

**Stratégia implementácie zákona  
č. 18/2018 Z. z. o ochrane osobných  
údajov do prostredia MV SR**

## Obsah

<b>1. Úvod</b>	<b>6</b>
1.1. Východiská	6
1.2. Pojmy a skratky	9
<b>2. Základné implementačné aktivity stratégie</b>	<b>10</b>
<b>3. Súvisiace výstupy</b>	<b>13</b>
3.1. Dotazníkový prieskum	13
3.2. GAP analýza	13
3.3. Klasifikácia IS MV SR	14
<b>4. Postup implementácie zákona do prostredia MV SR</b>	<b>17</b>
4.1. Požiadavky v kompetencii SKIS	17
4.2. Požiadavky v kompetencii gestora	18
4.3. Požiadavky v kompetencii SITB	21
<b>5. Požiadavky pre zaistenie súladu so zákonom na úrovni MV SR</b>	<b>24</b>
<b>5.1. Implementácia opatrení vyplývajúcich zo zásad spracúvania osobných údajov</b>	<b>24</b>
5.1.1. Zásada zákonnosti (§ 6)	24
5.1.2. Zásada obmedzenia účelu (§ 7)	25
5.1.3. Zásada minimalizácie údajov (§ 8)	25
5.1.4. Zásada správnosti (§ 9)	25
5.1.5. Zásada minimalizácie uchovávania (§ 10)	25
5.1.6. Zásada integrity a dôvernosti (§ 11)	26
5.1.7. Zásada zodpovednosti (§ 12)	26
5.1.8. Poskytovanie súhlasu so spracúvaním osobných údajov (§ 14)	27
5.1.9. Poskytovanie súhlasu v súvislosti so službami informačnej spoločnosti (§ 15)	27
<b>5.2. Implementácia opatrení vyplývajúcich z práv dotknutých osôb</b>	<b>27</b>
5.2.1. Právo na poskytované informácie pri získavaní osobných údajov (§ 19 - 20)	28
5.2.2. Právo na prístup k osobným údajom (§ 21)	28
5.2.3. Právo na opravu osobných údajov (§ 22)	28
5.2.4. Právo na výmaz osobných údajov (§ 23)	29
5.2.5. Právo na obmedzenie spracúvania osobných údajov (§ 24)	29
5.2.6. Oznamovacia povinnosť v súvislosti s opravou, vymazaním alebo obmedzením spracúvania osobných údajov (§ 25)	30
5.2.7. Právo na prenosnosť osobných údajov (§ 26)	30
5.2.8. Právo namietat' spracúvanie osobných údajov (§ 27)	30

5.2.9.	Právo na neúčinnosť automatizovaného individuálneho rozhodovania vrátane profilovania (§ 28)	31
5.2.10.	Povinnosti prevádzkovateľa pri uplatňovaní práv dotknutej osoby (§ 29).....	31
5.2.11.	Obmedzenie práv dotknutej osoby (§ 30).....	31
<b>5.3.</b>	<b>Implementácia opatrení vyplývajúcich zo všeobecných povinností prevádzkovateľa a sprostredkovateľa.....</b>	<b>32</b>
5.3.1.	Definovanie pravidiel špecificky navrhnutých a štandardnej ochrany osobných údajov (§ 32) .....	32
5.3.2.	Úprava pravidiel súvisiacich s využívaním sprostredkovateľov (§ 34) .....	33
5.3.3.	Vytvorenie záznamov o spracovateľských činnostiach (§ 37) .....	33
5.3.4.	Definovanie procesov súvisiacich s oznamovaním porušenia ochrany osobných údajov úradu (§ 40) a dotknutej osobe (§ 41) .....	34
5.3.5.	Definovanie pravidiel a zodpovedností súvisiacich s posúdením vplyvu na ochranu osobných údajov – DPIA (§ 42) .....	34
5.3.6.	Úprava procesov, postupov a zodpovedností súvisiacich so zodpovednou osobou (§ 44 - 46) ...	35
<b>5.4.</b>	<b>Implementácia opatrení vyplývajúcich z prenosu osobných údajov do tretej krajiny alebo medzinárodnej organizácii.....</b>	<b>35</b>
<b>5.5.</b>	<b>Implementácia osobitných situácií zákonného spracúvania osobných údajov .....</b>	<b>36</b>
<b>5.6.</b>	<b>Definovanie pravidiel pri kontakte s úradom .....</b>	<b>37</b>
<b>6.</b>	<b>Požiadavky pre zaistenie súladu so zákonom pre jednotlivé IS MV SR .....</b>	<b>39</b>
<b>6.1.</b>	<b>Požiadavky na všetky IS.....</b>	<b>39</b>
6.1.1.	Vytvorenie záznamov o spracovateľských činnostiach (§ 37) .....	39
6.1.2.	Uchovávanie údajov len po nevyhnutnú dobu (§ 10) .....	40
6.1.3.	Informovanie dotknutých osôb pri získavaní osobných údajov (§ 19 a 20) .....	40
6.1.4.	Právo na obmedzenie spracúvania osobných údajov (§ 24) .....	40
6.1.5.	Notifikácia tretích strán o vymazaní/obmedzení (§ 25) .....	41
6.1.6.	Prístup k osobným údajom (§ 21) .....	41
6.1.7.	Oprava osobných údajov (§ 22) .....	41
6.1.8.	Automatizované rozhodovanie a profilovanie (§ 28).....	41
6.1.9.	Privacy by design (§ 32).....	42
6.1.10.	Privacy by default (§ 32) .....	42
6.1.11.	Bezpečnosť spracúvania (§ 39) .....	42
6.1.12.	Posúdenie vplyvu na ochranu osobných údajov – DPIA (§ 42).....	43
6.1.13.	Sprostredkovatelia (§ 34 - § 36) .....	43
6.1.14.	Získavanie súhlasu (§ 14) .....	43
6.1.15.	Spätné získanie súhlasu (§ 14).....	43
6.1.16.	Kontrola veku (§ 15) .....	44
6.1.17.	Právo na výmaz osobných údajov (§ 23) .....	44
6.1.18.	Export údajov (§ 26) .....	44

---

<b>6.2. Požiadavky na IS spracúvajúce osobitnú kategóriu osobných údajov</b> .....	45
6.2.1. Bezpečnostný projekt a DPIA (§ 42) .....	45
6.2.2. Zaistenie dôvernosti IS (§ 39 ods. 1 písm. b)) .....	45
6.2.3. Zaistenie integrity IS (§ 39 ods. 1 písm. b)) .....	45
6.2.4. Pravidelné hodnotenie bezpečnosti (§ 39 ods. 1 písm. d)) .....	45
<b>6.3. Požiadavky na IS podporujúce plnenie úloh na účely trestného konania</b> .....	46
6.3.1. Zákonnosť spracúvania (§ 55) .....	46
6.3.2. Kategórie dotknutých osôb (§ 57) .....	46
6.3.3. Pôvod a pravdivosť osobných údajov (§ 58) .....	47
6.3.4. Informácie, ktoré sa majú sprístupniť alebo poskytnúť dotknutej osobe (§ 60 a 61) .....	47
6.3.5. Právo na opravu osobných údajov, právo na vymazanie osobných údajov a obmedzenie týchto práv (§ 62) .....	48
6.3.6. Obmedzenie poskytnutia informácií a práv dotknutej osoby (§ 63) .....	49
6.3.7. Automatizované individuálne rozhodovanie (§ 66) .....	49
6.3.8. Bezpečnostný projekt a DPIA (§ 42) .....	49
6.3.9. Bezpečnosť spracúvania osobných údajov (§ 71) .....	50
6.3.10. Vedenie logov (§ 69) .....	51
<b>6.4. Požiadavky na osobitne dôležité IS MV SR</b> .....	51
6.4.1. Bezpečnostný projekt a DPIA (§ 42) .....	51
6.4.2. Zaistenie dostupnosti (§ 39 ods. 1 písm. b)) .....	51
6.4.3. Zaistenie dôvernosti (§ 39 ods. 1 písm. b)) .....	52
6.4.4. Zaistenie integrity (§ 39 ods. 1 písm. b)) .....	52
6.4.5. Pravidelné hodnotenie bezpečnosti (§ 39 ods. 1 písm. d)) .....	52
<b>Príloha č. 1 – Zoznam IS podľa kategórií</b> .....	<b>53</b>
<b>Príloha č. 2 – Klasifikácia IS MV SR</b> .....	<b>55</b>
<b>Príloha č. 3 – Reakcia na požiadavky dotknutej osoby</b> .....	<b>79</b>
<b>Príloha č. 4 – Posúdenie vplyvu na ochranu osobných údajov (DPIA)</b> .....	<b>84</b>
<b>Príloha č. 5 – Prehľad povinností z nového zákona pri aktualizácii nariadenia č. 164/2013</b> .....	<b>87</b>
<b>Príloha č. 6 – Praktické naplnenie požiadaviek na bezpečnosť spracúvania</b> .....	<b>89</b>

## Popisné charakteristiky dokumentu

<b>Aktivita:</b>	Analytické činnosti vykonané s cieľom navrhnúť a optimalizovať postup implementácie zákona č. 18/2018 Z. z. o ochrane osobných údajov v prostredí MV SR
<b>Dokument:</b>	Stratégia implementácie zákona č. 18/2018 Z. z. o ochrane osobných údajov do prostredia MV SR
<b>Vypracovali:</b>	Mgr. Ivan Kopáček, CISA, CRISC, CGEIT Mgr. Anton Horváth, CISA, CISM Ing. Vladimír Kmeť
<b>Verzia:</b>	1.0
<b>Dátum:</b>	29. 3. 2018

# 1. Úvod

Stratégia implementácie zákona č. 18/2018 Z. z. o ochrane osobných údajov do prostredia MV SR je záverečným výstupom analytických činností vykonaných s cieľom navrhnuť a optimalizovať postup implementácie zákona č. 18/2018 Z. z. o ochrane osobných údajov v prostredí MV SR.

Za účelom včasnej a dostatočnej implementácie požiadaviek nového zákona (a tým aj nariadenia GDPR a smernice č. 2016/680) v prostredí MV SR boli na základe zmluvy<sup>1</sup> realizované nasledujúce činnosti:

1. analýza existujúcich procesov spracúvania osobných údajov (formou rozdielovej GAP analýzy), primárne z hľadiska aktuálneho splnenia alebo nesplnenia relevantných požiadaviek GDPR,
2. klasifikácia informačných systémov MV SR s ohľadom na požiadavky tak GDPR ako aj smernice č. 2016/680, ktorá sa v súvislosti s požiadavkami GDPR tiež musí uplatniť v podmienkach MV SR,
3. namapovanie technických požiadaviek GDPR a smernice č. 2016/680 na jednotlivé IS (nie všetky požiadavky sa týkajú všetkých IS),
4. identifikácia a vysvetlenie požiadaviek GDPR a smernice č. 2016/680 na MV SR ako prevádzkovateľa a návrh spôsobu ich plnenia,
5. vypracovanie dokumentu „Stratégia implementácie požiadaviek implementácie zákona č. 18/2018 Z. z. o ochrane osobných údajov (GDPR) do prostredia MV SR“.

Tento dokument komplexne a konkrétne špecifikuje okruhy, rozsah a postupnosť činností nevyhnutných pre dosiahnutie súladu MV SR so zákonom č. 18/2018 Z. z. o ochrane osobných údajov.

## 1.1. Východiská

Dňa 4. mája 2016 bolo v Úradnom vestníku Európskej únie zverejnené Nariadenie č. 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov<sup>2</sup> (z angl. „General data protection regulation – GDPR“). GDPR sa stalo platným 24. mája 2016 a nahradilo tak európsku smernicu o ochrane fyzických osôb v súvislosti so spracúvaním osobných údajov z roku 1995 s cieľom vytvoriť zjednotenú právnu úpravu v oblasti ochrany osobných údajov v celej Európskej únii.

<sup>1</sup> zmluva o dielo č. SITB-OB1-2017/001208-007

<sup>2</sup> <http://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:32016R0679&from=SK>

V prostredí MV SR musí byť zároveň s GDPR implementovaná aj Smernica európskeho parlamentu a rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV<sup>3</sup> (ďalej len „smernica č. 2016/680“). Nariadenie GDPR bude spolu so smernicou č. 2016/680 účinné a priamo aplikovateľné od 25. mája 2018 vo všetkých 28 členských štátoch Európskej únie. Do tohto dátumu musia mať všetky organizácie spracúvajúce osobné údaje implementované všetky opatrenia na dosiahnutie súladu s GDPR a smernicou č. 2016/680.

30. januára 2018 bol v Zbierke zákonov publikovaný zákon č. 18/2018 Z. z. o ochrane osobných údajov.<sup>4</sup> Týmto zákonom sa slovenský právny poriadok harmonizuje s nariadením GDPR a smernicou č. 2016/680. Podobne ako GDPR, aj tento zákon nadobúda účinnosť od 25. mája 2018.

Ako zdroje pre analýzu a vypracovanie tejto stratégie boli okrem týchto troch predpisov použité aj nasledovné usmernenia pracovnej skupiny WP29:

- Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016\_679,
- Guidelines on Personal data breach notification under Regulation 2016\_679,
- Usmernenia k právu na prenosnosť údajov,
- Usmernenia k určeniu vedúceho dozorného orgánu prevádzkovateľa alebo sprostredkovateľa,
- Usmernenia týkajúce sa zodpovedných osôb,
- Usmernenia týkajúce sa posúdenia vplyvu na ochranu údajov a stanovenie toho, či na účely nariadení a 2016\_679 spracúvanie pravdepodobne povedie k vysokému riziku,
- Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016\_679,
- Guidelines on Data protection Officers (DPO's),
- Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is likely to result in high risk,
- Guidelines on The Lead Supervisory Authority.

Najzásadnejšie zmeny, ktoré prináša GDPR a nový zákon pre prostredie MV SR:

- rozšírenie definície osobných údajov o nové typy údajov ako sú IP adresa alebo súbory cookies,

<sup>3</sup> <http://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:32016L0680&from=SK>

<sup>4</sup> <https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/18/20180525>

- úprava osobitných kategórií osobných údajov, pričom rodné číslo do tejto kategórie už nebude spadať,
- sprísnenie náležitostí súhlasu so spracovaním osobných údajov, ktorý musí byť konkrétny, slobodný, informovaný a jednoznačný prejav vôle,
- úprava v informačnej povinnosti prevádzkovateľa pri získavaní osobných údajov,
- zrušenie povinností viesť evidenciu informačného systému alebo oznamovať informačné systémy Úradu na ochranu osobných údajov, namiesto toho sa zavádza povinnosť viesť záznamy o spracovateľských činnostiach
- vypustenie povinnosti vypracovávať bezpečnostný projekt, jeho novou alternatívou je povinnosť vykonať posúdenie vplyvu (plánovaných spracovateľských operácií) na ochranu osobných údajov,
- nová povinnosť dokumentácie každého prípadu porušenia ochrany osobných údajov (bezpečnostného incidentu) a povinnosť oznámiť porušenie úradu do 72 hodín od jeho identifikácie (ak môže viesť k riziku pre práva fyzickej osoby)
- zavedenie štandardnej ochrany osobných údajov (data protection by default) v rámci organizačného prostredia MV SR,
- zavedenie špecifickej ochrany osobných údajov (data protection by design) v rámci jednotlivých informačných systémov,
- implementácia práva namietať spracúvanie osobných údajov a práva na obmedzenie spracúvania osobných údajov, kedy nie je možné údaje ďalej spracúvať, ak k tomu nie sú závažné, preukázateľné dôvody,
- sprísnenie povinnosti vymazať osobné údaje na žiadosť dotknutej osoby (pri splnení zákonom stanovených podmienok), a to tak, že osobné údaje majú byť vymazané nielen u prevádzkovateľa, ale aj u ďalších subjektov, ktoré tieto údaje spracúvajú,
- zavedenie prísnejších pokút za porušenie povinností spojených so spracúvaním a ochranou osobných údajov, a to až do výšky 20 000 000 EUR alebo do výšky 4 % celkového svetového ročného obratu za predchádzajúci účtovný rok.

Problematiku implementácie nového zákona a GDPR je potrebné zohľadňovať aj pri kľúčových rozvojových projektoch. MV SR je správcom a prevádzkovateľom ISVS vládneho cloudu, ktorého súčasťou v cieľovom riešení bude poskytovanie trojice služieb IaaS, PaaS a SaaS. Štúdia uskutočniteľnosti „Zavedenie služieb Platform as a Services“ priamo uvádza:

Súčasťou dodávky bude aj vytvorenie bezpečnostného projektu, ktorý bude musieť pokryť aj požiadavky GDPR. Predpokladané požiadavky na tento projekt sú:

- súlad s GDPR a požiadavkami na bezp. projekt podľa zákona 275/2006,
- preukázať splnenie požiadaviek GDPR a zároveň poskytnúť záruky na to, že sú prijaté primerané technické a organizačné opatrenia na strane cloudu,



- vzor sprostredkovateľských zmlúv odberateľa služieb s prevádzkovateľom cloudu,
- návrh a následná implementácia záznamov o spracovateľských činnostiach,
- preukázať splnenie bezpečnostných štandardov bežných pre cloud providerov.

## 1.2. Pojmy a skratky

V nasledujúcej tabuľke je uvedený popis pojmov a skratiek používaných v rámci predkladaného dokumentu.

Pojem/skratka	Význam
DPIA	Posúdenie vplyvu na ochranu osobných údajov (z angl. Data protection impact assessment)
GDPR	Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (všeobecné nariadenie o ochrane údajov)
IS	Informačný systém
MV SR	Ministerstvo vnútra Slovenskej republiky
OB SITB	Odbor bezpečnosti SITB
OÚ	Osobné údaje
Úrad	Úrad na ochranu osobných údajov SR
SITB	Sekcia informatiky, telekomunikácií a bezpečnosti
SKIS	Sekcia kontroly a inšpekčnej služby
Smernica č. 2016/680	Smernica európskeho parlamentu a rady (EÚ) 2016/680 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV
SR	Slovenská republika
Zákon	Zákon č. 18/2018 Z. z. o ochrane osobných údajov

## 2. Základné implementačné aktivity stratégie

V tejto kapitole je uvedený praktický postup realizácie stratégie implementácie požiadaviek implementácie zákona č. 18/2018 Z. z. o ochrane osobných údajov do prostredia MV SR. Finálnym cieľom je čo najefektívnejšia implementácia požiadaviek nového zákona. Za týmto účelom je navrhnutá vrcholová postupnosť krokov implementácie zákona v kontexte tohto dokumentu a popísané základné aktivity v kompetencii jednotlivých aktérov.

Implementáciu zákona je potrebné v prostredí MV SR pokryť plošne a na viacerých úrovniach. Pri implementácii zákona sú zainteresované najmä nasledované organizačné útvary – SKIS, SITB a gestori IS spracúvajúcich osobné údaje. Každému aktérovi musia byť v rámci implementácie zákona jasne a jednoznačne stanovené zodpovednosti a konkrétne aktivity, ktoré má vykonať na dosiahnutie súladu so zákonom.

V prostredí MV SR bolo historicky identifikovaných približne 200 účelov spracúvania osobných údajov, resp. IS spracúvajúcich osobné údaje (v elektronickej, ale aj písomnej forme). Tieto účely sú centrálné evidované na SKIS ako odborného gestora na úseku ochrany osobných údajov, ktorá súčasne vedie aj dokumentáciu evidenčných formulárov. Na základe dotazníkov od gestorov, ktoré predchádzali vytvoreniu tejto stratégie a boli jej podkladom, bolo však identifikovaných iba 79 IS<sup>5</sup>. Úlohou SKIS preto bude doplniť všetky ostávajúce IS z existujúcej evidencie IS do klasifikácie IS MV SR,<sup>6</sup> resp. kontaktovať tie organizačné útvary, v ktorých gescii sú chýbajúce IS a vyžiadať si potrebnú súčinnosť. Zaradenie týchto IS do klasifikácie IS MV SR je potrebné realizovať podľa postupu uvedeného v kapitole 3.3.

**SKIS** má v zmysle tejto stratégie za úlohu vrcholovo zastrešovať a dohliadať na projekt implementácie zákona do prostredia MV SR. Povinnosti a aktivity vyplývajúce pre SKIS sú definované v kapitole 4.1, konkrétnejšie sú tieto činnosti popísané v kapitole 5. Odporúčaný vrcholový postup realizácie aktivít v pôsobnosti SKIS:

1. informovať všetkých gestorov IS o ich úlohách vyplývajúcich zo stratégie implementácie zákona a realizovať školenie gestorov,
2. aktualizovať nariadenie č. 164/2013 o ochrane osobných údajov,
3. stanoviť jednotnú metodiku pre posúdenie vplyvu v prostredí MV SR,
4. stanoviť a implementovať proces spracovania žiadostí dotknutých osôb,
5. schvaľovať záznamy o spracovateľských činnostiach od gestorov IS a viesť aktuálne verzie záznamov o spracovateľských činnostiach,

<sup>5</sup> viaceré IS nebolo možné zahrnúť do výstupov, pretože sa gestorské organizačné útvary k dotazníku nevyjadrili

<sup>6</sup> príloha č. 2, resp. samostatný dokument vo formáte MS Excel

6. definovať štandardný vzor sprostredkovateľskej zmluvy, viesť evidenciu sprostredkovateľských zmlúv, kontrolovať a schvaľovať sprostredkovateľské zmluvy vytvorené jednotlivými gestormi,
7. viesť aktuálnu klasifikáciu IS MV SR.

Pre efektívnu implementáciu požiadaviek nového zákona do prostredia MV SR na základe tejto stratégie bude potrebné výrazné zapojenie gestorov jednotlivých IS spracúvajúcich osobné údaje. Preto je čo najskôr potrebné realizovať **školenie pre jednotlivých gestorov IS**, na ktorom je nutné vysvetliť ich povinnosti a postup, ako efektívne a správne realizovať činnosti, ktoré pre nich vyplývajú zo zákona a tejto stratégie implementácie.

Gestori budú následne zodpovední za implementáciu požiadaviek zákona pre všetky IS v ich gescii. Štandardná postupnosť krokov pre implementáciu zákona podľa tejto stratégie je nasledovná:

1. zaradenie IS do klasifikácie IS MV SR podľa kapitoly 3.3 (relevantné pre nové IS a IS neuvedené v dotazníkoch),
2. implementácia jednotlivých krokov v zmysle kapitoly 4,
3. splnenie požiadaviek pre všetky IS podľa kapitoly 6.1,
4. splnenie požiadaviek pre všetky ďalšie kategórie, do ktorých je IS zaradený (podľa kapitol 6.2, 6.3 a 6.4).

**Gestori IS** majú za úlohu pokryť IS vo svojej gescii podľa požiadaviek stratégie implementácie zákona. Povinnosti a aktivity vyplývajúce pre gestorov sú komplexne definované v kapitole 4.2, konkrétnejšie sú tieto činnosti popísané v kapitole 6. Odporúčaný vrcholový postup realizácie aktivít v pôsobnosti gestorov:

1. zdokumentovať spracúvanie osobných údajov vo forme záznamov o spracovateľských činnostiach, poskytnúť tieto záznamy na odsúhlasenie SKIS,
2. vytvoriť informačný list, ktorý má napĺňať informačnú povinnosť pri získavaní osobných údajov,
3. zabezpečiť predpoklady pre realizáciu práv dotknutých osôb (v súčinnosti so SITB),
4. prispôbiť existujúce súhlasy podľa nových požiadaviek zákona (v prípade, že je právny základ spracúvania súhlas),
5. vytvoriť sprostredkovateľské zmluvy, poskytnúť tieto zmluvy na odsúhlasenie SKIS,
6. zabezpečiť realizáciu bezpečnostného projektu a posúdenia vplyvu na ochranu osobných údajov,
7. zabezpečiť pravidelné hodnotenie bezpečnosti, resp. účinnosti technických a organizačných opatrení,
8. zabezpečiť splnenie špecifických požiadaviek pre príslušnú kategóriu IS.

**SITB** má za úlohu poskytnúť súčinnosť gestorom pri realizácii a implementácii technických požiadaviek vyplývajúcich zo zákona. Povinnosti a aktivity vyplývajúce zo stratégie pre SITB sú podrobnejšie definované v kapitole 4.3 tohto dokumentu. Kľúčové aktivity v pôsobnosti SITB sú:

1. poskytovať gestorovi súčinnosť pri technickej realizácii požiadaviek zákona (napr. práv dotknutých osôb, získavania súhlasu)
2. v súčinnosti s gestorom realizovať primerané technické a organizačné opatrenia na zaistenie úrovne bezpečnosti primeranej riziku pre práva fyzických osôb,
3. poskytovať súčinnosť gestorom pri vypracúvaní bezpečnostného projektu a posúdenia vplyvu na ochranu osobných údajov,
4. zabezpečiť splnenie špecifických technických požiadaviek pre príslušnú kategóriu IS (napr. šifrovanie, logovanie).

