VYHLÁŠKA ÚRADU NA OCHRANU OSOBNÝCH ÚDAJOV

z 29. mája 2018 č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobnýh údajov

Úrad na ochranu osobných údajov Slovenskej republiky (ďalej len „úrad“) podľa § 108 ods. 2 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „zákon“) ustanovuje:

§ 1

Táto vyhláška upravuje postup prevádzkovateľa pri posudzovaní vplyvu plánovaných spracovateľských operácií na ochranu osobných údajov (ďalej len „posúdenie vplyvu“) podľa § 42 ods. 1 a 3 zákona.

§ 2

Dokumentácia pri posúdení vplyvu obsahuje

a) opis plánovaného spracúvania,
b) posúdenie nevyhnutnosti a primeranosti v spojení s opatreniami na preukázanie súladu so zákonom,
c) posúdenie rizika pre práva fyzickej osoby v spojení s opatreniami na riešenie rizík,
d) dokumentáciu podľa § 6,
e) monitorovanie a preskúmanie.

§ 3

(1) Opis plánovaného spracúvania je systematickým opisom spracovateľských operácií zameraných na povahu, rozsah, kontext a účely spracúvania osobných údajov, ktorý obsahuje najmä

a) účely spracúvania osobných údajov,
b) ak sú osobné údaje spracúvané na základe § 13 ods. 1 písm. f) zákona, opis spracovateľských operácií obsahuje aj konkrétnu charakteristiku oprávneného záujmu prevádzkovateľa alebo tretej strany vrátane
   1. opisu posúdenia oprávnenosti záujmu prevádzkovateľa alebo tretej strany,
   2. opisu vzťahu prevádzkovateľa a dotknutých osôb,
   3. podmienok, na ktorých základe dotknutá osoba môže primerane očakávať spracovateľské operácie s osobnými údajmi, ktoré sa jej týkajú,
   4. posúdenia primeranosti spracovateľských operácií a odôvodnenia prevahy záujmu prevádzkovateľa alebo tretej strany nad právami fyzickej osoby,
c) zoznam alebo rozsah osobných údajov, ktoré sú predmetom spracúvania,
d) zoznam alebo okruh príjemcov, ktorým sú osobné údaje poskytnuté,
e) vymedzenie obdobia uchovávania osobných údajov.

(2) Ak sa na spracúvanie osobných údajov vzťahuje schválený kódex správania podľa § 85 zákona, súčasťou opisu spracovateľských operácií sú odkazy na tie časti kódexu správania, ktoré prevádzkovateľ pri posudzovaní vplyvu na ochranu osobných údajov zohľadnil.

(3) Ak sa na spracúvanie osobných údajov vzťahuje platný certifikát vydaný podľa § 86 zákona, súčasťou opisu spracovateľských operácií sú odkazy na tie časti žiadosti o vydanie certifikátu a jej príloh, ktoré preukazujú súlad spracúvania osobných údajov so zákonom a existenciu primeraných záruk ochrany osobných údajov.

§ 4

(1) Na zabezpečenie súladu so zákonom musí byť spracovateľská operácia vo vzťahu k účelu spracúvania osobných údajov nevyhnutná a primeraná. Nevyhnutnosť spracovateľskej operácie sa preukazuje jej posúdením vo vzťahu k požadovanému účelu spracúvania osobných údajov. Primeranosť spracovateľskej operácie sa preukazuje posúdením jej povahy, rozsahu a kontextu, ktorý musí zodpovedať účelu spracúvania osobných údajov.

