NÁRODNÍ KNIHOVNA ČESKÉ REPUBLIKY

opatření generálního ředitele č. 10/2018

K zajištění ochrany fyzických osob v souvislosti se zpracováním jejich osobních údajů na pracovištích Národní knihovny České republiky

Část první
Obecná ustanovení

Čl. I
Úvodní ustanovení

1) Toto opatření generálního ředitele Národní knihovny České republiky (dále jen „generální ředitel NK a „opatření") se vydává na základě Nařízení Evropského parlamentu a Rady Evropské unie (dále jen „EU") 2016/679 ze dne 27.04.2016, 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"). Nařízení je známé pod zkratkou GDPR - General Data Protection Regulation.

2) Opatření určuje obecné zásady, pravidla a konkrétní postupy týkající se ochrany fyzických osob v souvislosti se zpracováním, evidencí, ukládáním a likvidací (výmazem/zničením) jejich osobních údajů v Národní knihovně České republiky (dále jen „NK"). Jedná se o zaměstnance, návštěvníky a další fyzické osoby využívající služeb NK nebo služby NK poskytující a dále určuje konkrétní metodická, systémová a organizační opatření a postupy zajišťující ochranu těchto osob při zpracování jejich osobních údajů v NK.

Čl. II
Účel, cíl a vymezení působnosti

1) Účelem opatření je zajistit, aby ochrana fyzických osob byla v souvislosti se zpracováním jejich osobních a citlivých údajů (dále jen „osobní údaje") technologicky neutrální, tj. nezávislá na použitých technologiích zpracování.

2) Cílem opatření je, v souladu s konkrétními organizačními a pracovními podmínkami, standardizovat pracovní postupy zpracování osobních údajů na jednotlivých pracovištích NK tak, aby byl zajištěn a dodržen soulad s požadavky ochrany osobních údajů stanovenými Nařízením.

3) Všechna obecná i konkrétní ustanovení ochrany fyzických osob v souvislosti se zpracováním jejich osobních údajů platí bez ohledu na státní příslušnost nebo bydliště těchto osob; uplatňují se na všechny informace týkající se každé identifikované nebo identifikovatelné fyzické osoby. Osobní údaje, na něž byla uplatněna pseudonymizace a jež by mohly být přiřazeny fyzické osobě na základě dodatečných informací, jsou považovány za informace o identifikovatelné fyzické osobě.

4) Povinnost dodržovat toto opatření se vztahuje na všechny zaměstnance NK bez ohledu na jejich pracovněprávní nebo jiný právní vztah k NK, nebo na jejich pracovní nebo funkční zařazení. Vztahuje se rovněž na externí spolupracovníky, včetně např. dodavatelů zboží nebo služeb NK, pokud mají přístup k osobním údajům.

5) Toto opatření se vztahuje na zcela nebo částečně automatizované zpracování osobních údajů a na neautomatizované zpracování těch osobních údajů, které jsou obsaženy v evidencích NK, nebo do nich mají být zařazeny.

6) Opatření se nevztahuje na zpracování osobních údajů právnických osob spolupracujících s NK, a zejména podniků vytvořených jako právnické osoby, včetně názvu, právní formy a kontaktních údajů takové právnické osoby.

Čl. III
Vymezení pojmů

Pro účely tohoto opatření se rozumí:
Osobními údaji - veškeré informace o identifikované nebo identifikovatelné fyzické osobě. 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 (dále jen „subjekt údajů").

Citlivými údaji - zvláštní kategorie osobních údajů, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo o členství v odborech, zájmových organizacích apod. subjektu údajů, genetické a biometrické údaje, které jsou zpracovávány za účelem jedinečné identifikace subjektu údajů, údaje o zdravotním stavu (tj. osobní údaje týkající se tělesného nebo duševního zdraví, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o zdravotním stavu) či údaje o sexuálním životě nebo sexuální orientaci subjektu údajů. Citlivými údaji jsou rovněž veškeré osobní údaje, které se týkají osob mladších 13 let.

Biometrickými údaji - osobní údaje vyplývající z konkrétního technického zpracování, které se týká fyzických či fyziologických znaků nebo znaků chování subjektu údajů, které umožňují nebo potvrzují jedinečnou identifikaci, například zobrazení obličeje (foto) nebo daktyloskopické údaje.

Dozorovým úřadem - nezávislý orgán veřejné moci nebo jiná instituce v ČR či v rámci EU, které jsou zřízeny (a vybaveny kompetencemi) k výkonu kontrolní činnosti nad ochranou subjektů údajů v souvislosti se zpracováním jejich osobních údajů tak, aby byly v souladu s požadavky ochrany osobních údajů stanovenými Nařízením; v ČR je dozorovým úřadem Úřad pro ochranu osobních údajů (dále jen „ÚOOÚ").

Evidencí - jakýkoliv strukturovaný soubor osobních údajů vedený na pracovištích NK a přístupný podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle organizačního, funkčního či jiného hlediska.

Genetickými údaji - osobní údaje týkající se zděděných nebo získaných genetických znaků subjektu údajů, které poskytují jedinečné informace o jeho fyziologii či zdraví a které vyplývají zejména z analýzy biologického vzorku dotčeného subjektu údajů.

Omezením zpracování - označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu.

Porušením zabezpečení osobních údajů - porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů na pracovištích NK.

Profilováním - jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k subjektu údajů, zejména k rozboru nebo odhadu aspektů týkajících se jeho pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu.

Příjemcem - fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje zpracovávané na pracovištích NK poskytnuty, ať už se jedná o třetí stranu, či nikoli.

Pseudonymizací - zpracování osobních údajů tak, že 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 identifikovanému či identifikovatelnému subjektu údajů.

Souhlasem subjektu údajů - jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů na pracovištích NK.

Subjektem údajů - fyzická osoba, s jejímiž osobními údaji vykonává NK jako správce nebo určený zaměstnanec NK jako zpracovatel jakékoliv operace nebo soubor operací (zpracování).