Viaceré požiadavky zákona pravdepodobne nebude možné naplniť okamžite z dôvodu veľkého množstva IS, rozsiahlosti spracúvania a nedostatku finančných, personálnych či časových zdrojov. Preto je potrebná prioritizácia implementácie požiadaviek zákona na úrovni jednotlivých IS na základe ich dôležitosti. Rizikovými faktormi sú napr. rozsah poskytovaných služieb a ich kritickosť, citlivosť údajov, počet dotknutých osôb či chýbajúci bezpečnostný projekt. Tieto faktory sú zohľadnené aj v navrhovanej klasifikácii IS a preto navrhujeme prioritizáciu implementácie zákona podľa kategórie IS v nasledovnom poradí od najdôležitejšieho:

1. osobitne dôležité IS,
2. IS podporujúce plnenie úloh na účely trestného konania,
3. IS spracúvajúce osobitnú kategóriu osobných údajov,
4. ostatné IS spracúvajúce osobné údaje.

Jednotlivé implementačné činnosti je potrebné riadne plánovať, najmä z hľadiska potrebných zdrojov. Činnosti, ktoré si vyžadujú špecifickú odbornosť či významnejšie úsilie (napr. vypracovanie bezpečnostného projektu a posúdenia vplyvu, implementácia špecifickej funkcionality v IS – napr. pre vymazanie údajov) je možné riešiť aj dodávateľsky.

### 3. Súvisiace výstupy

Vypracovaniu tohto dokumentu predchádzali nasledovné aktivity so samostatnými výstupmi:

1. identifikácia existujúcich IS spracúvajúcich osobné údaje a stavu pokrytia vybraných požiadaviek zákona (dotazníkový prieskum),
2. analýza existujúcich procesov spracúvania osobných údajov (formou rozdielovej GAP analýzy), primárne z hľadiska aktuálneho splnenia alebo nespĺnenia relevantných požiadaviek GDPR,
3. klasifikácia informačných systémov MV SR s ohľadom na požiadavky tak GDPR ako aj smernice č. 2016/680,
4. mapovanie technických požiadaviek GDPR a smernice č. 2016/680 na jednotlivé IS (nie všetky požiadavky sa týkajú všetkých IS).

#### 3.1. Dotazníkový prieskum

Úlohou prieskumu bolo (formou otázok na gestorov) východiskovo zhodnotiť stav pokrytia základných požiadaviek GDPR a smernice č. 2016/680 na identifikované IS. Súčasťou bolo aj získanie informácií o parametroch následne použitých pri klasifikácii IS MV SR.

Miera reakcie respondentov však bola nedostatočná. Výsledky prieskumu nepokrývajú všetky účely spracúvania, resp. IS spracúvajúce osobné údaje v prostredí MV SR (napr. v porovnaní s evidenciou SKIS). Chýbajúce účely spracúvania a IS však je možné priamočiaro zaradiť do procesov implementácie zákona v zmysle nasledujúcich kapitol.

Výstup prieskumu je vo forme samostatného dokumentu (formát MS Excel).

#### 3.2. GAP analýza

Na základe získaných dotazníkov bola za účelom vyhodnotenia aktuálneho stavu naplnenia jednotlivých požiadaviek nového zákona v prostredí MV SR realizovaná rozdielová GAP analýza. V rámci nej boli posudzované existujúce procesy voči detailným požiadavkám zákona na úrovni jednotlivých paragrafov a vyhodnotená miera ich naplnenia na úrovni MV SR. Výstupy z rozdielovej GAP analýzy boli použité pri tvorbe tejto stratégie implementácie.

Výsledky GAP analýzy sú uvedené v samostatnom dokumente vo formáte MS Excel.

### 3.3. Klasifikácia IS MV SR

V rámci analytických činností bola navrhnutá klasifikácia IS MV SR na viaceré kategórie, ktorá má za cieľ jednoduchšiu a adresnejšiu implementáciu požiadaviek zákona v prostredí IS MV SR.

Informačné systémy MV SR boli v rámci klasifikácie kategorizované nasledovne:

1. IS spracúvajúce bežné osobné údaje,
2. IS spracúvajúce osobitnú kategóriu osobných údajov,
3. IS podporujúce plnenie úloh na účely trestného konania,
4. osobitne dôležité IS.

**Prvá kategória – IS spracúvajúce osobné údaje**, obsahuje všetky IS, v ktorých sú akýmkoľvek spôsobom spracúvané osobné údaje (a teda obsahuje aj všetky IS z ostatných kategórií). Podľa § 2 zákona sú osobnými údajmi údaje týkajúce sa identifikovanej fyzickej osoby alebo identifikovateľnej fyzickej osoby, ktorú možno identifikovať priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora, iného identifikátora, ako je napríklad meno, priezvisko, identifikačné číslo, lokalizačné údaje, alebo online identifikátor, alebo na základe jednej alebo viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú identitu, fyziologickú identitu, genetickú identitu, psychickú identitu, mentálnu identitu, ekonomickú identitu, kultúrnu identitu alebo sociálnu identitu. Požiadavky pre túto kategóriu tvoria nevyhnutný základ, ktorý je potrebné pri implementácii naplniť pre každý relevantný IS.

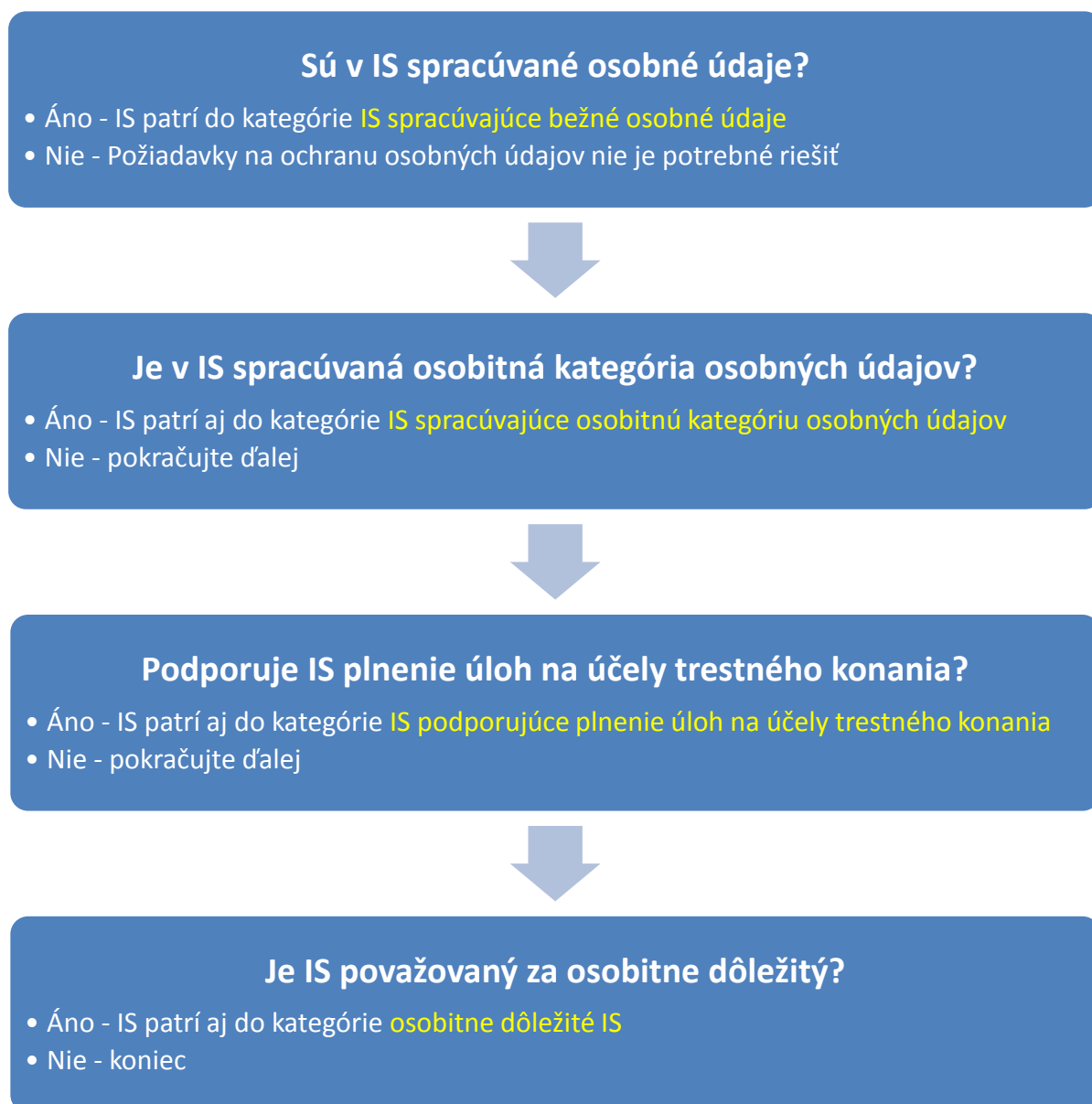
**Druhá kategória – IS spracúvajúce osobitnú kategóriu osobných údajov**, združuje IS spracúvajúce navyše osobné údaje definované v zákone ako osobitná kategória osobných údajov. Podľa § 16 ods. 1 zákona sú to údaje, ktoré odhaľujú rasový pôvod alebo etnický pôvod, politické názory, náboženskú vieru, filozofické presvedčenie, členstvo v odborových organizáciách, genetické údaje, biometrické údaje, údaje týkajúce sa zdravia alebo údaje týkajúce sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby. Požiadavky pre túto kategóriu musia byť implementované pre všetky IS spracúvajúce osobitnú kategóriu osobných údajov.

**Tretia kategória – IS podporujúce plnenie úloh na účely trestného konania**, obsahuje IS spracúvajúce osobné údaje v zmysle smernice európskeho parlamentu a rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV. Skrátený výraz „na účely trestného konania“ predstavuje formuláciu podľa §3 ods. 3 zákona – na účely predchádzania a odhaľovania trestnej činnosti, zisťovania páchatelov trestných činov, stíhania trestných činov alebo na účely

výkonu rozhodnutí v trestnom konaní vrátane ochrany pred ohrozením verejného poriadku a predchádzania takémuto ohrozeniu. Požiadavky pre túto kategóriu sú teda relevantné pre IS v pôsobnosti policajného zboru a ďalšie IS podporujúce plnenie úloh na účely trestného konania.

**Posledná kategória – osobitne dôležité IS**, obsahuje významné IS, ktoré sú rozhodujúce pre činnosti MV SR a ich zlyhanie okamžite ohrozuje poskytovanie dôležitých služieb a reputáciu MV SR. Tieto IS sú osobitne citlivé z hľadiska rozsahu spracúvaných údajov a dostupnosti ich služieb pre verejnosť a iné IS VS, preto je potrebné implementovať aj ďalšie požiadavky nad rámec ostatných kategórií. Označenie IS za osobitne dôležitý je v kompetencii odboru bezpečnosti SITB MV SR.

Nasledujúca schéma obsahuje postup pre určenie príslušnosti ľubovoľného IS ku jednotlivým kategóriám v zmysle definovanej klasifikácie.



Vyššie uvedené kategórie sa vzájomne nevylučujú a konkrétny IS MV SR môže byť zaradený len do prvej kategórie, ale aj do všetkých štyroch. Akýkoľvek nový alebo zatiaľ nezaradený IS je možné zaradiť do klasifikácie na základe predchádzajúcej schémy a popisu jednotlivých kategórií, voči ktorým je potrebné vyhodnotiť rozsah údajov, ktoré sú v IS spracúvané.

Vo fáze implementácie požiadaviek zákona do prostredia MV SR musia byť pre každý IS spracúvajúci osobné údaje implementované technické opatrenia špecifické pre príslušný IS, v závislosti od jeho kategórie (viď kap. 6).

Zaradenie všetkých IS, ktoré boli identifikované zo zaslaných dotazníkov od jednotlivých organizačných útvarov MV SR, do uvedených kategórií, je uvedené v prílohe č. 1. Počty IS v jednotlivých kategóriách sú na základe dotazníkov nasledovné:

1. 79 IS spracúvajúce bežné osobné údaje,
2. 22 IS spracúvajúce osobitnú kategóriu osobných údajov,
3. 23 IS podporujúce plnenie úloh na účely trestného konania,
4. 22 osobitne dôležitých IS.

Celá tabuľka klasifikácie IS MV SR vytvorená na základe zaslaných dotazníkov, je uvedená v prílohe č. 2.

Na tomto mieste je nutné uviesť, že výsledky dotazníkového prieskumu nepokrývajú všetky účely spracúvania, resp. IS spracúvajúce osobné údaje v prostredí MV SR (napr. v porovnaní s evidenciou SKIS). Chýbajúce účely spracúvania a IS však je možné priamočiaro zaradiť do procesov implementácie nového zákona v zmysle nasledujúcich kapitol.



## 4. Postup implementácie zákona do prostredia MV SR

V tejto kapitole je uvedený zoznam jednotlivých krokov implementácie zákona, rozdelený medzi jednotlivé organizačné útvary MV SR zainteresované v implementácii zákonných požiadaviek do prostredia MV SR. Jednotlivé požiadavky zákona sú podrobnejšie vysvetlené v kapitolách 5 a 6 tohto dokumentu, pri jednotlivých krokoch sú uvedené aj odkazy na konkrétne kapitoly stratégie.

### 4.1. Požiadavky v kompetencii SKIS

Pre SKIS vyplývajú v rámci implementácie požiadaviek zákona nasledujúce povinnosti a aktivity:

1. realizovať školenie pre gestorov súvisiace s novým zákonom č. 18/2018 Z. z. o ochrane osobných údajov a postupom jeho implementácie
2. aktualizovať nariadenie MV SR č. 164/2013 o ochrane osobných údajov a zahrnúť nové povinnosti vyplývajúce zo zákona do tohto nariadenia
  - podrobnejší popis požiadaviek na aktualizáciu je realizovaný v rámci kapitoly 5,
  - prehľad povinností podľa jednotlivých paragrafov zákona, o ktoré je potrebné uvedené nariadenie aktualizovať, je uvedený v prílohe č. 5,
3. zabezpečiť zverejnenie kontaktných údajov na vrcholovú zodpovednú osobu MV SR (napr. na internetovej stránke MV SR), prehodnotenie a potvrdenie menovania všetkých zodpovedných osôb MV SR, zabezpečenie školenia pre zodpovedné osoby na nový zákon (kap. 5.3.6),
4. stanoviť a implementovať proces spracovania žiadostí dotknutých osôb (viď príloha č. 3)
  - centralizovaný príjem žiadostí formou kontaktovania vrcholovej zodpovednej osoby,
  - vybavenie žiadostí (pre ktoré to je možné) priamo z pozície SKIS (najmä zamietnutia na základe rozporu so zákonom, príp. žiadosti spracovateľné na základe záznamov o spracovateľských činnostiach),
  - postúpenie opodstatnených nevybavených žiadostí na gestora konkrétneho účelu spracúvania,
  - súčinnosť SITB pri technickej realizácii naplnenia opodstatnených žiadostí, ktoré si to vyžadujú,
  - spätnú komunikáciu vrcholovej zodpovednej osoby k žiadateľovi.
5. schvaľovať záznamy o spracovateľských činnostiach od gestorov jednotlivých účelov spracúvania, viesť zoznam aktuálnych verzií záznamov o spracovateľských činnostiach pre všetky účely v prostredí MV SR (kap. 5.3.3),

6. kontrolovať sprostredkovateľské zmluvy vytvorené gestormi jednotlivých účelov spracúvania, viesť jednotnú evidenciu sprostredkovateľských zmlúv, definovať štandardný vzor sprostredkovateľskej zmluvy (kap. 5.3.2),
7. na základe pripravovanej vyhlášky úradu pre posúdenie vplyvu na ochranu osobných údajov stanoviť jednotnú metodiku pre posúdenie vplyvu v prostredí MV SR v súčinnosti s OB SITB (kap. 5.3.5),
8. definovať procesy súvisiace s oznamovaním porušenia ochrany osobných údajov úradu (§ 40 zákona) a dotknutej osobe (§ 41 zákona) a realizovať tieto oznámenia v praxi (v súčinnosti s gestorom a SITB) (kap. 5.3.4),
9. definovať pravidlá a povinnosti kontrolovaného subjektu – MV SR, ako aj zastupovanie MV SR pri kontakte s úradom (kap. 5.6).

## 4.2. Požiadavky v kompetencii gestora

Pre gestorov jednotlivých účelov spracúvania osobných údajov (resp. IS) vyplývajú v rámci implementácie požiadaviek zákona nasledujúce povinnosti a aktivity:

### Aktivity gestora súvisiace so všetkými IS MV SR:

1. vytvoriť záznamy o spracovateľských činnostiach pre každý účel spracúvania v pôsobnosti gestora (kap. 5.3.3, kap. 6.1.1),
  - vytvorené záznamy o spracovateľských činnostiach je potrebné poslať na schválenie SKIS, aktuálnu verziu záznamov o spracovateľských činnostiach eviduje gestor aj SKIS,
2. v rámci vytvárania záznamov o spracovateľských činnostiach vyhodnotiť pre každý účel spracúvania:
  - dodržanie zásady zákonnosti (kap. 5.1.1),
  - dodržanie zásady obmedzenia účelu (kap. 5.1.2),
  - dodržanie zásady minimalizácie údajov (kap. 5.1.3),
  - dodržanie zásady správnosti (kap. 5.1.4),
  - dodržanie zásady minimalizácie uchovávaní (kap. 5.1.5, kap. 6.1.2),
  - dodržanie zásady integrity a dôvernosti (kap. 5.1.6),
  - dodržanie zásady zodpovednosti (kap. 5.1.7),
  - pre IS podporujúce plnenie úloh na účely trestného konania je potrebné vyhodnotiť iba zásady uvedené v § 52 až § 58 zákona,
3. preskúmať jednotlivé právne základy spracúvania osobných údajov v jednotlivých účeloch spracúvania z pohľadu ich aktuálnosti a správnosti (kap. 5.1.1),
4. pre každý účel spracúvania vytvoriť informačný list, ktorý bude naplňovať informačnú povinnosť pri získavaní osobných údajov a obsahovať náležitosti podľa § 19 zákona (v prípade, že sú osobné údaje získané od dotknutej osoby), resp. podľa § 20 zákona (v prípade, ak nie sú osobné údaje získané od dotknutej osoby), zároveň bude potrebné zvoliť vhodný spôsob informovania dotknutých osôb o uvedených náležitostiach (napr. zverejnením na internetovej stránke,

- zahrnutím do súhlasu na spracúvanie osobných údajov, vyvesením na kontaktnom mieste) (kap. 5.2.1, kap. 6.1.3),
5. v prípade žiadostí dotknutých osôb je gestor povinný po postúpení odôvodnenej žiadosti zo strany SKIS zabezpečiť realizáciu práv dotknutých osôb (pri technickej realizácii spolupracuje SITB)
    - právo na prístup k osobným údajom (napr. zaslať potvrdenie o tom, že sa o dotknutej osobe spracúvajú osobné údaje, dotknutá osoba má právo získať prístup aj k dodatočným informáciám podľa uvedeného paragrafu) (kap. 5.2.2, kap. 6.1.6),
    - právo na opravu osobných údajov (kap. 5.2.3, kap. 6.1.7),
    - právo na obmedzenie osobných údajov (kap. 5.2.5, kap. 6.1.4),
    - realizácia oznamovacej povinnosti tretím stranám v súvislosti s opravou, vymazaním alebo obmedzením osobných údajov (kap. 5.2.6, kap. 6.1.5),
    - právo namietat' spracúvanie osobných údajov (kap. 5.2.8),
    - právo na neúčinnosť automatizovaného individuálneho rozhodovania vrátane profilovania (kap. 5.2.9),
  6. pri vývoji nového IS, resp. aktualizácii existujúceho IS, je gestor povinný zabezpečiť uplatňovanie pravidiel špecificky navrhutej a štandardnej ochrany osobných údajov (kap. 5.3.1, kap. 6.1.9, kap. 6.1.10),
  7. zabezpečiť vytvorenie sprostredkovateľských zmlúv (v prípade potreby v súčinnosti s OB SITB) a poskytnúť návrh týchto zmlúv na schválenie SKIS (kap. 5.3.2, kap. 6.1.13),
  8. zabezpečiť realizáciu posúdenia vplyvu na ochranu osobných údajov pre konkrétne účely spracúvania, ktorým táto povinnosť vyplýva zo zákona, príp. z pripravovanej vyhlášky úradu o posúdení vplyvu na ochranu osobných údajov (kap. 5.3.5, kap. 6.1.12),
  9. zabezpečiť súlad s požiadavkami vyplývajúcimi z realizácie prenosu osobných údajov do tretej krajiny alebo medzinárodnej organizácii (kap. 5.4).

Požiadavky súvisiace len s IS MV SR, v ktorých je právny základ **súhlas so spracúvaním osobných údajov**:

10. pre účely spracúvania, ktoré sú založené na základe súhlasu so spracúvaním osobných údajov, je potrebné daný súhlas prispôbiť požiadavkám zákona (kap. 5.1.8, kap. 6.1.14),
11. zabezpečiť implementáciu podmienok poskytnutia súhlasu v súvislosti so službami informačnej spoločnosti (kap. 5.1.9, kap. 6.1.16),
12. zabezpečiť spätné získavanie súhlasu so spracúvaním a koordináciu pri jeho technickej realizácii s SITB,
13. v prípade žiadostí dotknutých osôb je gestor povinný po postúpení odôvodnenej žiadosti zo strany SKIS zabezpečiť realizáciu práv dotknutých osôb (pri technickej realizácii spolupracuje SITB)
  - právo na výmaz osobných údajov pre IS (kap. 5.2.4, kap. 6.1.17),
  - právo na prenosnosť osobných údajov pre IS (kap. 5.2.7, kap. 6.1.18).

**Aktivity gestora súvisiace s IS MV SR spracúvajúcimi osobitnú kategóriu osobných údajov:**

1. zabezpečiť realizáciu bezpečnostného projektu a posúdenie vplyvu na ochranu osobných údajov pre konkrétne účely spracúvania, ktorým táto povinnosť vyplýva zo zákona, príp. z pripravovanej vyhlášky úradu o posúdení vplyvu na ochranu osobných údajov v súčinnosti s OB SITB (kap. 6.2.1),
2. zabezpečiť návrh a realizáciu opatrení na zabezpečenie dôvernosti a koordináciu technických opatrení s SITB (kap. 6.2.2),
3. zabezpečiť návrh a realizáciu opatrení na zabezpečenie integrity a koordináciu technických opatrení s SITB (kap. 6.2.3),
4. zabezpečiť realizáciu pravidelného hodnotenia bezpečnosti, resp. účinnosti technických a organizačných opatrení (kap. 6.2.4).

**Aktivity gestora súvisiace s IS MV SR podporujúcimi plnenie úloh na účely trestného konania:**

1. preskúmať zákonnosť spracúvania osobných údajov v rámci plnenia úloh na účely trestného konania (kap. 6.3.1),
2. zabezpečiť rozlišovanie medzi osobnými údajmi rôznych kategórií dotknutých osôb, naplnenie tejto požiadavky môže vyvolať technické zmeny, ktoré je nutné realizovať v súčinnosti s SITB (kap. 6.3.2),
3. zabezpečiť opatrenia súvisiace s pôvodom a pravdivosťou osobných údajov podľa § 58 (napr. označovanie osobných údajov založených na skutočnostiach a osobných údajov založených na osobných hodnoteniach, pripájanie informácií na posúdenie miery spoľahlivosti) (kap. 6.3.3),
4. zabezpečiť naplnenie informačnej povinnosti o spracúvaní osobných údajov (zverejnením na webovom sídle) a poskytovať informácie na základe žiadostí dotknutých osôb (kap. 6.3.4),
5. zabezpečiť realizáciu práv dotknutých osôb na opravu, vymazanie a obmedzenie spracúvania osobných údajov (kap. 6.3.5),
6. zabezpečiť realizáciu bezpečnostného projektu a posúdenie vplyvu na ochranu osobných údajov (napr. podľa pripravovanej vyhlášky úradu o posúdení vplyvu na ochranu osobných údajov) v súčinnosti s OB SITB (kap. 6.3.8),
7. zabezpečiť prijatie náležitých opatrení na základe výsledkov analýzy rizík a DPIA podľa § 71 písm. a) až k) v súčinnosti s SITB (kap. 6.3.9),
8. zabezpečiť opatrenia súvisiace s vedením logov v súčinnosti s SITB (kap. 6.3.10).

**Aktivity gestora súvisiace s osobitne dôležitými IS MV SR:**

1. zabezpečiť realizáciu bezpečnostného projektu a posúdenie vplyvu na ochranu osobných údajov pre konkrétne účely spracúvania v súčinnosti s OB SITB (kap. 6.4.1),
2. zabezpečiť návrh a realizáciu opatrení na zabezpečenie dostupnosti a koordináciu technických opatrení s SITB (kap. 6.4.2),
3. návrh a realizácia opatrení na zabezpečenie dôvernosti a koordinácia technických opatrení s SITB (kap. 6.4.2),

4. návrh a realizácia opatrení na zabezpečenie integrity a koordinácia technických opatrení s SITB (kap. 6.2.3),
5. realizácia pravidelného hodnotenia bezpečnosti resp. účinnosti technických a organizačných opatrení (kap. 6.2.4).

