

Prehľad povinností prevádzkovateľa vyplývajúcich z nového zákona o ochrane osobných údajov

Obsah

O novom zákone o ochrane osobných údajov a jeho vzťahu ku GDPR	2
Úvod – o dokumente a jeho využití.....	3
Kategorizácia prevádzkovateľov z pohľadu požiadaviek zákona	4
Prioritné povinnosti a úlohy prevádzkovateľa vyplývajúce z regulácií.....	6
1. Komplexné povinnosti prevádzkovateľa vyplývajúce zo zásad spracúvania osobných údajov	8
2. Povinnosti prevádzkovateľa vyplývajúce z podmienok spracúvania osobných údajov	9
3. Povinnosti prevádzkovateľa vyplývajúce z práv fyzických osôb.....	11
4. Priamo uložené povinnosti prevádzkovateľovi v Tretej hlave Druhej časti zákona.....	17
5. Povinnosti prevádzkovateľa pri prenose osobných údajov do tretej krajiny	24
6. Možné povinnosti prevádzkovateľa vyplývajúce zo Štvrtej časti zákona	26
7. Možné povinnosti prevádzkovateľa vyplývajúce zo Piatej časti zákona.....	28
Práva fyzických osôb	32

Vypracoval: RNDr. Michal Danilák, Lewik s.r.o.

© Lewik, Bratislava 2/2018



O novom zákone o ochrane osobných údajov a jeho vzťahu ku GDPR

Zákon bol schválený NR SR a podpísaný prezidentom republiky dňa 19.12.2017. Vyšiel v Zbierke zákonov pod č. 18/2018.¹

Citácia z dôvodovej správy k zákonu²:

„Účelom návrhu zákona o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „návrh zákona“) je dosiahnuť súlad vnútroštátneho právneho poriadku pre oblasť ochrany osobných údajov s Nariadením Európskeho parlamentu a rady (EÚ) č. 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016) (ďalej len „nariadenie“), ktoré vstúpilo do platnosti dňa 24. mája 2016 s dvojročným prechodným obdobím na zosúladienie sa s vnútroštátnymi právnymi poriadkami členských štátov, teda aj právnym poriadkom Slovenskej republiky. Nariadenie sa začne uplatňovať od 25. mája 2018.

Návrhom zákona sa zároveň transponuje Smernica Európskeho parlamentu a rady (EÚ) č. 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 (Ú. v. EÚ L 119, 4.5.2016) (ďalej len „smernica“) do právneho poriadku Slovenskej republiky.

Nariadenie a smernica vytvárajú nový modernizovaný právny rámec ochrany osobných údajov, ktorý má za cieľ zabezpečiť rešpektovanie základných práv a slobôd, predovšetkým práva na ochranu osobných údajov v prostredí nových a stále častejšie používaných informačných a komunikačných technológií a zároveň podporiť posilňovanie a zbližovanie ekonomík členských štátov Európskej únie v rámci vnútorného trhu Európskej únie.

V rámci všeobecnej ochrany osobných údajov predpisovej základne Slovenskej republiky sa bude uplatňovať:

1. pre spracúvanie osobných údajov v rámci činností, ktoré podliehajú právu Európskej únie tak nariadenie, ako aj zákon, s výnimkou 1. časti až 3. časti zákona.
2. pre spracúvanie osobných údajov v rámci činností, ktoré nepodliehajú právu Európskej únie zákon ako celok,
3. pre spracúvanie osobných údajov na účely plnenia trestného konania príslušným orgánom zákon, s výnimkou vybraných ustanovení 3. časti návrhu zákona.“

Je potrebné poznamenať, že v GDPR sú články, ktoré nie sú v našom zákone. Ide najmä o Kapitolu VII GDPR, články 77- 82; z nich najmä článok 79 - Právo na účinný súdny prostriedok nápravy voči prevádzkovateľovi alebo sprostredkovateľovi. Práve článok 79 spolu s článkom 80 vytvára nový, mimoriadne silný mechanizmus možných negatívnych dopadov na prevádzkovateľa.

¹ <https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/18/20180525>

² <https://www.nrsr.sk/web/Default.aspx?sid=zakony/zakon&MasterID=6535>

Úvod – o dokumente a jeho využití

Zhrnutie

Tento dokument je prehľadom povinností a následných úloh prevádzkovateľa³, ktoré vyplývajú z regulácií uvedených v novom zákone o ochrane osobných údajov v rozsahu GDPR (139 regulácií týkajúcich sa prevádzkovateľa uvedených v zákone).

Prehľad pre každú reguláciu uvádza ID regulácie, jej presnú citáciu zo zákona, paragraf / odsek ako aj následne povinnosti a úlohy, ktoré z danej regulácie vyplývajú. Povinnosti a úlohy sú formulované na základe dlhoročných praktických skúseností autora s reguláciami a ich dekompozíciou, implementáciou požiadaviek GDPR u ústredných orgánov štátnej správy aj podnikateľskej sféry.

Väčšina prevádzkovateľov sa týka len časť povinností v závislosti od toho, aké osobné údaje spracúvajú a v akom rozsahu. Preto je potrebné vykonať úvodné posúdenie, ktoré umožní prevádzkovateľovi venovať sa len tým reguláciám, ktoré sa ho týkajú.

Povinnosti a úlohy prevádzkovateľa sú z viacerých oblastí regulácií uvedených v zákone

- Všeobecné povinnosti vyplývajúce zo zásad spracúvania a podmienok spracúvania osobných údajov.
- Povinnosti, ktoré sú mu priamo uložené - najmä v Tretej hlave Druhej časti zákona.
- Povinnosti, ktoré mu vyplývajú zo zákonného napĺňania práv fyzických osôb, ktorých osobné údaje spracúva - práva sú uvedené najmä v Druhej hlave Druhej časti zákona.
- Povinnosti, ktoré mu môžu vyplývať z výkonu činnosti Úradu uvedené v Štvrtej a Piatej časti zákona.
- Povinnosti a úlohy, ktoré mu vyplývajú z praktickej implementácie požiadaviek regulácií (napr. zabezpečiť primerané finančné prostriedky v rámci plánovania, analýza rizík, úprava organizačného poriadku).

Spôsob využitia dokumentu

Tento dokument je možné využiť viacerými spôsobmi:

1. Ako podklad pre vedenie na ilustráciu komplexnosti a zložitosti požiadaviek zákona, k zdôvodneniu potrebných personálnych a finančných zdrojov na zabezpečenie súladu.
2. Ako podklad pre prípravu Akčného plánu alebo realizačných aktivít zabezpečenia súladu s požiadavkami zákona / GDPR.
3. **Ako kontrolný zoznam, či v rámci zabezpečovania súladu sú zohľadnené všetky požiadavky zákona na prevádzkovateľa.**
4. Ako kontrolný zoznam pre odborné útvary, ako sú na tom so zabezpečením súladu.
5. Na otestovanie kompetencií externých subjektov ponúkajúcich plné zabezpečenie súladu so zákonom / GDPR – aby konkretizovali, ako jednotlivé požiadavky zabezpečia.

³ V zmysle ustanovenia § 5 písm. o) sa **prevádzkovateľom** rozumie „každý, kto sám alebo spoločne s inými vymedzí účel a prostriedky spracúvania osobných údajov a spracúva osobné údaje vo vlastnom mene; prevádzkovateľ alebo konkrétne požiadavky na jeho určenie môžu byť ustanovené v osobitnom predpise alebo medzinárodnej zmluve, ktorou je Slovenská republika viazaná, ak takýto predpis alebo táto zmluva ustanovuje účel a prostriedky spracúvania osobných údajov,

Úvodné posúdenie dopadu zákona

- Daný subjekt musí posúdiť, či sa neho vzťahuje zákon.
 - Napr. zákon sa nevzťahuje na spracúvanie osobných údajov fyzickou osobou v rámci výlučne osobnej činnosti alebo domácej činnosti, Slovenskou informačnou službou, Vojenským spravodajstvom, ...
- Ak sa na daný subjekt môže zákon vzťahovať, musí posúdiť, či je prevádzkovateľom v zmysle definície prevádzkovateľa v zákone.
 - To znamená, že musí identifikovať údaje, ktoré spracúva a posúdiť, či medzi nimi nie sú osobné údaje. Táto úloha nie je triviálna, napr. medzi osobnými údajmi môžu byť logy z rôznych zariadení a aplikácií.
 - V novom zákone došlo k rozšíreniu definície osobných údajov, preto je potrebné prehodnotiť, či je po novom prevádzkovateľom alebo nie.
- Ak spracúva osobné údaje, tak posúdi, či je spracovanie vykonávané úplne alebo čiastočne automatizovanými prostriedkami alebo je spracúvanie osobných údajov inými než automatizovanými prostriedkami, ak ide o osobné údaje, ktoré tvoria súčasť informačného systému alebo sú určené na to, aby tvorili súčasť informačného systému.
 - Ak áno, prikróči k ďalšej úlohe – identifikovať, medzi aké kategórie prevádzkovateľov patrí.

Kategorizácia prevádzkovateľov z pohľadu požiadaviek zákona

Niektoré povinnosti vyplývajúce zo zákona sú podmienené – týkajú sa len istej kategórie prevádzkovateľov, niektoré sa týkajú všetkých prevádzkovateľov.