(2) Pri posúdení nevyhnutnosti a primeranosti spracovateľskej operácie sa zohľadní a odôvodní každé opatrenie prijaté na dosiahnutie súladu so zákonom, najmä

a) uplatnenie zásady zákonnosti podľa § 6 zákona,
b) uplatnenie zásady obmedzenia účelu podľa § 7 zákona,
c) uplatnenie zásady minimalizácie osobných údajov podľa § 8 zákona,
d) uplatnenie zásady správnosti podľa § 9 zákona,
e) uplatnenie zásady minimalizácie uchovávania podľa § 10 zákona,
f) uplatnenie zásady integrity a dôvernosti podľa § 11 zákona,
g) dodržiavanie postupov na uplatňovanie práv dotknutých osôb podľa § 19 až 28 zákona,
h) dodržiavanie postupov na zabezpečenie zákonného spracúvania osobných údajov sprostredkovateľom podľa § 34 zákona,
i) primerané záruky súvisiace s prenosom osobných údajov do tretej krajiny alebo medzinárodnej organizácii podľa § 47 až 51 zákona,
j) primerané technické a organizačné opatrenia podľa § 32 zákona,
k) názory dotknutých osôb alebo organizácií zastupujúcich záujmy dotknutých osôb na spracúvanie osobných údajov získané podľa § 42 ods. 6 zákona.

§ 5

(1) Prevádzkovateľ pri posúdení rizika pre práva fyzickej osoby zohľadní najmä

a) opis plánovaného spracúvania podľa § 3,
b) nevyhnutnosť a primeranosť spracovateľskej operácie podľa § 4,
c) opis podmienok spracúvania osobných údajov podľa § 39 ods. 1 zákona vrátane existujúcich bezpečnostných opatrení prijatých podľa § 39 zákona.

(2) Posúdenie rizika pre práva fyzickej osoby prevádzkovateľ vykonáva z pohľadu dopadov na fyzickú osobu, pričom zohľadňuje najmä riziko súvisiace s náhodným alebo nezákonným poškodením, zničením, stratou, zmenou, neoprávneným prístupom a poskytnutím alebo zverejnením osobných údajov, ako aj s akýmkoľvek iným neprípustným spôsobom spracúvania, pričom identifikuje

a) hrozby a pravdepodobnosť ich výskytu,
b) zraniteľnosti zneužiteľné hrozbami,
c) riziká a pravdepodobnosť ich výskytu a závažnosť,
d) a zhodnotí mieru dopadu na práva fyzickej osoby v dôsledku straty integrity, dôvernosti a dostupnosti údajov,
e) vysoké riziko pre práva fyzickej osoby, ak nepri-

jme opatrenia na zmiernenie rizika.
(3) Prevádzkovateľ pri posúdení rizík spracovateľských operácií môže postupovať aj podľa medzinárodných noriem.[1)]
(4) Prevádzkovateľ prijme primerané opatrenia na zmiernenie rizík vrátane záruk, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany osobných údajov a na preukázanie súladu so zákonom.
(5) Prevádzkovateľ prijme primerané opatrenia na zabezpečenie pravidelného monitorovania všetkých podmienok spracúvania osobných údajov, ktoré zohľadnil pri posudzovaní rizika pre práva fyzickej osoby podľa § 2 písm. a) až d), vrátane kontroly zavedených postupov. Prevádzkovateľ môže postupovať aj podľa medzinárodných noriem.[2)]
(6) Prevádzkovateľ pri prijímaní opatrení na zmiernenie rizík pre práva fyzickej osoby postupuje v primeranom rozsahu podľa prílohy.

§ 6

(1) Na preukazovanie súladu so zákonom podľa § 31 ods. 1 zákona, prevádzkovateľ zdokumentuje posúdenie vplyvu v rozsahu podľa § 2 písm. a) až c) a e).
(2) Dokumentáciou pri posúdení vplyvu podľa § 2 sa rozumie aj dokumentácia podľa osobitného predpisu,[3)] ak sa v nej preukazuje účel podľa odseku 1 spôsobom podľa tejto vyhlášky.

§ 7

Táto vyhláška nadobúda účinnosť 15. júna 2018.

Príloha k vyhláške č. 158/2018 Z. z.