### 4.3. Požiadavky v kompetencii SITB

Pre SITB vyplývajú v rámci implementácie požiadaviek zákona nasledujúce povinnosti:

#### **Aktivity SITB súvisiace so všetkými IS MV SR:**

1. zabezpečiť technickú realizáciu vymazania či anonymizácie osobných údajov v konkrétnom IS na základe dohody s gestorom (kap. 6.1.2),
2. zabezpečiť technickú realizáciu obmedzenia spracúvania osobných údajov na základe dohody s gestorom (kap. 6.1.4),
3. zabezpečiť technickú realizáciu výpisu osobných údajov z IS na základe mechanizmu dohodnutého s gestorom (kap. 6.1.6),
4. implementovať funkcionality na zmenu alebo doplnenie osobných údajov dotknutej osoby na základe dohody s gestorom (kap. 6.1.7),
5. spolupracovať na riešení bezpečnosti pri vývoji alebo aktualizácii IS (kap. 6.1.10),
6. zabezpečiť technickú realizáciu primeraných bezpečnostných opatrení na základe posúdenia miery rizika gestorom a OB SITB (kap. 6.1.11),
7. poskytovať súčinnosť gestorovi pri vypracúvaní posúdenia vplyvu na ochranu osobných údajov (kap. 6.1.12).

Požiadavky súvisiace s IS MV SR, v ktorých je právny základ **súhlas so spracúvaním osobných údajov**:

8. zabezpečiť technickú realizáciu získavania súhlasu (napr. checkbox), technickú realizáciu práva na odvolanie súhlasu (na čo môže byť potrebné upraviť používateľské rozhranie) na základe postupu dohodnutého s gestorom (kap. 6.1.14),
9. zabezpečiť technickú realizáciu spätného získavania súhlasu na základe postupu dohodnutého s gestorom (kap. 6.1.15),
10. zabezpečiť technickú realizáciu opatrení na získanie súhlasu zákonného zástupcu detí do veku 16 rokov na základe dohody s gestorom (kap. 6.1.16),
11. zabezpečiť technickú realizáciu funkcionality na vymazanie osobných údajov na základe dohody s gestorom (napr. prispôsobenie dátového modelu, vytvorenie automatizovanej funkcionality) (kap. 6.1.17),
12. zabezpečiť technickú realizáciu funkcionality na export údajov z IS na základe postupu dohodnutého s gestorom (kap. 6.1.18).

**Aktivity SITB súvisiace s IS MV SR spracúvajúcimi osobitnú kategóriu osobných údajov:**

1. poskytovať súčinnosť gestorovi pri vypracúvaní bezpečnostného projektu (a súvisiacej analýzy rizík) a posúdenia vplyvu na ochranu osobných údajov (kap. 6.2.1),
2. zabezpečiť technickú realizáciu opatrení na zaistenie dôvernosti IS na základe výsledkov bezpečnostného projektu, posúdenia vplyvu na ochranu osobných údajov a na základe dohody s gestorom IS (kap. 6.2.2),
3. zabezpečiť technickú realizáciu opatrení na zaistenie integrity IS na základe výsledkov bezpečnostného projektu a posúdenia vplyvu na ochranu osobných údajov, na základe dohody s gestorom IS (kap. 6.2.3),
4. poskytovať súčinnosť gestorovi IS pri pravidelnom hodnotení bezpečnosti, napr. pri aktualizácii analýzy rizík (kap. 6.2.4).

**Aktivity SITB súvisiace s IS MV SR podporujúcimi plnenie úloh na účely trestného konania:**

1. zabezpečiť technickú realizáciu opatrení súvisiacich s rozlišovaním medzi osobnými údajmi rôznych kategórií dotknutých osôb na základe postupu dohodnutého s gestorom IS (kap. 6.3.2),
2. poskytovať súčinnosť pri zabezpečení opatrení súvisiacich s pôvodom a pravdivosťou osobných údajov podľa § 58 (napr. označovanie osobných údajov založených na skutočnostiach a osobných údajov založených na osobných hodnoteniach, pripájanie informácií na posúdenie miery spoľahlivosti) (kap. 6.3.3),
3. poskytovať súčinnosť pri technickej realizácii informačnej povinnosti o spracúvaní osobných údajov a poskytovaní informácií na základe oprávnených žiadostí dotknutých osôb (kap. 6.3.4),
4. v odôvodnených prípadoch zabezpečiť technickú realizáciu práv dotknutých osôb na opravu, vymazanie a obmedzenie spracúvania osobných údajov (kap. 6.3.5),
5. poskytovať súčinnosť gestorovi pri vypracúvaní bezpečnostného projektu (a súvisiacej analýzy rizík) a posúdenia vplyvu na ochranu osobných údajov (kap. 6.3.8),
6. zabezpečiť technickú realizáciu náležitých opatrení na základe výsledkov analýzy rizík a DPIA podľa § 71 písm. a) až k), na základe dohody s gestorom (kap. 6.3.9),
7. zabezpečiť technickú realizáciu opatrení súvisiacich s vedením logov na základe dohody s gestorom (kap. 6.3.10).

**Aktivity SITB súvisiace s osobitne dôležitými IS MV SR:**

1. poskytovať súčinnosť gestorovi pri vypracúvaní bezpečnostného projektu (a súvisiacej analýzy rizík) a posúdenia vplyvu na ochranu osobných údajov (kap. 6.4.1),
2. zabezpečiť technickú realizáciu opatrení na zaistenie dostupnosti IS na základe výsledkov bezpečnostného projektu, posúdenia vplyvu na ochranu osobných údajov a na základe dohody s gestorom IS (kap. 6.4.2),

- 
3. zabezpečiť technickú realizáciu opatrení na zaistenie dôvernosti IS na základe výsledkov bezpečnostného projektu a posúdenia vplyvu na ochranu osobných údajov, na základe dohody s gestorom IS (kap. 6.4.3),
  4. zabezpečiť technickú realizáciu opatrení na zaistenie integrity IS na základe výsledkov bezpečnostného projektu a posúdenia vplyvu na ochranu osobných údajov, na základe dohody s gestorom IS (kap. 6.4.4),
  5. poskytovať súčinnosť gestorovi IS pri pravidelnom hodnotení bezpečnosti, napr. pri aktualizácii analýzy rizík (kap. 6.4.5).

## 5. Požiadavky pre zaistenie súladu so zákonom na úrovni MV SR

Pre MV SR ako prevádzkovateľa vyplýva zo zákona viacero povinností, ktoré je možno rozdeliť do oblastí definovaných priamo v zákone:

1. implementácia opatrení vyplývajúcich zo zásad spracúvania osobných údajov,
2. implementácia opatrení vyplývajúcich z práv dotknutých osôb,
3. implementácia opatrení vyplývajúcich zo všeobecných povinností prevádzkovateľa a sprostredkovateľa,
4. implementácia opatrení vyplývajúcich z prenosu osobných údajov do tretej krajiny alebo medzinárodnej organizácii,
5. implementácia osobitných situácií zákonného spracúvania osobných údajov,
6. definovanie pravidiel pri kontakte s úradom.

### 5.1. Implementácia opatrení vyplývajúcich zo zásad spracúvania osobných údajov

Pre MV SR ako prevádzkovateľa vyplývajú v oblasti implementácie jednotlivých zásad spracúvania osobných údajov nasledovné povinnosti:

- povinnosť dodržať všetky zásady spracúvania v každom účele spracúvania osobných údajov vyplývajúce zo zákona musí byť premietnutá do aktualizácie nariadenia č. 164/2013 o ochrane osobných údajov,
- zásady spracúvania osobných údajov vyplývajúce zo zákona musia byť dodržané v každom účele spracúvania osobných údajov.

V nasledujúcom texte sú jednotlivé zásady spracúvania osobných údajov ako aj prípadné špecifiká pre prostredie MV SR (najmä pre prípady spracúvania osobných údajov na plnenie úloh na účely trestného konania) bližšie vysvetlené.

#### 5.1.1. Zásada zákonnosti (§ 6)

- každé spracúvanie osobných údajov musí byť zákonné, aby nedošlo k porušeniu základných práv dotknutej osoby. Pre naplnenie tejto podmienky upravuje zákon v § 13 právne základy pre spracúvanie osobných údajov, v § 16 právne základy pre spracúvanie osobitnej kategórie osobných údajov a v § 55 a 56 právne základy pre spracúvanie osobných údajov na plnenie úloh na účely trestného konania,
- prevažná väčšina účelov spracúvania a súvisiacich osobných údajov je spracúvaná na právnom základe, ktorým je osobitný predpis. V tomto prípade je zásada zákonnosti naplnená práve spracúvaním osobných údajov podľa osobitného predpisu. V prípade spracúvania osobných údajov podľa iných



právnych základov bude nevyhnutné posúdiť, či sa právny základ spracúvania osobných údajov nezmenil, resp. či je v súlade so zákonom.

#### 5.1.2. Zásada obmedzenia účelu (§ 7)

- osobné údaje musia byť vo všetkých identifikovaných účeloch spracúvania MV SR spracúvané podľa aktuálne platnej legislatívy výhradne na konkrétne určený, výslovne uvedený a oprávnený účel,
- osobné údaje nesmú byť ďalej spracúvané spôsobom, ktorý je s týmito účelmi nezlučiteľný, ďalšie spracúvanie pre účely archivácie vo verejnom záujme, pre účely vedeckého či historického výskumu alebo pre štatistické účely sa podľa § 78 ods. 8 zákona nepovažuje za nezlučiteľné s pôvodnými účelmi,
- v súvislosti s plnením úloh na účely trestného konania môže príslušný orgán spracúvať osobné údaje na archiváciu, na vedecký účel, na účel historického výskumu alebo na štatistický účel, ak prijme primerané záruky ochrany práv dotknutej osoby (§ 53).

#### 5.1.3. Zásada minimalizácie údajov (§ 8)

- osobné údaje musia byť v identifikovaných účeloch spracúvania MV SR spracúvané iba v nevyhnutnom rozsahu, prevažná väčšina účelov spracúvania je spracúvaná na základe osobitných predpisov, ktoré rozsah osobných údajov priamo upravujú (resp. by mali upravovať),
- zásada minimalizácie spracúvaných osobných údajov musí byť naplnená posúdením nevyhnutnosti spracúvaných osobných údajov vo vzťahu k účelu spracúvania ako aj zvážením všetkých spracovateľských operácií vo vzťahu k danému účelu a možnému zásahu do práv a slobôd fyzických osôb, ako aj zavedením primeraných technických a organizačných opatrení, ktoré povedú k minimalizácii údajov.

#### 5.1.4. Zásada správnosti (§ 9)

- MV SR môže spracúvať výhradne správne a podľa potreby aktualizované osobné údaje,
- prevádzkovateľ musí mať prijaté náležité opatrenia, prípadne mechanizmy na identifikáciu osobných údajov, ktoré je potrebné opraviť,
- na túto zásadu sa viažu aj ďalšie povinnosti prevádzkovateľa (napr. § 22 Právo na opravu osobných údajov či § 24 Právo na obmedzenie spracúvania osobných údajov).

#### 5.1.5. Zásada minimalizácie uchovávaní (§ 10)

- osobné údaje môžu byť v identifikovaných účeloch spracúvania MV SR uchovávané najneskôr dovtedy, kým je to potrebné na konkrétny účel spracúvania,

- osobné údaje sa môžu v prostredí MV SR uchovávať dlhšie, ak sa majú spracúvať výlučne na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel na základ osobitného predpisu a ak sú dodržané primerané záruky ochrany práv dotknutej osoby podľa § 78 ods. 8 zákona,
- pri spracúvaní osobných údajov v prostredí MV SR na plnenie úloh na účely trestného konania môžu byť tieto osobné údaje uchovávané vo forme, ktorá umožňuje identifikáciu dotknutej osoby najneskôr dovtedy, kým je to potrebné na účel, na ktorý sa osobné údaje spracúvajú,
- v prostredí MV SR je zásada minimalizácie uchovávania osobných údajov v niektorých účeloch spracúvania nedodržiavaná a bude potrebné realizovať náležité opatrenia na dosiahnutie súladu s touto povinnosťou (preskúmať jednotlivé účely spracúvania a v prípade nesúladu správne nastaviť dobu uchovávania týchto osobných údajov).

#### 5.1.6. Zásada integrity a dôvernosti (§ 11)

- spracúvanie osobných údajov je na základe uskutočnenej analýzy vo väčšine prípadov v jednotlivých identifikovaných účeloch spracúvania v prostredí MV SR realizované prostredníctvom primeraných technických a organizačných opatrení, ktoré zabezpečujú primeranú bezpečnosť spracúvaných osobných údajov z pohľadu zabezpečenia integrity a dôvernosti,
- podmienky a súvisiace povinnosti pri prijímaní bezpečnostných opatrení upravujú najmä § 32 zákona (Špecificky navrhnutá a štandardná ochrana osobných údajov (privacy by default and design) a § 39 zákona (bezpečnosť spracúvania),
- dodržiavanie tejto zásady je uvedené aj v kapitole 6 Požiadavky pre zaistenie súladu so zákonom pre jednotlivé IS MV SR.

#### 5.1.7. Zásada zodpovednosti (§ 12)

- MV SR ako prevádzkovateľ je povinné súlad so zásadami spracúvania osobných údajov preukázať (napr. na požiadanie úradu). Pre každý účel spracúvania musia byť v prostredí MV SR jednotlivé zásady spracúvania osobných údajov vyhodnotené (napr. v rámci vytvorenia záznamov o spracovateľských činnostiach) a prijaté prípadné nápravné opatrenia,
- povinnosti prevádzkovateľa vo vzťahu k zásade zodpovednosti podrobnejšie upravuje § 31 zákona, podľa ktorého musí prevádzkovateľ posudzovať riziká pri spracúvaní osobných údajov a v prípade možného zásahu do práv a slobôd dotknutých osôb prijať vhodné technické a organizačné opatrenia (tieto povinnosti je možné porovnať s povinnosťou mať vypracovaný bezpečnostný projekt podľa zákona č. 122/2013 Z. z. o ochrane osobných údajov),
- MV SR musí byť schopné tento súlad preukázať, forma preukazovania však nie je v zákone určená, odkazuje sa však na medzinárodné normy a štandardy

ako napr. ISO/IEC 27001 a ISO/IEC 27002, riešením môže byť práve realizácia analýzy bezpečnosti daného IS podľa týchto medzinárodných štandardov.

#### **5.1.8. Poskytovanie súhlasu so spracúvaním osobných údajov (§ 14)**

- v prostredí MV SR je prevažná väčšina účelov spracúvaná na základe osobitného predpisu, tento paragraf sa tým pádom pre tieto účely spracúvania osobných údajov neuplatňuje,
- pre všetky ostatné účely spracúvania, kde je právny základ súhlas so spracúvaním osobných údajov, bude nevyhnutné požiadavky tohto paragrafu implementovať, najmä povinnosť preukázať, že dotknutá osoba poskytla súhlas so spracúvaním svojich osobných údajov, odlíšenie súhlasu od iných skutočností, vyjadrenie súhlasu jasne a v zrozumiteľnej a ľahko dostupnej forme či implementáciu práva dotknutej osoby kedykoľvek odvolať súhlas so spracovaním osobných údajov.

#### **5.1.9. Poskytovanie súhlasu v súvislosti so službami informačnej spoločnosti (§ 15)**

- v prostredí MV SR sa spracúvanie osobných údajov dotknutých osôb mladších ako 16 rokov uskutočňuje podľa analýzy najmä na základe osobitného predpisu, ktoré takéto spracúvanie osobných údajov dotknutých osôb mladších ako 16 rokov umožňuje,
- pre účely spracúvania, kde je právny základ súhlas so spracúvaním osobných údajov, a zároveň sú spracúvané osobné údaje dotknutých osôb mladších ako 16 rokov, bude nevyhnutné implementovať náležité opatrenia vyplývajúce z tohto paragrafu (najmä vynaložiť primerané úsilie, aby sa overilo, že zákonný zástupca dotknutej osoby poskytol alebo schválil súhlas so spracúvaním osobných údajov, pričom je potrebné zohľadniť dostupnú technológiu).

## **5.2. Implementácia opatrení vyplývajúcich z práv dotknutých osôb**

Pre MV SR ako prevádzkovateľa vyplývajú v oblasti implementácie opatrení vyplývajúcich z práv dotknutých osôb najmä nasledovné povinnosti:

- procesy súvisiace s právami dotknutých osôb vyplývajúce zo zákona musia byť nastavené a premietnuté do aktualizácie nariadenia č. 164/2013 o ochrane osobných údajov.

V nasledujúcom texte sú jednotlivé práva dotknutých osôb bližšie vysvetlené spolu s ich možnosťami realizácie v prostredí MV SR.

### 5.2.1. Právo na poskytované informácie pri získavaní osobných údajov (§ 19 - 20)

- pre všetky účely spracúvania je potrebné poskytnúť dotknutým osobám všetky informácie vyžadované zákonom, v prípade, že sú osobné údaje získané od dotknutej osoby, je prevádzkovateľ povinný poskytnúť dotknutej osobe pri ich získavaní informácie podľa § 19 zákona, v prípade, že nie sú osobné údaje získané od dotknutej osoby, je prevádzkovateľ povinný poskytnúť dotknutej osobe informácie podľa § 20 zákona,
- pri spracúvaní osobných údajov v prostredí MV SR na plnenie úloh na účely trestného konania je potrebné splniť požiadavky podľa kap. 6.3.4 (§ 60 zákona),
- pri získavaní osobných údajov bude potrebné poskytnúť informačný list, ktorý bude obsahovať náležitosti podľa § 19 resp. § 20 zákona.

### 5.2.2. Právo na prístup k osobným údajom (§ 21)

- každá dotknutá osoba má právo od prevádzkovateľa *získať potvrdenie* o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú. MV SR ako prevádzkovateľ musí reagovať na každú žiadosť s otázkou, či sa o dotknutej osobe spracúvajú osobné údaje, odpovedať je nevyhnutné aj vtedy, ak bude právo na prístup k osobným údajom dotknutej osoby z niektorého zákonného dôvodu obmedzené (odpoveď bude potrebné v tomto prípade formulovať napr. nasledovne: „MV SR nemôže ani potvrdiť, ani poprieť, že sa spracúvajú osobné údaje, ktoré sa Vás týkajú“),
- na žiadosť dotknutej osoby je MV SR povinné *poskytnúť dotknutej osobe osobné údaje*, ktoré o nej spracúva. Ak dotknutá osoba podala žiadosť elektronicky a ak nepožiadala o iný spôsob poskytnutia, musí prevádzkovateľ poskytnúť tieto informácie v bežne používanej elektronickej podobe,
- dotknutá osoba má právo aj na *d ďalšie informácie* o spôsobe spracúvania osobných údajov, ktoré sú uvedené v tomto paragrafe v ods. 1 písm. a) až h),
- pri spracúvaní osobných údajov v prostredí MV SR na plnenie úloh na účely trestného konania musí MV SR postupovať podľa kap. 6.3.4 (§ 61 zákona),
- navrhovaný proces reakcie na požiadavky dotknutej osoby je uvedený v prílohe č. 3.

### 5.2.3. Právo na opravu osobných údajov (§ 22)

- každá dotknutá osoba má právo na to, aby prevádzkovateľ opravil nesprávne osobné údaje a právo na doplnenie neúplných osobných údajov, toto právo je v korelácii so zásadou správnosti definovanou v § 9 zákona,
- v prípade, že nesprávne osobné údaje zistí prevádzkovateľ na základe vlastných činností a kontrol, musí o zistení dotknutú osobu informovať a požiadať o správne osobné údaje,

- prevádzkovateľ nenesie zodpovednosť za spracúvanie nesprávnych osobných údajov v prípade, že ich poskytla samotná dotknutá osoba (pokiaľ nevyplýva prevádzkovateľovi z osobitného predpisu povinnosť preveriť správnosť údajov),
- pri spracúvaní osobných údajov v prostredí MV SR na plnenie úloh na účely trestného konania musí MV SR pri procesoch súvisiacich s opravou osobných údajov postupovať podľa kap. 6.3.5 (§ 62 ods. 1 zákona), právo na opravu osobných údajov môže MV SR obmedziť na základe § 65 zákona (ak osobné údaje sú súčasťou vyšetrovacieho spisu alebo súdneho spisu v rámci trestného konania).

#### 5.2.4. Právo na výmaz osobných údajov (§ 23)

- dotknutá osoba má právo na to, aby MV SR zabezpečilo vymazanie osobných údajov vo všetkých prípadoch, ktoré sú uvedené v ods. 2 písm. a) až f) tohto paragrafu,
- právo na výmaz osobných údajov zahŕňa nielen právo na vymazanie osobných údajov, ale aj zamedzenie ďalšieho šírenia týchto údajov (prevádzkovateľ má povinnosť informovať všetky tretie strany, ktorým tieto osobné údaje poskytol o povinnosti vymazať všetky osobné údaje na základe žiadosti dotknutej osoby),
- prevádzkovateľ nie je povinný osobné údaje dotknutej osoby vymazať a tá musí ich spracúvanie strpieť, ak existuje niektorý z dôvodov uvedených v ods. 3 písm. a) až e) tohto paragrafu,
- pri spracúvaní osobných údajov v prostredí MV SR na plnenie úloh na účely trestného konania musí MV SR pri procesoch súvisiacich s výmazom osobných údajov postupovať podľa kap. 6.3.5 (§ 62 ods. 2 zákona), právo na výmaz osobných údajov môže MV SR obmedziť na základe § 65 zákona (ak osobné údaje sú súčasťou vyšetrovacieho spisu alebo súdneho spisu v rámci trestného konania).

#### 5.2.5. Právo na obmedzenie spracúvania osobných údajov (§ 24)

- dotknutá osoba má právo na to, aby MV SR obmedzilo spracúvanie osobných údajov pre prípady uvedené v ods. 1 písm. a) až d) tohto paragrafu zákona,
- realizácia tohto práva v praxi znamená, že všetky ďalšie spracovateľské operácie s osobnými údajmi MV SR pozastaví, ďalej ich nebude používať ale len uchovávať, pričom bude potrebné tieto osobné údaje náležite označiť, aby sa zamedzilo ich ďalšiemu používaniu v budúcnosti,
- v prípade, že je spracúvanie osobných údajov obmedzené na základe žiadosti dotknutej osoby, môže MV SR tieto osobné údaje používať len na základe súhlasu dotknutej osoby, súhlas sa však nevyžaduje na spracovateľské operácie ako sú uchovávanie, preukazovanie a obhajovanie právnych nárokov, prípadne z dôvodov verejného záujmu,

- o zrušení obmedzenia osobných údajov musí prevádzkovateľ dotknutú osobu informovať,
- pri spracúvaní osobných údajov v prostredí MV SR na plnenie úloh na účely trestného konania musí MV SR pri procesoch súvisiacich s obmedzením spracúvania osobných údajov postupovať podľa kap. 6.3.5 (§ 62 ods. 3 a 4 zákona), právo na obmedzenie spracúvania osobných údajov môže MV SR obmedziť na základe § 65 zákona (ak osobné údaje sú súčasťou vyšetrovacieho spisu alebo súdneho spisu v rámci trestného konania).

#### **5.2.6. Oznamovacia povinnosť v súvislosti s opravou, vymazaním alebo obmedzením spracúvania osobných údajov (§ 25)**

- MV SR je povinné oznámiť všetkým príjemcom opravu, vymazanie alebo obmedzenie spracúvania osobných údajov ak sa to neukáže ako nemožné alebo si to nevyžaduje neprimerané úsilie,
- MV SR o týchto príjemcoch musí dotknutú osobu informovať, ak to dotknutá osoba požaduje.

#### **5.2.7. Právo na prenosnosť osobných údajov (§ 26)**

- dotknutá osoba má právo na prenosnosť osobných údajov iba v prípadoch, v ktorých je spracúvanie osobných údajov založené výhradne na súhlase so spracúvaním osobných údajov prípadne je spracúvanie realizované na účely zmluvy,
- dotknutá osoba má právo získať osobné údaje, ktoré sa jej týkajú a ktoré poskytla prevádzkovateľovi v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte, cieľom tohto práva je uľahčiť premiestňovanie, či kopírovanie vlastných osobných údajov z jedného IS do druhého IS, či už do vlastného systému dotknutej osoby, prípadne systémov tretích strán alebo nových prevádzkovateľov.