Ak sa má prevádzkovateľ správne kategorizovať, musí spraviť isté úvodné aktivity:

- Posúdiť, či medzi osobnými údajmi nie sú osobitné kategórie osobných údajov.
- Posúdiť, či osobné údaje nie sú prenášané do tretej krajiny alebo k medzinárodnej organizácii.
- Posúdiť, či poskytuje aj služby informačnej spoločnosti.⁴
- Posúdiť, či na spracúvaní osobných údajov sa nepodieľajú aj ďalšie subjekty buď v roli sprostredkovateľa alebo spoločného prevádzkovateľa.
- Posúdiť, či je orgánom verejnej moci (môžu to byť aj súkromné organizácie s prenesenou právomocou).

Dôležité kategórie

1. Prevádzkovateľ, ktorého sídlo, miesto podnikania, organizačná zložka, prevádzkareň alebo trvalý pobyt je na území Slovenskej republiky.
 - a. Prevádzkovateľ, ktorého sídlo, miesto podnikania, organizačná zložka, prevádzkareň alebo trvalý pobyt nie je na území Slovenskej republiky, ale je v mieste, kde sa na základe medzinárodného práva verejného uplatňuje právny poriadok Slovenskej republiky.
 - b. Prevádzkovateľ, ktorého sídlo, miesto podnikania, organizačná zložka, prevádzkareň alebo trvalý pobyt nie je v členskom štáte, pričom spracúvanie osobných údajov súvisí s ponukou tovaru alebo služieb tejto dotknutej osobe na území Slovenskej republiky bez ohľadu na

⁴ Zákon č. 22/2004 Z. z. o elektronickom obchode a o zmene a doplnení zákona č. 128/2002 Z. z. o štátnej kontrole vnútorného trhu vo veciach ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov v znení zákona č. 284/2002 Z. z. v znení neskorších predpisov.

to, či sa od dotknutej osoby vyžaduje platba alebo nie, alebo so sledovaním jej správania na území Slovenskej republiky.

- c. Iný prevádzkovateľ mimo horeuvedených kategórií – netýka sa ho zákon.
2. Prevádzkovateľ, ktorý je Policajným zborom, Vojenskou políciou, Zborom väzenskej a justičnej stráže, Finančnou správou, prokuratúrou a súdom spracúvajúci osobné údaje na účely predchádzania a odhaľovania trestnej činnosti, zisťovania páchatel'ov trestných činov, stíhania trestných činov alebo na účely výkonu rozhodnutí v trestnom konaní vrátane ochrany pred ohrozením verejného poriadku a predchádzania takémuto ohrozeniu.
 3. Prevádzkovateľ, ktorý je orgánom verejnej moci.
 4. Prevádzkovateľ využívajúci služby sprostredkovateľov.
 5. Prevádzkovateľ s prenosom osobných údajov do tretej krajiny alebo k medzinárodnej organizácii.
 6. Prevádzkovateľ ponúkajúci služby informačnej spoločnosti.
 - a. Prevádzkovateľ ponúkajúci služby informačnej spoločnosti aj osobám do 16 rokov.
 7. Prevádzkovateľ spracúvajúci osobitné kategórie osobných údajov.
 - a. Prevádzkovateľ s hromadným spracovaním osobitných kategórií osobných údajov.
 - b. Prevádzkovateľ s hromadným spracovaním osobitných kategórií osobných údajov a vysokou mierou rizika (kvôli posúdeniu vplyvov - DPIA).
 8. Prevádzkovateľ s IS, ktorý zabezpečuje automatizované individuálne rozhodovanie vrátane profilovania.
 9. Zamestnávateľ s menej ako 250 zamestnancami, ak nezahŕňa osobitné kategórie osobných údajov.

Prioritné povinnosti a úlohy prevádzkovateľa vyplývajúce z regulácií

Niektoré z množstva povinností uvedené v nasledujúcom prehľade sú časovo a vecne prioritnejšie ako ostatné. Niektoré organizácie už ich majú možno splnené, ale významná časť subjektov je v počiatočnom štádiu ich riešenia.

Uvádzame odporúčanie na prioritné úlohy pre väčšie organizácie, v ktorých je plnenie požiadaviek zákona komplikovanejšie.

Organizačné úlohy

- Mať podporu vedenia pre potrebné aktivity.
 - o Tento dokument je jedným z nástroj na získanie adekvátnej podpory vedenia.
- Mať vytvorený realizačný tím pre implementáciu požiadaviek zákona.
 - o Tím je odborne zdatný na plnenie požiadaviek zákona (ak nie, využiť aj externé zdroje).
 - o Menovať zodpovednú osobu (DPO), ak je zákonom požadovaná a zabezpečiť jej podmienky výkonu činnosti podľa zákona.
 - o Realizovať potrebné aktivity ako interný projekt s určeným vedúcim projektu.
- Zabezpečiť súčinnosť organizačných jednotiek (napr. prostredníctvom úvodných seminárov).
- Mať vypracovaný Akčný plán pre rok 2018; v ktorom je určené, čo bude dosiahnuté do dňa účinnosti zákona.
- Zabezpečiť na r. 2018 aspoň čiastočné finančné zdroje.
- Plánovať zdroje na r. 2019.
- Nezabudnúť na prípadné metodické usmernenie podriadených organizácií.

Identifikačné aktivity

- Identifikovať doteraz realizované činnosti z pohľadu ochrany osobných údajov (bezpečnostné projekty, evidenčné listy, bezpečnostné mechanizmy, opatrenia a smernice, ...).
- Identifikovať **všetky** IS v organizácii (a následne posudzovať, či sú v nich osobné údaje).
 - o Ak to bolo kedysi vykonané, urobiť review na základe identifikácie všetkých IS, keďže sa rozšírila definícia osobných údajov. Táto úloha je vo veľkých organizáciách netriviálna.
- Identifikovať IS s osobnými údajmi (**nezabúdať na sieťové zariadenia, bezpečnostné a monitorovacie aplikácie s logmi používateľských činností**; ale ani na excelovské tabuľky, ktoré tiež môžu byť IS s osobnými údajmi v zmysle definície IS).
 - o Identifikovať IS s osobitnými kategóriami osobných údajov.
- Identifikovať spracovateľské operácie s osobnými údajmi, dátové toky, kategórie údajov, účely, právne základy a pod. v rozsahu terajších evidenčných listov IS.
- Identifikovať všetkých dodávateľov IS a tretie strany prístupujúce k IS organizácie.
 - o Posúdiť, či niektoré z týchto tretích strán nie sú sprostredkovateľmi.
 - o Ak áno, vstúpiť s nimi do rokovaní ohľadom plnenia povinností zákona.
 - o Dodávateľov osloviť, ako sú na tom ich riešenia / zariadenia / aplikácie z pohľadu požiadaviek GDPR / zákona.
- Identifikovať, či organizácia nie je v roli sprostredkovateľa alebo spoločného prevádzkovateľa (napr. ak sa orgány verejnej správy pripájajú na RIS, Štátnu pokladnicu a iné centralizované IS alebo z nich preberajú údaje).
 - o Ak áno, vstúpiť s prevádzkovateľmi do rokovaní ohľadom plnenia povinností zákona.

Analytické povinnosti

- Identifikovať a analyzovať rozdiel medzi terajším stavom a požiadavkami zákona na základe realizácie identifikačných aktivít - tzv. gap analýza.
- Identifikovať a analyzovať dopady zákona na organizáciu ako celok, chod jednotlivých agend, IS a spracovateľských operácií - tzv. dopadová analýza.
- Vykonať alebo aktualizovať analýzy rizík.
 - o Analýza rizík musí obsahovať aj riziká pre práva fyzických osôb, čo doteraz nebolo bežné.
 - o Bez analýzy rizík nie je možné preukázať primeranosť technických a organizačných opatrení na zabezpečenie ochrany osobných údajov. Toto preukázanie môže byť úradom požadované. Okrem toho je potrebná pre výber vhodných bezpečnostných mechanizmov.
- Ak je vyžadované pre niektoré IS posúdenie vplyvov (DPIA), čím skôr spustiť túto aktivitu.

Informačné povinnosti

- Pripraviť nové agendy súvisiace s informačnými povinnosťami voči fyzickým osobám aj Úradu na ochranu osobných údajov. Agendy sú uvedené v následnom prehľade.
 - o Upraviť organizačný poriadok, ďalšiu riadiacu dokumentáciu.
- V organizáciách s veľkým počtom IS alebo dotknutých osôb technicky riešiť otázku plnenia informačných povinností: **ako efektívne zistiť, v ktorých IS a aké osobné údaje sú o fyzickej osobe vedené** (aj vrátane rôznych excelov a logov zo zariadení a aplikácií).
 - o Pri veľkom počte žiadateľov manuálne riešenie nie je asi priechodné – organizačné jednotky by len preverovali, či žiadatelia nie sú v ich IS.

Technické povinnosti

- U existujúcich IS na základe analýzy rizík a rokovaní s dodávateľmi navrhnúť dodatočné bezpečnostné opatrenia v rámci štandardnej ochrany osobných údajov.
- Rozhodnúť, čo je realizovateľné v rámci danej SLA, čo si vyžaduje zmenové konanie a čo verejné obstarávanie.
- Zabezpečiť zdroje na zmenové konania, prípadne verejné obstarávanie.
- Verejné obstarávania sú časovo náročnejšie, niektoré sa do termínu účinnosti zákona ani nestihnú uzavrieť – preto budú **zostatkové riziká pokryté až po obstaraní a implementácii**.
- U novo nasadzovaných a plánovaných IS vyžadovať ich súlad so zákonom / GDPR; vychádzať aj zo špecificky navrhutej ochrany osobných údajov.
 - o Pri príprave špecifikácie, štúdie uskutočniteľnosti, verejného obstarávania zohľadniť doleuvedené požiadavky zákona.