Správcem – NK jako právnická osoba, která určuje účely, postupy a prostředky zpracování osobních údajů na svých pracovištích a vykonává průběžnou kontrolní činnost nad dodržováním této směrnice.

Třetí stranou - 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 oprávněn ke zpracování osobních údajů.

Zpracováním - jakékoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, 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, které jsou prováděny pomocí či bez pomoci automatizovaných postupů.

Zpracovatelem – fyzická osoba (zpravidla zaměstnanec NK), právnická osoba, agentura nebo jiný subjekt, který má přístup k osobním údajům a zpracovává tyto osobní údaje pro správce.

Část druhá

Zásady, pravidla a postupy pro zpracování osobních údajů

Čl. I
Odpovědnost za zpracování

1) Osobní údaje musí být:
   a) ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem;
   b) shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být zpracovávány způsobem, který je s těmito účely neslučitelný; další zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely se nepovažuje za neslučitelné s původními účely (účelové omezení);
   c) přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány (minimalizace údajů);
   d) přesné a v případě potřeby aktualizované; ze strany správce a zpracovatele musí být průběžně přijímána veškerá rozumná opatření, aby osobní údaje, 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) osobní údaje lze uložit po delší dobu, pokud se zpracovávají výhradně pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely, a to za předpokladu provedení příslušných technických a organizačních opatření s cílem zaručit práva a svobody subjektu údajů (omezení uložení);
   g) zpracovávány způsobem, který zajistí jejich náležité zabezpečení (včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření) před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením (integrita a důvěrnost).

2) Správce odpovídá za dodržování zásad a pravidel podle předchozího odst. 1) a musí být schopen toto dodržování doložit (odpovědnost).

Čl. II
Zákonnost zpracování

1) Zpracování je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu:
   a) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;
   b) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;
   c) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;

d) 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;
e) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;
f) zpracování je nezbytné pro účely oprávněných zájmů správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektů údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.

2) Základ pro zpracování podle předchozího odst. 1, písm. a) a b) musí být stanoven:
a) právem EU;
b) právní normou ČR, která se na správce vztahuje.

3) Pokud zpracování pro jiný účel, než pro který byly osobní údaje shromážděny, není založeno na souhlasu subjektu údajů nebo na právu EU či ČR, zohlední správce v zájmu zjištění toho, zda je zpracování pro jiný účel slučitelné s účely, pro něž byly osobní údaje původně shromážděny, mimo jiné:
a) jakoukoli vazbu mezi účely, kvůli nimž byly osobní údaje shromážděny, a účely zamýšleného dalšího zpracování;
b) okolnosti, za nichž byly osobní údaje shromážděny, zejména pokud jde o vztah mezi subjekty údajů a správcem;
c) povahu osobních údajů, zejména zda jsou zpracovávány i citlivé údaje.

Čl. III
Zabezpečení zpracování

1) 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 subjektů údajů, provedou správce a zpracovatel vhodná technická a organizační opatření tak, aby zajistili úroveň zabezpečení zpracování 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.

2) Při posuzování vhodné úrovně bezpečnosti se zohlední především 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.

Čl. IV
Zabezpečení osobních údajů a ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu a dotčenému subjektu údajů

1) Jakékoli porušení zabezpečení osobních údajů správce bez zbytečného odkladu a do sedmdesáti dvou (72) hodin od okamžiku, kdy se o něm dozvěděl, ohlásí dozorovému úřadu, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody subjektů údajů.

2) Správce se zpravidla dozví o porušení zabezpečení osobních údajů od zpracovatele nebo i jiného zaměstnance NK, nebo prostřednictvím zpracovateli či jinému zaměstnanci nadřízeného zaměstnance, a to přímo osobním sdělením, nebo s využitím běžných komunikačních prostředků (telefonicky, SMS, e-mailem).

3) Pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody subjektů údajů, oznámí správce toto porušení dotčenému subjektu údajů bez zbytečného odkladu.

4) Oznámení subjektu údajů uvedené v odst. 3) 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 je například šifrování;
   b) správce přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektu údajů se již pravděpodobně neprojeví;
   c) vyžadovalo by to nepřiměřené úsilí; v takovém případě musí být subjekt údajů informován stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

5) 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, provede správce před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů. Pro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení.

6) Posouzení vlivu na ochranu osobních údajů je nutné zejména v těchto případech:
   a) systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se subjektů údajů, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k subjektům údajů právní účinky nebo mají na subjekty údajů podobně závažný dopad;
   b) rozsáhlé zpracování citlivých údajů;
   c) rozsáhlé systematické monitorování veřejně přístupných prostorů.

7) Správce konzultuje před zpracováním s dozorovým úřadem, pokud z posouzení vlivu na ochranu osobních údajů vyplývá, že by dané zpracování mělo za následek vysoké riziko v případě, že by správce nepřijal opatření ke zmírnění tohoto rizika.

8) Předávání osobních údajů do určité třetí země nebo určité mezinárodní organizaci se může uskutečnit pouze za předpokladu, že budou dodrženy obecné zásady a pravidla takového předání, uvedené v Nařízení.

Čl. V
Jmenování pověřence pro ochranu osobních údajů

1) Správce jmenuje pověřence pro ochranu osobních údajů – Data Protection Officer (dále jen „DPO“) vzhledem k tomu, že NK jako správce:
   a) provádí zpracování jako veřejný subjekt;
   b) vykonává hlavní činnosti správce nebo zpracovatele, které spočívají v operacích zpracování, a které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů;

Část třetí
Metodická, systémová a organizační opatření a postupy zajišťující ochranu osobních údajů při jejich zpracování

Čl. I
Základní ustanovení

1) Organizačním útvarem, který realizuje práva a výkon povinností správce v souvislosti se zajištěním ochrany osobních údajů při jejich zpracování je Organizační oddělení a Archiv NK.