#### **5.2.8. Právo namietať spracúvanie osobných údajov (§ 27)**

- právo namietať spracúvanie osobných údajov patrí dotknutej osobe vtedy, ak sa domnieva, že spracúvanie už obmedzuje jej práva alebo do nich zasahuje a ak sa spracúvanie uskutočňuje na právnom základe podľa § 13 písm. e) zákona (spracúvanie je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi) alebo § 13 písm. f) zákona (spracúvanie je nevyhnutné na účel oprávnených záujmov prevádzkovateľa alebo tretej strany) alebo je spracúvanie realizované na účely priameho marketingu (nie je prípad MV SR),
- dotknutá osoba nemá právo namietať spracúvanie osobných údajov, ak ide o spracúvanie osobných údajov nevyhnutné na plnenie úlohy z dôvodov verejného záujmu a spracúvanie na vedecký účel, na účel historického výskumu alebo na štatistický účel.

### 5.2.9. Právo na neúčinnosť automatizovaného individuálneho rozhodovania vrátane profilovania (§ 28)

- dotknutá osoba má právo na to, aby sa na ňu nevzťahovalo rozhodnutie, ktoré je založené výlučne na automatizovanom spracúvaní osobných údajov vrátane profilovania a ktoré má právne účinky, ktoré sa jej týkajú alebo ju obdobne významne ovplyvňujú. Toto právo sa však neuplatňuje, ak je rozhodnutie nevyhnutné na uzavretie zmluvy alebo plnenie zmluvy, vykonané na základe osobitného predpisu alebo medzinárodnej zmluvy alebo je rozhodnutie založené na výslovnom súhlase dotknutej osoby,
- na základe získaných výsledkov z dotazníkov sa v prostredí MV SR takáto forma spracúvania v súčasnosti nerealizuje, v opačnom prípade by bolo nevyhnutné vykonať vhodné opatrenia, a to najmä právo na overenie rozhodnutia nie automatizovaným spôsobom zo strany MV SR, práva vyjadriť svoje stanovisko a právo napadnúť rozhodnutie,
- pri spracúvaní osobných údajov v prostredí MV SR na plnenie úloh na účely trestného konania musí v prípade využívania automatizovaného individuálneho rozhodovania postupovať podľa kap. 6.3.7 (§ 66 zákona).

### 5.2.10. Povinnosti prevádzkovateľa pri uplatňovaní práv dotknutej osoby (§ 29)

- v prostredí MV SR sa odporúča pre zjednotenie a zjednodušenie pravidiel pri zabezpečovaní práv dotknutých osôb zahrnúť požiadavky § 29 do aktualizácie nariadenia č. 164/2013 o ochrane osobných údajov,
- v rámci definovania uvedených pravidiel je vhodné definovať konkrétnych zamestnancov MV SR (napr. zodpovedné osoby) a ich zodpovednosti pri uplatňovaní práv dotknutej osoby, spôsob a formu spätnej reakcie (napr. poskytovanie odpovede v takej forme, v akej bola prijatá požiadavka, ak si dotknutá osoba nepožiadala o iný spôsob), procesy na overenie totožnosti dotknutej osoby (aby sa predišlo tomu, že akákoľvek anonymná osoba si môže vyžiadať citlivé osobné údaje o inej osobe), procesy súvisiace s lehotami a poplatkami na vybavenie žiadosti dotknutej osoby.

### 5.2.11. Obmedzenie práv dotknutej osoby (§ 30)

- MV SR môže za podmienok ustanovených osobitným predpisom alebo medzinárodnou zmluvou, ktorou je SR viazaná obmedziť rozsah povinností a práv dotknutej osoby v prípadoch uvedených v ods. 1) body a) až k) zákona,
- všetky prípady a procesy súvisiace s obmedzením práv dotknutej osoby bude potrebné stanoviť vo vnútorných predpisoch MV SR (napr. v aktualizácii nariadenia č. 164/2013 o ochrane osobných údajov),
- tento paragraf sa v prostredí MV SR uplatňuje najmä v prípadoch pri IS na plnenie úloh na účely trestného konania,

- MV SR môže obmedziť práva dotknutej osoby len vtedy, ak tento osobitný predpis alebo medzinárodná zmluva ustanovuje jednotlivé náležitosti (ako sú účel spracúvania, kategórie osobných údajov, rozsah obmedzenia, záruky, lehotu uchovávanía, riziká pre práva dotknutej osoby a práva dotknutej osoby na informovanie o obmedzení, ak tým nie je ohrozený účel obmedzenia).

### **5.3. Implementácia opatrení vyplývajúcich zo všeobecných povinností prevádzkovateľa a sprostredkovateľa**

Pre MV SR ako prevádzkovateľa vyplývajú v oblasti implementácie vyplývajúcich zo všeobecných povinností prevádzkovateľa nasledovné povinnosti:

- premietnuť jednotlivé povinnosti, procesy a zodpovednosti z tejto časti zákona do aktualizácie nariadenia č. 164/2013 o ochrane osobných údajov,
- uplatňovať pravidlá špecificky navrhutej a štandardnej ochrany osobných údajov a ich jednotné uplatňovanie v prostredí MV SR,
- upraviť pravidlá súvisiace s využívaním sprostredkovateľov, úprava existujúcich zmlúv podľa požiadaviek zákona č. 18/2018,
- definovať procesy súvisiace so záznamami o spracovateľských činnostiach, vytvorenie náležitých záznamov,
- definovať procesy súvisiace s oznamovaním porušenia ochrany osobných údajov úradu a dotknutej osobe,
- definovať procesy a pravidlá súvisiace s posúdením vplyvu na ochranu osobných údajov pre konkrétne IS v prostredí MV SR,
- definovať/upraviť procesy, postupy a zodpovednosti súvisiace so zodpovednou osobou.

V nasledujúcom texte sú jednotlivé povinnosti a prípadné špecifiká pre prostredie MV SR bližšie vysvetlené.

#### **5.3.1. Definovanie pravidiel špecificky navrhutej a štandardnej ochrany osobných údajov (§ 32)**

- špecificky navrhnutá ochrana osobných údajov – súčasťou vývoja IS musí byť od začiatku aj riešenie ochrany osobných údajov, na základe ktorého je potrebné prijať primerané technické a organizačné opatrenia, táto požiadavka je štandardne riešená v bezpečnostnom projekte,
- štandardná ochrana osobných údajov – vyžaduje sa, aby sa už pri určovaní prostriedkov spracúvania osobných údajov (teda už vo fáze vývoja novej aplikácie alebo zavádzaní novej služby či IS) implementovali také technické a bezpečnostné opatrenia, ktoré vzhľadom na najnovšie poznatky a náklady na



ich realizáciu, budú funkčné počas celého procesu spracúvania osobných údajov,

- tieto princípy a povinnosť ich dodržiavania v prostredí MV SR je nevyhnutné premietnuť do vnútorných predpisov.

### 5.3.2. Úprava pravidiel súvisiacich s využívaním sprostredkovateľov (§ 34)

- procesy súvisiace s využívaním sprostredkovateľov pri spracúvaní osobných údajov sa významne nezmenili, zásadnou zmenou je však to, že prevádzkovateľ preberá významnú mieru zodpovednosti za osobné údaje, ktoré zveril na spracúvanie sprostredkovateľovi,
- prevádzkovateľ musí pred zverením osobných údajov sprostredkovateľovi posúdiť prijaté bezpečnostné opatrenia v prostredí sprostredkovateľa, toto posúdenie zahŕňa prijaté technické ako aj organizačné opatrenia (tieto musia zahŕňať aj opatrenia podľa § 39 Bezpečnosť spracúvania),
- MV SR musí zároveň vo svojich podmienkach stanoviť procesy a postupy, ktoré zabezpečia priebežné monitorovanie činností sprostredkovateľa pri spracúvaní zverených osobných údajov, na tento účel môže prevádzkovateľ vykonať v prostredí sprostredkovateľa kontrolu alebo audit, sprostredkovateľ musí takúto kontrolu alebo audit strieť a byť v celom procese nápomocný,
- so všetkými sprostredkovateľmi musí mať MV SR uzatvorenú sprostredkovateľskú zmluvu, náležitosti tejto zmluvy sú definované v ods. 3 tohto paragrafu zákona, zároveň je potrebné preskúmať všetky existujúce zmluvy so sprostredkovateľmi a posúdiť, či spĺňajú všetky náležitosti predpísané zákonom (v prípade neúplných zmlúv bude potrebné zmluvy prepracovať a dať nanovo podpísať sprostredkovateľom),
- zoznam sprostredkovateľov môže byť zverejnený na internetovej stránke MV SR.

### 5.3.3. Vytvorenie záznamov o spracovateľských činnostiach (§ 37)

- záznamy o spracovateľských činnostiach sú obdobou evidenčných formulárov (resp. oznamovacej povinnosti a osobitnej registrácie) podľa starého zákona, v prostredí MV SR bude tieto záznamy nevyhnutné vytvoriť pre všetky identifikované účely spracúvania osobných údajov,
- požiadavky na obsah záznamov sú pre prevádzkovateľa uvedené v ods. 1 písm. a) až g) tohto paragrafu, záznam je po novom povinný vytvoriť aj sprostredkovateľ podľa požiadaviek ods. 2 tohto paragrafu,
- vzor záznamu o spracovateľských činnostiach zverejní úrad na svojom webovom sídle,
- gestor zasiela vytvorené záznamy o spracovateľských činnostiach na sprípomienkovanie a schválenie SKIS, vedenie zoznamu aktuálnych verzií záznamov o spracovateľských činnostiach v gescii MV SR je v zodpovednosti SKIS.

#### 5.3.4. Definovanie procesov súvisiacich s oznamovaním porušenia ochrany osobných údajov úradu (§ 40) a dotknutej osobe (§ 41)

- z definície podľa § 5 ods. m) zákona je porušením ochrany osobných údajov porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene alebo k neoprávnenému poskytnutiu prenášaných, uchovávaných alebo inak spracúvaných osobných údajov, alebo k neoprávnenému prístupu k nim,
- vo vnútorných predpisoch (napr. v aktualizácii nariadenia č. 164/2013 o ochrane osobných údajov) bude nevyhnutné definovať konkrétne procesy súvisiace s oznamovaním porušenia ochrany osobných údajov úradu ako aj dotknutým osobám,
- MV SR ako prevádzkovateľ musí mať pre svoje prostredie definované procesy a mechanizmy, ktoré majú včas identifikovať bezpečnostný incident, posúdiť, či bezpečnostný incident súvisí so spracúvaním osobných údajov a posúdiť mieru rizika, ktoré z tohto bezpečnostného incidentu vyplývajú pre dotknutú osobu,
- pri posudzovaní, či bezpečnostný incident možno považovať za porušenie ochrany osobných údajov, bude nevyhnutné posúdiť, či došlo k narušeniu dôvernosti a/alebo integrity a/alebo dostupnosti osobných údajov a súčasne či bezpečnostný incident vedie k riziku pre práva a slobody fyzických osôb, v prípade, že bezpečnostný incident sa vyhodnotí ako porušenie ochrany osobných údajov, vzniká MV SR povinnosť v lehote do 72 hodín oznámiť tento incident úradu, MV SR je zároveň povinné posúdiť, či porušenie povedie k vysokému riziku pre práva a slobody dotknutých osôb, čoho následkom vzniká povinnosť oznámiť toto porušenie aj dotknutým osobám.

#### 5.3.5. Definovanie pravidiel a zodpovedností súvisiacich s posúdením vplyvu na ochranu osobných údajov – DPIA (§ 42)

- pre viaceré účely spracúvania v prostredí MV SR bude nevyhnutné posúdenie vplyvu na ochranu osobných údajov realizovať, táto povinnosť sa týka aj IS, v ktorých sa realizuje spracúvanie osobných údajov týkajúcich sa uznania viny za spáchanie trestného činu alebo priestupku podľa § 17 zákona,
- štandardne by malo byť posúdenie vplyvu na ochranu osobných údajov zastrešené v bezpečnostnom projekte IS, povinnosť realizovať v konkrétnych prípadoch toto posúdenie bude potrebné premietnuť aj do procesov resp. vnútorných predpisov MV SR (napr. do aktualizácie nariadenia č. 164/2013 o ochrane osobných údajov) spolu s definovaním jednotnej metodiky pre celé prostredie MV SR,
- pracovná skupina WP 29 vydala na podporu realizácie DPIA usmernenie, z ktorého možno pri realizácii posúdenia vplyvu na ochranu osobných údajov vychádzať, úrad zároveň pripravuje novú vyhlášku súvisiacu s podmienkami

realizácie posúdenia, požiadavky tejto vyhlášky bude potrebné zohľadniť aj pri stanovení jednotnej metodiky v prostredí MV SR ako aj pri realizácii v konkrétnych účeloch spracúvania osobných údajov,

- MV SR bude musieť s úradom konzultovať spracúvanie osobných údajov, ak z posúdenia vplyvu na ochranu osobných údajov vyplynie, že spracúvanie povedie k vysokému riziku pre práva fyzických osôb a ak MV SR neprijme opatrenia na zmiernenie tohto rizika. Túto povinnosť je vhodné premietnuť aj do vnútorných predpisov MV SR.

#### **5.3.6. Úprava procesov, postupov a zodpovedností súvisiacich so zodpovednou osobou (§ 44 - 46)**

- v prostredí MV SR je určená vrcholová zodpovedná osoba, pre veľkú časť účelov spracúvania je určená aj konkrétna zodpovedná osoba za ochranu osobných údajov v súlade s existujúcou legislatívou (zákon č. 122/2013). Zodpovedná osoba poverená podľa doterajšieho zákona, ktorá spĺňa podmienky podľa nového zákona sa považuje za zodpovednú osobu podľa predpisov účinných od 25. mája 2018 (§ 110 ods. 12 zákona),
- vo vnútorných predpisoch (napr. v aktualizácii nariadenia č. 164/2013 o ochrane osobných údajov) bude nevyhnutné procesy súvisiace so zodpovednou osobou v prostredí MV SR náležite upraviť podľa požiadaviek zákona najmä procesy súvisiace s určením, postavením a jednotlivými úlohami zodpovednej osoby, o týchto zmenách bude potrebné informovať aj konkrétne zodpovedné osoby,
- MV SR je povinné zverejniť (napr. na webovom sídle) kontaktné údaje vrcholovej zodpovednej osoby a v prípade zmeny v obsadení pozície zodpovednej osoby túto skutočnosť oznámiť úradu.

#### **5.4. Implementácia opatrení vyplývajúcich z prenosu osobných údajov do tretej krajiny alebo medzinárodnej organizácii**

V prostredí MV SR dochádza vo viacerých účeloch spracúvania k prenosu osobných údajov do tretích krajín. Tento prenos je realizovaný podľa aktuálne platnej legislatívy a primeraných záruk v nej uvedených. Podmienky medzinárodného prenosu osobných údajov bude nevyhnutné definovať aj v aktualizácii nariadenia č. 164/2013 o ochrane osobných údajov.

Nový zákon v podstate zachováva súčasnú podobu princípov, právnych nástrojov a inštitútov, ktoré sú využívané už v súčasnosti pri cezhraničnom prenose osobných údajov. V jednotlivých účeloch spracúvania, kde dochádza k prenosu osobných údajov do tretej krajiny alebo medzinárodnej organizácii však bude potrebné overiť

existenciu primeraných záruk podľa zákona. Ako primerané záruky môžu byť použité opatrenia, ktoré sú definované v § 48 ods. 2) písm. a) až f).

Zákon obmedzuje prenosy osobných údajov do tretích krajín bez toho, aby boli zabezpečené a upravené už v existujúcich právnych dokumentoch ako sú napr. štandardné zmluvné doložky či záväznú vnútropodnikové pravidlá.

Novinkou podľa zákona je skutočnosť, že na realizáciu medzinárodného prenosu osobných údajov budú môcť byť využívané aj schválené certifikačné mechanizmy ako sú napr. pečate a značky ochrany osobných údajov vydané certifikovaným subjektom. Ďalšou novinkou je aj to, že podľa zákona už schvaľovanie cezhraničného prenosu pred jeho vykonaním zo strany úradu nebude potrebné.

Na postup príslušných orgánov pri spracúvaní osobných údajov na plnenie úloh na účely trestného konania sa uplatňujú § 48 zákona (rozhodnutie Komisie, že tretia krajina poskytuje primeranú úroveň ochrany osobných údajov) a § 50 zákona (prenos alebo poskytnutie osobných údajov, ktoré právny poriadok v SR nepovoľuje) rovnako. Zároveň sa zaručuje aj prenos osobných údajov medzi príslušnými orgánmi a orgánmi členských štátov príslušnými na plnenie úloh na účely trestného konania, ak takýto prenos vyžaduje podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je SR viazaná.

## 5.5. Implementácia osobitných situácií zákonného spracúvania osobných údajov

Štvrtá časť zákona upravuje osobitné situácie zákonného spracúvania osobných údajov:

1. Možnosť spracúvať osobné údaje bez súhlasu dotknutej osoby aj vtedy, ak je to nevyhnutné na *akademický účel, umelecký účel alebo literárny účel*
  - uvedené neplatí, ak sa spracúvaním porušia práva dotknutej osoby na ochranu jej osobnosti alebo súkromia alebo také spracúvanie vylučuje osobitný predpis alebo medzinárodná zmluva, ktorou je SR viazaná.
2. Možnosť spracúvať osobné údaje bez súhlasu dotknutej osoby aj vtedy, ak spracúvanie osobných údajov je nevyhnutné pre potreby *informovania verejnosti masovokomunikačnými prostriedkami* a ak osobné údaje spracúva prevádzkovateľ, ktorému to vyplýva z predmetu činnosti
  - uvedené neplatí, ak sa spracúvaním porušia práva dotknutej osoby na ochranu jej osobnosti alebo súkromia alebo také spracúvanie vylučuje osobitný predpis alebo medzinárodná zmluva, ktorou je SR viazaná.

3. MV SR je oprávnené *poskytovať osobné údaje alebo zverejniť osobné údaje zamestnanca* v rozsahu titul, meno, priezvisko, pracovné zaradenie, služobné zaradenie, funkčné zaradenie, osobné číslo zamestnanca alebo zamestnanecké číslo zamestnanca, odborný útvar, miesto výkonu práce, telefónne číslo, faxové číslo, adresu elektronickej pošty na pracovisko a identifikačné údaje zamestnávateľa.
4. Na účely identifikovania fyzickej osoby môže MV SR využiť *všeobecne použiteľný identifikátor (rodné číslo)* len vtedy, ak jeho využitie je nevyhnutné na dosiahnutie daného účelu spracúvania. Zverejňovať všeobecne použiteľný identifikátor sa zakazuje (to neplatí, ak všeobecne použiteľný identifikátor zverejní sama dotknutá osoba).
5. Prevádzkovateľ je oprávnený spracúvať *genetické údaje, biometrické údaje a údaje týkajúce sa zdravia* aj na právnom základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je SR viazaná.
6. Osobné údaje o dotknutej osobe možno získať od inej fyzickej osoby a spracúvať v IS len s predchádzajúcim písomným súhlasom dotknutej osoby (okrem prípadov uvedených v paragrafe 78 ods. 6) zákona).
7. Ak *dotknutá osoba nežije*, súhlas vyžadovaný podľa zákona alebo osobitného predpisu môže poskytnúť jej blízka osoba. Súhlas nie je platný, ak čo len jedna blízka osoba písomne vyslovila nesúhlas.
8. Povinnosť pre prevádzkovateľa prijať primerané záruky (technické a organizačné opatrenia) pre práva dotknutej osoby, ak sa spracúvajú osobné údaje na účel *archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel*.
  - práva dotknutých osôb môžu byť obmedzené osobitným prepisom alebo medzinárodnou zmluvou.

## 5.6. Definovanie pravidiel pri kontakte s úradom

Piata časť zákona (§ 80 - § 106) upravuje postavenie, pôsobnosť a organizáciu úradu, upravuje procesy súvisiace s kódexmi správania, certifikátmi a akreditáciou, popisuje spôsob a priebeh kontroly úradu a súvisiace konanie o ochrane osobných údajov spolu s právnymi deliktami.

Pre MV SR sa odporúča z tejto časti zákona najmä úprava povinností a oprávnení kontrolovaného subjektu vo vnútorných predpisoch (napr. nariadenie MV SR č. 164/2013 o ochrane osobných údajov).



## 6. Požiadavky pre zaistenie súladu so zákonom pre jednotlivé IS MV SR

Požiadavky popísané v predchádzajúcej kapitole sú všeobecne platné v celom prostredí IS MV SR, pre ich implementáciu na úrovni jednotlivých IS však je potrebná ich konkretizácia. V tejto kapitole požiadavky zákona ďalej rozvádzame z pohľadu gestora a technického prevádzkovateľa, ktorí v rámci svojej pôsobnosti budú zodpovední za realizáciu jednotlivých krokov implementácie nového zákona do praxe.

Požiadavky sú rozdelené na 4 skupiny podľa kategórií IS definovaných v klasifikácii IS popísanej v kapitole 3.3. Pre každý IS je teda nutné mať identifikované jeho zaradenie do jednotlivých kategórií a následne naplniť požiadavky v každej z podkapitol príslušných k jeho kategóriám.

### 6.1. Požiadavky na všetky IS

Nasledovné opatrenia sa týkajú všetkých IS spracúvajúcich osobné údaje, vrátane tých, kde je právnym základom osobitný predpis či úloha realizovaná vo verejnom záujme. V prípade IS podporujúcich plnenie úloh na účely trestného konania sú tieto požiadavky obmedzené na základe § 63 a § 65 zákona.

#### 6.1.1. Vytvorenie záznamov o spracovateľských činnostiach (§ 37)

- gestor musí pre každý účel, resp. IS vytvoriť a viesť záznamy o spracovateľských činnostiach, za ktoré je zodpovedný, pokiaľ je to možné, v elektronickej forme,
- vzor záznamu o spracovateľských činnostiach zverejní na svojej stránke úrad, záznam však musí obsahovať:
  - a) identifikačné údaje a kontaktné údaje prevádzkovateľa a zodpovednej osoby,
  - b) účel spracúvania osobných údajov,
  - c) opis kategórií dotknutých osôb a kategórií osobných údajov,
  - d) kategórie príjemcov vrátane príjemcu v tretej krajine alebo medzinárodnej organizácii,
  - e) označenie tretej krajiny alebo medzinárodnej organizácie, ak prevádzkovateľ zamýšľa prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii a dokumentáciu o primeraných zárukách, ak prevádzkovateľ zamýšľa prenos podľa § 51 ods. 1 a 2 zákona,
  - f) predpokladané lehoty na vymazanie rôznych kategórií osobných údajov,
  - g) všeobecný opis technických a organizačných bezpečnostných opatrení podľa § 39 ods. 1 zákona.

- záznam o kategóriách spracovateľských činností musí vytvoriť a viesť aj sprostredkovateľ, rozsah stanovuje § 37 ods. 2 zákona,

#### **6.1.2. Uchovávanie údajov len po nevyhnutnú dobu (§ 10)**

- osobné údaje môžu byť v IS spracúvané len po dobu nevyhnutnú na splnenie účelu spracúvania, následne ich treba zmazať alebo anonymizovať,
- lehota na vymazanie údajov musí zohľadňovať relevantnú legislatívu a interné predpisy (napr. registratúrny plán), jej stanovenie je súčasťou záznamov o spracovateľských činnostiach,
- technickú realizáciu vymazania či anonymizácie v konkrétnom IS zabezpečuje SITB, pričom môže byť realizovaná automatizovanou funkcionalitou, ale aj manuálnym zásahom správcu (pričom však treba dbať na vymazanie všetkých údajov),
- pri vymazaní osobných údajov je potrebné brať o úvahy aj zálohy, príp. tretie strany, ktorým boli poskytnuté (viď aj právo na výmaz a notifikácia tretích strán o vymazaní).

#### **6.1.3. Informovanie dotknutých osôb pri získavaní osobných údajov (§ 19 a 20)<sup>7</sup>**

- gestor vytvorí pre každý spôsob získavania údajov dotknutej osoby informačný list a v spolupráci s SITB (ktorá rieši technickú realizáciu v IS) navrhne mechanizmus pre informovanie dotknutej osoby,
- rozsah údajov, ktoré je potrebné zdokumentovať na informačný list a poskytovať dotknutým osobám je v závislosti od spôsobu získavania osobných údajov (priamo od dotknutej osoby alebo nepriamo) stanovený v § 19 a § 20,
- v rámci rozšírenia definície osobných údajov aj o údaje typu IP adresa či súbory cookies je potrebné zabezpečiť informačnú povinnosť aj v rámci webových portálov MV SR, ktoré zbierajú a spracúvajú tento typ údajov o aktivitách používateľov (stránka, z ktorej bol súbor vyžiadaný, meno súboru, dátum a čas dopytu, prenesené množstvá údajov, stav prístupu a pod.).

#### **6.1.4. Právo na obmedzenie spracúvania osobných údajov (§ 24)<sup>8</sup>**

- v rámci definovaných scenárov v tomto paragrafe má dotknutá osoba právo, aby bolo obmedzené spracúvanie jej osobných údajov, za týmto účelom musí byť dostupná možnosť označenia údajov ako obmedzené (na strane prevádzkovateľa, príp. aj používateľa) a dodržiavané reštrikcie na ich spracúvanie,
- obmedzené údaje by následne nemali byť vo výstupoch z IS,

<sup>7</sup> pre IS podporujúce plnenie úloh na účely trestného konania je táto požiadavka upravená v kap. 6.3.4

<sup>8</sup> pre IS podporujúce plnenie úloh na účely trestného konania je táto požiadavka upravená v kap. 6.3.5



- technická realizácia obmedzenia spracúvania je v kompetencii SITB.