1. Komplexné povinnosti prevádzkovateľa vyplývajúce zo zásad spracúvania osobných údajov

Tieto povinnosti sú bezpodmienečné - týkajú sa všetkých prevádzkovateľov. Sú komplexné, na ich splnenie je potrebné realizovať množstvo čiastkových aktivít. U týchto povinností sa predpokladá, že sú identifikované všetky IS s osobnými údajmi, spracovateľské operácie a sú posúdené riziká.

ID	Text zákona / regulácia	Vyplývajúce povinnosti a úlohy	§
1.1	Zásada zákonnosti - Osobné údaje možno spracúvať len zákonným spôsobom a tak, aby nedošlo k porušeniu základných práv dotknutej osoby.	P 1.1.1 Zabezpečiť zákonnosť spracúvania osobných údajov (u existujúceho aj pripravovaného spracúvania) – vid' § 13. P 1.1.2 Preveriť, či pri spracúvaní nedochádza k porušeniu základných práv dotknutej osoby. Ak áno, zabezpečiť nápravu alebo ukončiť spracúvanie.	§ 6
1.2	Zásada obmedzenia účelu - Osobné údaje sa môžu získavať len na konkrétne určený, výslovne uvedený a oprávnený účel a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmto účelom; ďalšie spracúvanie osobných údajov na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel, ak je v súlade s osobitným predpisom a ak sú dodržané primerané záruky ochrany práv dotknutej osoby podľa § 78 ods. 8, sa nepovažuje za nezlučiteľné s pôvodným účelom.	P 1.2.1 Posúdiť, či sú osobné údaje získavané len na konkrétne určený, výslovne uvedený a oprávnený účel. Ak nie, zastaviť ich spracúvanie. P 1.2.2 V prípade spracúvania osobných údajov na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel preveriť, či je to v súlade s osobitným predpisom a či sú dodržané primerané záruky ochrany práv dotknutej osoby. Ak nie, zabezpečiť nápravu alebo ukončiť spracúvanie.	§ 7
1.3	Zásada minimalizácie osobných údajov - Spracúvané osobné údaje musia byť primerané, relevantné a obmedzené na nevyhnutný rozsah daný účelom, na ktorý sa spracúvajú.	P 1.3.1 Preveriť, či spracúvané osobné údaje sú primerané, relevantné a obmedzené na nevyhnutný rozsah. Ak nie, zabezpečiť nápravu alebo ukončiť spracúvanie.	§ 8
1.4	Zásada správnosti - Spracúvané osobné údaje musia byť správne a podľa potreby aktualizované; musia sa prijať primerané a účinné opatrenia na zabezpečenie toho, aby sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bez zbytočného odkladu vymazali alebo opravili.	P 1.4.1 Mať nástroje na overenie správnosti osobných údajov a overovať, či sú osobné údaje správne a aktualizované. P 1.4.2 Mať nástroje na opravu alebo výmaz nesprávnych osobných údajov z hľadiska účelu spracúvania.	§ 9
1.5	Zásada minimalizácie uchovávania - Osobné údaje musia byť uchovávané vo forme, ktorá umožňuje identifikáciu dotknutej osoby najneskôr dovtedy, kým je to potrebné na účel, na ktorý sa osobné údaje spracúvajú; osobné údaje sa môžu uchovávať dlhšie, ak sa majú spracúvať výlučne na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel na základe osobitného predpisu a ak sú dodržané primerané záruky ochrany práv dotknutej osoby podľa § 78 ods. 8.	P 1.5.1 Mať určenú dobu pre uchovávanie osobných údajov so zohľadnením účelu ich spracúvania. P 1.5.2 Uchovávať osobné údaje tak, aby bola možná identifikácia dotknutej osoby. P 1.5.3 Ak je potreba uchovávať osobné údaje dlhšie, preveriť, či je to na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel a v súlade s osobitným predpisom a či sú dodržané primerané záruky ochrany práv dotknutej osoby. Ak nie, zabezpečiť nápravu alebo ukončiť spracúvanie.	§ 10



1.6	Zásada integrity a dôvernosti - Osobné údaje musia byť spracúvané spôsobom, ktorý prostredníctvom primeraných technických a organizačných opatrení zaručuje primeranú bezpečnosť osobných údajov vrátane ochrany pred neoprávneným spracúvaním osobných údajov, nezákonným spracúvaním osobných údajov, náhodnou stratou osobných údajov, výmazom osobných údajov alebo poškodením osobných údajov.	P 1.6.1 Posúdiť, či je zaručená primeraná bezpečnosť osobných údajov vrátane ochrany pred neoprávneným spracúvaním osobných údajov, nezákonným spracúvaním osobných údajov, náhodnou stratou osobných údajov, výmazom osobných údajov alebo poškodením osobných údajov. Posúdenie je možné vykonať prostredníctvom analýzy rizík. P 1.6.2 Zabezpečiť primeranú bezpečnosť, ak tak nie je.	§ 11
1.7	Zásada zodpovednosti - Prevádzkovateľ je zodpovedný za dodržiavanie základných zásad spracúvania osobných údajov, za súlad spracúvania osobných údajov so zásadami spracúvania osobných údajov a je povinný tento súlad so zásadami spracúvania osobných údajov na požiadanie úradu preukázať.	P 1.7.1 Zabezpečiť dodržiavanie základných zásad spracúvania osobných údajov a súlad spracúvania osobných údajov so zásadami spracúvania osobných údajov. P 1.7.2 Mať nástroje na overenie, či dodržiavanie a súlad sú aktuálne zabezpečované a pravidelne to overovať (následné udržiavanie súladu). P 1.7.3 Mať pripravené podklady na preukázanie súladu so zásadami spracúvania osobných údajov. P 1.7.3 Povinnosť preukázať súlad so zásadami spracúvania osobných údajov na požiadanie úradu.	§ 12

2. Povinnosti prevádzkovateľa vyplývajúce z podmienok spracúvania osobných údajov

ID	Text zákona / regulácia	Vyplývajúce povinnosti a úlohy	§
2.1	Zákonnosť spracúvania - Spracúvanie osobných údajov je zákonné, ak sa vykonáva na základe aspoň jedného z týchto právnych základov ...	P 2.1.1 Identifikovať všetky IS a príslušné spracovateľské operácie s osobnými údajmi (týka sa to aj IS plánovaných a vyvíjaných). P 2.1.2 Pri identifikácii IS nezabudnúť na zariadenie generujúce logy o činnostiach používateľov (napr. sieťové zariadenia, medicínske prístroje, SW pre monitoring a bezpečnosť). P 2.1.3 Overiť si, či sú pre jednotlivé spracovateľské operácie s osobnými údajmi správne identifikované právne základy. Ak nie, zabezpečiť nápravu alebo ukončiť spracúvanie.	§ 13, ods. (1)
2.2	Spracúvané osobné údaje na základe osobitného zákona možno z informačného systému poskytnúť, preniesť alebo zverejniť len vtedy, ak osobitný zákon ustanovuje účel poskytovania alebo účel zverejňovania, zoznam spracúvaných osobných údajov alebo rozsah spracúvaných osobných údajov, ktoré možno poskytnúť alebo zverejniť, prípadne príjemcov, ktorým sa osobné údaje poskytnú.	P 2.2.1 V prípade aplikácie osobitného zákona si overiť, či ustanovuje účel poskytovania alebo zverejňovania, zoznam spracúvaných osobných údajov alebo rozsah spracúvaných osobných údajov, ktoré možno poskytnúť alebo zverejniť, prípadne príjemcov, ktorým sa osobné údaje poskytnú.	§ 13, ods. (2)
2.3	Ak spracúvanie osobných údajov na iný účel ako na účel, na ktorý boli osobné údaje získané, nie je založené na súhlase dotknutej osoby alebo na osobitnom predpise, prevádzkovateľ na zistenie toho, či je spracúvanie osobných údajov na	P 2.3.1 Povinnosť zohľadniť požiadavky § 13, ak spracúvanie osobných údajov na iný účel ako na účel, na ktorý boli osobné údaje získané, nie je založené na súhlase dotknutej osoby alebo na osobitnom predpise.	§ 13, ods. (3)