2) Oddělení organizační a Archiv NK má v této souvislosti kompetence, které v součinnosti s vedoucími všech útvarů NK (na všech organizačních úrovních) a se všemi zaměstnanci NK zajistí splnění úkolů a povinností stanovených správci tak, jak jsou popsány v tomto opatření. Jde zejména o:
   a) koordinační činnost, včetně ukládání konkrétních úkolů a termínů jejich splnění vedoucím organizačních útvarů i jednotlivým zaměstnancům NK, k realizaci metodických, systémových a organizačních opatření a postupů zajišťujících ochranu subjektů údajů v souvislosti se zpracováním jejich osobních údajů na pracovištích NK, a to i nad rámec této směrnice, pokud jsou tyto úkoly v souladu s Nařízením,
   b) výkon funkce ohlašovacího místa pro zaměstnance NK v souvislosti s porušením zabezpečení osobních údajů, a pro ohlašování případů porušení zabezpečení osobních údajů ÚOOÚ a dotčenému subjektu údajů,
   c) kontrolní činnost nad dodržováním této směrnice a plnění úkolů ve stanovených termínech, uložených podle písm. a) na všech pracovištích NK,
   d) spolupráci s DPO při plnění všech úkolů, které se týkají ochrany osobních údajů.

Čl. II
Zdroje osobních údajů

1) Popisem zdrojů osobních údajů v NK se rozumí výsledek prvotní analytické etapy, který je samostatnou přílohou této směrnice. Tento výsledek je zaznamenán a do budoucna bude udržován v aktuálním stavu, včetně historie jeho vývoje. V tomto dokumentu jsou vedeny potřebné údaje v následujícím detailu:

1.1 Digitální dokumenty a jejich metadata:
   a) informační systémy (dále jen „IS"), které obsahují osobní údaje, jejich bližší popisy z hlediska Nařízení, zda jsou vedeny u zpracovatele, v cloudu apod;
   b) úložiště s dokumenty s osobními údaji, jejich bližší popisy z hlediska Nařízení, zda jsou vedeny u zpracovatele, v cloudu apod;
   c) digitální dokumenty s osobními údaji mimo centrální IS NK (servery), např. lokální IS na PC;
   d) IS v režimu, kdy NK je jako zpracovatel dokumentů s osobními údaji pro jinou organizaci, jejich bližší popis z hlediska Nařízení a specifikace postupů jak zpracovávat standardní i akutní požadavky od zadavatelské organizace;
   e) popis předávání osobních a citlivých údajů třetím stranám.

1.2 Listinné dokumenty a jejich metadata:
   a) s metadaty v centrálním IS NK a s podrobností kde jsou vedeny a jaká je organizace jejich fyzického uložení v NK;
   b) s metadaty v listinné podobě (případně bez metadat) s podrobností kde jsou vedeny a jaká je organizace jejich fyzického uložení v NK.

1.3 Unikátní označení a kategorizace jednotlivých zdrojů (ID_IS, popis IS, platnost od, platnost do, odpovědnost kdo, splnění nároků Nařízení, ...), pro odlišení jednotlivých IS NK a v nich vedených osobních údajů.

2) Popis zdrojů citlivých údajů je obsahově i v detailu shodný s předchozím odst. 1).

3) Popis procesů spojených se zpracováním osobních údajů pro jednotlivé osobní údaje či skupiny těchto údajů podle agend podporovaných IS NK, Document management systémem (dále jen „DMS") NK či jinou evidencí:
   a) proces přijetí zahrnuje právní důvod zpracování osobních údajů (včetně podrobnosti kdo a kdy je přijal), podrobnosti o transakčním protokolu, kontroly dle nařízení EU o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (eIDAS), odpovědnost za proces atd;
   b) proces zpracování zahrnuje podrobnost, kdo a kdy údaje zpracovává, kdo je odpovědný za jejich správu a vyřizování, tedy za přiřazení (v souladu s Nařízením) spisového znaku, skartačního znaku a lhůty, od kdy se počítá skartace (spouštěcí událost), kdo vede transakční protokol a má odpovědnost za proces (dle agend);
   c) proces skartační řízení dat daného osobního údaje či skupiny údajů vyžaduje důsledné vedení transakčního protokolu - obdobně jako u elektronické spisové služby (dále jen „eSSL"), a určení osobní odpovědnosti za jednotlivé procesy;
   d) proces odstranění (po odvolání souhlasu se zpracováním osobních údajů, pokud byl tento souhlas jediným právním důvodem jejich zpracování) vyžaduje okamžité rozhodnutí a řešení mimo běžné skartační řízení (tj. následující rok) – jedná se např. o trvalý skartační souhlas, ale důkaz o takto provedené skartaci musí být zapsán v transakčním protokolu;
   e) proces předání třetí straně stanoví, kdo a kdy osobní údaje předal, kdo nese odpovědnost za předání a jaká je technika předání (podle agend).

4) Popis procesů spojených se zpracováním citlivých údajů je obsahově i v detailu shodný s odst. 3).

5) Rejstřík vedených osobních údajů (případně i citlivých údajů):

a) odkazuje na rejstříky osob v jednotlivých IS NK, které jsou vedeny v souladu s Nařízením;
b) zaznamenává konkrétní položky osobních údajů jednotlivých subjektů údajů vedených v IS NK, které nejsou v souladu s Nařízením (jedná se např. o jméno subjektu údajů, výčet všech IS NK, ve kterých jsou o něm vedeny osobní údaje, případně bližší specifikace metadat k těmto údajům), další údaje, kterými mohou být např. fulltextové indexy obsahů s osobními údaji v jednotlivých IS NK.

6) GDPR plán, ve kterém jsou odděleně zaznamenány osobní a citlivé údaje v následující skladbě a struktuře, obsahuje mj:
   a) kategorie údajů vedené v rejstříku osobních údajů, obdobně jako ve spisovém a skartačním plánu;
   b) spisový a skartační plán eSSL doplněný např. o odkazy na právní předpisy.

