

ZBIERKA ZÁKONOV SLOVENSKEJ REPUBLIKY

Ročník 2018

Vyhlásené: 7. 6. 2018

Časová verzia predpisu účinná od: 15. 6.2018

Obsah dokumentu je právne záväzný.

158

VYHLÁŠKA

Úradu na ochranu osobných údajov Slovenskej republiky

z 29. mája 2018

o postupe pri posudzovaní vplyvu na ochranu osobných 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 neprijme 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.

Soňa Pötheová v. r.

**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 požiarňa 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, pravidiel 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.