	iný účel zlučiteľné s účelom, na ktorý boli osobné údaje pôvodne získané okrem iného musí zohľadniť ...		
2.4	Podmienky poskytnutia súhlasu so spracúvaním osobných údajov - Ak je spracúvanie osobných údajov založené na súhlase dotknutej osoby, prevádzkovateľ je povinný kedykoľvek vedieť preukázať, že dotknutá osoba poskytla súhlas so spracúvaním svojich osobných údajov.	P 2.4.1 Zabezpečiť agendu manažmentu súhlasov a súhlasy dotknutých osôb. P 2.4.2 Vedieť kedykoľvek vedieť preukázať, že dotknutá osoba poskytla súhlas so spracúvaním svojich osobných údajov.	§ 14, ods. (1)
2.5	Ak prevádzkovateľ žiada o udelenie súhlasu na spracovanie osobných údajov dotknutú osobu, tento súhlas musí byť odlišený od iných skutočností a musí byť vyjadrený jasne a v zrozumiteľnej a ľahko dostupnej forme.	P 2.5.1 Povinnosť mať súhlas odlišený od iných skutočností a vyjadrený jasne a v zrozumiteľnej a ľahko dostupnej forme.	§ 14, ods. (2)
2.6	Podmienky poskytnutia súhlasu v súvislosti so službami informačnej spoločnosti - Prevádzkovateľ v súvislosti s ponukou služieb informačnej spoločnosti spracúva osobné údaje na základe súhlasu dotknutej osoby zákonne, ak dotknutá osoba dovŕšila 16 rokov veku. Ak má dotknutá osoba menej ako 16 rokov, takéto spracúvanie osobných údajov je zákonné iba za podmienky a v rozsahu, v akom takýto súhlas poskytol alebo schválil jej zákonný zástupca.	P 2.6.1 Overiť si v súvislosti s ponukou služieb informačnej spoločnosti, či dotknutá osoba dovŕšila 16 rokov veku. P 2.6.2 Ak má osoba menej ako 16 rokov, zabezpečiť agendu a súhlas od zákonného zástupcu.	§ 15, ods. (1)
2.7	Prevádzkovateľ je povinný vynaložiť primerané úsilie, aby si overil, že zákonný zástupca dotknutej osoby poskytol alebo schválil súhlas so spracúvaním osobných údajov podľa odseku 1, pričom zohľadní dostupnú technológiu.	P 2.7.1 Vybrať vhodnú technológiu alebo postup na overenie si, či zákonný zástupca dotknutej osoby poskytol alebo schválil súhlas so spracúvaním osobných údajov. P 2.7.2 Implementovať vybranú technológiu / postup pre overenie. P 2.7.3 Vedieť preukázať vynaloženie primeraného úsilia.	§ 15, ods. (2)
2.8	Spracúvanie osobitných kategórií osobných údajov - Zakazuje sa spracúvanie osobitných kategórií osobných údajov. Osobitnými kategóriami osobných údajov sú 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.	P 2.8.1 Posúdiť, či prevádzkovateľ spracúva aj osobitné kategórie osobných údajov. P 2.8.2 Pri posudzovaní je potrebné mať prehľad spracovávaných osobných údajov v jednotlivých IS. Stačí, ak niekde v personálnej agende sú posudky týkajúce sa zdravotného stavu – už je tu osobitná kategória.	§ 16, ods. (1)
2.9	Zákaz spracúvania osobitných kategórií osobných údajov neplatí, ak je splnená aspoň jedna z podmienok § 16, ods. (2).	P 2.9.1 Ak prevádzkovateľ spracúva osobitné kategórie osobných údajov, posúdiť, či existuje právny základ pre jednotlivé spracovateľské operácie.	§ 16, ods. (2)
2.10	Spracúvanie týkajúcich sa uznania viny za spáchanie trestného činu alebo priestupku - Spracúvať osobné údaje týkajúce sa uznania viny za spáchanie trestného činu alebo priestupku alebo súvisiacich bezpečnostných opatrení možno len na základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je	P 2.10.1 Posúdiť, či prevádzkovateľ spracúva túto kategóriu osobných údajov. P 2.10.2 Ak áno, posúdiť, či spĺňa na spracovanie zákonné podmienky.	§ 17



	Slovenská republika viazaná, ktoré poskytujú primerané záruky ochrany práv dotknutej osoby.		
2.11	Spracúvanie osobných údajov bez potreby identifikácie - (1) Ak si účel, na ktorý prevádzkovateľ spracúva osobné údaje, vyžaduje alebo vyžadoval od prevádzkovateľa, aby identifikoval dotknutú osobu, prevádzkovateľ nie je povinný uchovávať, získať alebo spracúvať dodatočné informácie na zistenie totožnosti dotknutej osoby výlučne na to, aby dosiahol súlad s týmto zákonom. (2) Ak v prípadoch uvedených v odseku 1 prevádzkovateľ vie preukázať, že dotknutú osobu nie je schopný identifikovať, je povinný ju o tom primeraným spôsobom informovať, ak je to možné. V takýchto prípadoch sa § 21 až 26 neuplatňujú okrem toho, ak dotknutá osoba na účel vykonania svojich práv podľa uvedených ustanovení poskytne dodatočné informácie umožňujúce jej identifikáciu.	P 2.11.1 Posúdiť, či prevádzkovateľ spracúva osobné údaje bez potreby identifikácie. P 2.11.2 Zabezpečiť agendu a informovať dotknutú osobu, ak je to možné.	§ 18

3. Povinnosti prevádzkovateľa vyplývajúce z práv fyzických osôb

Právo fyzickej osoby zakladá povinnosti pre prevádzkovateľa, ktorý osobné údaje danej osoby spracúva.

ID	Text zákona / regulácia	Vyplývajúce povinnosti a úlohy	§
3.1	Dotknutá osoba má právo kedykoľvek odvolať súhlas so spracovaním osobných údajov, ktoré sa jej týkajú. Odvolanie súhlasu nemá vplyv na zákonnosť spracúvania osobných údajov založenom 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.	P 3.1.1 Zabezpečiť agendu a splnenie skutočností vyplývajúcich z odvolaného súhlasu. P 3.1.2 Informovať pred poskytnutím súhlasu osobu o skutočnosti, že Odvolanie súhlasu nemá vplyv na zákonnosť spracúvania osobných údajov založenom na súhlase pred jeho odvolaním. P 3.1.3 Zabezpečiť, aby dotknutá osoba vedela súhlas odvolať rovnakým spôsobom akým súhlas udelila.	§ 14, ods. (3)
3.2	Pri posudzovaní, či bol súhlas poskytnutý slobodne, sa najmä zohľadní skutočnosť, či sa plnenie zmluvy vrátane poskytnutia služby podmieňuje súhlasom so spracúvaním osobných údajov, ktorý nie je na plnenie tejto zmluvy nevyhnutný.	P 3.2.1 Zabezpečiť, aby bol súhlas poskytnutý slobodne. P 3.2.2 Vedieť preukázať, že bol súhlas poskytnutý slobodne.	§ 14, ods. (4)



3.3	Poskytované informácie, ak osobné údaje sú získané od dotknutej osoby - (1) Ak sa od dotknutej osoby získavajú osobné údaje, ktoré sa jej týkajú, je prevádzkovateľ povinný poskytnúť dotknutej osobe pri ich získavaní ...	P 3.3.1 Zabezpečiť agendu a poskytnutie požadovaných informácií dotknutej osobe pri ich získavaní. P 3.3.2 Vedieť preukázať poskytnutie požadovaných informácií dotknutej osobe pri ich získavaní.	§ 19, ods. (1)
3.4	(2) Okrem informácií podľa odseku 1 je prevádzkovateľ povinný pri získavaní osobných údajov poskytnúť dotknutej osobe informácie o ...	P 3.4.1 Zabezpečiť poskytnutie ďalších požadovaných informácií dotknutej osobe pri ich získavaní. P 3.4.2 Vedieť preukázať poskytnutie požadovaných informácií dotknutej osobe pri ich získavaní.	§ 19, ods. (2)
3.5	(3) Prevádzkovateľ je povinný poskytnúť dotknutej osobe pred ďalším spracúvaním osobných údajov informácie o inom účele a ďalšie relevantné informácie podľa odseku 2, ak má prevádzkovateľ v úmysle ďalej spracúvať osobné údaje na iný účel ako ten, na ktorý boli získané.	P 3.5.1 Zabezpečiť poskytnutie požadovaných informácií dotknutej osobe pri ich získavaní na iné účely. P 3.5.2 Vedieť preukázať poskytnutie požadovaných informácií dotknutej osobe pri ich získavaní.	§ 19, ods. (3)
3.6	Poskytované informácie, ak osobné údaje nie sú získané od dotknutej osoby - (1) Ak osobné údaje neboli získané od dotknutej osoby, prevádzkovateľ je povinný dotknutej osobe poskytnúť ...	P 3.6.1 Zabezpečiť poskytnutie požadovaných informácií dotknutej osobe, ak osobné údaje nie sú získané od nej. P 3.6.2 Vedieť preukázať poskytnutie požadovaných informácií dotknutej osobe.	§ 20, ods. (1)
3.7	(2) Okrem informácií podľa odseku 1 je prevádzkovateľ povinný poskytnúť dotknutej osobe informácie o ...	P 3.4.1 Zabezpečiť poskytnutie ďalších požadovaných informácií dotknutej osobe, ak osobné údaje nie sú získané od nej P 3.4.2 Vedieť preukázať poskytnutie požadovaných informácií dotknutej osobe.	§ 20, ods. (2)
3.6	Poskytované informácie, ak osobné údaje nie sú získané od dotknutej osoby - (1) Ak osobné údaje neboli získané od dotknutej osoby, prevádzkovateľ je povinný dotknutej osobe poskytnúť ...	P 3.6.1 Zabezpečiť poskytnutie požadovaných informácií dotknutej osobe, ak osobné údaje nie sú získané od nej. P 3.6.2 Vedieť preukázať poskytnutie požadovaných informácií dotknutej osobe.	§ 20, ods. (1)
3.7	(2) Okrem informácií podľa odseku 1 je prevádzkovateľ povinný poskytnúť dotknutej osobe informácie o ...	P 3.7.1 Zabezpečiť poskytnutie ďalších požadovaných informácií dotknutej osobe, ak osobné údaje nie sú získané od nej. P 3.7.2 Vedieť preukázať poskytnutie požadovaných informácií dotknutej osobe.	§ 20, ods. (2)
3.6	(3) Prevádzkovateľ je povinný poskytnúť informácie podľa odsekov 1 a 2 a) najneskôr do jedného mesiaca po získaní osobných údajov, pričom zohľadní konkrétne okolnosti, za ktorých sa osobné údaje spracúvajú, b) najneskôr v čase prvej komunikácie s touto dotknutou osobou, ak sa osobné údaje majú použiť na komunikáciu s dotknutou osobou, alebo c) najneskôr vtedy, keď sa osobné údaje prvýkrát poskytnú, ak sa predpokladá poskytnutie osobných údajov ďalšiemu príjemcovi.	P 3.6.1 Zabezpečiť splnenie zákonných lehôt na poskytnutie požadovaných informácií dotknutej osobe. P 3.6.2 Vedieť preukázať poskytnutie požadovaných informácií dotknutej osobe v zákonných lehotách.	§ 20, ods. (3)
3.7	(4) Prevádzkovateľ je povinný poskytnúť dotknutej osobe pred ďalším spracúvaním osobných údajov informácie o inom účele a ďalšie relevantné informácie podľa odseku 2, ak má prevádzkovateľ v úmysle ďalej spracúvať osobné údaje na iný účel ako ten, na ktorý boli získané.	P 3.7.1 Zabezpečiť poskytnutie požadovaných informácií dotknutej osobe, ak osobné údaje nie sú získané od nej. P 3.7.2 Vedieť preukázať poskytnutie požadovaných informácií dotknutej osobe.	§ 20, ods. (4)