7) Popis podpůrných evidencí a procesů s nimi spojených zahrnuje:
   a) vedení metadat pro digitální či listinné dokumenty s osobními a citlivými údaji, které nejsou v IS NK obsaženy (v časové ose od zahájení dopředu), s možností např. zaznamenat transakční protokol, tedy kdo, kdy a co s těmito údaji vykonal, právní důvod takových operací, přiřazení skartačních znaků apod;
   b) vedení metadat pro digitální či listinné dokumenty s osobními a citlivými údaji, které nejsou v IS NK (zpětně, tj. už uložených v NK); lze zaznamenat alespoň některá metadata (pro digitální dokumenty povinně, pro listinné dokumenty nepovinně s odkazem na nepřiměřené náklady);
   c) evidence smluv spojených s vedením a zpracováním osobních údajů konkrétního subjektu údajů (pokud nejsou vedeny v jiném IS v souladu s Nařízením);
   d) evidence souhlasů spojených s vedením a zpracováním osobních údajů konkrétního subjektu údajů (pokud nejsou vedeny v jiném IS v souladu s Nařízením).

8) Evidence hlášení narušení bezpečnosti osobních a citlivých údajů od subjektů údajů, tedy od uživatelů NK, zaměstnanců NK, ostatních fyzických osob (např. dodavatelů služeb NK a dalších) s popisem procesu administrace, s možnostmi:
   a) zahrnout je do samostatné evidence hlášení např. v rámci eSSL
   b) evidovat jako příchozí záznam do vstupní evidence eSSL (jako ostatní příchozí poštu), vhodně doplnit zpracování v eSSL pro jednotlivé typy hlášení (dle závažnosti), až po odchozí dokumenty ÚOOÚ a subjektům údajů (včetně sledování dodržení lhůty do 72 hod.).

9) Evidence žádostí subjektů údajů o sdělení informace o svých osobních údajích, žádostí o jejich opravu či doplnění, výmaz, omezení zpracování atd. s popisem procesů administrace k jednotlivým typům žádostí, s možnostmi:
   a) zahrnout do samostatné evidence žádostí např. v rámci eSSL
   b) evidovat jako příchozí záznam do vstupní evidence eSSL (jako ostatní příchozí poštu), vhodné doplnit zpracování v eSSL pro jednotlivé typy žádostí (akce, tvorba odpovědi), až po vypravení odpovědi subjektům údajů.

10) Evidence hromadných exportů jiné organizaci – popis, kdo a jak schvaluje a stav vyřízení (ponechat jako individuální žádost příchozí a vypravenou přes standardní eSSL).

11) Popis a evidence vnitřních předpisů spojených s Nařízením, která slouží především jako důkaz při řešení interních problémů souvisejících s Nařízením.

12) Popis a evidence akcí DPO, která slouží především pro přehled a pro kontrolu vykonávanou generálním ředitelem NK či ÚOOÚ. Evidence je vedena např. v eSSL (popis procesů a aktivit: jak často, výsledky a závěry, připojené akce a uložené úkoly), včetně detailního popisu práce DPO.

13) Popis a evidence akcí auditora slouží především pro přehled a pro kontrolu vykonávanou generálním ředitelem NK. Evidence je vedena např. v eSSL (popis procesů a aktivit: jak často, výsledky, připojené akce a uložené úkoly), včetně detailního popisu práce auditora.

Čl. III
Práva a povinnosti subjektů údajů a správce

1) Subjekt údajů má vůči správci následující práva:
   1.1 **požadovat od správce přístup** ke svým evidovaným a zpracovávaným osobním údajům, dále má právo na opravu těchto údajů,
   1.2 **požadovat omezení zpracování** svých osobních údajů či vznést námitku proti zpracování v případě, že jejich zpracování správcem je protiprávní nebo je správce nepotřebuje pro zákonné účely zpracování, omezení zpracování správcem trvá po dobu vyřešení požadavku,
   1.3 **vznést námitku** proti zpracování správcem, pokud:
      a) je zpracování prováděno pro splnění úkolu ve veřejném zájmu či při výkonu státní moci;
      b) je zpracování prováděno v oprávněném zájmu správce nebo třetí strany, či v souladu práva na přenositelnost svých osobních údajů,
   1.4 **podat stížnost** na ÚOOÚ v případě, že se domnívá, že dochází k porušení Nařízení správcem nebo zpracovatelem. Stížnost můžete také podat dozorovému úřadu v místě, kde došlo k údajnému porušení,
   1.5 **právo na výmaz** svých osobních údajů, které je však omezeno při zpracovávání osobních údajů ze zákonných důvodů,
   1.6 **právo na přenositelnost** svých evidovaných a zpracovávaných osobních údajů, které lze uplatnit, jen pokud je jejich zpracovávání založeno na smlouvě či souhlasu a probíhá pouze automatizované.

2) Pokud je zpracování osobních údajů prováděno správcem na základě zákona, má subjekt údajů povinnost tyto osobní údaje správci poskytnout a správce má povinnost je od subjektu údajů požadovat. V případě, že subjekt údajů osobní údaje neposkytnete, správce neposkytne subjektu údajů příslušnou službu.