#### 6.1.5. Notifikácia tretích strán o vymazaní/obmedzení (§ 25)

- o vymazaní/obmedzení je nutné informovať aj všetkých príjemcov, ktorým boli predmetné údaje poskytnuté
- v ideálnom prípade by na tento účel mohlo byť vytvorené API na strane integrovaných IS a vymazanie/obmedzenie by malo byť priamo realizované (platí aj naopak a obdobné API je potrebné vytvoriť aj v IS, ktoré získavajú osobné údaje z iných IS),
- alternatívne môže byť stanovený aj manuálny proces notifikácie tretích strán.

#### 6.1.6. Prístup k osobným údajom (§ 21)<sup>9</sup>

- dotknutá osoba má právo získať informáciu o tom, či sa spracúvajú jej osobné údaje a ak áno, prístup k nim a ďalším informáciám v podobnom rozsahu ako v kap. 6.1.3,
- údaje by mali byť poskytnuté v človekom čitateľnej podobe,
- nie je určená forma výstupu (elektronická/listinná) ani spôsob sprístupnenia (automatizované v IS/manuálnym zásahom),
- nemusí vždy ísť o registrovaných používateľov, treba mať určené aj metódy dopytu pre ľubovoľnú fyzickú osobu (získanie takých údajov potom ale napr. nemusí byť automatizované).

#### 6.1.7. Oprava osobných údajov (§ 22)<sup>10</sup>

- dotknutá osoba má právo na opravu nesprávnych osobných údajov a právo na doplnenie neúplných osobných údajov,
- vhodné je implementovať funkcionality na zmenu alebo doplnenie osobných údajov dotknutej osoby, napr. v prípade nesprávnosti,
- v zásade sa môže robiť aj manuálne (napr. na základe nejakého formulára).

#### 6.1.8. Automatizované rozhodovanie a profilovanie (§ 28)<sup>11</sup>

- rozhodnutie, ktoré má pre dotknutú osobu právne účinky by nemalo byť založené len na automatizovanom spracúvaní,
- procesy by mali byť nastavené tak, aby bolo možné rozhodnutie overiť aj manuálne oprávnenou osobou a aby existovala možnosť vyjadriť svoje stanovisko či napadnúť rozhodnutie zo strany dotknutej osoby.

<sup>9</sup> pre IS podporujúce plnenie úloh na účely trestného konania je táto požiadavka upravená v kap. 6.3.4

<sup>10</sup> pre IS podporujúce plnenie úloh na účely trestného konania je táto požiadavka upravená v kap. 6.3.5

<sup>11</sup> pre IS podporujúce plnenie úloh na účely trestného konania je táto požiadavka upravená v kap. 6.3.7

#### 6.1.9. Privacy by design (§ 32)

- súčasťou vývoja IS musí byť od začiatku aj riešenie ochrany osobných údajov, na základe ktorého je potrebné prijať primerané technické a organizačné opatrenia (viď nasledujúce 2 podkapitoly),
- táto požiadavka je v prostredí MV SR štandardne riešená v bezpečnostnom projekte.

#### 6.1.10. Privacy by default (§ 32)

- je potrebné dodržiavať pravidlá MV SR pre štandardné riešenie ochrany osobných údajov a opatrenia na zabezpečenie spracúvania osobných údajov len na konkrétny účel, minimalizácie množstva získaných osobných údajov a rozsahu ich spracúvania, doby uchovávanania a dostupnosti osobných údajov,
- osobné údaje nemajú byť bez zásahu fyzickej osoby štandardne prístupné neobmedzenému počtu fyzických osôb (riadenie prístupu).

#### 6.1.11. Bezpečnosť spracúvania (§ 39)

- MV SR ako prevádzkovateľ je povinné prijať primerané technické a organizačné opatrenia na zaistenie úrovne bezpečnosti primeranej riziku pre práva fyzických osôb (s ohľadom na najnovšie poznatky, náklady na vykonanie opatrení, na povahu, rozsah, kontext a účel spracúvania osobných údajov)
- uvedené opatrenia môžu zahŕňať najmä<sup>12</sup>
  - a) pseudonymizáciu a šifrovanie osobných údajov,
  - b) zabezpečenie trvalej dôvernosti, integrity, dostupnosti a odolnosti systémov spracúvania osobných údajov,
  - c) proces obnovy dostupnosti osobných údajov a prístup k nim v prípade fyzického incidentu alebo technického incidentu,
  - d) proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania osobných údajov,
- pri posudzovaní primeranej úrovne bezpečnosti sa prihliada na riziká, ktoré predstavuje spracúvanie osobných údajov, a to najmä náhodné zničenie alebo nezákonné zničenie, strata, zmena alebo neoprávnené poskytnutie prenášaných osobných údajov, uchovávaných osobných údajov alebo inak spracúvaných osobných údajov, alebo neoprávnený prístup k takýmto osobným údajom.

<sup>12</sup> príklady praktickej realizácie týchto opatrení uvádzame v prílohe č. 6

#### 6.1.12. Posúdenie vplyvu na ochranu osobných údajov – DPIA (§ 42)

- ak môže spracúvanie osobných údajov v konkrétnom IS viesť k vysokému riziku pre práva dotknutých osôb, bude nevyhnutné realizovať posúdenie vplyvu na ochranu osobných údajov – DPIA,
- pracovná skupina WP 29 vydala na podporu realizácie DPIA usmernenie, z ktorého možno pri realizácii DPIA vychádzať,<sup>13</sup>
- úrad zároveň pripravuje novú vyhlášku súvisiacu s podmienkami realizácie DPIA, požiadavky tejto vyhlášky bude potrebné zohľadniť aj pri realizácii DPIA v konkrétnych IS MV SR,
- štandardne by malo byť posúdenie vplyvu na ochranu osobných údajov zastrešené v bezpečnostnom projekte IS.

#### 6.1.13. Sprostredkovatelia (§ 34 - § 36)

- ak tretie strany (napr. dodávatelia) akokoľvek spracúvajú osobné údaje v IS v mene MV SR, musia byť postavení do role sprostredkovateľa,
- sprostredkovateľ musí poskytnúť dostatočné záruky na prijatie primeraných technických a organizačných opatrení tak, aby bol dodržiavaný zákon a aby sa zabezpečila ochrana práv dotknutej osoby,
- s každým sprostredkovateľom musí byť uzavretá písomná zmluva v zmysle § 34 ods. 3.

---

Ďalšie požiadavky sú relevantné len pre **IS spracúvajúce osobné údaje na základe súhlasu dotknutej osoby**.

#### 6.1.14. Získavanie súhlasu (§ 14)

- v prípade, že sú údaje spracúvané na základe súhlasu, nestačí už jeden všeobecný súhlas („súhlasím so spracúvaním osobných údajov“, či len s podmienkami využívania služby), každá spracovateľská operácia by mala mať samostatný súhlas (napr. checkbox),
- tieto súhlasy je vhodné uchovávať aj v samostatnom stĺpci DB, pretože ich musí byť možné aj odvolať (na čo je potrebný interface),
- súhlas nesmie byť označený vopred, musí to urobiť používateľ.

#### 6.1.15. Spätné získanie súhlasu (§ 14)

- ak už získané súhlasy nespĺňajú nové podmienky na súhlas, treba ich získať opätovne,
- treba mať vyriešený spôsob kontaktovania všetkých dotknutých používateľov a spôsob získania súhlasu.

---

<sup>13</sup> [http://ec.europa.eu/newsroom/just/document.cfm?doc\\_id=48464](http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48464)

#### 6.1.16. Kontrola veku (§ 15)

- pre spracúvanie osobných údajov detí do veku 16 rokov na základe súhlasu je vyžadovaný súhlas zákonného zástupcu,
- na zistenie a overenie veku sa má využiť „primerané úsilie“ (nie je napr. možné ošetriť, že používateľ klame),
- musí byť pripravený spôsob, ako získať súhlas zákonného zástupcu (napr. zadaním emailu rodiča a zaslaním linky, na ktorej súhlas udelí).

#### 6.1.17. Právo na výmaz osobných údajov (§ 23)<sup>14</sup>

- je potrebné mať vytvorenú funkcionality resp. proces na zmazanie všetkých osobných údajov dotknutej osoby v rámci daného IS (resp. účelu spracúvania), ide napr. o prípady, kedy dotknutá osoba odvolá súhlas so spracúvaním (§ 13 ods. 1 písm. a), §16 ods. 2 písm. a)), namieta spracúvanie osobných údajov (§27), zistí sa nezákonnosť spracúvania či naplnenie povinností vyplývajúcich z osobitného predpisu (napr. zákona),
- na tento účel môže byť prispôsobený aj dátový model, aby bolo priamočiaro možné odstrániť dáta vo všetkých relevantných tabuľkách, vymazať je v tomto prípade potrebné aj osobné údaje uložené v zálohách či logoch,
- túto požiadavku je možné naplniť automatizovanou funkcionality, ale aj manuálnym zásahom správcu (pričom však treba dbať na vymazanie všetkých údajov),
- o vymazaní je nutné informovať aj všetkých príjemcov, ktorým boli predmetné údaje poskytnuté (viď kap. 6.1.5).

#### 6.1.18. Export údajov (§ 26)

- je potrebné vytvoriť funkcionality alebo postup, ktorý na vyžiadanie exportuje všetky údaje o používateľovi, rozsah údajov by mal byť minimálne ako v prípade vymazania,
- formát nie je stanovený (môže byť napr. XML, JSON, ale aj CSV), export nemusí byť dostupný na počkanie, ale aj dodatočne, príp. nemusí byť ani plne automatizovaný,
- právo exportu sa týka len osobných údajov spracúvaných na základe súhlasu dotknutej osoby (§13 ods. 1 písm. a), §16 ods. 2 písm. a)), resp. zmluvného základu spracúvania (§13 ods. 1 písm. b)).

<sup>14</sup> pre IS podporujúce plnenie úloh na účely trestného konania je táto požiadavka upravená v kap. 6.3.5

## **6.2. Požiadavky na IS spracúvajúce osobitnú kategóriu osobných údajov**

Požiadavky na IS MV SR uvedené v tejto kapitole sa týkajú IS spracúvajúcich osobitnú kategóriu osobných údajov. Tieto IS musia spĺňať aj požiadavky definované v kapitole 6.1 a ak to je pre konkrétny IS relevantné, aj požiadavky v kapitole 6.3 a 6.4.

Osobitné požiadavky na IS spracúvajúce osobitnú kategóriu OÚ vychádzajú tak zo znenia zákona ako aj z pravidiel dobrej praxe a sú nasledovné:

### **6.2.1. Bezpečnostný projekt a DPIA (§ 42)**

- za účelom komplexného riešenia informačnej bezpečnosti je pre IS spracúvajúce osobitnú kategóriu osobných údajov potrebné vypracovať bezpečnostný projekt, ktorého súčasťou je aj analýza rizík,
- ak sa osobitné kategórie osobných údajov spracúvajú vo veľkom rozsahu, je tiež potrebné realizovať posúdenie vplyvu na ochranu osobných údajov, v rámci ktorého sa musia posúdiť riziká narušenia práv dotknutých fyzických osôb a navrhnúť opatrenia na ich minimalizáciu.

### **6.2.2. Zaistenie dôvernosti IS (§ 39 ods. 1 písm. b))**

- dôvernosť musí byť zaručená relevantnými technickými i organizačnými opatreniami, opatrenia na zaistenie dôvernosti IS musia pokrývať všetky významné identifikované riziká narušenia dôvernosti z analýzy rizík podľa kap. 6.2.1,
- musí byť zabezpečená ochrana dôvernosti údajov pri prenose v sieti (napr. šifrovaným komunikačným kanálom).

### **6.2.3. Zaistenie integrity IS (§ 39 ods. 1 písm. b))**

- integrita musí byť zaručená relevantnými technickými i organizačnými opatreniami, opatrenia na zaistenie integrity IS musia pokrývať všetky významné identifikované riziká narušenia integrity z analýzy rizík podľa kap. 6.2.1,
- integrita údajov pri prenose v sieti musí byť chránená kryptograficky.

### **6.2.4. Pravidelné hodnotenie bezpečnosti (§ 39 ods. 1 písm. d))**

- musí byť stanovený a zavedený proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania osobných údajov v IS,
- súčasťou tohto procesu musí byť aj aktualizácia analýzy rizík podľa kap. 6.2.1.

### **6.3. Požiadavky na IS podporujúce plnenie úloh na účely trestného konania**

Požiadavky na IS uvedené v tejto kapitole sa týkajú IS spracúvajúcich osobné údaje v prostredí MV SR na účely predchádzania a odhaľovania trestnej činnosti, zisťovania páchatelov trestných činov, stíhania trestných činov alebo na účely výkonu rozhodnutí v trestnom konaní vrátane ochrany pred ohrozením verejného poriadku a predchádzania takémuto ohrozeniu (v tomto dokumente aj „IS podporujúce plnenie úloh na účely trestného konania“). V rámci zákona sa osobitnými pravidlami ochrany osobných údajov podľa tejto kapitoly zaoberá tretia časť (§ 52 – 77). IS podporujúce plnenie úloh na účely trestného konania musia spĺňať aj požiadavky definované v kapitole 6.1 a ak to je relevantné, aj požiadavky v kapitole 6.2 a 6.4.

#### **6.3.1. Zákonnosť spracúvania (§ 55)**

- MV SR je oprávnené spracúvať osobné údaje na plnenie úloh na účely trestného konania podľa zákona, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je SR viazaná,
- spracúvať osobné údaje na plnenie úloh na účely trestného konania, ktoré boli pôvodne získané na iný účel, je možné, ak spracúvanie osobných údajov je na účel trestného konania nevyhnutné a primerané,
- MV SR je oprávnené spracúvať osobné údaje aj na iný účel, ako je plnenie úloh na účely trestného konania, ak to je zlučiteľné s účelom, na ktorý sa zhromaždili, a ak spracúvanie je na tento iný účel nevyhnutné a primerané,
- osobitné kategórie osobných údajov môžu byť spracúvané len v zmysle § 56 zákona, a to vtedy ak
  - a) ich preukázateľne poskytla dotknutá osoba,
  - b) je ich spracúvanie nevyhnutné podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je SR viazaná,
  - c) je ich spracúvanie nevyhnutné na ochranu života, zdravia alebo majetku dotknutej osoby alebo inej fyzickej osoby.

#### **6.3.2. Kategórie dotknutých osôb (§ 57)**

- v IS podporujúcich plnenie úloh na účely trestného konania, ak je to možné, rozlišovať medzi osobnými údajmi rôznych kategórií dotknutých osôb (ako napr. osoby, u ktorých sa možno odôvodnene domnievať, že spáchali alebo majú v úmysle spáchať trestný čin, osoby odsúdené za spáchanie trestného činu, obeť trestného činu, svedkovia),
- naplnenie tejto požiadavky môže vyvolať technické zmeny (ako napr. vytvorenie novej funkcionality, prispôsobenie dátového modelu).

### 6.3.3. Pôvod a pravdivosť osobných údajov (§ 58)

- MV SR je povinné označiť, ak je to možné, osobné údaje založené na skutočnostiach a osobné údaje založené na osobných hodnoteniach,
- pred poskytnutím alebo prenosom je nutné overiť ich správnosť, úplnosť a aktuálnosť, ak je to možné, a prijať opatrenia na zabezpečenie toho, aby sa neposkytovali alebo neprenášali osobné údaje, ktoré sú nesprávne, neúplné alebo neaktuálne,
- k poskytnutiu a prenosu osobných údajov je potrebné pripojiť dostupné informácie, ktoré umožnia prijímajúcemu príslušnému orgánu posúdiť ich mieru správnosti, úplnosti, aktuálnosti a spoľahlivosti, ak to okolnosti dovoľujú,
- nesprávne osobné údaje MV SR nemôže poskytovať a prenášať, neoverené osobné údaje príslušný orgán musí pri poskytovaní alebo prenose takto označiť a musí uviesť mieru ich spoľahlivosti,
- ak MV SR neoprávnene poskytne osobné údaje alebo neoprávnene prenesie osobné údaje alebo poskytne nesprávne osobné údaje alebo prenesie nesprávne osobné údaje, je povinné bez zbytočného odkladu informovať príjemcu a žiadať príjemcov osobných údajov, ktorým sa také osobné údaje poskytli, aby ich bez zbytočného odkladu opravili, doplnili, vymazali alebo aby obmedzili spracúvanie takých osobných údajov.

### 6.3.4. Informácie, ktoré sa majú sprístupniť alebo poskytnúť dotknutej osobe (§ 60 a 61)

- MV SR (resp. policajný zbor) je povinné na svojom webovom sídle sprístupniť najmä
  - a) svoje identifikačné údaje a kontaktné údaje,
  - b) kontaktné údaje zodpovednej osoby,
  - c) informácie o účele spracúvania, na ktoré sú osobné údaje určené,
  - d) kontaktné údaje úradu,
  - e) informácie o práve podať návrh na začatie konania podľa § 100,
  - f) informácie o práve žiadať prístup k osobným údajom, ktoré sa dotknutej osoby týkajú, ich opravu, vymazanie alebo obmedzenie ich spracúvania,
- na žiadosť dotknutej osoby je MV SR povinné poskytnúť v osobitných prípadoch dotknutej osobe informácie v rozsahu § 60 ods. 2,
- dotknutá osoba má tiež právo získať potvrdenie o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú, a ak to tak je, má právo získať prístup k týmto osobným údajom a informácie v zmysle § 61,
- v tomto rozsahu vytvorí gestor informačný list a v spolupráci s SITB (ktorá rieši technickú realizáciu v IS) navrhne mechanizmus pre informovanie dotknutej osoby,
- údaje by mali byť poskytnuté v človekom čitateľnej podobe,

- nie je určená forma výstupu (elektronická/listinná) ani spôsob sprístupnenia (automatizovane v IS/manuálnym zásahom),
- je potrebné mať určené metódy dopytu pre ľubovoľnú fyzickú osobu (získanie takých údajov potom ale napr. nemusí byť automatizované),
- právo na prístup k osobným údajom môže MV SR obmedziť pri niektorom z prípadov definovaných v § 63 zákona alebo na základe § 65 zákona (ak osobné údaje sú súčasťou vyšetrovacieho spisu alebo súdneho spisu v rámci trestného konania).

### **6.3.5. Právo na opravu osobných údajov, právo na vymazanie osobných údajov a obmedzenie týchto práv (§ 62)**

- dotknutá osoba má právo na to, aby MV SR bez zbytočného odkladu opravilo nesprávne osobné údaje, príp. doplnilo neúplné údaje, ktoré sa jej týkajú,
- dotknutá osoba má právo na to, aby MV SR bez zbytočného odkladu vymazalo osobné údaje, ktoré sa jej týkajú, a príslušný orgán je povinný bez zbytočného odkladu vymazať osobné údaje, ak
  - a) spracúvanie osobných údajov je v rozpore so zásadami spracúvania osobných údajov podľa § 52 až 55,
  - b) spracúvanie osobných údajov je v rozpore s § 56, alebo
  - c) výmaz osobných údajov je nevyhnutný na účel splnenia povinností podľa zákona, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je SR viazaná,
- namiesto vymazania MV SR obmedzí spracúvanie osobných údajov, ak
  - a) dotknutá osoba napadla správnosť osobných údajov a ich správnosť alebo nesprávnosť nemožno určiť, alebo
  - b) osobné údaje sa musia zachovať na účely dokazovania,
- ak je obmedzené spracúvanie osobných údajov podľa predchádzajúceho bodu (§ 62 ods. 3 písm. a), MV SR je povinné pred zrušením obmedzenia spracúvania osobných údajov o tom dotknutú osobu informovať,
- MV SR je povinné písomne informovať dotknutú osobu o zamietnutí práva na opravu, vymazanie alebo obmedzenie spracúvania osobných údajov podľa predchádzajúcich bodov a o dôvodoch zamietnutia,
- technická realizácia opravy, vymazania a obmedzenia spracúvania je v kompetencii SITB, tieto požiadavky je možné naplniť automatizovanou funkcionalitou, ale aj manuálnym zásahom správcu,
- na tento účel môže byť prispôsobený aj dátový model, aby bolo priamočiaro možné odstrániť či obmedziť dáta vo všetkých relevantných tabuľkách, ďalej je potrebné myslieť na všetky výskyty osobných údajov, vrátane záloh či logov,
- právo na opravu, vymazanie a obmedzenie spracúvania môže MV SR obmedziť pri niektorom z prípadov definovaných v § 63 zákona alebo na základe § 65 zákona (ak osobné údaje sú súčasťou vyšetrovacieho spisu alebo súdneho spisu v rámci trestného konania).



### 6.3.6. Obmedzenie poskytnutia informácií a práv dotknutej osoby (§ 63)

- MV SR môže odložiť poskytnutie informácií, obmedziť poskytnutie informácií alebo upustiť od poskytnutia informácií podľa § 60 ods. 2 zákona, úplne alebo čiastočne obmedziť právo na prístup podľa § 61 alebo môže úplne alebo čiastočne obmedziť povinnosť informovať podľa § 62 ods. 5, ak
  - a) by mohlo dôjsť k ovplyvňovaniu alebo mareniu úradného postupu alebo súdneho postupu alebo šetrenia,
  - b) by mohlo dôjsť k ohrozeniu plnenia úloh na účely trestného konania,
  - c) je to potrebné na zabezpečenie ochrany verejného poriadku alebo bezpečnosti štátu, alebo
  - d) je to potrebné na ochranu práv iných osôb.
- osobitný predpis môže ustanoviť kategórie spracúvania osobných údajov, ktoré sa vzťahujú predchádzajúci bod,
- MV SR je povinné písomne informovať dotknutú osobu o zamietnutí práva na prístup alebo obmedzení práva na prístup podľa § 61 a o dôvodoch tohto zamietnutia alebo obmedzenia, to neplatí, ak by sa poskytnutím takej informácie ohrozil účel podľa prvého bodu.

### 6.3.7. Automatizované individuálne rozhodovanie (§ 66)

- rozhodnutie, ktoré má pre dotknutú osobu nepriaznivé právne účinky, nesmie byť založené len na automatizovanom spracúvaní vrátane profilovania, ak to neustanovuje osobitný predpis alebo medzinárodná zmluva, ktorou je SR viazaná (musí však určovať primerané záruky ochrany práv dotknutej osoby, najmä právo na manuálne overenie rozhodnutia),
- procesy by mali byť nastavené tak, aby bolo možné rozhodnutie overiť aj manuálne oprávnenou osobou a aby existovala možnosť vyjadriť svoje stanovisko či napadnúť rozhodnutie zo strany dotknutej osoby,
- rozhodnutie podľa prvého bodu nesmie byť založené na osobitných kategóriách osobných údajov, ak sa neuplatňujú vhodné opatrenia na zaručenie práv a oprávnených záujmov dotknutej osoby,
- profilovanie, ktoré vedie k diskriminácii osôb na základe osobitných kategórií osobných údajov, je zakázané.

### 6.3.8. Bezpečnostný projekt a DPIA (§ 42)

- za účelom komplexného riešenia informačnej bezpečnosti je pre IS podporujúce plnenie úloh na účely trestného konania potrebné vypracovať bezpečnostný projekt, ktorého súčasťou je aj analýza rizík,
- keďže sa spracúvajú osobné údaje týkajúce sa uznania viny za spáchanie trestného činu alebo priestupku, je nevyhnutné realizovať posúdenie vplyvu na ochranu osobných údajov, v rámci ktorého sa musia posúdiť riziká narušenia práv dotknutých fyzických osôb a navrhnúť opatrenia na ich minimalizáciu,

- ak zo spracúvania osobných údajov na základe posúdenia vplyvu vyplynie vysoké riziko pre práva fyzických osôb, uskutoční MV SR pre spracúvaním osobných údajov konzultáciu s úradom, ktorý mu následne poskytne poradenstvo v zmysle § 70.