3.8	(5) Odseky 1 až 4 sa neuplatňujú, ak ...	P 3.8.1 Ak prevádzkovateľ neplánuje uplatniť požiadavky odsekov 1 - 4, musí posúdiť oprávnenosť dôvodov tak konať. P 3.8.2 Vedieť preukázať dôvody na neuplatnenie požiadaviek odsekov 1 - 4.	§ 20, ods. (5)
3.9	Právo na prístup k osobným údajom - (1) Dotknutá osoba má právo získať od prevádzkovateľa potvrdenie o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú. Ak prevádzkovateľ takéto osobné údaje spracúva, dotknutá osoba má právo získať prístup k týmto osobným údajom a informácie o ...	P 3.9.1 Zabezpečiť agendu a poskytnutie potvrdenia, či sa spracúvajú údaje o dotknutej osobe. P 3.9.2 Pri veľkom počte IS si to vyžaduje nástroje na identifikáciu príslušných osobných údajov v každom IS. P 3.9.3 Zabezpečiť agendu a prístup k osobným údajom osobe. Pri veľkom počte žiadostí, veľkom počte IS a kombinácii papierového a elektronického spracovania je to komplexná úloha.	§ 21, ods. (1)
3.10	(2) Dotknutá osoba má právo byť informovaná o primeraných zárukách týkajúcich sa prenosu podľa § 48 ods. 2 až 4, ak sa osobné údaje prenášajú do tretej krajiny alebo medzinárodnej organizácii.	P 3.10.1 Zabezpečiť agendu a požadované informácie o zárukách.	§ 21, ods. (2)
3.11	(3) Prevádzkovateľ je povinný poskytnúť dotknutej osobe jej osobné údaje, ktoré spracúva. Za opakované poskytnutie osobných údajov, o ktoré dotknutá osoba požiada, môže prevádzkovateľ účtovať primeraný poplatok zodpovedajúci administratívnym nákladom. Prevádzkovateľ je povinný poskytnúť osobné údaje dotknutej osobe spôsobom podľa jej požiadavky.	P 3.11.1 Zabezpečiť agendu a poskytnutie osobných údajov osobe. P 3.11.2 Pri veľkom počte IS a veľkom počte žiadostí je to netriviálna úloha a vyžaduje si preto nástroje na identifikáciu príslušných osobných údajov v každom IS a ich automatizované poskytnutie.	§ 21, ods. (3)
3.12	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.	P 3.12.1 Zabezpečiť agendu a opravu nesprávnych osobných údajov, prípadne doplnenie neúplných osobných údajov.	§ 22
3.13	Právo na výmaz osobných údajov - (1) Dotknutá osoba má právo na to, aby prevádzkovateľ bez zbytočného odkladu vymazal osobné údaje, ktoré sa jej týkajú. (2) Prevádzkovateľ je povinný bez zbytočného odkladu vymazať osobné údaje, ak dotknutá osoba uplatnila právo na výmaz podľa odseku 1, ak ...	P 3.13.1 Zabezpečiť agendu a vymazanie osobných údajov, prepojiť to s agendou odvolania súhlasov a namietania spracovania osobných údajov. P 3.13.2 Riešiť výmaz osobných údajov zo záloh a situáciu, ak ide o kombinované spracovanie osobných údajov v papierovej a elektronickej podobe.	§ 23, ods. (1) ods. (2)
3.14	(3) Ak prevádzkovateľ zverejnil osobné údaje a je povinný ich podľa odseku 1 vymazať, je zároveň povinný prijať primerané bezpečnostné opatrenia vrátane technických opatrení so zreteľom na dostupnú technológiu a náklady na ich vykonanie, za účelom informovania ostatných prevádzkovateľov, ktorí spracúvajú osobné údaje dotknutej osoby o jej žiadosti, aby títo prevádzkovatelia vymazali odkazy na jej osobné údaje a ich kópie alebo odpisy.	P 3.14.1 Zabezpečiť agendu a informovanosť ostatných prevádzkovateľov, aby vymazali odkazy na osobné údaje dotknutej osoby a ich kópie alebo odpisy. P 3.14.2 Zabezpečiť vhodné technické opatrenia na automatizovanú informovanosť ostatných prevádzkovateľov, ak je táto udalosť vysoko frekvencovaná. Príklad problematických IS sú niektoré základné registre, z ktorých sa robia kópie alebo odpisy množstvom iných IS.	§ 23, ods. (3)
3.15	(4) Odseky 1 a 2 sa neuplatňujú, ak je spracúvanie osobných údajov potrebné na ...	P 3.15.1 Posúdiť, či je možné sa vyhnúť plneniu povinností podľa odseku (1) a (2), keďže táto povinnosť môže byť technicky náročná.	§ 23, ods. (4)



3.16	(1) Dotknutá osoba má právo na to, aby prevádzkovateľ obmedzil spracúvanie osobných údajov, ak ... (2) Ak sa spracúvanie osobných údajov obmedzilo podľa odseku 1, okrem uchovávaní môže osobné údaje prevádzkovateľ spracúvať len so súhlasom dotknutej osoby alebo za účelom uplatnenia právneho nároku, na ochranu osôb alebo z dôvodov verejného záujmu.	P 3.16.1 Minimalizovať možnosť vzniku tejto udalosti, napr. zabezpečením zákonnosti spracúvania. P 3.16.2 Zabezpečiť agendu a obmedzenie spracúvania osobných údajov.	§ 24, ods. (1)
3.17	(3) Dotknutú osobu, ktorej spracúvanie osobných údajov sa obmedzí podľa odseku 1, je prevádzkovateľ povinný informovať pred tým, ako bude obmedzenie spracúvania osobných údajov zrušené.	P 3.17.1 Zabezpečiť informovanosť dotknutej osoby.	§ 24, ods. (3)
3.18	Oznamovacia povinnosť v súvislosti s opravou, vymazaním alebo obmedzením spracúvania osobných údajov - (1) 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. (2) Prevádzkovateľ o príjemcoch podľa odseku 1 informuje dotknutú osobu, ak to dotknutá osoba požaduje.	P 3.18.1 Posúdiť, či si plnenie oznamovacej povinnosti nevyžaduje neprimerané úsilie, alebo je to nemožné. Ak áno, je to potrebné vedieť preukázať. P 3.18.2 Zabezpečiť agendu a plnenie oznamovacích povinností.	§ 25
3.19	Právo na prenosnosť osobných údajov - (1) 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.	P 3.19.1 Posúdiť, či je technicky možné zabezpečiť prenosnosť osobných údajov. Ak nie, je to potrebné vedieť preukázať. P 3.19.2 Zabezpečiť agendu a poskytnutie osobných údajov v prenosnej forme.	§ 26, ods. (1)
3.20	Právo namietat' spracúvanie osobných údajov - (1) Dotknutá osoba má právo namietat' 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. Prevádzkovateľ nesmie ďalej spracúvať osobné údaje, ak nepreukáže nevyhnutné oprávnené záujmy na spracúvanie osobných údajov, ktoré prevažujú nad právami alebo záujmami dotknutej osoby, alebo dôvody na uplatnenie právneho nároku. (4) V súvislosti s používaním služieb informačnej spoločnosti môže dotknutá osoba svoje právo namietat' uplatňovať automatizovanými prostriedkami s použitím technických špecifikácií.	P 3.20.1 Minimalizovať možnosť vzniku tejto udalosti, napr. obmedzením profilovania, preukázaním oprávneného záujmu, právneho nároku. P 3.20.2 Zabezpečiť agendu namietania a zastavenie spracúvania osobných údajov, vrátane automatizovaných prostriedkov namietania.	§ 27, ods. (1) ods. (4)
3.21	(2) Dotknutá osoba má právo namietat' spracúvanie osobných údajov, ktoré sa jej týkajú, na účel priameho marketingu vrátane profilovania v rozsahu, v akom súvisí s priamym marketingom. Ak dotknutá osoba namieta spracúvanie osobných údajov na účel priameho marketingu, prevádzkovateľ ďalej osobné údaje na účel priameho marketingu nesmie spracúvať.	P 3.21.1 Zabezpečiť agendu a zastavenie spracúvania osobných údajov na účel priameho marketingu.	§ 27, ods. (2)



