanovení

- (1) Gestorem této směrnice je pověřenec.
- (2) Kontrolu dodržování této směrnice vykonává pověřenec.
- (3) Povinnost prokazatelně seznámit s touto směrnicí své podřízené má každý vedoucí zaměstnanec, kterému je přiznán příplatek za vedení, pakliže neprovedla toto prokazatelné seznámení osoba uvedená v čl. 3.
- (4) Tato směrnice nabývá platnosti a účinnosti dnem vydání.

Č.j.: PA-1071-2/ČJ-2018-820000

doc. JUDr. Mgr. Josef Salač, Ph.D., dr. h. c.
rektor
schváleno elektronicky

1. KATEGORIE OBLASTÍ ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ NA PA ČR

Přehled hlavních kategorií

1. Řízení, samospráva a provoz PA ČR
2. Ostraha majetku, bezpečnost
3. Vzdělávací činnost
4. Vědecká, výzkumná a vývojová činnost
5. Tvůrčí činnost
6. Habilitační, profesorská a rigorózní řízení
7. Informační a propagační činnost
8. Poskytování veřejných služeb
9. Komerční činnost

Charakteristika kategorií

1. Řízení, samospráva a provoz PA ČR

- řízení organizace
- výkon samosprávy
- vědecká rada, akademické senáty
- personalistika
- hospodaření
- správa majetku
- provozní služby
 - knihovní služby
 - nakladatelské služby
 - podpora osob se specifickými nároky
 - datové a komunikační služby, telefonie
 - další
- správní činnosti
- smlouvy a smluvní vztahy

2. Ostraha majetku, bezpečnost

- kamerové systémy, přístupové systémy
- sledování síťového provozu
- záznamy z informačních a přihlašovacích systémů

3. Vzdělávací činnost

- vysokoškolské vzdělávání (akreditované studijní programy)
- celoživotní vzdělávání
- další vzdělávací činnost
- kurzy, placené vzdělávání
- přijímací řízení
- akreditace
- matrika studentů
- populárně naučné aktivity pro děti
- další komerční služby
- stipendia
- poplatky za studium
- zahraniční výměnné programy pro studenty a zaměstnance
- praxe studentů
- studijní a vzdělávací ocenění
- disciplinární řízení
- vysokoškolské kvalifikační práce

4. Vědecká, výzkumná a vývojová činnost

- evidence projektů
- publikační činnost
- duševní vlastnictví a transfer technologií
- konference
- projekty a výzkumná data
- smluvní výzkum
- vědecko-výzkumná spolupráce
- čestné vědecké hodnosti a tituly, medaile a ceny

5. Další tvůrčí činnost

- čestné vědecké hodnosti a tituly, medaile a ceny
- další

6. Habilitační, profesorská a rigorózní řízení

- habilitační řízení
- řízení ke jmenování profesorem
- rigorózní řízení

7. Informační a propagační činnost

- veřejné weby
- marketing a propagace
- absolventi

8. Poskytování veřejných služeb

- pořádání veřejných akcí
- spolupráce se státním a neziskovým sektorem

9. Komerční činnost

- prodej knih, reklamních předmětů PA ČR
- ubytovací a stravovací služby
- poradenství a expertní služby

2. KATEGORIE OSOBNÍCH ÚDAJŮ

Přehled

1. Adresní a identifikační údaje
2. Citlivé údaje
3. Popisné údaje
4. Studijní údaje
5. Ekonomické údaje
6. Pracovní údaje
7. Provozní a lokační údaje
8. Údaje o aktivitách subjektu
9. Údaje o jiné osobě
10. Jiné

Charakteristika kategorií

1. Adresní a identifikační údaje

- jméno, příjmení, datum a místo narození, rodinný stav, rodné číslo, titul, státní příslušnost, adresa (včetně elektronické), telefonní číslo, číslo osobního dokladu, digitální identifikátor, podpis apod.