### 6.3.9. Bezpečnosť spracúvania osobných údajov (§ 71)

MV SR musí pri automatizovanom spracúvaní osobných údajov prijať na základe vyhodnotenia rizík opatrenia na:

- a) kontrolu prístupu k zariadeniam, aby sa zabránilo neoprávnenému prístupu k zariadeniam na spracúvanie osobných údajov, ktoré sa používajú na spracúvanie,
- b) kontrolu nosičov osobných údajov, aby sa zabránilo neoprávnenému čítaniu nosičov osobných údajov, kopírovaniu nosičov osobných údajov, pozmeňovaniu nosičov osobných údajov alebo odstráneniu nosičov osobných údajov,
- c) kontrolu uchovávaní osobných údajov, aby sa zabránilo neoprávnenému vkladaniu osobných údajov do informačného systému a neoprávnenému prehliadaniu osobných údajov v informačnom systéme, pozmeňovaniu osobných údajov v informačnom systéme alebo vymazaniu osobných údajov z informačného systému,
- d) kontrolu užívateľa informačného systému, aby sa zabránilo použitiu systémov automatizovaného spracúvania neoprávnenými osobami pomocou zariadenia na prenos osobných údajov,
- e) kontrolu prístupu k osobným údajom, aby sa zabezpečilo, že osoby oprávnené používať systém automatizovaného spracúvania budú mať prístup iba k tým osobným údajom, na ktoré sa vzťahuje ich oprávnenie na prístup,
- f) kontrolu prenosu údajov, aby sa zabezpečila možnosť overiť a zistiť subjekty, ktorým sa preniesli osobné údaje alebo poskytl osobné údaje, alebo overiť a zistiť subjekty, ktorým sa môžu preniesť osobné údaje, alebo poskytnúť osobné údaje prostredníctvom zariadenia na prenos osobných údajov,
- g) kontrolu vkladania údajov do informačného systému, aby sa zabezpečilo, že bude možné overiť a zistiť, aké osobné údaje sa vložili do systému automatizovaného spracúvania, a kedy a kto ich tam vložil,
- h) kontrolu prepravy osobných údajov, aby sa zabránilo neoprávnenému čítaniu osobných údajov, kopírovaniu osobných údajov, pozmeňovaniu osobných údajov alebo vymazaniu osobných údajov počas ich prenosu alebo počas prepravy nosiča osobných údajov,
- i) obnovu osobných údajov, aby sa zabezpečilo, že sa inštalované systémy obnovia, ak dôjde k ich prerušeniu,
- j) zabezpečenie spoľahlivosti informačného systému, aby sa zabezpečilo, že funkcie tohto systému fungujú a hlási sa výskyt chýb v jeho funkciách,
- k) zabezpečenie integrity informačného systému, aby sa uchovávané osobné údaje nemohli poškodiť, ak nastane porucha tohto systému.

#### **6.3.10. Vedenie logov (§ 69)**

- MV SR musí pri získavaní, zmene, prehliadaní, poskytovaní vrátane prenosu, kombinovaní a vymazaní osobných údajov v systéme automatizovaného spracúvania uchovávať logy,
- z logov o prehliadaní a poskytovaní musí byť možné určiť dôvod, dátum a čas prehliadania alebo poskytovania a identifikačné údaje osoby, ktorá tieto osobné údaje prehliadala alebo ich poskytovala, ako aj totožnosť príjemcov,
- MV SR je povinné zabezpečiť vedenie logov podľa § 69 v IS zriadených podľa doterajších predpisov od 6. mája 2023, ak by to spôsobilo vážne problémy pre fungovanie daného IS, je povinné zabezpečiť vedenie logov podľa § 69 najneskôr od 6. mája 2026.

### **6.4. Požiadavky na osobitne dôležité IS MV SR**

Požiadavky na IS MV SR uvedené v tejto kapitole sa týkajú osobitne dôležitých IS MV SR spracúvajúcich osobné údaje. Tieto IS musia spĺňať aj požiadavky definované v kapitole 6.1 a ak to je relevantné, aj požiadavky v kapitole 6.2 a 6.3.

Osobitne dôležité IS obsahujú aktíva rozhodujúce pre činnosti MV SR, zlyhanie bezprostredne ohrozuje poskytovanie dôležitých služieb a reputáciu MV SR, vyžaduje sa aplikačná podpora pre vysokú dostupnosť. Priradenie tejto kategórie konkrétnym IS realizuje OB SITB.

Požiadavky na osobitne dôležité IS vychádzajú tak zo znenia zákona ako aj z pravidiel dobrej praxe a sú nasledovné:

#### **6.4.1. Bezpečnostný projekt a DPIA (§ 42)**

- za účelom komplexného riešenia informačnej bezpečnosti je pre osobitne dôležité IS povinné vypracovať bezpečnostný projekt, ktorého súčasťou je aj analýza rizík,
- rovnako je nutné realizovať posúdenie vplyvu na ochranu osobných údajov, v rámci ktorého sa musia posúdiť riziká narušenia práv dotknutých fyzických osôb a navrhnúť opatrenia na ich minimalizáciu.

#### **6.4.2. Zaistenie dostupnosti (§ 39 ods. 1 písm. b))**

- dostupnosť osobitne dôležitých IS musí byť zaručená relevantnými technickými i organizačnými opatreniami, za týmto účelom je okrem iného potrebné zaistiť aplikačnú podporu pre vysokú dostupnosť,

- dostupnosť IS musí byť pokrytá platnou SLA,
- okrem primárnej prevádzkovej lokality by malo byť sprevádzkované aj záložné prevádzkové prostredie schopné zabezpečiť dočasnú náhradnú prevádzku,
- opatrenia na zaistenie dostupnosti IS musia pokrývať všetky identifikované riziká narušenia dostupnosti z analýzy rizík podľa kap. 6.4.1,
- musí byť vypracovaný a otestovaný proces obnovy dostupnosti osobných údajov (podľa § 39 ods. 1 písm. c)).

#### **6.4.3. Zaistenie dôvernosti (§ 39 ods. 1 písm. b))**

- dôvernosť musí byť zaručená relevantnými technickými i organizačnými opatreniami, opatrenia na zaistenie dôvernosti IS musia pokrývať všetky významné identifikované riziká narušenia dôvernosti z analýzy rizík podľa kap. 6.4.1,
- musí byť zabezpečená ochrana dôvernosti údajov pri prenose v sieti (napr. šifrovaným komunikačným kanálom).

#### **6.4.4. Zaistenie integrity (§ 39 ods. 1 písm. b))**

- integrita musí byť zaručená relevantnými technickými i organizačnými opatreniami, opatrenia na zaistenie integrity IS musia pokrývať všetky významné identifikované riziká narušenia integrity z analýzy rizík podľa kap. 6.4.1,
- integrita údajov pri prenose v sieti musí byť chránená kryptograficky.

#### **6.4.5. Pravidelné hodnotenie bezpečnosti (§ 39 ods. 1 písm. d))**

- musí byť stanovený a zavedený proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania osobných údajov v IS,
- súčasťou tohto procesu musí byť aj aktualizácia analýzy rizík podľa kap. 6.4.1,
- v pravidelných intervaloch musí byť realizované aj penetračné testovanie osobitne dôležitých IS.

## Príloha č. 1 – Zoznam IS podľa kategórií

Nad rámec bežných IS spracúvajúcich osobné údaje boli na základe dotazníkov v jednotlivých kategóriách podľa klasifikácie identifikované nasledovné IS.

IS spracúvajúce osobitnú kategóriu osobných údajov:

1. CODIS – Combined DNA Index System, CODIS WEB,
2. AFIS (Automatizovaný systém daktyloskopickkej identifikácie osôb),
3. Dátový fond medzinárodnej ochrany informačného systému migrácia a medzinárodná ochrana,
4. APV personalizačných liniek ID1,
5. APV personalizačných liniek ID3,
6. IS REGOB (evidencia osôb),
7. DSA (dopravnosprávne agendy),
8. IS EVO (evidencia vozidiel),
9. IS PZ DANAU,
10. IS PZ REGOB,
11. IS SAP Infotyp 9011 Zdravotná starostlivosť, 9010 Zdravotné dáta, modul Kúpeľná starostlivosť,
12. Kamerové systémy v rámci MV SR,
13. Denník oznámení protispoločenskej činnosti, denník lustrácií pre NBÚ, denník oznámení o trestnej činnosti, denník kontrol, denník petícií, denník sťažností, denník iných podaní, denník ochrany osobných údajov, DVS,
14. IS databáza meritórnych rozhodnutí
15. IS Poznatkový fond,
16. IS IZS (Integrovaný záchranný systém),
17. APV REZ Politické strany,
18. APV REZ,
19. IS MIGRA,
20. IS INBO,
21. IS UMPS,
22. IS Medzinárodná policajná spolupráca.

IS podporujúce plnenie úloh na účely trestného konania:

1. CODIS – Combined DNA Index System, CODIS WEB,
2. IS EVIDENCE,
3. AFIS (Automatizovaný systém daktyloskopickkej identifikácie osôb),
4. MS Word (Evidencia odtlačkov častí ľudského tela (známych páchatel'ov)),
5. IS OEZ (Operatívna evidencia zbraní, streliva, munície a výbušnín),
6. IS REGOB (evidencia osôb),
7. DSA (dopravnosprávne agendy),
8. IS EVO (evidencia vozidiel),
9. IS PZ DANAU,

10. IS PZ REGOB,
11. Kamerané systémy v rámci MV SR,
12. Denník oznámení protispoločenskej činnosti, denník lustrácií pre NBÚ, denník oznámení o trestnej činnosti, denník kontrol, denník petícií, denník sťažností, denník iných podaní, denník ochrany osobných údajov, DVS,
13. IS databáza meritórnych rozhodnutí,
14. IS Poznatkový fond,
15. IS IZS (Integrovaný záchranný systém),
16. IS MIGRA,
17. IS INBO,
18. IS DVS,
19. IS FADO (Národný informačný systém sfalšovaných a autentických dokladov),
20. IS FALZO (Informačný systém Evidencia falšovaných a pozmenených peňazí a platobných kariet),
21. IS UMPS modul INTERPOL,
22. IS Medzinárodná policajná spolupráca.

Osobitne dôležité IS:

1. Dátový fond medzinárodnej ochrany informačného systému migrácia a medzinárodná ochrana,
2. IS O EZ (Informačný systém Operatívna evidencia zbraní, streliva, munície a výbušnín),
3. APV personalizačných liniek ID1,
4. APV personalizačných liniek ID3,
5. IS REGOB (evidencia osôb),
6. IS PZ DANAU,
7. IS PZ REGOB,
8. IIS SAP modul HR PA,
9. IIS SAP modul PD,
10. IIS SAP modul SP,
11. IS SAP HR SZ,
12. Kamerané systémy v rámci MV SR,
13. IS IZS (Integrovaný záchranný systém),
14. IS FABASOFT Automatizovaná správa registratúry,
15. IS RFO,
16. IS register rodných čísel,
17. IS CO,
18. IS CISMA,
19. APV REZ Politické strany,
20. IS MIGRA,
21. VIS MV SR,
22. IS EMON.

## Príloha č. 2 – Klasifikácia IS MV SR

Účel spracúvania	IS	forma spracúvania	osobitná kategória	trestné konanie	osobitne dôležitý IS	gestor	právny základ	bezp. projekt
Evidencia dochádzky zamestnancov OÚ Brezno	IS Fingera v 5.4.1	automatizovaná	nie	nie	nie	Okresný úrad Brezno	zákon č. 55/2017 Z. z. o štátnej službe, zákon č. 552/2003 Z. z. o výkone práce vo verejnom záujme, vnút. predpis č.1/2016	áno
Evidencia o vydaní osvedčení o odbornej spôsobilosti technikov a špecialistov požiarnej ochrany	MS Word, Excel, Outlook, Fabasoft	obe formy	nie	nie	nie	Prezídium Hasičského a záchranného zboru	zákon č. 314/2001 Z.z. o ochrane pred požiarmi v znení neskorších predpisov	nie
Personálna evidencia	IS Personálna evidencia, Microsoft Access	obe formy	nie	nie	nie	Kriminalistický a expertízny ústav PZ	Nariadenie ministra vnútra SR o vedení personálnej evidencie	nie
Národná databáza DNA profilov - CODIS	CODIS – Combined DNA Index System, CODIS WEB	automatizovaná	áno	áno	nie	Kriminalistický a expertízny ústav PZ	Zákon č. 171/1993 Z. z. o PZ, zákon č. 417/2002 Z. z. Zákon o používaní analýzy deoxyribonukleovej kyseliny na identifikáciu osôb	áno
Evidencia prípadov a zaistených stôp - EVIDENCE II	IS EVIDENCE	obe formy	nie	áno	nie	Kriminalistický a expertízny ústav PZ	splnenie úlohy vo verejnom záujme alebo pri výkone moci zverenej prevádzkovateľovi	áno

<b>Evidencia osôb, ktoré nadobudli odbornú spôsobilosť na výkon pyrotechnických činností</b>	IS evidencia osôb s odbornou spôsobilosťou	obe formy	nie	nie	nie	Kriminalistický a expertízny ústav PZ	Nariadenie MV SR o pyrotechnickej činnosti	neaktuálny
<b>Automatizovaný systém daktyloskopickej identifikácie - AFIS</b>	AFIS - Automatizovaný systém daktyloskopickej identifikácie osôb	obe formy	áno	áno	nie	Kriminalistický a expertízny ústav PZ	Zákon č. 171/1993 Z. z. o PZ	áno
<b>Psychofyzologické overovanie pravdivosti - audio/video záznam</b>	Evidencia hmotných nosičov, Zápisník oprávnenej osoby	obe formy	nie	nie	nie	Kriminalistický a expertízny ústav PZ	interné potreby	nie
<b>Zbierka odtlačkov uší, pier, zubov známych osob</b>	MS Word - Evidencia odtlačkov častí ľudského tela (známych páchateľov)	obe formy	nie	áno	nie	Kriminalistický a expertízny ústav PZ	potreby kriminalistickej praxe	áno
<b>Evidencia žiadateľov o udelenie azylu, azylantov, cudzincov, ktorým sa poskytla doplnková ochrana, cudzincov žiadajúcich o poskytnutie dočasného útočiska, odídencom, cudzincov odovzdaných na konanie do iného štátu, cudzincov u ktorých prebieha konanie podľa nariadenia Európskeho parlamentu a Rady (EU) č. 604/2013 z 26. júna 2013, ktorým sa stanovujú kritériá a</b>	Dátový fond medzinárodnej ochrany informačného systému migrácia a medzinárodná ochrana	obe formy	áno	nie	áno	Migračný úrad	Zákon č. 480/2002 Z. z. o azyle a o zmene a doplnení niektorých zákonov v znení neskorších predpisov Nariadenie ministra vnútra č. 18/2010 o požívaní informačného systému migrácia a medzinárodná ochrana a o zmene a doplnení niektorých interných aktov riadenia v znení neskorších predpisov Nariadenie Európskeho	áno



mechanizmy na určenie členského štátu zodpovedného za posúdenie žiadosti o medzinárodnú ochranu podanej štátnym príslušníkom tretej krajiny alebo osobou bez štátnej príslušnosti v jednom z členských štátov.							parlamentu a Rady (EU) č. 604/2013 z 26. júna 2013, ktorým sa stanovujú kritériá a mechanizmy na určenie členského štátu zodpovedného za posúdenie žiadosti o medzinárodnú ochranu podanej štátnym príslušníkom tretej krajiny alebo osobou bez štátnej príslušnosti v jednom z členských štátov	
<b>Operatívna evidencia zbraní, streliva, munície a výbušnín</b>	Informačný systém Operatívna evidencia zbraní, streliva, munície a výbušnín (IS OEZ)	automatizovaná	nie	áno	áno	Národná kriminálna agentúra Prezídia Policajného zboru	právny predpis: zákon Národnej rady Slovenskej republiky číslo 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov interný predpis: nariadenie Ministerstva vnútra Slovenskej republiky číslo 148/2015 o o operatívnej evidencii zbraní, streliva, munície a výbušnín	áno
<b>Vnútoraná agenda NPC</b>	IS SAP, IS Fabasoft, MS Excel	obe formy	nie	nie	nie	Národné personalizačné centrum MV SR	súhlas so spracovaním OÚ	nie

<b>Oddelenie personalizácie identifikačných kariet ID1</b>	APV personalizačných liniek ID1	obe formy	áno	nie	áno	Národné personalizačné centrum MV SR	splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi, zákon č.8/2009 Z. z. - o cestnej premávke, zákon č. 224/2006 Z. z. - o občianskych preukazoch, zákon č. 253/1998 Z. z. - o hlásení pobytu občanov SR a registri obyvateľov SR, zákon č. 404/2011 Z. z. - o pobyte cudzincov	neaktuálny
<b>Oddelenie personalizácie cestovných dokladov ID3</b>	APV personalizačných liniek ID3	obe formy	áno	nie	áno	Národné personalizačné centrum MV SR	splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi, zákon č. 647/2007 Z. z - o cestovných dokladoch	neaktuálny
<b>Stážnosti</b>	CEVISTA	obe formy	nie	nie	nie	SKIS MV SR vybavovanie sťažností	zák. č. 9/2010 v Z. z. o sťažnostiach	nie
<b>Kontrola</b>		písomná	nie	nie	nie	SKIS MV SR	zák. č. 10/1996 Z. z. o kontrole	nie
<b>Evidencia vozidiel</b>	EVO (Evidovanie vozidiel)	automatizovaná	nie	nie	nie	Odbor dokladov a evidencií Prezídia PZ	Zákon č. 8/2009 Z. z. o cestnej premávke a o zmene a doplnení niektorých zákonov v znení neskorších predpisov	n/a

<b>Evidencia zbraní, streliva a strelníc</b>	EZP (zbraní, streliva a strelníc)	automatizovaná	nie	nie	nie	Odbor dokladov a evidencií Prezídia PZ	Zákon č. 190/2003 Z. z. o strelných zbraniach a strelive a o zmene a doplnení niektorých zákonov vznen neskorších predpisov	n/a
<b>Vyvolávací informačný systéme pre občanov</b>	VYSYS (Vyvolávací informačný systéme pre občanov)				nie	Odbor dokladov a evidencií Prezídia PZ		n/a
<b>Centrálna evidencia splnomocnení pre viaceré IS vo verejnej správe</b>	CESP (centrálna evidencia splnomocnení pre viaceré IS vo verejnej správe)	automatizovaná	nie	nie	nie	Odbor dokladov a evidencií Prezídia PZ	Zákon č. 8/2009 Z. z. o cestnej premávke a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ďalšie zákony	n/a
<b>Medzinárodné komunikačné rozhranie na evidenciu vozidiel a vodičských preukazov</b>	EUCARIS (medzinárodné komunikačné rozhranie na evidenciu vozidiel a vodičských preukazov)	automatizovaná	nie	nie	nie	Odbor dokladov a evidencií Prezídia PZ	Zmluva o pristúpení SR k systému EUCARIS, zverejnená v zbierke zákonov č. 17/2011 Z. z.	n/a
<b>Evidencia vodičských preukazov a dopravnosprávna agenda</b>	DSA (evidencia vodičských preukazov a dopravnosprávna agenda)	automatizovaná	nie	nie	nie	Odbor dokladov a evidencií Prezídia PZ	Zákon č. 8/2009 Z. z. o cestnej premávke a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ďalšie zákony	n/a
	IDC (občianske preukazy)	automatizovaná			nie	Odbor dokladov a evidencií Prezídia PZ	Zákon č. 224/2006 Z. z. o občianskych preukazoch a o zmene a doplnení niektorých zákonov v znení neskorších predpisov	n/a

	CDO (cestovné doklady)	automatizovaná			nie	Odbor dokladov a evidencií Prezídia PZ	Zákon č. 647/2007 Z. z. o cestovných dokladoch a o zmene a doplnení niektorých zákonov v znení neskorších predpisov	n/a
<b>Evidencia dopravných nehôd</b>	IS REGOB (evidencia osôb), DSA (dopravnosprávne agendy), IS EVO (evidencia vozidiel)	automatizovaná	áno	áno	nie	Odbor dopravnej polície Prezídia PZ	§ 67 zákona č. 8/2009 Z. z. o cestnej premávke a o zmene a doplnení niektorých zákonov v znení neskorších predpisov	neaktuálny
<b>Vedenie evidencie obecných polícií v SR</b>	IS EVO POL (evidencia obecných polícií)	automatizovaná	nie	nie	nie	Odbor poriadkovej polície Prezídia PZ	zákon SNR č. 564/1991 Zb. o obecnej polícii	neaktuálny
<b>Centrálna evidencia správnych deliktov a priestupkov</b>	modul CESDaP IS SAP	obe formy	nie	nie	nie	Odbor poriadkovej polície Prezídia PZ	Zákon č. 372/1990 Zb. o priestupkoch v znení neskorších predpisov	áno
<b>Vytváranie, spracovávanie, prenášanie a ukladanie osobných údajov a informácií podľa § 69 až § 69g zákona NR SR č. 171/1993 Z. z. o PZ v znení neskorších predpisov.</b>	IS PZ DANAU, IS PZ REGOB, MS Excel	automatizovaná	áno	áno	áno	ORKA P PZ	v zmysle § 69 až § 69g zákona Národnej rady Slovenskej republiky č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov.	áno
<b>Zdravotná starostlivosť, kúpeľná starostlivosť</b>	IS SAP Infotyp 9011 Zdravotná starostlivosť, 9010 Zdravotné dáta, Modul Kúpeľná starostlivosť	písomná	áno	nie	nie	Odbor zdravotníctva, SPSČ a OÚ MV SR	Nariadenie Ministerstva vnútra Slovenskej republiky č. 146/2013 o integrovanom informačnom systéme SAP	nie

<b>Riadenie ľudských zdrojov - personalistika</b>	IIS SAP modul HR PA	obe formy	nie	nie	áno	Sekcia personálnych a sociálnych činností a osobný úrad MV SR Personálny odbor	Zákon č.: 122/2013 Z.z., 73/1998 Z.z., 315/2001 Z. z., 55/2017 Z.z., 553/2003 Z. z., 311/2001 Z. z. súhlas so spracovaním osobných údajov	n/a
<b>Personálna dokumentácia</b>	IIS SAP modul PD	obe formy	nie	nie	áno	Sekcia personálnych a sociálnych činností a osobný úrad MV SR Personálny odbor	Zákon č.: 122/2013 Z.z., 73/1998 Z.z., 315/2001 Z. z., 55/2017 Z.z., 553/2003 Z. z., 311/2001 Z. z. súhlas so spracovaním osobných údajov	n/a
<b>Služobné preukazy</b>	IIS SAP modul SP	obe formy	nie	nie	áno	Sekcia personálnych a sociálnych činností a osobný úrad MV SR Personálny odbor	Zákon č.: 122/2013 Z.z., 73/1998 Z.z., 315/2001 Z. z., 55/2017 Z.z., 553/2003 Z. z., 311/2001 Z. z. súhlas so spracovaním osobných údajov	n/a
	IS SAP HR SZ	obe formy	nie	nie	áno	Odbor sociálneho zabezpečenia sekcia personálnych a sociálnych činností a osobný úrad MV SR	súhlas so spracúvaním OÚ, zákon č. 328/2002 Z. z. o sociálnom zabezpečení policajtov a vojakov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákon č. 461/2003 Z. z. o sociálnom poistení v znení neskorších predpisov a zákon č. 315/2001 o Hasičskom a	neaktuálny

							záchrannom zbore v znení neskorších predpisov	
Monitorovanie priestorov kamerovými systémami	Kamerové systémy v rámci MV SR	automatizovaná	áno	áno	áno	SKIS MV SR	Zákon č. 122/2013 Z. z. o OOÚ v znení zákona č. 84/2014 Z. z., Zákon č. 215/2004 Z. z. o utajovaných skutočnostiach v znení neskorších predpisov, Zákon č. 404/2011 Z. z. o pobyte cudzincov a o zmene a doplnení niektorých zákonov, Zákon č. 171/1993 Z. z. o Policajnom zbore, Zákon č. 73/1998 Z. z. o štátnej službe príslušníkov Policajného zboru, Slovenskej informačnej služby, Zboru väzenskej a justičnej stráže Slovenskej republiky a Železničnej polície v znení neskorších predpisov.	áno