3) Subjekt údajů a správce mají z hlediska Nařízení tato další práva a povinnosti:
   3.1 **právo na transparentní, srozumitelné a snadno přístupným způsobem dostupné informace o osobních údajích,** které byly o subjektu údajů získány správcem s jeho souhlasem, nebo i bez souhlasu. Na základě písemné, elektronické nebo ústní žádosti jsou subjektu údajů tyto informace správcem poskytnuty transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků. Informace jsou poskytnuty na základě žádosti, lhůta pro vyřízení žádosti je jeden (1) měsíc (je ji možno prodloužit v odůvodněných případech maximálně dvakrát),
   3.2 **právo na informace poskytované v případě, že osobní údaje nebyly získány od subjektu údajů**. Správce je povinen tyto informace subjektu údajů poskytnout. Toto ustanovení však neplatí v případě, že:

a) subjekt údajů tyto osobní údaje již má;
b) poskytnutí těchto osobních údajů by vyžadovalo nepřiměřené úsilí (zejména pro archivaci ve veřejném zájmu, pro vědecký a historický výzkum a pro statistické účely);
c) získávání těchto osobních údajů je stanoveno právními předpisy ČR nebo právem EU;
d) tyto osobní údaje musí s ohledem na povinnost zachovávat mlčenlivost zůstat důvěrnými,

3.3 **právo na přístup k osobním údajům**. Správce vydá potvrzení o tom, zda osobní údaje, které se týkají daného subjektu údajů, jsou či nejsou zpracovávány. Správce poskytne kopii zpracovávaných osobních údajů (za další kopie na žádost subjektu údajů může správce účtovat přiměřený poplatek odpovídající administrativním nákladům). Jestliže subjekt údajů podá žádost v elektronické formě, informace jsou poskytovány v elektronické formě, která se běžně používá, pokud subjekt údajů nepožádá o jiný způsob.

3.4 **právo na opravu a právo na doplnění neúplných osobních údajů**. Správce bez zbytečného odkladu opraví nepřesné osobní údaje, které se týkají subjektu údajů, neúplné osobní údaje doplní,

3.5 **právo na výmaz** (právo být zapomenut). Správce má povinnost osobní údaje bez zbytečného odkladu vymazat, pokud je dán jeden z těchto důvodů:
a) osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovávány;
b) subjekt údajů odvolá souhlas, na jehož základě byly údaje zpracovány, a neexistuje žádný další právní důvod pro zpracování;
c) subjekt údajů vznese námitky proti zpracování, ve které prokáže, že neexistují žádné převažující oprávněné důvody pro zpracování;
d) osobní údaje byly zpracovány protiprávně;
e) osobní údaje musí být vymazány ke splnění právní povinnosti stanovené v právu ČR nebo EU, které se na správce vztahuje;
f) osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti,

3.6 **právo na omezení zpracování**. Správce omezí zpracování, v kterémkoli z následujících případů:
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 svých právních nároků;
d) subjekt údajů vznesl námitku proti zpracování, dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody subjektu údajů,

3.7 **oznamovací povinnost ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování**. Správce oznamuje jednotlivým příjemcům, jimž byly osobní údaje zpřístupněny, veškeré opravy nebo výmazy osobních údajů nebo omezení zpracování, s výjimkou případů, kdy se to ukáže jako nemožné nebo to vyžaduje nepřiměřené úsilí. Správce informuje subjekt údajů o těchto příjemcích, pokud to subjekt údajů požaduje,

3.8 **právo na přenositelnost údajů**. Správce má povinnost předat osobní údaje druhému správci (za předpokladu technické proveditelnosti) a pouze za kumulativního splnění následujících dvou (2) podmínek:
a) zpracování je založeno na souhlasu subjektu údajů nebo smlouvě;
b) jedná se o automatizované zpracování,

3.9 **právo vznést námitku** proti zpracování osobních údajů, které se subjektu údajů týkají. 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,

3.10 **právo na to, aby subjekt údajů nebyl předmětem automatizovaného rozhodování**, včetně profilování. Správce nesmí provádět výhradně automatizované individuální rozhodování, včetně profilování, s následujícími výjimkami:
   a) je stanoveno zákonem,
   b) je založeno na souhlasu subjektu,
   c) je nezbytné pro uzavření smlouvy nebo jejího plnění se subjektem,

3.11 **právo podat stížnost u dozorového úřadu** - správce se stává součástí, resp. předmětem šetření,

3.12 **právo na účinnou soudní ochranu** vůči dozorovému úřadu,

3.13 **právo na účinnou soudní ochranu** vůči správci nebo zpracovateli - správce se stává stranou soudního sporu,

3.14 **právo na to být zastoupen** neziskovým subjektem, organizací nebo sdružením. Je povinností správce jednat s takovýmto subjektem, který zastupuje subjekt údajů, např. v případě podání stížnosti,

3.15 **právo na náhradu újmy**. Vznikne-li subjektu údajů újma, ať již hmotná, či nehmotná, má správce povinnost tuto újmu nahradit.

Čl. IV
Zabezpečení osobních údajů

1) Správce je povinen zabezpečit zpracování osobních údajů a ohlašovat případy porušení ochrany osobních údajů dozorovému úřadu, i subjektu údajů.

2) Zabezpečení zpracování spočívá v provedení vhodných technických a organizačních opatření. Tato opatření provedou správce a zpracovatel, a to 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 subjektů údajů, 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.

3) Správce a zpracovatel přijmou opatření pro zajištění, aby jakákoli fyzická osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo ČR nebo EU. Jedním z prvků, kterými lze prokázat soulad, je dodržování schváleného etického kodexu

chování. V minimální podobě lze prokázat soulad záznamy o činnostech zpracování (transakční protokol).

Část čtvrtá
Konkrétní postupy a opatření zpracovatele a správce při zpracování osobních údajů

Čl. I
Podmínky, za kterých je možné zpracovávat osobní údaje

1) Osobní údaje jsou zpracovávány na základě:
   a) souhlasu subjektu údajů, který musí být vyjádřen svobodně, konkrétně, informovaně a jednoznačně;
   b) smlouvy uzavřené na žádost subjektu údajů (smlouva s externími spolupracovníky, včetně např. dodavatelů zboží nebo služeb) nebo pro provedení opatření přijatých ještě před uzavřením takové smlouvy na žádost subjektu údajů (osobní údaje jsou např. nezbytným podkladem pro uzavření smlouvy); ve smlouvě musí být mj. ustanoveno, že v případě porušení této smlouvy neoprávněnými úkony při zpracování osobních údajů, stává se externí spolupracovník správcem takových údajů namísto NK, se všemi důsledky, které z toho vyplývají,
   c) právní povinnosti správce;
   d) životně důležitého zájmu subjektu údajů nebo jiné fyzické osoby;
   e) veřejného zájmu;
   f) oprávněného zájmu správce, pokud však nepřeváží zájem subjektu údajů (jedná se např. o instalaci kamerového systému k ochraně majetku).