3.22	(3) Prevádzkovateľ je povinný dotknutú osobu výslovne upozorniť na práva podľa odsekov 1 a 2 najneskôr pri prvej komunikácii s ňou, pričom informácia o tomto práve musí byť uvedená jasne a oddelene od akýchkoľvek iných informácií.	P 3.22.1 Zabezpečiť upozornenie dotknutej osoby výslovne na práva, najvhodnejšie v rámci jednej agendy plnenia informačných / oznamovacích povinností.	§ 27, ods. (3)
3.23	Automatizované individuálne rozhodovanie vrátane profilovania - (1) 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.	P 3.23.1 Minimalizovať možnosť vzniku tejto udalosti, napr. obmedzením profilovania založenom výlučne na automatizovanom spracúvaní osobných údajov P 3.23.2 Zabezpečiť agendu a právo fyzickej osoby na vylúčenie z rozhodnutia automatizovaného profilovania.	§ 28, ods. (1)
3.24	(2) Odsek 1 sa neuplatňuje, ak je rozhodnutie ... (3) V prípadoch podľa odseku 2 písm. a) a c) je prevádzkovateľ povinný vykonať vhodné opatrenia na ochranu práv a oprávnených záujmov dotknutej osoby, a to najmä práva na overenie rozhodnutia nie automatizovaným spôsobom zo strany prevádzkovateľa, práva vyjadriť svoje stanovisko a práva napadnúť rozhodnutie.	P 3.24.1 Zabezpečiť agendu a vykonať vhodné opatrenia na ochranu práv a oprávnených záujmov dotknutej osoby , a to najmä práva na overenie rozhodnutia nie automatizovaným spôsobom zo strany prevádzkovateľa, práva vyjadriť svoje stanovisko a práva napadnúť rozhodnutie.	§ 28, ods. (2) ods. (3)
3.25	Osobitné povinnosti prevádzkovateľa - (1) 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.	P 3.25.1 Pri plnení horeuvedených informačných agend použiť informácie v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme, formulované jasne, a to najmä pri informáciách určených osobitne dieťaťu. P 3.25.2 Zabezpečiť informačné agendy aj listinnej podobe, prípadne ústne.	§ 29, ods. (1)
3.26	(2) 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.	P 3.26.1 Zabezpečiť súčinnosť dotknutej osobe pri uplatňovaní jej práv v rámci horeuvedených informačných agend.	§ 29, ods. (2) ods. (3)
3.27	(3) Prevádzkovateľ je povinný poskytnúť dotknutej osobe informácie o opatreniach, ktoré sa prijali na základe jej žiadosti podľa § 21 až 28, do jedného mesiaca od doručenia žiadosti. Uvedenú lehotu môže prevádzkovateľ v odôvodnených prípadoch s ohľadom na komplexnosť a počet žiadostí predĺžiť o ďalšie dva mesiace, a to aj opakovane. Prevádzkovateľ je povinný informovať o každom takomto predĺžení dotknutú osobu do jedného mesiaca od doručenia žiadosti spolu s dôvodmi predĺženia lehoty. Ak dotknutá osoba podala žiadosť v elektronickej podobe, prevádzkovateľ poskytne informácie v elektronickej podobe, ak dotknutá osoba nepožiadala o poskytnutie informácie iným spôsobom.	P 3.27.1 Zabezpečiť informačné povinnosti do jedného mesiaca od doručenia žiadosti. P 3.27.2 V prípade predĺženého termínu informovať dotknutú osobu.	§ 29, ods. (3)
3.28	(4) Ak prevádzkovateľ neprijme opatrenia na základe žiadosti dotknutej osoby, je povinný do jedného mesiaca od doručenia žiadosti, informovať dotknutú osobu o dôvodoch nekonania a o možnosti podať návrh podľa § 100 na úrad.	P 3.28.1 V prípade neprijatia opatrenia na základe žiadosti dotknutej osoby, informovať dotknutú osobu.	§ 29, ods. (4)



3.29	(5) Informácie podľa § 19 a 20 a oznámenia a opatrenia prijaté podľa § 21 až 28 a 41 sa poskytujú bezodplatne. Ak je žiadosť dotknutej osoby zjavne neopodstatnená alebo neprimeraná, najmä pre jej opakujúcu sa povahu, prevádzkovateľ môže a) požadovať primeraný poplatok zohľadňujúci administratívne náklady na poskytnutie informácií alebo primeraný poplatok zohľadňujúci administratívne náklady na oznámenie alebo primeraný poplatok zohľadňujúci administratívne náklady na uskutočnenie požadovaného opatrenia, alebo b) odmietnuť konať na základe žiadosti. (6) Zjavnú neopodstatnenosť žiadosti alebo neprimeranosť žiadosti preukazuje prevádzkovateľ.	P 3.29.1 Nastaviť informačné agendy tak, aby boli bezodplatné, ale finančne a časovo čo najmenej náročné. P 3.29.2 V rámci informačných agend mať k dispozícii postup na identifikáciu zjavnej neopodstatnenosti alebo neprimeranosti žiadosti. P 3.29.3 Vedieť preukázať zjavnú neopodstatnenosť žiadosti alebo neprimeranosť žiadosti.	§ 29, ods. (5) ods. (6)
3.30	(7) Prevádzkovateľ môže požiadať o poskytnutie dodatočných informácií potrebných na potvrdenie totožnosti dotknutej osoby, ak má oprávnené pochybnosti o totožnosti fyzickej osoby, ktorá podáva žiadosť podľa § 21 až 27; ustanovenie § 18 tým nie je dotknuté.	P 3.30.1 Rozhodnúť o primeraných opatreniach na potvrdenie totožnosti dotknutej osoby. <i>Je potrebné si uvedomiť, že hackerovi nie je problém elektronicky vystupovať v mene inej osoby a žiadať osobné údaje.</i> P 3.30.2 Zabezpečiť agendu a výkon overovania totožnosti dotknutej osoby.	§ 29, ods. (7)
3.31	(8) Informácie, ktoré sa majú poskytnúť dotknutej osobe podľa § 19 a 20, možno podať v kombinácii so štandardizovanými ikonami s cieľom poskytnúť dobre viditeľný, jasný a zrozumiteľný prehľad zamýšľaného spracúvania osobných údajov. Štandardizované ikony musia byť strojovo čitateľné, ak sú použité v elektronickej podobe. (9) Informácie, ktoré majú byť obsiahnuté v štandardizovaných ikonách a postupy určovania štandardizovaných ikon, ustanoví všeobecne záväzný právny predpis, ktorý vydá úrad.	P 3.31.1 Zabezpečiť štandardizované ikony pri elektronickom poskytovaní informácií.	§ 29, ods. (8) ods. (9)
3.32	Obmedzenie práv dotknutej osoby - (1) 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 ...	P 3.32.1 Posúdiť, či existuje právny základ pre obmedzenie práv dotknutej osoby a v akom rozsahu je aplikovateľný.	§ 30, ods. (1)
3.33	Právo na náhradu škody a zodpovednosť - (1) Každá osoba, ktorej vznikla majetková ujma alebo nemajetková ujma v dôsledku porušenia tohto zákona, má právo na náhradu škody od prevádzkovateľa alebo sprostredkovateľa. (2) Prevádzkovateľ, ktorý sa zúčastnil na spracúvaní osobných údajov, je zodpovedný za škodu spôsobenú nezákonným spracúvaním.	P 3.33.1 Minimalizovať riziko vzniku majetkovej alebo nemajetkovej ujmy pre osobu. Vychádzať najmä z posúdenia rizík pre práva dotknutých osôb. P 3.33.2 Zabezpečiť agendu a riešenie požadovaných náhrad za škodu od fyzickej osoby.	§ 38, ods. (1) ods. (2)
3.34	(3) Prevádzkovateľ sa môže zbaviť zodpovednosti podľa odseku 2, ak preukáže, že vznik škody nevznikol.	P 3.34.1 Mať k dispozícii podklady a nástroje, ktorými môže prevádzkovateľ preukázať, že škodu nevznikol (napr. logy z prístupu k osobným údajom, primerané bezpečnostné opatrenia).	§ 38, ods. (3)
3.35	(4) Ak sa na tom istom spracúvaní osobných údajov zúčastnil viac než jeden prevádzkovateľ alebo sprostredkovateľ alebo prevádzkovateľ aj sprostredkovateľ	P 3.35.1 Riešiť so spoločnými prevádzkovateľmi a sprostredkovateľmi zodpovednosť za možnú budúcu škodu – napr. vyjasniť si podiely zodpovednosti za prípadné škody.	§ 38, ods. (4) ods. (5)



	spoločne a sú podľa odsekov 2 a 3 zodpovední za škodu spôsobenú spracúvaním osobných údajov, za škodu zodpovedajú spoločne a nerozdielne. (5) Ak prevádzkovateľ alebo sprostredkovateľ v súlade s odsekom 4 uhradil náhradu škody v plnej výške, má právo žiadať od ostatných prevádzkovateľov alebo sprostredkovateľov zapojených do toho istého spracúvania osobných údajov tú časť náhrady škody, ktorá zodpovedá ich podielu zodpovednosti za škodu za podmienok ustanovených v odseku 2.	P 3.35.2 V prípade požiadaviek na náhradu škody vstúpiť do jednaní so spoločnými prevádzkovateľmi a sprostredkovateľmi s cieľom minimalizovať dopad škody na svoju organizáciu.	
--	--	---	--