Prijímanie, evidovanie, analýza obsahu, preverovanie, prešetrovanie alebo vybavenie podnetov iným spôsobom, vykonávanie vnútorných kontrol, prerokovanie protokolu, resp. záznamu o výsledku kontroly, zakladanie, evidovanie, vedenie a vyradovanie vyšetrovacích spisov...	denník oznámení protispoločenskej činnosti, denník lustrácií pre NBÚ, denník oznámení o trestnej činnosti, denník kontrol, denník petícií, denník sťažností, denník iných podaní, denník ochrany osobných údajov, DVS	obe formy	áno	áno	nie	SKIS MV SR	Zákon č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov, zákon č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov, zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov, zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov, zákon č. 153/2001 Z. z. o prokuratúre v znení neskorších predpisov, zákon č. 9/2010 Z. z. o sťažnostiach v znení neskorších predpisov, zákon č. 85/1990 Zb. o petičnom práve v znení neskorších predpisov, zákon č. 10/1996 Z. z. o kontrole v štátnej správe, zákon č. 307/2014 Z. z. o niektorých opatreniach súvisiacich s oznamovaním protispoločenskej činnosti a o zmene a doplnení niektorých zákonov a ďalšie	áno
--	---	-----------	-----	-----	-----	------------	--	-----

zhromažďovanie, uchovávanie, spracovávanie a poskytovanie meritórnych rozhodnutí, návrhov a uznesení vydaných na úseku trestného konania	IS databáza meritórnych rozhodnutí	obe formy	áno	áno	nie	SKIS MV SR	Zákon č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov, zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov, zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov, zákon č. 153/2001 Z. z. o prokuratúre v znení neskorších predpisov...	áno
Na účely trestného konania, výkon rozhodnutí v trestnom konaní, predchádzania a odhaľovania trestnej činnosti, podklady k skvalitneniu personálneho výberu	IS Poznatkový fond	obe formy	áno	áno	nie	SKIS MV SR	Zákon č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov, zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov...	áno
<b>Menné zoznamy a počty členov ústredného krízového štábu</b>	MS Excel, MS Word	obe formy	nie	nie	nie	Sekcia krízového riadenia MV SR	Uznesenie Vlády SR č. 186 z 26.marca 2008 k návrhu na zmenu štatútu ústredného krízového štábu	nie
<b>Menné zoznamy a počty členov krízového štábu Ministerstva vnútra SR</b>	MS Excel, MS Word	obe formy	nie	nie	nie	Sekcia krízového riadenia MV SR	Nariadenie Ministerstva vnútra SR č. 110/2014 z 23.októbra 2014 o zriadení krízového štábu Ministerstva vnútra SR a o zmene nariadenia Ministerstva vnútra SR č. 42/2004 o zriadení a zložení poradných orgánov ministra vnútra SR a ktorým sa dopĺňa	nie



							nariadenie Ministerstva vnútra SR č. 18/2003 o zriadení krízových štábov v znení nariadenia Ministerstva vnútra SR č. 12/2004 v znení neskorších predpisov	
<b>Informačný systém evidencie záznamov o registrovaných pracovných úrazoch zamestnancov MVSR</b>	žiadne	písomná	nie	nie	nie	Sekcia krízového riadenia MV SR	zákony č. 122/2013 Z. z., 125/2006 Z. z., 124/2006 Z. z., N MV SR č. 135/2014, vyhl. MZ SR č. 500/2006 Z. z.,	áno
<b>Informačný systém IZS - CoordCom - Pomoc v tiesni, ak je ohrozený život, zdravie, majetok alebo životné prostredie</b>	IS IZS	automatizovaná	áno	áno	áno	Sekcia krízového riadenia MV SR	Osobné údaje sa spracúvajú pri poskytovaní pomoci v tiesni, ak je ohrozený život, zdravie, majetok alebo životné prostredie v zmysle zákona č. 129/2002 Z. z. o integrovanom záchrannom systéme, zákon č. 42/1994 o civilnej ochrane, atď.	neaktuálny
<b>Menné zoznamy a počty oslobodených zamestnancov od mimoriadnej a alternatívnej služby vedené v elektronickej podobe</b>	MS word	obe formy	nie	nie	nie	Sekcia krízového riadenia MV SR	zákon č. 570/2005 a 569/2005	chýba

<p><b>Vedenie správy registratúry v integrácii s vybranými špeciálnymi agendovými systémami organizačných útvarov rezortu MV SR</b></p>	<p>Informačný systém FABASOFT Automatizovaná správa registratúry</p>	<p>obe formy</p>	<p>nie</p>	<p>nie</p>	<p>áno</p>	<p>odbor archívov a registratúr SVS MV SR, odborné útvary rezortu MV SR zodpovedné za vecne príslušnú agendu evidovanú v IS Fabasoft</p>	<p>osobitné predpisy: - zákon č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov, - zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (zákon o e-Governmente), - vyhláška MV SR č. 410/2015 Z. z. o podrobnostiach výkonu správy registratúry orgánov verejnej moci a o tvorbe spisu, - nariadenie MV SR č. 98/2016 o registratúrnom poriadku, - nariadenie MV SR č. 22/2012 o používaní informačného systému FABASOFT Automatizovaná správa registratúry, - plnenie úloh vo verejnom záujme alebo pri výkone verejnej moci</p>	<p>áno</p>
---	--	------------------	------------	------------	------------	--	--	------------

<p><b>Využívanie elektronických služieb štátnych archívov a odboru archívov a registratúr SVS MVSR, integrácia s vybranými externými IS a internými agendovými systémami MV SR</b></p>	Informačný systém Elektronický archív MV SR	automatizovaná	nie	nie	nie	odbor archívov a registratúr SVS MV SR	1. Zákon č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov 2. Vyhláška Ministerstva vnútra Slovenskej republiky č. 628/2002 Z. z., ktorou sa vykonávajú niektoré ustanovenia zákona o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov 3. Výnos Ministerstva vnútra Slovenskej republiky č. 525/2011 Z. z. o štandardoch pre elektronické informačné systémy na správu registratúry 4. Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov 5. Vyhláška Úradu na ochranu osobných údajov Slovenskej republiky č. 164/2013 Z. z. o rozsahu a dokumentácii bezpečnostných opatrení 6. 136/2014 Z. z. Úplné znenie zákona č.	áno
--	---	----------------	-----	-----	-----	--	---	-----

							122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov 7. Výnos Ministerstva financií Slovenskej republiky 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy	
<b>Evidencia fyzických osôb v registri obyvateľov</b>	IS REGOB a správne agendy	automatizovaná	nie	nie	áno	oddelenie správy registrov	zákon č. 253/1998 Z. z. o hlásení pobytu občanov Slovenskej republiky a registri obyvateľov Slovenskej republiky v znení neskorších predpisov	neaktuálny
<b>Evidencia fyzických osôb v registri fyzických osôb</b>	IS RFO	automatizovaná	nie	nie	áno	oddelenie správy registrov	zákon č. 253/1998 Z. z. o hlásení pobytu občanov Slovenskej republiky a registri obyvateľov Slovenskej republiky v znení neskorších predpisov	neaktuálny

<b>Evidencia údajov v registri rodných čísel</b>	IS register rodných čísel	automatizovaná	nie	nie	áno	oddelenie správy registrov	Zákon č. 301/1995 Z. z. o rodnom čísle v znení neskorších predpisov	neaktuálny
<b>Evidencia údajov za účelom monitorovania prístupov oprávnených osôb</b>	IS Logcentral	automatizovaná	nie	nie	nie	oddelenie správy registrov	zákon č. 253/1998 Z. z. o hlásení pobytu občanov Slovenskej republiky a registri obyvateľov Slovenskej republiky v znení neskorších predpisov	neaktuálny
<b>Evidencia údajov o pobyte občanov SR</b>	IS CO	obe formy	nie	nie	áno	oddelenie hlásenia pobytu a elektronizácie	osobitný predpis - zákon č. 253/1998 Z.z. o hlásení pobytu občanov Slovenskej republiky a registri obyvateľov Slovenskej republiky	neaktuálny
<b>Evidencia matričných údajov občanov SR</b>	IS CISMA	obe formy	nie	nie	áno	Sekcia verejnej správy, odbor registrov, matrik a hlásenia pobytu, oddelenie matrik	súhlas so spracúvaním OÚ	neaktuálny
<b>Ústredná evidencia nadobudnutia a straty štátneho občianstva SR</b>	APV Win Štátne občianstvo	obe formy	nie	nie	nie	odbor štátneho občianstva, sekcia verejnej správy	zák. NR SR č. 40/1993 Z.z. o štátnom občianstve SR v znení neskorších predpisov (cudzinci, štátni občania SR)	neaktuálny
<b>Register politických strán a politických hnutí</b>	APV REZ Politické strany	automatizovaná	áno	nie	áno	odbor volieb, referenda a politických strán MV SR	zákon č. 85/2005 Z.z. o politických stranách a politických hnutiach v znení neskorších predpisov	áno

<b>Zoznam občianskych združení; evidencia odborových organizácií a organizácií zamestnávateľov</b>	APV REZ	obe formy	áno	nie	nie	odbor všeobecnej vnútornej správy MV SR	zákon č. 83/199 Zb. o združovaní občanov v znení neskorších predpisov	áno
<b>Register združení obcí</b>	APV REZ	obe formy	nie	nie	nie	odbor všeobecnej vnútornej správy MV SR	zákon č. 369/1990 Zb. o obecnom zriadení v znení neskorších predpisov	áno
<b>Register neinvestičných fondov</b>	APV REZ	obe formy	nie	nie	nie	odbor všeobecnej vnútornej správy MV SR	zákon č. 147/1997 Z.z. o neinvestičných fondoch a o doplnení zákona Národnej rady Slovenskej republiky č. 207/1996 Z. z. v znení neskorších predpisov	áno
<b>Register organizácií s medzinárodným prvkom</b>	APV REZ	obe formy	nie	nie	nie	odbor všeobecnej vnútornej správy MV SR	zákon č. 116/1985 Zb. o podmienkach činnosti organizácií s medzinárodným prvkom v Československej socialistickej republike v znení neskorších predpisov	áno
<b>Register nadácií</b>	APV REZ	obe formy	nie	nie	nie	odbor všeobecnej vnútornej správy	zákon č. 34/2002 Z.z. o nadáciách a o zmene Občianskeho zákonníka v znení neskorších predpisov v znení neskorších predpisov	áno
<b>Register neziskových organizácií poskytujúcich všeobecne prospešné služby</b>	APV REZ	obe formy	nie	nie	nie	odbor všeobecnej vnútornej správy MV SR	zákon č. 213/1997 Z.z. o neziskových organizáciách poskytujúcich všeobecne prospešné služby v znení neskorších predpisov	áno

<b>Register záujmových združení právnických osôb</b>	APV REZ	obe formy	nie	nie	nie	odbor všeobecnej vnútornej správy MV SR	zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov v znení neskorších predpisov	áno
<b>Register spoločenstiev vlastníkov bytov a nebytových priestorov</b>	APV REZ	obe formy	nie	nie	nie	odbor všeobecnej vnútornej správy MV SR	zákon č. 182/1993 Z.z. o vlastníctve bytov a nebytových priestorov v znení neskorších predpisov	áno
<b>Register verejných zbierok</b>	RegiZ	obe formy	nie	nie	nie	odbor všeobecnej vnútornej správy MV SR	zákon č. 162/2014 Z. z. o verejných zbierkach a o zmene a doplnení niektorých zákonov	áno
	IS Cezir	obe formy	nie	nie	nie	Sekcia verejnej správy, odbor živnostenského podnikania	§ 45 zákona č. 455/1991 Zb. o živnostenskom podnikaní (živnostenský zákon) v znení neskorších predpisov	nie
<b>Evidencia cudzincov, ktorí neoprávnene prekročili štátnu hranicu alebo majú neoprávnený pobyt.</b>	IS MIGRA	automatizovaná	áno	nie	áno	Úrad hraničnej a cudzineckej polície Prezídia Policajného zboru	Zákon č. 404/2011 Z. z. o pobyte cudzincov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákon č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov	áno
<b>Evidencia cudzincov, ktorým bol odopretý alebo zamietnutý vstup na územie SR.</b>	IS MIGRA	automatizovaná	áno	nie	áno	Úrad hraničnej a cudzineckej polície Prezídia Policajného zboru	Zákon č. 404/2011 Z. z. o pobyte cudzincov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákon č. 171/1993 Z. z. o Policajnom zbore v znení	áno

							neskorších predpisov	
<b>Evidencia cudzincov, ktorí boli riešení útvaram hraničnej a cudzineckej polície v súvislosti s páchaním priestupku alebo trestného činu.</b>	IS MIGRA	automatizovaná	áno	áno	áno	Úrad hraničnej a cudzineckej polície Prezídia Policajného zboru	Zákon č. 404/2011 Z. z. o pobyte cudzincov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákon č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov	áno
<b>Evidencia cudzincov, ktorí boli vrátení na územie SR na základe readmisnej dohody, inej dohody alebo dohovoru.</b>	IS MIGRA	automatizovaná	áno	nie	áno	Úrad hraničnej a cudzineckej polície Prezídia Policajného zboru	Zákon č. 404/2011 Z. z. o pobyte cudzincov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákon č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov	áno
<b>Evidencia nežiaducich osôb - cudzincov</b> - ktorí boli administratívne vyhostení s určením zákazu vstupu, alebo im bol uložený zákaz vstupu; - ktorým bol súdom uložený trest vyhostenia; - ktorým má byť odopretý vstup na územie Slovenskej republiky z bezpečnostných dôvodov a nespádajú do vyššie uvedených kategórií.	IS INBO	automatizovaná	áno	nie	nie	Úrad hraničnej a cudzineckej polície Prezídia Policajného zboru	Zákon č. 404/2011 Z. z. o pobyte cudzincov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákon č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov, zákon č. 300/2005 Z. z. TZ	áno



<p>Evidencia blokovaných osôb, dopravných prostriedkov a vecí na hraničných priechodoch.</p>	<p>IS INBO</p>	<p>automatizovaná</p>	<p>áno</p>	<p>áno</p>	<p>nie</p>	<p>Úrad hraničnej a cudzineckej polície Prezídia Policajného zboru</p>	<p>Zákon č. 404/2011 Z. z. o pobyte cudzincov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov , zákon č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov, zákon č. 301/2005 Z. z. TP</p>	<p>áno</p>
<p>Evidencia cudzincov s povoleným pobytom v zmysle zákona č. 404/2011 Z. z. o pobyte cudzincov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Zmluva č. 441/2008 Z. z. medzi Slovenskou republikou a Ukrajinou o malom pohraničnom styku.</p>	<p>IS ECU</p>	<p>obe formy</p>	<p>nie</p>	<p>nie</p>	<p>nie</p>	<p>Úrad hraničnej a cudzineckej polície Prezídia Policajného zboru</p>	<p>Zákon č. 404/2011 Z. z. o pobyte cudzincov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov</p>	<p>áno</p>
<p>Evidencia o cudzincoch, pre ktorých bolo overené pozvanie a o osobách, ktoré cudzincov pozývajú, o cudzincoch žiadateľoch o víza, o cudzincoch žiadateľoch o pobyt za účelom vykonávania bezpečnostných previerok. Informácie o pozývateľovi a pozývanej osobe, pri ktorej bola podaná žiadosť o overenie pozvania, Informácie o štátnych príslušníkoch tretích krajín,</p>	<p>VIS MV SR</p>	<p>obe formy</p>	<p>nie</p>	<p>nie</p>	<p>áno</p>	<p>Úrad hraničnej a cudzineckej polície Prezídia Policajného zboru</p>	<p>Nariadenie Európskeho parlamentu a Rady (ES) č. 767/2008 o vízovom informačnom systéme (VIS) a výmene údajov o krátkodobých vízach medzi členskými štátmi (nariadenie o VIS)</p>	<p>áno</p>

<p>ktorí sú žiadateľmi o udelenie víza na ZÚ SR, GK SR, na HP alebo na ZÚ iných členských štátov, Informácie o cudzincoch, ktorí sú žiadateľmi o udelenie, predĺženie pobytu na území SR. Uvedené informácie sú spracovávané za účelom vykonávania bezpečnostných previerok.</p>								
<p>Výber, príprava a vysielanie policajtov zahraničnej jednotky Policajného zboru.</p>	<p>MS Excel</p>	<p>obe formy</p>	<p>nie</p>	<p>nie</p>	<p>nie</p>	<p>Úrad hraničnej a cudzineckej polície Prezídia Policajného zboru</p>	<p>Súhlas so spracúvaním OÚ, nariadenie MV SR č. 40/ 2016 o zahraničnej jednotke Policajného zboru, od 7.4.2017 účinné nariadenie MV SR č. 37/2017 o zahraničnej jednotke PZ , Nariadenie Rady (ES) č. 2007/2004 z 26. októbra 2004 o zriadení Európskej agentúry pre riadenie operačnej spolupráce na vonkajších hraniciach členských štátov Európskej únie, od 6.10. 2016 účinné nariadenie Európskeho parlamentu a Rady (EÚ) 2016/1624 o európskej pohraničnej a pobrežnej strážii, ktorým sa mení nariadenie</p>	<p>áno</p>

							Európskeho parlamentu a Rady (EÚ) 2016/399 a ktorým sa zrušuje nariadenie Európskeho parlamentu a Rady (ES) č. 863/2007, nariadenie Rady (ES) č. 2007/2004 a rozhodnutie Rady 2005/267/ES	
<b>centrálne evidencie vyšetrovacích spisov</b>	IS DVS	obe formy	nie	áno	nie	Úrad kriminálnej polície P PZ	zákon NR SR č. 171/1993 Z. z. o PZ v znení neskorších predpisov	neaktuálny
<b>Pátranie po umeleckých predmetoch pochádzajúcich z trestnej činnosti a pátranie po pôvode neznámych nájdených umeleckých predmetov</b>	IS DIELA	automatizovaná	nie	nie	nie	Úrad kriminálnej polície P PZ	zákon NR SR č. 171/1993 Z. z. o PZ v znení neskorších predpisov	nie
<b>pátranie po osobách a veciach</b>	IS PATROS, PATRMV, PATRDOC, PATRBZRANE, PATRVECI	automatizovaná	nie	nie	nie	Úrad kriminálnej polície P PZ	zákon č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov	nie
<b>monitorovanie objektov</b>	IS EMON	automatizovaná	nie	nie	áno	Úrad kriminálnej polície P PZ	zákon č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov	chýba

<b>Eviduje, zhromažďuje a uchováva obrazové a dátové informácie o autentických dokladoch a zistených sfaľovaných a pozmenených dokladoch</b>	IS FADO (Národný informačný systém sfaľovaných a autentických dokladov)	automatizovaná	nie	áno	nie	Úrad kriminálnej polície Prezídia Policajného zboru	Osobitný predpis, zákon NR SR č. 171/1993 Z. z. o PZ v znení neskorších predpisov	nie
<b>Eviduje, zhromažďuje a uchováva obrazové a dátové informácie o výskyte falošných a pozmenených paňazí a platobných kariet</b>	IS FALZO (Informačný systém Evidencia falošných a pozmenených peňazí a platobných kariet)	automatizovaná	nie	áno	nie	Úrad kriminálnej polície Prezídia Policajného zboru	Osobitný predpis, zákon NR SR č. 171/1993 Z. z. o PZ v znení neskorších predpisov	nie
<b>Pátranie po umeleckých predmetoch pochádzajúcich z trestnej činnosti a pátranie po pôvode neznámych nájdených umeleckých predmetov</b>	IS DIELA (Informačný systém evidencia odcudzených a nájdených umeleckých predmetov)	automatizovaná	nie	nie	nie	Úrad kriminálnej polície Prezídia Policajného zboru	Osobitný predpis, zákon NR SR č. 171/1993 Z. z. o PZ v znení neskorších predpisov	nie
<b>Používanie, zhromažďovanie a ukladanie identifikačných údajov o zaistených, vydaných, odňatých, prevzatých a nájdených vozidlách</b>	IS EZVO (Informačný systém evidencia zaistených vozidiel)	automatizovaná	nie	nie	nie	Úrad kriminálnej polície Prezídia Policajného zboru	Osobitný predpis, zákon NR SR č. 171/1993 Z. z. o PZ v znení neskorších predpisov	nie
<b>Medzinárodná výmena operatívnych informácií pri predchádzaní a v boji proti organizovanej a závažnej trestnej činnosti v informačnom systéme UMPS P PZ</b>	IS UMPS	obe formy	áno	áno	nie	Úrad medzinárodnej policajnej spolupráce P PZ	Zákon Národnej rady Slovenskej republiky č. 171/1993 Z.z. o Policajnom zbore v znení neskorších predpisov Nariadenie Európskeho parlamentu a Rady EÚ 2016/794 o Agentúre EÚ pre spoluprácu v oblasti presadzovania práva (Europol)	nie

<b>Výmena informácií v rámci medzinárodnej policajnej spolupráce</b>	IS UMPS modul INTERPOL	obe formy	nie	áno	nie	NÚI ÚMPS PPZ	Zákon Národnej rady Slovenskej republiky č. 171/1993 Z.z. o Policajnom zbore v znení neskorších predpisov	áno
<b>Budapeštiansky dohovor</b>	IS UMPS modul INTERPOL	obe formy	nie	áno	nie	NÚI ÚMPS PPZ	Zákon Národnej rady Slovenskej republiky č. 171/1993 Z.z. o Policajnom zbore v znení neskorších predpisov, Dohovor o počítačovej kriminalite Oznámenie MZV SR č. 137/2008 Z.z Ministerstva zahraničných vecí SR publ. pod č. 137/2008 Z.z.	áno
<b>Medzinárodná výmena informácií v oblasti pátrania po osobách a veciach</b>	IS Medzinárodná policajná spolupráca	automatizovaná	áno	áno	nie	úrad medzinárodnej policajnej spolupráce Prezídia PZ	zákon Národnej rady Slovenskej republiky č. 171/1993 Z.z. o Policajnom zbore v znení neskorších predpisov právne akty k Schengenskému informačnému systému	áno
<b>Medzinárodná výmena informácií v oblasti imigračnej agendy</b>	IS Medzinárodná policajná spolupráca	automatizovaná	áno	áno	nie	úrad medzinárodnej policajnej spolupráce Prezídia PZ	zákon Národnej rady Slovenskej republiky č. 171/1993 Z.z. o Policajnom zbore v znení neskorších predpisov právne akty k Schengenskému informačnému systému	áno

<b>Medzinárodná výmena informácií o pasažieroch</b>	IS Medzinárodná policajná spolupráca	automatizovaná	áno	áno	nie	úrad medzinárodnej policajnej spolupráce Prezídia PZ	Smernica EU, 681/2016, V. Hlava zákona Národnej rady Slovenskej republiky č. 171/1993 Z.z. o Policajnom zbore v znení neskorších predpisov , termín spustenia systému: 25.5.2018	áno
<b>Medzinárodná policajná spolupráca</b>	IS Medzinárodná policajná spolupráca	automatizovaná	áno	áno	nie	úrad medzinárodnej policajnej spolupráce Prezídia PZ	zákon Národnej rady Slovenskej republiky č. 171/1993 Z.z. o Policajnom zbore v znení neskorších predpisov právne akty k Schengenskému informačnému systému bilaterálne zmluvy SR s CZ, RR, PR , MR	áno
<b>Databáza príslušníkov PZ pre mierové misie</b>	excel	automatizovaná	nie	nie	nie	OPPaMM ÚMPS PPZ	N MV SR 42/2018	nie
<b>Zabezpečenie výkonu služby policajtov</b>	IS s názvom tabuľky spojenia	písomná	nie	nie	nie	Úrad pre ochranu ústavných činiteľov a diplomatických misií MV SR	osobitný predpis zák. č. 171/1993 Z. z. o Policajnom zbore, splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi	nie

## Príloha č. 3 – Reakcia na požiadavky dotknutej osoby

Proces reakcie na požiadavky dotknutej osoby musí byť zahrnutý do aktualizácie nariadenia č. 164/2013 o ochrane osobných údajov.

V tomto procese by mali byť zvážené viaceré okolnosti a špecifiká prostredia MV SR, uvádzame návrh jednotlivých krokov, ktoré môžu byť pri definovaní tohto procesu využité:

1. príjem žiadostí dotknutých osôb by mal byť centralizovaný – kontaktovaním vrcholovej zodpovednej osoby MV SR, povinnosť zverejniť kontaktné osoby zodpovednej osoby vyplýva pre prevádzkovateľa priamo zo zákona,
2. zber, evidencia a prvotné vyhodnotenie prijatých žiadostí dotknutých osôb odporúčame realizovať priamo z pozície SKIS, výsledkom posúdenia môže byť napr.:
  - a. zamietnutie žiadosti na základe rozporu so zákonom<sup>15</sup>,
  - b. vybavenie žiadosti na základe centrálnych záznamov o spracovateľských činnostiach a ďalších zdrojoch súvisiacich s osobnými údajmi
3. postúpenie opodstatnených nevybavených žiadostí na gestora konkrétneho účelu spracúvania,
4. pri technickej realizácii naplnenia opodstatnených žiadostí, ktoré si to vyžadujú, môže gestor alebo SKIS vyžadovať súčinnosť SITB,
5. žiadosť dotknutej osoby sa môže vybaviť priamo z pozície gestora, o spôsobe a okolnostiach je však potrebné informovať SKIS, ktorá vyriešenie žiadosti centrálné zaeviduje, prípadne môže byť proces nastavený tak, že všetky žiadosti a spätná komunikácia k žiadateľovi musí ísť vždy výhradne od vrcholovej zodpovednej osoby MV SR.

### Prehľad práv dotknutých osôb podľa jednotlivých paragrafov zákona

Dotknutá osoba má vo všeobecnosti zákonom stanovené viaceré práva, ktoré si môže uplatňovať. Medzi tieto práva patria najmä nasledovné:

#### § 14 Podmienky poskytnutia súhlasu so spracúvaním osobných údajov

Dotknutá osoba má právo kedykoľvek odvolať súhlas so spracovaním osobných údajov, ktoré sa jej týkajú. Odvolanie súhlasu nemá vplyv na zákonnosť spracúvania osobných údajov založeného na súhlase pred jeho odvolaním; pred poskytnutím súhlasu musí byť dotknutá osoba o tejto skutočnosti informovaná. Dotknutá osoba môže súhlas odvolať rovnakým spôsobom, akým súhlas udelila.