Čl. II
Postupy a opatření při zpracování osobních údajů

1) Zpracovatel nebo správce při zpracování osobních údajů vychází z předchozích ustanovení tohoto opatření a z analýzy rizik; při realizaci některých postupů a opatření zastupuje zpracovatel správce. Při zpracování osobních údajů, musí být dodrženy následující postupy a opatření:
   a) zpracovatel si vytvoří vlastní anonymizovaný seznam všech subjektů údajů, u kterých jejich osobní údaje potřebuje ke své práci, nebo v tomto smyslu posoudí stávající seznamy. U každého subjektu údajů v seznamu si ujasní, které osobní údaje o něm eviduje (rozsah zpracování osobních údajů) a na kterých elektronických či fyzických uložištích je má uloženy,
   b) v seznamu, vytvořeném a posouzeném podle předchozího písm. a) správce určí, k čemu jednotlivé osobní údaje potřebuje. Nepotřebné osobní údaje ze všech svých evidencí (elektronických, analogových) bez náhrady odstraní, a to včetně případné likvidace všech elektronických i analogových dokumentů, které takové údaje obsahují,
   c) upravený seznam podle předchozího písm. b) zpracovatel vyhodnotí, zda osobní údaje v něm uvedené byly získány a jsou dále zpracovávány na základě právního důvodu vycházejícího z právních předpisů ČR nebo EU, případně jsou získány na základě předchozího písemného souhlasu příslušného subjektů údajů,
   d) od subjektů údajů, u kterých není právní důvod ke zpracování jejich osobních údajů, a které dříve nedaly písemný souhlas ke zpracování těchto údajů, si zpracovatel jejich

souhlas vyžádá. Pokud některý z těchto subjektů na vyžádání tento souhlas zpracovateli neposkytne, zpracovatel všechny jeho osobní údaje ze všech svých evidencí (elektronických, analogových) bez náhrady odstraní.

2) Správce prostřednictvím zpracovatele zajistí, aby každý subjekt údajů byl dostatečně a srozumitelně informován zejména o tom, které jeho osobní údaje zpracovává a proč, kdo má k těmto údajům přístup (případně kterým jiným správcům a zpracovatelům jsou tyto údaje poskytovány a za jakým účelem), po jakou dobu zpracování osobních údajů probíhá a jaká práva ve vztahu ke svým osobním údajům může uplatnit. K informování subjektů údajů podle tohoto ustanovení může být využito sdělení zveřejněné na webových stránkách NK. V takovém sdělení musí být informace formulovány jednoduše, srozumitelně, transparentně a úplně, bez zamlčování rozhodných skutečností.

3) Zpracovatel je povinen vést záznamy o činnostech zpracování osobních údajů (transakční protokol). Součástí těchto záznamů musí být (kromě kontaktních údajů správce) uveden účel a rozsah zpracování, informace o příjemcích osobních údajů, lhůty pro výmaz a popis přijatých technických a organizačních opatření k zajištění ochrany osobních údajů. Na žádost ÚOOÚ je správce povinen tyto záznamy zpřístupnit.

4) Pokud zpracovatel sdílí (využívá) některý seznam či databázi subjektů údajů s jejich osobními údaji (nebo databázi dokumentů, které tyto údaje obsahují) spolu s dalšími zpracovateli NK, realizuje postupy a opatření podle tohoto článku v koordinaci a v dohodě s nimi. Tuto koordinaci na základě dispozic správce zajišťují vedoucí zaměstnanci jednotlivých útvarů NK.

Čl. III
Bezpečnostní opatření ze strany zpracovatele a správce při ochraně osobních údajů v souvislosti s jejich zpracováním

1) Zpracovatel a správce zajistí dodržování základních zásad bezpečnosti a ochrany zpracovávaných osobních údajů. V této souvislosti je zejména:
   a) zpracovatel zabezpečí přístup do svého počítače (respektive ke svému uživatelskému účtu) heslem tak, aby osobní údaje subjektů údajů (a dokumenty, které tyto údaje obsahují) v něm uložené, nebo jeho prostřednictvím přístupné, byly chráněny před přístupem nepovolaných osob. Současně respektuje zákaz kopírovat databáze s osobními údaji na soukromý e-mail, USB disky či jiný technický prostředek; aby v tomto smyslu nedošlo ke zneužití počítače zpracovatele nepovolanou osobou, odhlásí se zpracovatel z elektronických systémů vždy před opuštěním svého pracoviště,
   b) zpracovatel zabezpečí ochranu analogových dokumentů obsahujících osobní údaje subjektů údajů jejich neponecháním bez dozoru zpracovatele v době, kdy je potřebuje k výkonu své práce. Po ukončení práce s nimi je vždy uloží na určené zabezpečené místo.
   c) správce zajistí trvalé a bezporuchové používání firewallu, pravidelné aktualizování antivirové ochrany a provádění průběžné kontroly, zda nejsou data obsahující osobní údaje ukládána na veřejných úložištích.

2) V případech zdůvodněné potřeby může správce po posouzení oprávněnosti takového požadavku zpracovatele vyslovit souhlas s používáním bezpečných cloudových služeb, garantujících soulad s Nařízením či souhlas se zavedením šifrování souborů za účelem vyšší jistoty bezpečnosti dat. Bez souhlasu a doporučení správce nesmí zpracovatel tyto služby a

technologie využít. Podmínkou vyslovení souhlasu je uzavření smlouvy s dodavatelem cloudových služeb, na základě které se stává zpracovatelem osobních údajů pro NK.