2. Citlivé údaje

- národnostní, rasový nebo etnický původ [údaj o státní příslušnosti není citlivý údaj]
- členství v odborových organizacích
- politické postoje
- náboženské a filosofické přesvědčení
- odsouzení za trestný čin [výpis z rejstříku trestů, který dokládá beztrestnost, není citlivým údajem]
- zdravotní stav [potvrzení lékaře nebo zdravotnického zařízení (např. ze vstupní nebo preventivní lékařské prohlídky) o tom, zda pracovník je nebo není schopen vykonávat svoji práci, není citlivým údajem vypovídajícím o zdravotním stavu]
- sexuální orientace/život
- genetické údaje
- biometrické údaje [Za biometrický údaj se nepovažuje údaj o výšce, váze, barvě očí, konfekčních velikostech nebo rozměrech subjektů údajů apod., neboť tyto údaje neumožňují přímou identifikaci nebo autentizaci subjektu údajů].

[V případě provozování prostého kamerového systému se nejedná o zpracování biometrického údaje. Ke zpracování biometrických údajů by docházelo pouze, pokud by byly porovnávány některé biometrické charakteristiky subjektu údajů (systém identifikace lidské tváře, biometrické charakteristiky chůze apod.).]

3. Popisné údaje

- vzdělání, znalost cizích jazyků, odborná kvalifikace, znalosti a dovednosti, počet dětí, portrétní fotografie, video/audio záznam o osobě, vojenská služba, předchozí zaměstnání, zdravotní pojišťovna, členství v zájmových organizacích, trestní bezúhonnost, apod.

4. Studijní údaje

- záznamy o studiu a studijních aktivitách, studijní výsledky, studijní ocenění apod.

5. Ekonomické údaje

- bankovní spojení, bankovní karty, mzda, odměny, poplatky, závazky a pohledávky, objednávky, nákupy, ekonomická situace, vlastnictví a majetek, daně apod.

6. Pracovní údaje

- záznamy o práci a pracovních aktivitách, zaměstnavatel, pracoviště, pracovní zařazení a pozice, pracovní hodnocení, pracovní ocenění a tresty apod.

7. Provozní a lokační údaje

- typicky údaje z elektronických systémů vztahujících se ke konkrétnímu subjektu údajů — např. údaje o využití informačních systémů, o datovém provozu a elektronické komunikaci, o využívání telefonu, o přístupu do různých prostor, záznamy z kamerových systémů apod.

8. Údaje o aktivitách subjektu

- publikační činnost, údaje o odborných aktivitách, účasti na konferencích, zapojení do projektů, údaje o pracovních či studijních cestách apod.

9. Údaje o jiné osobě

- adresní a identifikační údaje člena rodiny, manžel/manželka, dítě, partner apod.

10. Jiné údaje

- uveďte jaké

3. KATEGORIE SUBJEKTŮ ÚDAJŮ

Přehled

1. Zaměstnanci
2. Studenti
3. Osoby se specifickými potřebami
4. Absolventi
5. Uchazeči (o studium, o zaměstnání)
6. Děti
7. Zákazníci
8. Účastníci výzkumu
9. Školitelé, spoluřešitelé, spoluautoři, autoři
10. Návštěvníci a účastníci akcí
11. Účastníci správního řízení
12. Jiné osoby

Charakteristika kategorií

1. Zaměstnanci

osoby v pracovně-právním vztahu k PA ČR (včetně zaměstnanců na dohodu - smluvních externistů), pracovníci na výměnných pobytech/stážích apod.

2. Studenti

studenti všech forem studia na PA ČR, studenti na výměnných pobytech apod.

3. Osoby se specifickými potřebami

osoby se zdravotním znevýhodněním (studenti, zaměstnanci, klienti, návštěvníci).

4. Absolventi

absolventi všech forem studia na PA ČR, vzdělávacích kurzů, školení, stáží apod.

5. Uchazeči

zájemci o studium, uchazeči o zaměstnání, účastníci výběrových a poptávkových řízení.

6. Děti

do 15 let věku [věková hranice dle národní úpravy o ochraně osobních údajů dětí]
(např. účastníci dětské univerzity či jiných akcí pořádaných PA ČR).