4. Priamo uložené povinnosti prevádzkovateľovi v Tretej hlave Druhej časti zákona

ID	Text zákona / regulácia	Vyplývajúce povinnosti a úlohy	§
4.1	(1) S ohľadom na povahu, rozsah, a účel spracúvania osobných údajov a na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva fyzickej osoby je prevádzkovateľ povinný prijať vhodné technické a organizačné opatrenia na zabezpečenie a preukázanie toho, že spracúvanie osobných údajov sa vykonáva v súlade s týmto zákonom. Uvedené opatrenia je prevádzkovateľ povinný podľa potreby aktualizovať. (2) Opatrenia podľa odseku 1 zahŕňajú zavedenie primeraných postupov ochrany osobných údajov zo strany prevádzkovateľa, ak je to vzhľadom na spracovateľské činnosti primerané.	P 4.1.1 Prijat' a implementovať vhodné technické a organizačné opatrenia na zabezpečenie a preukázanie toho, že spracúvanie osobných údajov sa vykonáva v súlade s týmto zákonom. Táto povinnosť je veľmi netriviálna a náročná, nakoľko je otázne, čo sú vhodné a primerané technické opatrenia a postupy (u organizačných je to jasnejšie). Kľúčom k rozhodnutiu o technických opatreniach je analýza rizík. P 4.1.3 Pred prijatím vhodných opatrení realizovať analýzu rizík alebo ju aktualizovať (ak bola kedysi realizovaná napr. ako súčasť bezpečnostného projektu). P 4.1.3 Aktualizovať opatrenia podľa potreby. <i>Opäť vágne definovaná povinnosť; ale je potrebné zdôvodniť, ak došlo k porušeniu zákona – prečo neboli opatrenia aktualizované (napr. sa objavil nový zero-day attack alebo zraniteľnosť).</i>	§ 31, ods. (1) ods. (2)
4.2	(3) Na preukázanie splnenia povinností podľa odseku 1 môže prevádzkovateľ použiť schválený kódex správania podľa § 85 alebo certifikát podľa § 86.	P 4.2.1 Rozhodnúť sa, či sa bude preukazovať splnenie povinností kódexom správania alebo certifikátom. P 4.2.2 Ak sa bude preukazovať kódexom správania, tak k nemu pristúpiť a implementovať jeho požiadavky. P 4.2.3 Ak sa bude preukazovať certifikátom, tak spustiť prípravu certifikačného procesu, výber certifikačnej autority a následne samotnú certifikáciu.	§ 31, ods. (3)
4.3	(4) Prevádzkovateľ je povinný pravidelne preverovať trvanie účelu spracúvania osobných údajov a po jeho splnení bez zbytočného odkladu zabezpečiť výmaz osobných údajov; to neplatí, ak osobné údaje sú súčasťou registratúrneho záznamu.	P 4.3.1 Zabezpečiť agendu a pravidelné preverovanie trvania účelu spracúvania dotknutej osoby. P 4.3.2 Zabezpečiť bez zbytočného odkladu zabezpečiť výmaz osobných údajov.	§ 31, ods. (4)



4.4	(5) Prevádzkovateľ zabezpečuje vyradenie registratúrneho záznamu, ktorý obsahuje osobné údaje, podľa osobitného predpisu.	P 4.4.1 Zabezpečiť agendu a vyrad'ovanie registratúrnych záznamov, ktoré obsahujú osobné údaje.	§ 31, ods. (5)
4.5	Špecificky navrhnutá a štandardná ochrana osobných údajov - (1) Prevádzkovateľ je povinný pred spracúvaním osobných údajov zaviesť a počas spracúvania osobných údajov mať zavedenú špecificky navrhnutú ochranu osobných údajov, ktorá spočíva v prijatí primeraných technických a organizačných opatrení, najmä vo forme pseudonymizácie, na účinné zavedenie primeraných záruk ochrany osobných údajov a dodržiavanie základných zásad podľa § 6 až 12.	P 4.5.1 Zabezpečiť určenie primeraných technických a organizačných opatrení a následnú implementáciu špecificky navrhutej ochrany osobných údajov. P 4.5.2 Zabezpečiť, aby požiadavky na špecificky navrhnutú ochranu osobných údajov boli zahrnuté už štádiu špecifikácie požiadaviek na nový IS a pri jeho obstarávaní.	§ 32, ods. (1)
4.6	(2) Prevádzkovateľ je povinný pri špecificky navrhutej ochrane osobných údajov podľa odseku 1 zohľadniť najnovšie poznatky ochrany osobných údajov, náklady na vykonanie opatrení podľa odseku 1, povahu, rozsah, kontext a účel spracúvania osobných údajov a riziká spracúvania osobných údajov s rôznou pravdepodobnosťou a závažnosťou, ktoré spracúvanie osobných údajov predstavuje pre práva dotknutej osoby.	P 4.6.1 Zabezpečiť posúdenie povahy, rozsahu, kontextu a účelu spracúvania osobných údajov, následne rizík v prvej fáze prípravy špecificky navrhutej ochrany, potom zohľadniť najnovšie poznatky ochrany osobných údajov, náklady na vykonanie opatrení podľa odseku 1.	§ 32, ods. (2)
4.7	(3) Prevádzkovateľ je povinný zaviesť štandardnú ochranu osobných údajov, ktorá spočíva v prijatí primeraných technických a organizačných opatrení na zabezpečenie spracúvania osobných údajov len na konkrétny účel, minimalizácie množstva získaných osobných údajov a rozsahu ich spracúvania, doby uchovávania a dostupnosti osobných údajov. Prevádzkovateľ je povinný zabezpečiť, aby osobné údaje neboli bez zásahu fyzickej osoby štandardne prístupné neobmedzenému počtu fyzických osôb.	P 4.7.1 Zabezpečiť určenie primeraných technických a organizačných opatrení a následnú implementáciu štandardne navrhutej ochrany osobných údajov. P 4.7.2 Zabezpečiť, aby požiadavky na štandardne navrhnutú ochranu osobných údajov boli zahrnuté v požiadavkách na dodávku IS. P 4.7.3 Zabezpečiť, aby osobné údaje neboli bez zásahu fyzickej osoby štandardne prístupné neobmedzenému počtu fyzických osôb.	§ 32, ods. (3)
4.8	(4) Na preukázanie splnenia povinností podľa odsekov 1 až 3 môže prevádzkovateľ použiť certifikát podľa § 86.	P 4.8.1 Rozhodnúť, či sa využije certifikát na preukázanie splnenia povinností. P 4.8.2 Ak áno, zabezpečiť certifikačný proces. <i>S ohľadom na vágnosť pojmu „primerané opatrenia“ sa javí využitie certifikátu ako vhodný prístup.</i>	§ 32, ods. (4)
4.9	Spoloční prevádzkovatelia - (1) Spoločnými prevádzkovateľmi sú dvaja prevádzkovatelia alebo viacerí prevádzkovatelia, ktorí si dohodou určia účel a prostriedky spracúvania osobných údajov. V dohode sú zároveň povinní transparentne určiť zodpovednosť každého z nich za plnenie povinností a úloh podľa tohto zákona, najmä ak ide o vykonávanie práv dotknutej osoby, a svoje povinnosti poskytovať informácie podľa § 19 a 20, ak nie sú tieto povinnosti prevádzkovateľa ustanovené osobitným predpisom alebo medzinárodnou zmluvou, ktorou je Slovenská republika viazaná. V dohode sa tiež určí kontaktné miesto pre dotknutú osobu.	P 4.9.1 Zistiť, či organizácia v rámci niektorého IS nie je v roli spoločného prevádzkovateľa (napr. ak ide o veľké štátne IS). P 4.9.2 Ak áno, pripraviť alebo aktualizovať existujúcu dohodu s určením účelu a prostriedkov spracúvania osobných údajov, rozdelenie zodpovednosti, kontaktné miesto.	§ 33, ods. (1)