Čl. IV

Postupy vyřizování žádostí subjektů údajů a fyzických osob o informace ke zpracování svých osobních údajů

1) Subjekt údajů právo na to být informován o zpracování svých osobních údajů. Tím se rozumí právo na určité informace o zpracování jeho osobních údajů tak, aby byla především naplněna zásada transparentnosti zpracování. Jde zejména o informace o účelu zpracování, totožnosti správce, o jeho oprávněných zájmech, o příjemcích jeho osobních údajů a další. V tomto případě jde o pasivní právo, jelikož aktivitu musí vůči subjektu údajů vyvinout správce zpravidla prostřednictvím zpracovatele tak, aby požadované informace stanovené v Nařízení a tomto opatření, subjektu údajů poskytl, resp. zpřístupnil.

2) Na základě své aktivní žádosti má každá fyzická osoba, tedy i subjekt údajů (dále jen „žadatel") právo přístupu ke svým osobním údajům, tedy získat od správce informaci (potvrzení), zda jsou či nejsou jeho osobní údaje zpracovávány a pokud jsou zpracovávány, má žadatel právo tyto osobní údaje získat a zároveň má právo získat především následující informace:
   a) účely zpracování;
   b) kategorie dotčených osobních údajů;
   c) příjemci nebo kategorie příjemců, kterým osobní údaje žadatele byly nebo budou zpřístupněny;
   d) plánovaná doba, po kterou budou osobní údaje žadatele uloženy;
   e) existence práva požadovat od správce opravu nebo výmaz svých osobních údajů a práva vznést námitku;
   f) existence práva podat stížnost u ÚOOÚ;
   g) veškeré dostupné informace o zdroji osobních údajů žadatele, pokud nejsou získány od něj;
   h) pokud dochází k automatizovanému rozhodování, včetně profilování, informaci o této skutečnosti.

3) Pokud správce o žadateli žádné údaje nezpracovává, poskytne mu informaci, že jeho osobní údaje nejsou předmětem zpracování osobních údajů ze strany NK.

4) Každá aktivní žádost žadatele ve věci jeho osobních údajů, adresována kterémukoliv zaměstnanci nebo pracovišti NK, musí být v den jejího doručení zaevidována v eSSL a bezodkladně předána správci k dalšímu řízení.

5) Správce na základě vlastních informačních zdrojů nebo ve spolupráci se zpracovatelem, který mu informace o žadateli následně předá v rozsahu a struktuře tak, jak jsou pro daný případ nutné, vypracuje a odešle žadateli odpověď na jeho žádost. Odpověď odešle bez zbytečného odkladu, nejpozději však do jednoho (1) měsíce od obdržení žádosti.

6) Lhůtu dle odst. 5) lze ve výjimečných případech prodloužit o další dva (2) měsíce, o čemž musí být žadatel ze strany správce informován, včetně důvodů prodloužení; důvody prodloužení lhůty musí být správce schopen prokazatelně doložit.

7) Informace, veškerá sdělení a úkony se činí a následně žadateli poskytují bezplatně. Pouze v případě, kdy jsou žádosti podané žadatelem zjevně nedůvodné nebo nepřiměřené, zejména proto, že se např. bezdůvodně opakují (zneužití práva žadatele), může správce buď uložit přiměřený poplatek, nebo odmítnout žádosti vyhovět. Zjevnou nedůvodnost musí být správce schopen prokazatelně doložit.

8) Zneužitím práva žadatele však nelze a priori rozumět výkon práv žadatele stanovených Nařízením a tímto opatřením.

Čl. V
Bezpečnostní incidenty a postupy jejich řešení

1) Bezpečnostním incidentem se rozumí zejména stav, kdy přes použití patřičných technických a organizačních opatření k náležitému zajištění a zabezpečení osobních údajů, došlo k porušení jejich zabezpečení tím, že došlo k jejich neoprávněnému nebo protiprávnímu zpracování, ztrátě, zničení nebo poškození (porušení důvěrnosti, dostupnosti, integrity). Jedná se zejména o:
   a) neoprávněné nebo protiprávní zpracování osobních údajů, které zahrnuje zpřístupnění osobních údajů příjemcům, kteří nemají oprávnění tyto osobní údaje získat nebo mít k nim přístup, nebo o jakoukoli jinou formu zpracování, která je v rozporu s Nařízením a tímto opatřením;
   b) ztrátu, kterou se rozumí stav, kdy osobní údaje sice mohou stále existovat, avšak správce (zpracovatel) nad nimi ztratil kontrolu nebo přístup k nim, či je už nemá v držení;
   c) poškození, kterým se rozumí případ, kdy osobní údaje byly pozměněny nebo už nejsou úplné;
   d) zničení, kterým se rozumí případ, kdy osobní údaje už neexistují vůbec nebo přinejmenším ne v podobě, aby byly správcem využity k účelu, pro který byly získány.

2) Pokud kterýkoliv zpracovatel zjistí bezpečnostní incident, tj. porušení zabezpečení osobních údajů, jež pro správce zpracovává, nebo se o takovém incidentu (i náhodně) dozví (a to i v případě, že se jedná o osobní údaje, které pro správce zpracovává např. externí zpracovatel), je jeho povinností ohlásit to ihned svému bezprostředně nadřízenému zaměstnanci. Dále, bez zbytečného odkladu osobně nebo prostřednictvím tohoto nadřízeného, ohlásí takový bezpečnostní incident správci tak, aby mu umožnil začít případ okamžitě řešit a zejména co nejrychleji určit, zda bude nutné ohlásit jej dozorovému úřadu.

3) Ohlašovací povinnost podle odst. 2), týkající se zpracovatele, v plném rozsahu platí pro všechny zaměstnance NK, bez ohledu na jejich pracovněprávní nebo jiný právní vztah k NK, anebo na jejich pracovní nebo funkční zařazení. Vztahuje se i na externí spolupracovníky, včetně např. dodavatelů zboží nebo služeb, pokud mají přístup k osobním údajům zpracovávaným v rámci NK.