7. Zákazníci

fyzické osoby s komerčním vztahem k PA ČR (účastníci placených kurzů a akcí, externí čtenáři knihoven, klienti poskytovaných služeb — externí strážníci, hosté ubytovacích zařízení apod.)

8. Účastníci výzkumu

osoby účastnící se v roli zkoumaných subjektů či respondentů výzkumu realizovaného PA ČR.

9. Školitelé, spoluřešitelé, spoluautoři

osoby bez pracovně-právního vztahu k PA ČR podílející se na vzdělávacích či výzkumných aktivitách PA ČR v roli externích školitelů, konzultantů, spoluřešitelů projektů, spoluautorů publikací, autoři samostatných autorských děl, apod.

10. Návštěvníci a účastníci akcí

osoby účastnící se na nekomerčním základě akcí pořádaných PA ČR (dny otevřených dveří, exkurze, semináře, školení, konference, společenské akce) či navštěvující PA ČR z jiných důvodů (návštěvy, kontroly, aj.)

11. Účastníci správního řízení

osoby účastnící se správního řízení ve vztahu k PA ČR, stěžovatelé, žadatelé o přístup k informacím podle zákona o svobodném přístupu k informacím apod.

12. Jiné osoby

uved'te jaké

4. PRÁVNÍ DŮVOD ZPRACOVÁNÍ OÚ

Zpracování je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu.

Přehled

1. Ze zákona

2. Souhlas subjektu údajů
3. Plnění smlouvy
4. Zájem subjektu údajů
5. Zájem správce
6. Veřejný zájem

Charakteristika kategorií

1. Ze zákona

Zpracování je nezbytné pro splnění zákonné povinnosti, která se na PA ČR vztahuje.

2. Souhlas subjektu údajů

Subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů.

3. Plnění smlouvy

Zpracování je nezbytné pro jednání o uzavření nebo plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů.

4. Zájem subjektu údajů

Zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby.

5. Zájem správce

Zpracování je nezbytné pro účely oprávněných zájmů PA ČR či třetí strany.

6. Veřejný zájem

Zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřena PA ČR, 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.

5. TYP ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

1. manuální - vlastními zaměstnanci PA ČR
2. manuální - zpracovatelem
3. automatizované - vlastními systémy PA ČR
4. automatizované zpracovatelem
5. kamerovými systémy
6. biometrické systémy
7. jiný způsob zpracování – specifikujte

Minimální záznam o činnosti zpracování osobních údajů

1. **Název činnosti zpracování osobních údajů**
 - stručný a výstižný název
2. **Účel zpracování**
 - PROČ, za jakým účelem se daná činnost provádí, k čemu slouží, je nezbytné zpracovávat?
3. **Popis zpracování**
 - JAK a CO se při zpracování s osobními údaji provádí, podrobnější popis činnosti zpracování; systém/systémy používané při zpracování; vazba na jiné systémy
4. **Správce dat**
 - název organizace (PA ČR) a organizační jednotky organizace (součásti PA ČR); kontaktní (zodpovědná) osoba, případně vlastník procesu (byl-li již určen)
5. **Zpracovatel dat**
 - název organizace a organizační jednotky (jen je-li jiný než PA ČR); údaje o smlouvě se zpracovatelem, délka platnosti smlouvy
6. **Popis osobních údajů**
 - Výčet OÚ: podrobný výčet osobních údajů, které se v činnosti zpracování vyskytují;
 - Kategorie OÚ: soupis kategorií OÚ (viz číselník Příloha 1);
 - Doba uchovávání OÚ: jak dlouho se osobní údaje uchovávají, kdo nebo kde je určena délka uchovávání
7. **Subjekty osobních údajů**
 - Kategorie subjektů osobních údajů: kategorie subjektů údajů (SÚ), kterých se činnost týká (viz číselník Příloha 1)
 - Řákový počet SÚ: orientační počet SÚ (řádově)
8. **Právní důvod pro zpracování OÚ**
 - Viz číselník (ze zákona, plnění smlouvy, souhlas SÚ, atd.). V případě, že garant není schopen určit – pak uvést poznámku „Nutná konzultace s pověřencem.“
9. **Typ zpracování a způsob uložení dat**
 - v jaké podobě jsou OÚ primárně zpracovávány [automatizovaně/manuálně/kamery] a uchovávány [digitální/fyzické]