OPATRENIE NA ELIMINÁCIU RIZÍK PRE PRÁVA FYZICKEJ OSOBY

1. Technické opatrenia
1.1 Technické opatrenie realizované prostriedkami fyzickej povahy
1.1.1 Zabezpečenie objektu pomocou mechanických zábranných prostriedkov (napr. uzamykateľné dvere, okná, mreže) a aj pomocou technických zabezpečovacích prostriedkov (napr. elektrický zabezpečovací systém objektu, elektrická požiarna signalizácia).
1.1.2 Zabezpečenie chráneného priestoru jeho oddelením od ostatných častí objektu (napr. steny, mreže alebo presklenia).
1.1.3 Umiestnenie dôležitých prostriedkov informačných technológií v chránenom priestore a ochrana informačnej infraštruktúry pred fyzickým prístupom neoprávnených osôb a nepriaznivými vplyvmi okolia.
1.1.4 Bezpečné uloženie fyzických nosičov osobných údajov vrátane bezpečného uloženia listinných dokumentov.
1.1.5 Opatrenie na zamedzenie náhodného prečítania osobných údajov zo zobrazovacích jednotiek (napr. vhodné umiestnenie zobrazovacích jednotiek).
1.2 Ochrana pred neoprávneným prístupom
1.2.1 Šifrová ochrana uložených a prenášaných údajov, pravidlá pre kryptografické opatrenia.
1.2.2 Pravidlá prístupu tretích strán k informačnému systému, ak k takému prístupu dochádza.
1.3 Riadenie prístupu poverených osôb
1.3.1 Riadenie prístupov a opatrenia na zaručenie platných politík riadenia prístupov (napr. identifikácia, autentizácia a autorizácia osôb v informačnom systéme).
1.3.2 Riadenie privilegovaných prístupov v informačnom systéme.
1.3.3 Zaznamenávanie prístupu a aktivít poverených osôb v informačnom systéme.
1.4 Riadenie zraniteľností
1.4.1 Opatrenia na detekciu a odstránenie škodlivého kódu a nápravu následkov škodlivého kódu.
1.4.2 Ochrana pred nevyžiadanou elektronickou poštou.
1.4.3 Používanie legálneho a prevádzkovateľom schváleného softvéru.
1.4.4 Opatrenia na zaručenie pravidelnej aktualizácie operačných systémov a programového aplikačného vybavenia.
1.4.5 Pravidlá sťahovania súborov z verejne prístupnej počítačovej siete a spôsob ich overovania. Filtrovanie sieťovej komunikácie.
1.4.6 Zhromažďovanie informácií o technických zraniteľnostiach informačných systémov, vyhodnocovanie úrovne rizík a implementácia opatrení na potlačenie týchto rizík.
1.5 Sieťová bezpečnosť
1.5.1 Kontrola, obmedzenie alebo zamedzenie prepojenia informačného systému, v ktorom sú spracúvané osobné údaje s verejne prístupnou počítačovou sieťou.
1.5.2 Ochrana vonkajšieho a vnútorného prostredia prostredníctvom nástrojov sieťovej bezpečnosti (napr. firewall), segmentácia počítačovej siete.
1.5.3 Pravidlá prístupu do verejne prístupnej počítačovej siete, opatrenia na zamedzenie pripojenia k určitým adresám, pravidlá používania sieťových protokolov.
1.5.4 Ochrana proti iným hrozbám pochádzajúcim z verejne prístupnej počítačovej siete (napr. hackerský útok).
1.5.5 Aktualizácia operačného systému a programového aplikačného vybavenia.
1.6 Zálohovanie
1.6.1 Test funkčnosti záložných dátových nosičov.
1.6.2 Vytváranie záloh s vopred zvolenou periodicitou.
1.6.3 Určenie doby uchovávania záloh a kontrola jej dodržiavania.
1.6.4 Test obnovy informačného systému zo zálohy.
1.6.5 Bezpečné ukladanie záloh.
1.7 Likvidácia osobných údajov a dátových nosičov
1.7.1 Technické opatrenia na bezpečné vymazanie osobných údajov z dátových nosičov.