<sup>15</sup> na každú, aj neopodstatnenú žiadosť dotknutej osoby je nevyhnutné odpovedať

*§ 19 Poskytované informácie, ak osobné údaje sú získané od dotknutej osoby*  
Prevádzkovateľ je povinný poskytnúť dotknutej osobe pri získavaní osobných údajov priamo od dotknutej osoby informácie v rozsahu tohto paragrafu.

*§ 20 Poskytované informácie, ak osobné údaje nie sú získané od dotknutej osoby*  
Prevádzkovateľ je povinný poskytnúť dotknutej osobe pri získavaní osobných údajov v prípade, že ich nezískal od dotknutej osoby informácie v rozsahu tohto paragrafu.

*§ 21 Právo na prístup k osobným údajom*  
Dotknutá osoba má právo získať od prevádzkovateľa potvrdenie o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú.

*§ 22 Právo na opravu osobných údajov*  
Dotknutá osoba má právo na to, aby prevádzkovateľ bez zbytočného odkladu opravil nesprávne osobné údaje, ktoré sa jej týkajú. So zreteľom na účel spracúvania osobných údajov má dotknutá osoba právo na doplnenie neúplných osobných údajov.

*§ 23 Právo na výmaz osobných údajov*  
Dotknutá osoba má právo na to, aby prevádzkovateľ bez zbytočného odkladu vymazal osobné údaje, ktoré sa jej týkajú podľa podmienok definovaných v tomto paragrafe.

*§ 24 Právo na obmedzenie spracúvania osobných údajov*  
Dotknutá osoba má právo na to, aby prevádzkovateľ obmedzil spracúvanie osobných údajov, ak

- a) dotknutá osoba namieta správnosť osobných údajov, a to počas obdobia umožňujúceho prevádzkovateľovi overiť správnosť osobných údajov,
- b) spracúvanie osobných údajov je nezákonné a dotknutá osoba namieta vymazanie osobných údajov a žiada namiesto toho obmedzenie ich použitia,
- c) prevádzkovateľ už nepotrebuje osobné údaje na účel spracúvania osobných údajov, ale potrebuje ich dotknutá osoba na uplatnenie právneho nároku, alebo
- d) dotknutá osoba namieta spracúvanie osobných údajov podľa § 27 ods. 1, a to až do overenia, či oprávnené dôvody na strane prevádzkovateľa prevažujú nad oprávnenými dôvodmi dotknutej osoby.

*§ 25 Oznamovacia povinnosť v súvislosti s opravou, vymazaním, obmedzením*  
Prevádzkovateľ je povinný oznámiť príjemcovi opravu osobných údajov, vymazanie osobných údajov alebo obmedzenie spracúvania osobných údajov uskutočnené podľa § 22, § 23 ods. 1 alebo § 24, ak sa to neukáže ako nemožné alebo si to nevyžaduje neprimerané úsilie.

Prevádzkovateľ o príjemcoch podľa informuje dotknutú osobu, ak to dotknutá osoba požaduje.



### § 26 Právo na prenosnosť osobných údajov

Dotknutá osoba má právo získať osobné údaje, ktoré sa jej týkajú a ktoré poskytla prevádzkovateľovi, v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte a má právo preniesť tieto osobné údaje ďalšiemu prevádzkovateľovi, ak je to technicky možné a ak:

a) sa osobné údaje spracúvajú podľa § 13 ods. 1 písm. a), § 16 ods. 2 písm. a) alebo § 13 ods. 1 písm. b) a

b) spracúvanie osobných údajov sa vykonáva automatizovanými prostriedkami.

Uplatnením práva uvedeného v odseku 1 nie je dotknuté právo podľa § 23. Právo na prenosnosť sa nevzťahuje na spracúvanie osobných údajov nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi.

### § 27 Právo namietať spracúvanie osobných údajov

Dotknutá osoba má právo namietať spracúvanie jej osobných údajov z dôvodu týkajúceho sa jej konkrétnej situácie vykonávané podľa § 13 ods. 1 písm. e) alebo písm. f) vrátane profilovania založeného na týchto ustanoveniach.

Dotknutá osoba má právo namietať spracúvanie osobných údajov, ktoré sa jej týkajú, z dôvodov týkajúcich sa jej konkrétnej situácie, okrem prípadov, keď je spracúvanie osobných údajov nevyhnutné na plnenie úlohy z dôvodov verejného záujmu, ak sa osobné údaje spracúvajú na vedecký účel, na účel historického výskumu alebo na štatistický účel podľa § 78 ods. 8.

### § 29 Povinnosti prevádzkovateľa pri uplatňovaní práv dotknutej osoby

Prevádzkovateľ je povinný prijať vhodné opatrenia a poskytnúť dotknutej osobe informácie podľa § 19 a 20 a oznámenia podľa § 21 až 28 a 41, ktoré sa týkajú spracúvania jej osobných údajov, v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme, formulované jasne, a to najmä pri informáciách určených osobitne dieťaťu. Informácie je povinný poskytnúť v listinnej podobe alebo elektronickej podobe, spravidla v rovnakej podobe, v akej bola podaná žiadosť. Ak o to požiada dotknutá osoba, informácie môže prevádzkovateľ poskytnúť aj ústne, ak dotknutá osoba preukáže svoju totožnosť iným spôsobom.

Prevádzkovateľ poskytuje súčinnosť dotknutej osobe pri uplatňovaní jej práv podľa § 21 až 28. V prípadoch uvedených v § 18 ods. 2 nemôže prevádzkovateľ odmietnuť konať na základe žiadosti dotknutej osoby pri výkone jej práv podľa § 21 až 28, ak nepreukáže, že dotknutú osobu nie je schopný identifikovať.

### § 30 Obmedzenie práv dotknutej osoby

Prevádzkovateľ alebo sprostredkovateľ môže za podmienok ustanovených osobitným predpisom alebo medzinárodnou zmluvou, ktorou je Slovenská republika viazaná, obmedziť rozsah povinností a práv podľa § 19 až 29 a podľa § 41, ako aj zásady podľa § 6 až 12, ak sa týkajú práv a povinností podľa § 19 až 29, ak je také obmedzenie ustanovené s cieľom zaistiť: (body a) až h).

## **Nasledovné práva dotknutých osôb sú aplikovateľné pri spracúvaní osobných údajov na plnenie úloh na účely trestného konania**

### *§ 60 Informácie, ktoré sa majú sprístupniť alebo poskytnúť dotknutej osobe*

Na postup príslušných orgánov pri spracúvaní osobných údajov na plnenie úloh na účely trestného konania sa vzťahuje § 29 rovnako.

### *§ 61 Právo na prístup k osobným údajom*

Dotknutá osoba má právo získať od príslušného orgánu potvrdenie o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú, a ak to tak je, má právo získať prístup k týmto osobným údajom a informácie o:

- a) účele spracúvania osobných údajov a právnom základe spracúvania osobných údajov,
- b) kategórii spracúvaných osobných údajov,
- c) príjemcovi alebo kategórii príjemcov, ktorým boli alebo majú byť osobné údaje poskytnuté, najmä o príjemcovi v tretej krajine alebo o medzinárodnej organizácii,
- d) dobe uchovávanía osobných údajov, ak to nie je možné, informáciu o kritériách jej určenia,
- e) práve žiadať od príslušného orgánu opravu osobných údajov týkajúcich sa dotknutej osoby alebo ich vymazanie alebo obmedzenie spracúvania osobných údajov alebo práve namietať spracúvanie osobných údajov,
- f) kontaktných údajoch úradu,
- g) práve podať návrh na začatie konania podľa § 100,
- h) zdroji osobných údajov, ak sú dostupné.

### *§ 62 Právo na opravu, vymazanie a obmedzenie osobných údajov*

Dotknutá osoba má právo na to, aby príslušný orgán bez zbytočného odkladu opravil nesprávne osobné údaje, ktoré sa jej týkajú. So zreteľom na účel spracúvania osobných údajov má dotknutá osoba právo na doplnenie neúplných osobných údajov.

Dotknutá osoba má právo na to, aby príslušný orgán bez zbytočného odkladu vymazal osobné údaje, ktoré sa jej týkajú podľa podmienok definovaných v tomto paragrafe.

Namiesto vymazania príslušný orgán obmedzí spracúvanie osobných údajov, ak:

- a) dotknutá osoba napadla správnosť osobných údajov a ich správnosť alebo nesprávnosť nemožno určiť, alebo
- b) osobné údaje sa musia zachovať na účely dokazovania.

### *§ 63 Obmedzenie poskytnutia informácií a práv dotknutej osoby*

Dotknutá osoba má právo získať od príslušného orgánu potvrdenie o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú.

---

Pre vybavenie žiadosti resp. podaní dotknutej osoby musí byť preto zadefinovaný explicitný proces. Podľa nariadenia č.164/2013 o ochrane osobných údajov je proces aktuálne stanovený, v rámci aktualizácie uvedeného nariadenia však bude tento proces nevyhnutné aktualizovať.

## Príloha č. 4 – Posúdenie vplyvu na ochranu osobných údajov (DPIA)

Ak typ spracúvania osobných údajov, najmä s využitím nových technológií a s ohľadom na povahu, rozsah, kontext a účel spracúvania osobných údajov, môže viesť k vysokému riziku pre práva fyzických osôb, prevádzkovateľ je povinný pred spracúvaním osobných údajov vykonať posúdenie vplyvu plánovaných spracovateľských operácií na ochranu osobných údajov. Pre súbor podobných spracovateľských operácií, ktoré predstavujú podobné vysoké riziko, postačí jedno posúdenie. Jeho úlohou je aj prispieť k riadeniu rizík pre práva fyzických osôb vyplývajúcich zo spracúvania osobných údajov. V rámci výkonu posúdenia sa tieto riziká identifikujú, posúdia a určia sa opatrenia na ich pokrytie.

Posúdenie vplyvu je nová zákonná požiadavka, ktorá bola v predchádzajúcom znení zákona na ochranu osobných údajov čiastočne riešená prostredníctvom bezpečnostného projektu. Podľa zákona č. 18/2018 Z.z. sa posúdenie vplyvu na ochranu osobných údajov sa vyžaduje najmä, ak ide o:

- a) systematické a rozsiahle hodnotenie osobných znakov alebo charakteristík týkajúcich sa dotknutej osoby, ktoré je založené na automatizovanom spracúvaní osobných údajov vrátane profilovania a z ktorého vychádzajú rozhodnutia s právnymi účinkami týkajúcimi sa dotknutej osoby alebo s podobne závažným vplyvom na ňu,
- b) spracúvanie vo veľkom rozsahu osobitných kategórií osobných údajov podľa § 16 ods. 1 alebo osobných údajov týkajúcich sa uznania viny za spáchanie trestného činu alebo priestupku podľa § 17, alebo
- c) systematické monitorovanie verejne prístupných miest vo veľkom rozsahu.

V tomto zozname nie sú uvedené všetky prípady. V prostredí MV SR môžu existovať spracovateľské operácie s vysokým rizikom, ktoré nie sú v tomto zozname uvedené, ale predstavujú podobne vysoké riziko, a teda vyžadujú si posúdenie vplyvu. Ďalšie prípady spracovateľských operácií, ktoré podliehajú posúdeniu vplyvu na ochranu osobných údajov a postup pri posudzovaní vplyvu na ochranu osobných údajov podľa zákona ustanoví všeobecne záväzný právny predpis, ktorý vydá úrad.

Posúdenie vplyvu na ochranu osobných údajov obsahuje najmä:

- a) systematický opis plánovaných spracovateľských operácií a účel spracúvania osobných údajov vrátane uvedenia prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ,
- b) posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu,
- c) posúdenie rizika pre práva dotknutej osoby a
- d) opatrenia na elimináciu rizík vrátane záruk, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany osobných údajov a na preukázanie

súladu s týmto zákonom s prihliadnutím na práva a oprávnené záujmy dotknutej osoby a ďalších fyzických osôb, ktorých sa to týka.

Pri určovaní spracovateľských operácií, ktoré si vyžadujú posúdenie vplyvu na ochranu údajov, by sa podľa usmernenia WP248 malo zvážiť nasledovných deväť kritérií:

1. Hodnotenie alebo pridelovanie bodov vrátane profilovania a predpovedania, najmä z „*aspektov súvisiacich s výkonnosťou dotknutej osoby v práci, jej majetkovými pomermi, zdravím, osobnými preferenciami alebo záujmami, spoľahlivosťou alebo správaním, polohou alebo pohybom*“. Príkladom tohto postupu by mohla byť inštitúcia, ktorá preveruje svojich klientov / občanov prostredníctvom databázy obsahujúcej informácie o praní špinavých peňazí a financovaní terorizmu alebo databázy s informáciami o podvodoch.
2. Automatizované rozhodovanie s právnym alebo podobne závažným účinkom: spracúvanie, ktorého cieľom je prijatie rozhodnutí o dotknutých osobách „s právnymi účinkami týkajúcimi sa fyzickej osoby alebo s podobne závažným vplyvom na ňu“. Spracúvanie môže napríklad viesť k vylúčeniu jednotlivcov alebo k diskriminácii voči nim. Spracúvanie s malým alebo žiadnym vplyvom na jednotlivcov nespĺňa toto špecifické kritérium.
3. Systematické monitorovanie: spracúvanie používané na pozorovanie, monitorovanie alebo kontrolu dotknutých osôb vrátane údajov získaných prostredníctvom sietí alebo „systematického monitorovania verejne prístupných miest“. Tento typ monitorovania je kritériom, pretože osobné údaje sa môžu získavať za okolností, keď dotknuté osoby nemusia vedieť, kto zbiera ich údaje a ako sa budú používať.
4. Citlivé údaje alebo údaje veľmi osobnej povahy: zahŕňa to osobitné kategórie osobných údajov, ako aj osobné údaje týkajúce sa uznania viny za trestné činy a priestupky.
5. Údaje spracúvané vo veľkom rozsahu: v zákone o ochrane údajov sa nevymedzuje, čo predstavuje veľký rozsah. Odporúča sa, aby sa pri posudzovaní toho, či sa spracúvanie vykonáva vo veľkom rozsahu, zvažilo predovšetkým:
  - a) počet dotknutých osôb, ktorých sa to týka, buď ako konkrétne číslo alebo ako podiel relevantnej populácie;
  - b) objem údajov a/alebo rozsah rôznych údajových položiek, ktoré sa spracúvajú;
  - c) dĺžka trvania alebo nemennosť činnosti spracúvania údajov;
  - d) geografický rozsah činnosti spracúvania.
6. Spájanie alebo kombinovanie súborov údajov, napr. údajov pochádzajúcich z dvoch alebo viacerých operácií spracúvania údajov vykonaných na rozdielne účely a/alebo rozličnými prevádzkovateľmi údajov takým spôsobom, ktorý by prekročil rozumné očakávania dotknutej osoby.
7. Údaje týkajúce sa zraniteľných dotknutých osôb: spracúvanie tohto druhu údajov je kritériom z dôvodu zvýšenej nerovnováhy moci medzi dotknutými osobami a prevádzkovateľom, čo znamená, že jednotlivci sa môžu nachádzať v pozícii, že nemôžu jednoduchým spôsobom vyjadriť súhlas so spracúvaním svojich údajov, namietat' voči nemu ani vykonávať svoje práva. Zraniteľné dotknuté osoby môžu

zahŕňať deti (možno ich považovať osoby, ktoré nie sú schopné vedome a na základe uváženia namietat' voči spracúvaniu svojich údajov alebo s ním súhlasiť), zamestnanci, zraniteľnejšie časti obyvateľstva vyžadujúce si osobitnú ochranu (mentálne postihnuté osoby, žiadatelia o azyl, staršie osoby atď.) a v každom prípade také osoby, v súvislosti s ktorými možno identifikovať nerovnováhu vo vzťahu medzi postavením dotknutej osoby a prevádzkovateľa.

8. Inovačné využitie alebo uplatňovanie nových technologických alebo organizačných riešení, napr. kombinácia využitia odtlačkov prstov a rozpoznávania tváří pre lepšiu kontrolu fyzického prístupu atď. GDPR jednoznačne uvádza (v článku 35 ods. 1 a v odôvodneniach 89 a 91), že využitie novej technológie vymedzenej v „súlade s dosiahnutým stavom technologických znalostí“, môže viesť k tomu, že bude potrebné vykonať posúdenie vplyvu na ochranu údajov.
9. Keď samotné spracúvanie bráni dotknutým osobám uplatniť svoje právo alebo využiť službu alebo zmluvu. Zahŕňa to spracovateľské operácie, ktorých cieľom je umožniť, upraviť alebo odmietnuť prístup dotknutých osôb k službe alebo uzavretiu zmluvy.

Vo väčšine prípadov môže prevádzkovateľ predpokladať, že spracúvanie, ktoré spĺňa dve kritéria, bude vyžadovať vykonanie posúdenia vplyvu na ochranu údajov. Čím viac kritérií spracúvanie spĺňa, tým je pravdepodobnejšie, že predstavuje vysoké riziko pre práva dotknutých osôb, a preto si vyžaduje posúdenie vplyvu na ochranu údajov.

V prostredí MV SR je efektívne realizovať posúdenie vplyvov ako súčasť analýzy rizík resp. bezpečnostného projektu daného IS. Pri prijímaní bezpečnostných opatrení a pri posudzovaní vplyvu na ochranu osobných údajov sa postupuje primerane podľa medzinárodných noriem a štandardov bezpečnosti.

## Príloha č. 5 – Prehľad povinností z nového zákona pri aktualizácii nariadenia č. 164/2013

Nariadenie MV SR č. 164/2013 o ochrane osobných údajov je nevyhnutné aktualizovať podľa požiadaviek nového zákona. Pri aktualizácii nariadenia je potrebné zohľadniť:

- zásady spracúvania osobných údajov
  - zahrnutie povinnosti dodržiavať zásadu zákonnosti podľa § 6,
  - zahrnutie povinnosti dodržiavať zásadu obmedzenia účelu podľa § 7,
  - zahrnutie povinnosti dodržiavať zásadu minimalizácie údajov podľa § 8,
  - zahrnutie povinnosti dodržiavať zásadu správnosti podľa § 9,
  - zahrnutie povinnosti dodržiavať zásadu minimalizácie uchovávania podľa § 10,
  - zahrnutie povinnosti dodržiavať zásadu integrity a dôvernosti podľa § 11,
  - zahrnutie povinnosti dodržiavať zásadu zodpovednosti podľa § 12,
  - zahrnutie povinnosti súvisiacich s podmienkami poskytnutia súhlasu so spracúvaním osobných údajov podľa § 14,
  - zahrnutie povinností vyplývajúcich z poskytnutia súhlasu v súvislosti so službami informačnej spoločnosti podľa § 15,
  - zahrnutie zákazu spracúvania osobitných kategórií osobných údajov a výnimiek, kedy je toto spracúvanie možné podľa § 16,
  - zahrnutie procesov súvisiacich so zásadami spracúvania osobných údajov v prípade spracúvania príslušnými orgánmi na plnenie úloh na účely trestného konania podľa § 52 – 58,
- práva dotknutých osôb
  - zahrnutie procesov súvisiacich s právom na informácie pri získavaní OÚ od dotknutej osoby ako aj v prípade, že OÚ nie sú získané od dotknutej osoby podľa § 19 a § 20,
  - zahrnutie procesov súvisiacich s právom na prístup k osobným údajom podľa § 21,
  - zahrnutie procesov súvisiacich s právom na opravu osobných údajov podľa § 22,
  - zahrnutie procesov súvisiacich s právom na výmaz osobných údajov podľa § 23,
  - zahrnutie procesov súvisiacich s právom na obmedzenie spracúvania osobných údajov podľa § 24,
  - zahrnutie procesov súvisiacich s oznamovacou povinnosťou v súvislosti s opravou, vymazaním alebo obmedzením spracúvania podľa § 25,
  - zahrnutie procesov súvisiacich s právom na prenosnosť podľa § 26,
  - zahrnutie procesov súvisiacich s právom namietať spracúvanie podľa § 27,

- zahrnutie procesov súvisiacich s právom na neúčinnosť automatizovaného individuálneho rozhodovania vrátane profilovania podľa § 28,
- zahrnutie procesov súvisiacich s povinnosťami prevádzkovateľa pri uplatňovaní práv dotknutej osoby podľa § 29,
- zahrnutie procesov súvisiacich s obmedzením práv dotknutej osoby podľa § 30,
- zahrnutie procesov súvisiacich s právami dotknutých osôb v prípade spracúvania osobných údajov príslušnými orgánmi na plnenie úloh na účely trestného konania podľa § 59 – 66,
- všeobecné povinnosti prevádzkovateľa a sprostredkovateľa
  - zahrnutie povinnosti prevádzkovateľa prijať náležité technické a organizačné opatrenia podľa paragrafu 31,
  - definovanie pravidiel špecificky navrhutej a štandardnej ochrany OÚ podľa § 32,
  - definovanie pravidiel súvisiacich s využívaním sprostredkovateľov podľa § 34,
  - zahrnutie procesu, na základe ktorého môže sprostredkovateľ spracúvať OÚ len na základe pokynov prevádzkovateľa alebo podľa osobitného predpisu alebo medzinárodnej zmluvy podľa § 36,
  - definovanie procesov súvisiacich s vytváraním záznamov o spracovateľských činnostiach podľa § 37,
  - definovanie procesov súvisiacich s oznamovaním porušenia ochrany OÚ úradu a dotknutej osobe podľa § 40 – 41,
  - definovanie povinnosti realizovať posúdenie vplyvu na ochranu osobných údajov pre IS, ktorým to vyplýva zo zákona podľa § 42,
  - úprava procesov súvisiacich so zodpovednými osobami podľa § 44 – 46,
  - implementácia procesov vyplývajúcich z práv a povinností príslušného orgánu a sprostredkovateľa v prípade spracúvania osobných údajov na plnenie úloh na účely trestného konania podľa § 67 – 72,
- úpravu procesov súvisiacich s prenosom osobných údajov do tretej krajiny alebo medzinárodným organizáciám podľa § 47 – 48,
- zahrnutie procesov súvisiacich s prenosom osobných údajov do tretej krajiny alebo medzinárodnej organizácii v prípade spracúvania osobných údajov príslušnými orgánmi na plnenie úloh na účely trestného konania podľa § 73 – 77,
- osobitné situácie zákonného spracúvania osobných údajov (napr. spracúvanie bez súhlasu dotknutej osoby, na účely informovania verejnosti masovokomunikačnými prostriedkami, spracúvanie osobných údajov zamestnancov, spracúvanie všeobecne použiteľného identifikátora, vedecké, historické, štatistické účely) podľa § 78 a 79,
- definovanie povinností kontrolovanej osoby a oprávnenia kontrolovanej osoby podľa § 94 - 95.



## Príloha č. 6 – Praktické naplnenie požiadaviek na bezpečnosť spracúvania

Pre požiadavky podľa § 39 ods. 1 zákona (bezpečnosť spracúvania) uvádzame príklady ich praktického naplnenia v prostredí IS MV SR:

- a) *pseudonymizácia a šifrovanie osobných údajov*, napr.
  - vyžadovaná pseudonymizácia pri vývoji a testovaní IS,
  - šifrovanie pri prenose sieťou (IPSec, HTTPS), šifrovanie údajov v databáze, šifrovanie údajov na zálohách,
- b) *zabezpečenie trvalej dôverylosti IS*, napr.
  - prístup k údajom iba prostredníctvom vopred definovaných služieb a iba v povolenom rozsahu,
  - ukladanie výhradne na určených zariadeniach IS,
  - zabezpečenie ochrany údajov pri prenose v sieti (napr. kryptografickými prostriedkami),
- c) *zabezpečenie trvalej integrity IS*, napr.
  - vytvorenie údajov alebo ich modifikácia iba prostredníctvom definovaných služieb systému a iba pre schválené subjekty,
  - integrita údajov pri prenose v sieti chránená kryptografickými prostriedkami,
  - realizácia overenia integrity údajov pri integrácii s inými IS (napr. kryptografickou hashovacou funkciou),
- d) *zabezpečenie trvalej dostupnosti IS*, napr.
  - služby dostupné iba pre autorizovaných používateľov podľa definovaných požiadaviek,
  - požiadavky na dostupnosť zapracované do SLA,
  - zdvojené sieťové, hardvérové a softvérové prvky,
  - záložné prevádzkové prostredie,
- e) *zabezpečenie trvalej odolnosti IS*, napr.
  - schopnosť IS pokračovať v poskytovaní služieb aj v situácii, keď je vystavený útoku alebo keď je časť IS vyradená z prevádzky,
- f) *proces obnovy dostupnosti osobných údajov a prístup k nim v prípade fyzického alebo technického incidentu*, napr.
  - procesy obnovy dostupnosti OÚ a súvisiace riadenie kontinuity činností realizované spôsobom, aby bolo možné pokračovať v prevádzke aj v prípade prerušenia bežnej prevádzky, havárie či počas krízovej situácie.
- g) *proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania osobných údajov*, napr.
  - interný audit, externý audit, analýza rizík, bezpečnostný projekt, posúdenie vplyvu na ochranu osobných údajov (DPIA), penetračné testovanie.