10. Přístup k osobním údajům

- Kdo má k OÚ přístup a v jakém rozsahu?: popište slovně
- Kategorie příjemců OÚ: komu jsou OÚ předávána (v rámci organizace/ČR/EU);
- Předávání OÚ mimo EU: ne / ano (komu, která OÚ, jak)

11. Pořizovatelé dat

- kdo a jakým způsobem OÚ pořizuje, odkud se přebírají, apod.

12. Priorita [prioritní/neprioritní]

- Prioritní: činnost zpracování představuje vysoké riziko pro práva a svobody SÚ, je třeba řešit ji přednostně.
- Neprioritní: nejde o vysoce rizikové zpracování, lze řešit až ve druhém plánu

Vzor Obsah ohlášení případů porušení zabezpečení osobních údajů

Porušením zabezpečení OÚ je chápána jakákoliv událost, která by mohla mít za následek porušení důvěrnosti, integrity nebo dostupnosti OÚ. Přesněji se dá porušení zabezpečení popsat jako neoprávněné zničení, ztráta, změna, neautorizované odhalení nebo neoprávněný přístup k OÚ. Mezi tyto případy patří **neúmyslné** i **záměrné** porušení ochrany. Konkrétními příklady porušení zabezpečení OÚ mohou být:

- přístup k OÚ neautorizovanou osobou,
- odeslání OÚ nesprávnému adresátu,
- ztráta nebo krádež zařízení obsahující OÚ,
- ztráta dostupnosti OÚ,
- neoprávněná změna OÚ.

Proces reakce na porušení zabezpečení:

1. Detekce a evidence

- odhalení případu porušení zabezpečení OÚ je následně zavedeno pověřencem do evidence incidentů.
- Způsoby detekce:
 - aktivity OIT — odhalení útoků, výsledky penetračních testů
 - oznámení realizované řadovým zaměstnancem, studentem anebo jakoukoli fyzickou osobou, která porušení zabezpečení odhalí (ztráta zařízení obsahující OÚ, nesprávná konfigurace použitého systému nebo nezajištění papírových dokumentů s OÚ, apod.)
 - oznámení na základě automatizovaných nástrojů za účelem detekce takových případů (automatizovaný monitoring síťového provozu, automatizované sledování pohybu OÚ v cloudovém prostředí.
 - oznámení od zpracovatele OÚ — kromě popsanych úkonů mohou být vykonány právní úkony vyplývající z uzavřené smlouvy se zpracovatelem OÚ.
- Po nahlášení bezpečnostního incidentu na centrálním místě (pověřenec) je tato událost zaevidovaná v centrální evidenci. Následně by mělo proběhnout vyšetření incidentu, které poskytne odpovědi na základní otázky:
 - Co bylo zdrojem, příčinou porušení zabezpečení?
 - Jaké osobní údaje a fyzické osoby byli tímto porušením dotknuty?

2. Kategorizace

- posouzení případu porušení zabezpečení ve smyslu určení potenciálních dopadů na dotčené fyzické osoby

3. Oznámení případu porušení zabezpečení relevantním subjektům — dozorovému orgánu nebo dotčeným fyzickým osobám.

- V případě, že je nepravděpodobné, že porušení zabezpečení má za následek nějaké riziko pro práva a svobody konkrétních fyzických osob, nemusí PA ČR tuto skutečnost nikomu oznamovat. Zdůvodnění neoznámení této skutečnosti musí být zdokumentované na centrálním místě.
- V případě, že je pravděpodobné, že porušení zabezpečení má za následek nějaké riziko pro práva a svobody fyzických osob, oznámí PA ČR tuto skutečnost příslušnému dozorovému orgánu.