4) Externí spolupracovníci ohlásí bezpečnostní incident zpracovateli, který jim zákonným způsobem umožnil přístup k osobním údajům zpracovávaným v rámci NK a jeho prostřednictvím správci, anebo bezpečnostní incident ohlásí správci přímo.

5) Zpracovatel je povinen průkazným a srozumitelným způsobem, zpravidla písemně, informovat externí spolupracovníky, kterým zákonným způsobem umožnil přístup k osobním údajům zpracovávaným v rámci NK, o jejich ohlašovací povinnosti podle odst. 3) a 4).

6) V oznámení oznamovatel uvede zejména:
   a) popis povahy daného bezpečnostního incidentu, pokud je to možné i kategorii subjektů údajů, kterých se incident týká (zaměstnanci, návštěvníci, externí spolupracovníci apod.), případně typy záznamů v těchto osobních údajích (čísla osobních dokladů, čísla bankovních účtů a další finanční údaje apod.);
   b) počet dotčených subjektů osobních údajů, nebo alespoň přibližný odhad množství dotčených záznamů osobních údajů;
   c) popis pravděpodobných důsledků daného bezpečnostního incidentu; zde uvede např. nebezpečí zneužití osobních údajů k podvodu, nebezpečí finanční ztráty, ohrožení obchodního tajemství, případně další podrobnosti;
   d) popis okamžitých opatření, které byly ihned po zjištění bezpečnostního incidentu přijaty, nebo které se k přijetí navrhují s cílem vyřešit daný bezpečnostní incident;
   e) návrh případných dalších opatření ke zmírnění možných nepříznivých dopadů daného bezpečnostního incidentu.

7) Správce (po oznámení bezpečnostního incidentu a získání informací podle odst. 6) bezpečnostní incident posoudí a v součinnosti s DPO, je-li jmenován, rozhodne o jeho závažnosti a o postupu jeho řešení. Současně bezodkladně o tomto bezpečnostním incidentu a navrženém postupu jeho řešení informuje dotčený subjekt údajů. V této souvislosti rovněž rozhodne dle závažnosti bezpečnostního incidentu o jeho ohlášení či neohlášení ÚOOÚ. O všech svých rozhodnutích a opatřeních podle tohoto odst. 7) správce sepíše záznam, ve kterém bezpečnostní incident se všemi jeho možnými důsledky podrobně popíše, zdůvodní navržený postup jeho řešení a zejména zdůvodní svoje případné rozhodnutí neohlásit dotčený bezpečnostní incident ÚOOÚ.

8) Správce je povinen ke každému bezpečnostnímu incidentu vést průkaznou a úplnou evidenci založením samostatného spisu. Spis založí v rámci základní evidenční pomůcky, kterou je eSSL, a průběžně sleduje a vyhodnocuje jeho vyřizování. Správce do spisu vkládá elektronické i písemné dokumenty vztahující se ke konkrétnímu bezpečnostnímu incidentu, které jsou mu doručeny, a rovněž záznamy o přijatých opatřeních i záznamy z osobních jednání vedených k této věci apod. Všechny jednotlivé dokumenty zařazené nebo nově vkládané do takového spisu, tedy i záznamy z osobních jednání, musí být evidovány v eSSL.

Část pátá
Ostatní ustanovení

Čl. I
Společná ustanovení

1) Úkony a postupy podle tohoto opatření vykonávají všichni zaměstnanci NK v zastoupení správce (zejména ti, kteří jsou zpracovateli, tedy mají přístup k osobním údajům subjektů údajů) vždy zásadně v součinnosti, v dohodě a s vědomím správce.

2) Všichni zaměstnanci NK a všichni externí spolupracovníci NK, na které se vztahuje působnost tohoto opatření, stvrdí svým podpisem, že byli seznámeni s tímto opatřením a zavazují se k jejímu dodržování.

3) Všem zaměstnancům NK, na které se vztahuje působnost tohoto opatření se stanovuje povinnost zúčastnit se (případně i opakovaně) školení k problematice ochrany osobních údajů, které NK zorganizuje anebo jinak zajistí.

4) Pokud subjekt údajů ve smyslu některého ustanovení tohoto opatření uplatní právo na výmaz svých osobních údajů, zajistí naplnění tohoto práva zaměstnanec NK, který je zpracovatelem osobních údajů tohoto subjektu údajů. Postup při tomto výmazu osobních údajů je upraven vnitřním předpisem.

Čl. II
Zrušovací ustanovení

1) Publikace Ochrana osobních údajů - Příručka pro knihovníky, vydaná Knihovnickým institutem a zveřejněná na www stránkách NK, zůstává v platnosti s výjimkou těch ustanovení, která jsou nebo by mohla být v rozporu s Nařízením a tímto opatřením. Příručku lze využít jako rámcový metodický návod a inspirační zdroj pro realizaci konkrétních opatření souvisejících se zpracováním osobních údajů, a to s přihlédnutím na specifické podmínky vykonávané činnosti.

2) Toto opatření bude upraveno na základě vydání účinného obecně závazného právního předpisu v rámci českého právního řádu (zákon), bude-li to nutné. Do vydání takového právního předpisu je obecně závaznou normou pro působnost opatření Nařízení a právní předpisy ve všech těch ustanoveních, která nejsou v rozporu s Nařízením.

3) Ustanovení všech vnitřních předpisů NK, která jsou anebo by mohla být v rozporu s Nařízením a tímto opatřením se nepoužijí.

Čl. III
Platnost, účinnost

Toto opatření nabývá platnosti dnem vydání, tj. dnem podpisu generálním ředitelem NK a účinnosti nabývá dnem 25.5.2018.

V Praze dne 16-5-2018

PhDr. Martin Kocanda
generální ředitel
Národní knihovny České republiky