1.7.2 Zariadenie na mechanické zničenie dátových nosičov osobných údajov (napr. zariadenie na skartovanie listín a dátových médií).

2. Organizačné opatrenia
2.1 Personálne opatrenia
2.1.1 Poverenie osoby prevádzkovateľom alebo sprostredkovateľom, ktorá má prístup k osobným údajom.
2.1.2 Pokyny prevádzkovateľa na spracúvanie osobných údajov, najmä
2.1.2.1 vymedzenie osobných údajov, ku ktorým má mať konkrétna osoba prístup na plnenie jej povinností alebo úloh,
2.1.2.2 určenie postupov, ktoré je poverená osoba povinná uplatňovať pri spracúvaní osobných údajov,
2.1.2.3 vymedzenie základných postupov alebo operácií s osobnými údajmi,
2.1.2.4 vymedzenie zodpovednosti za porušenie zákona.
2.1.3 Poučenie poverených osôb o postupoch spojených s automatizovanými prostriedkami spracúvania a súvisiacich právach a povinnostiach (v priestoroch prevádzkovateľa a mimo týchto priestorov).
2.1.4 Určenie zodpovednej osoby podľa § 44 zákona.
2.1.5 Vzdelávanie poverených osôb (napr. právna oblasť, oblasť informačných technológií).
2.1.6 Postup pri ukončení pracovného alebo obdobného pracovného vzťahu alebo obdobného pomeru poverenej osoby (napr. odovzdanie pridelených aktív, zrušenie prístupových práv, poučenie o následkoch porušenia zákonnej alebo zmluvnej povinnosti mlčanlivosti).
2.1.7 Práca na diaľku a pravidlá mobilného spracovania dát.
2.2 Riadenie aktív
2.2.1 Vedenie inventárneho zoznamu aktív a jeho pravidelná aktualizácia.
2.2.2 Evidencia všetkých miest prepojenia sietí vrátane prepojení s verejne prístupnou počítačovou sieťou.
2.2.3 Určenie vlastníctva aktív a zodpovednosti za riziká.
2.2.4 Pravidlá a postupy klasifikácie informácií.
2.2.5 Pravidlá a postupy na označovanie informácií a zaobchádzanie s nimi v súlade s platnou klasifikačnou schémou.
2.2.6 Pravidlá na prijateľné používanie informácií a aktív spojených s prostriedkami na spracúvanie informácií.
2.2.7 Opatrenia na vrátenie aktív (napr. prostriedkov spracúvania osobných údajov) patriacich prevádzkovateľovi po ukončení pracovného pomeru, po vypršaní uzatvorenej dohody alebo zmluvy, pri zmene pracovného miesta alebo pracovného zaradenia a pod.
2.3 Riadenie prístupu osôb k osobným údajom
2.3.1 Pravidlá fyzického vstupu do objektu a chránených priestorov prevádzkovateľa.
2.3.2 Správa prístupových prostriedkov a zariadení do objektov (individuálne prideľovanie kľúčov, elektronických kľúčov, vstupných kariet a bezpečné ukladanie ich rezerv).
2.3.3 Pravidlá prideľovania prístupových práv a úrovní prístupu (rolí) povereným osobám.
2.3.4 Politika hesiel a pravidlá používania autorizačných a autentizačných prostriedkov.
2.3.5 Pravidlá vzájomného zastupovania poverených osôb (napr. pri nehode, dočasnej pracovnej neschopnosti, ukončení pracovného alebo obdobného pomeru).
2.3.6 Pravidlá odstránenia alebo zmeny prístupových práv poverených osôb a zariadení na spracúvanie informácií pri ukončení zamestnania, zmluvy alebo dohody, alebo prispôsobenie zmenám rolí.
2.4 Organizácia spracúvania osobných údajov
2.4.1 Pravidlá spracúvania osobných údajov v chránenom priestore.
2.4.2 Nepretržitá prítomnosť poverenej osoby v chránenom priestore, ak sa v ňom nachádzajú aj iné ako poverené osoby.
2.4.3 Režim údržby a upratovania chránených priestorov.
2.4.4 Pravidlá spracúvania osobných údajov mimo chráneného priestoru, ak sa také spracúvanie predpokladá
2.4.4.1 pravidlá manipulácie s fyzickými nosičmi osobných údajov (napr. listiny, fotografie) mimo chránených priestorov a vymedzenie zodpovedností,
2.4.4.2 pravidlá používania automatizovaných prostriedkov spracúvania (napr. notebooky) mimo chránených priestorov a vymedzenie zodpovedností,
2.4.4.3 pravidlá používania prenosných dátových nosičov mimo chránených priestorov a vymedzenie zodpovedností.
2.5 Likvidácia osobných údajov
2.5.1 Určenie postupov likvidácie osobných údajov s vymedzením súvisiacej zodpovednosti jednotlivých poverených osôb (bezpečné vymazanie osobných údajov z dátových nosičov, likvidácia dátových nosičov a fyzických nosičov osobných údajov).
2.6 Porušenia ochrany osobných údajov
2.6.1 Postup pri oznamovaní porušenia ochrany osobných údajov úradu a dotknutej osobe na včasné prijatie preventívnych alebo nápravných opatrení.
2.6.2 Pravidelné preskúmavanie záznamov udalostí, záznamov o aktivitách používateľov, záznamov o výnimkách.
2.6.3 Evidencia porušení ochrany osobných údajov a použitých riešení.
2.6.4 Postup identifikácie a riešenia jednotlivých typov porušení ochrany osobných údajov.

2.6.5 Postup odstraňovania následkov porušení ochrany osobných údajov.
2.6.6 Postupy zaručenia kontinuity pri havárii alebo inej mimoriadnej udalosti.
2.6.7 Postup pri poruche, údržbe alebo oprave automatizovaných prostriedkov spracúvania.
2.7 Kontrolná činnosť
2.7.1 Kontrolná činnosť zameraná na dodržiavanie prijatých bezpečnostných opatrení s určením spôsobu, formy a periodicity jej realizácie (napr. pravidelné kontroly prístupov).
2.7.2 Informovanie osôb o kontrolnom mechanizme,[4)] ak ho prevádzkovateľ alebo sprostredkovateľ má zavedený (rozsah kontroly a spôsoby jej uskutočňovania).
2.7.3 Postupy monitorovania súladu spracúvania osobných údajov podľa § 42 ods. 7 zákona.
2.8 Dodávateľské vzťahy
2.8.1 Postup overenia dostatočných záruk.
2.8.2 Začlenenie požiadaviek na ochranu údajov do požiadaviek nových systémov a do pravidiel vývoja a nákupu systémov.
2.8.3 Začlenenie požiadaviek na ochranu údajov do zmluvných vzťahov s dodávateľmi a tretími stranami.
2.8.4 Testovanie bezpečnostných funkcií počas vývoja systémov.
2.8.5 Monitorovanie a pravidelné preskúmavanie úrovne bezpečnosti služieb poskytovaných dodávateľmi.

ODKAZY

1) Napríklad ISO/IEC 29134 Information technology - Security techniques - Guidelines for privacy impact assessment (ISO/IEC 29134:2017), Medzinárodná organizácia pre normalizáciu (ISO); LINDDUN (privacy threat analysis methodology), STRIDE (Threat Model).
2) Napríklad STN ISO/IEC 27005 Informačné technológie. Bezpečnostné metódy. Riadenie rizík informačnej bezpečnosti (ISO/IEC 27005:2011).
3) Napríklad § 20 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.
4) Čl. 11 a § 13 Zákonníka práce; čl. 9 a § 5 zákona č. 55/2017 Z. z. o štátnej službe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.