4.10	(2) Základné náležitosti dohody podľa odseku 1 je prevádzkovateľ povinný poskytnúť dotknutej osobe, a to najmä identifikáciu zmluvných strán, predmet zmluvy, dobu platnosti zmluvy, ustanovenia upravujúce výkon práv dotknutej osoby, povinnosti prevádzkovateľov poskytovať informácie podľa § 19 a 20 a kontaktné miesto pre dotknutú osobu.	P 4.10.1 Poskytnúť základné náležitosti dohody podľa odseku 1 dotknutým osobám.	§ 33, ods. (2)
4.11	Sprostredkovateľ - (1) Ak sa má spracúvanie osobných údajov uskutočniť v mene prevádzkovateľa, prevádzkovateľ môže poveriť len sprostredkovateľa, ktorý poskytuje dostatočné záruky na prijatie primeraných technických a organizačných opatrení tak, aby spracúvanie osobných údajov spĺňalo požiadavky tohto zákona a aby sa zabezpečila ochrana práv dotknutej osoby. Na poverenie sprostredkovateľa spracúvaním osobných údajov podľa prvej vety sa súhlas dotknutej osoby nevyžaduje.	P 4.11.1 Rozhodnúť o tom, či budú sa na spracovaní podieľať aj sprostredkovatelia. P 4.11.1 Ak áno - overiť si, či vybraný sprostredkovateľ poskytuje dostatočné záruky na prijatie primeraných technických a organizačných opatrení tak, aby spracúvanie osobných údajov spĺňalo požiadavky tohto zákona a aby sa zabezpečila ochrana práv dotknutej osoby	§ 34, ods. (1)
4.12	(2) Sprostredkovateľ nesmie poveriť spracúvaním osobných údajov ďalšieho sprostredkovateľa bez predchádzajúceho osobitného písomného súhlasu prevádzkovateľa alebo všeobecného písomného súhlasu prevádzkovateľa. Sprostredkovateľ je povinný vopred informovať prevádzkovateľa o poverení ďalšieho sprostredkovateľa, ak sa poverenie vykonalo na základe všeobecného písomného súhlasu.	P 4.12.1 Overiť si, či sprostredkovateľ, nepoveril spracúvaním osobných údajov ďalšieho sprostredkovateľa bez predchádzajúceho osobitného písomného súhlasu prevádzkovateľa alebo všeobecného písomného súhlasu prevádzkovateľa. P 4.12.2 Ak áno, riešiť vzniknutý stav.	§ 34, ods. (2)
4.13	(3) Spracúvanie osobných údajov sprostredkovateľom sa riadi zmluvou alebo iným právnym úkonom, ktorý zaväzuje sprostredkovateľa voči prevádzkovateľovi a v ktorom je ustanovený predmet a doba spracúvania, povaha a účel spracúvania, zoznam alebo rozsah osobných údajov, kategórie dotknutých osôb a povinnosti a práva prevádzkovateľa. V zmluve alebo inom právnom úkone sa musí najmä ustanoviť, že sprostredkovateľ je povinný ...	P 4.13.1 Zabezpečiť zmluvu so sprostredkovateľom, alebo aktualizovať už existujúcu zmluvu tak, aby mala náležitosti v zmysle nového zákona.	§ 34, ods. (3)
4.14	(4) Sprostredkovateľ je povinný bez zbytočného odkladu informovať prevádzkovateľa, ak má za to, že sa pokynom prevádzkovateľa porušuje tento zákon, osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, ktoré sa týkajú ochrany osobných údajov.	P 4.13.1 Zabezpečiť, aby sprostredkovateľ bez zbytočného odkladu informoval prevádzkovateľa, ak má za to, že sa pokynom prevádzkovateľa porušuje tento zákon, osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, ktoré sa týkajú ochrany osobných údajov.	§ 34, ods. (4)
4.15	(5) Ak sprostredkovateľ zapojí do vykonávania osobitných spracovateľských činností v mene prevádzkovateľa ďalšieho sprostredkovateľa, tomuto ďalšiemu sprostredkovateľovi v zmluve alebo iného právneho úkonu je povinný uložiť rovnaké povinnosti týkajúce sa ochrany osobných údajov ako sú ustanovené v zmluve alebo v inom právnom úkone medzi prevádzkovateľom a sprostredkovateľom podľa odseku 3, a to najmä poskytnutie dostatočných záruk na prijatie primeraných technických a organizačných opatrení tak, aby spracúvanie osobných údajov spĺňalo požiadavky tohto zákona.	P 4.13.1 Zabezpečiť, aby v prípade zapojenie ďalšieho sprostredkovateľa primárny sprostredkovateľ v zmluve uložil rovnaké povinnosti týkajúce sa ochrany osobných údajov ako sú ustanovené v zmluve alebo v inom právnom úkone medzi prevádzkovateľom a sprostredkovateľom. <i>Napr. vyžiadanim si zmluvy pred udelením súhlasu na ďalšieho sprostredkovateľa.</i>	§ 34, ods. (5)
4.16	(8) Sprostredkovateľ, ktorý porušil tento zákon tým, že určí účel a prostriedky spracúvania osobných údajov, sa považuje v súvislosti s týmto spracúvaním osobných údajov za prevádzkovateľa; ustanovenie § 38 a § 104 až 106 tým nie je dotknuté.	P 4.13.1 Zabezpečiť, aby sa organizácia v roli sprostredkovateľa nechtiac nestala prevádzkovateľom.	§ 34, ods. (8)



4.17	Zástupca prevádzkovateľa alebo zástupca sprostredkovateľa - (1) Prevádzkovateľ alebo sprostredkovateľ, ktorý nemá sídlo, organizačnú zložku, prevádzkareň alebo trvalý pobyt v členskom štáte, je povinný písomne poveriť svojho zástupcu na území členského štátu, ak vykonáva spracúvanie osobných údajov dotknutej osoby, ktorá sa nachádza na území Slovenskej republiky, pričom spracovateľská činnosť súvisí ...	P 4.17.1 Zabezpečiť si a písomne poveriť zástupcu, ak ide o prevádzkovateľa, ktorý nemá sídlo, organizačnú zložku, prevádzkareň alebo trvalý pobyt v členskom štáte.	§ 35, ods. (1)
4.18	(3) Úrad a dotknutá osoba môžu požadovať informácie týkajúce sa spracúvania osobných údajov na účely zabezpečenia súladu s týmto zákonom okrem prevádzkovateľa a sprostredkovateľa aj zástupcu prevádzkovateľa alebo zástupcu sprostredkovateľa.	P 4.18.1 Zabezpečiť poskytnutie požadovaných informácií úradu a dotknutej osobe.	§ 35, ods. (3)
4.19	Spracúvanie osobných údajov pod dohľadom prevádzkovateľa alebo sprostredkovateľa - Sprostredkovateľ a každá osoba konajúca za prevádzkovateľa alebo sprostredkovateľa, ktorá má prístup k osobným údajom, môže spracúvať tieto osobné údaje len na základe pokynov prevádzkovateľa alebo podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná.	P 4.19.1 Zabezpečiť pokyny pre sprostredkovateľa a každú osobu konajúcu za prevádzkovateľa alebo sprostredkovateľa, ktorá má prístup k osobným údajom.	§ 36
4.20	Záznamy o spracovateľských činnostiach - (1) Prevádzkovateľ a zástupca prevádzkovateľa, ak bol poverený, je povinný viesť záznam o spracovateľských činnostiach, za ktoré je zodpovedný. Tento záznam musí obsahovať ...	P 4.20.1 Najprv je potrebné mať identifikované všetky IS s osobnými údajmi a spracovateľské činnosti s nimi súvisiace. P 4.20.2 Zabezpečiť agendu, vypracovať a následne viesť záznamy o spracovateľských činnostiach.	§ 37, ods. (1)
4.21	(2) Sprostredkovateľ a zástupca sprostredkovateľa, ak bol poverený, je povinný viesť záznam o kategóriách spracovateľských činností, ktoré vykonal v mene prevádzkovateľa. Tento záznam musí obsahovať ...	P 4.21.1 Overiť si, či sprostredkovateľ vedie záznam o kategóriách spracovateľských činností, ktoré vykonal v mene prevádzkovateľa v požadovanej štruktúre.	§ 37, ods. (2)
4.22	(4) Prevádzkovateľ alebo sprostredkovateľ a zástupca prevádzkovateľa alebo zástupca sprostredkovateľa, ak bol poverený, sú povinní na požiadanie sprístupniť záznam o spracovateľských činnostiach úradu.	P 4.22.2 Mať pripravené záznamy o spracovateľských činnostiach a sprístupniť ich úradu na požiadanie.	§ 37, ods. (4)
4.23	Bezpečnosť spracúvania - (1) Prevádzkovateľ a sprostredkovateľ sú povinní prijať so zreteľom na najnovšie poznatky, na náklady na vykonanie opatrení, na povahu, rozsah, kontext a účel spracúvania osobných údajov a na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva fyzických osôb primerané technické a organizačné opatrenia na zaistenie úrovne bezpečnosti primeranej tomuto riziku, pričom uvedené opatrenia môžu zahŕňať najmä a) pseudonymizáciu a šifrovanie osobných údajov, b) zabezpečenie trvalej dôverylosti, 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.	P 4.23.1 Identifikovať riziká pre práva fyzických osôb. <i>V doterajších analýzach rizík sa riziká pre práva osôb príliš nezohľadňovali, pretože neboli identifikované ako významné aktívum. Preto aj existujúce analýzy rizík je potrebné aktualizovať.</i> P 4.23.2 Rozhodnúť o rozsahu využitia pseudonymizácie a šifrovania. P 4.23.3 Rozhodnúť o spôsobe zabezpečenia trvalej dôverylosti, integrity, dostupnosti a odolnosti systémov spracúvania osobných údajov. P 4.23.4 Rozhodnúť o spôsobe zabezpečenia proces obnovy dostupnosti osobných údajov a prístup k nim v prípade fyzického incidentu alebo technického incidentu. P 4.23.5 Zabezpečiť adekvátne personálne a finančné zdroje na implementáciu opatrení. P 4.23.6 V prípade využitia externých subjektov pripraviť a realizovať obstaranie požadovaných tovarov a služieb.	§ 39, ods. (1)



		P 4.23.7 Zabezpečiť primerané technické a organizačné opatrenia na zaistenie úrovne bezpečnosti primeranej rizikám. P 4.23.8 Mať pripravené všetky podklady pre preukázanie prijatých opatrení.	
4.24	(2) 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.	P 4.24.1 V rámci identifikácie rizík zohľadniť aj riziká ako sú náhodné 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.	§ 39, ods. (2)
4.25	(3) Súlad s požiadavkami uvedenými v odseku 1 možno preukázať schváleným kódexom správania podľa § 85 alebo certifikátom podľa § 86.	P 4.25.1 Rozhodnúť, či bude prevádzkovateľ spĺňať podmienky kódexu správania, alebo získa certifikát. P 4.25.2 Využitie kódexu alebo certifikátu si vyžaduje spustenie prípravy na ich získanie, zdroje a čas. V rámci tejto prípravy aj tak bude potrebné posúdiť riziká.	§ 39, ods. (3)
4.26	(4) Prevádzkovateľ a sprostredkovateľ sú povinní zabezpečiť, aby fyzická osoba konajúca za prevádzkovateľa alebo sprostredkovateľa, ktorá má prístup k osobným údajom, spracúvala tieto údaje len na základe pokynov prevádzkovateľa alebo podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná.	P 4.26.1 Vypracovať pokyny k spracúvaniu osobných údajov. P 4.26.2 Preniesť pokyny prevádzkovateľa ku konajúcim fyzickým osobám. P 4.26.3 Mať k dispozícii nástroje, aby bolo možné overiť, že fyzická osoba konajúca za prevádzkovateľa, ktorá má prístup k osobným údajom, spracúva tieto údaje len na základe pokynov prevádzkovateľa alebo podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná.	§ 39, ods. (4)
4.27	Oznámenie porušenia ochrany osobných údajov úradu - (1) Prevádzkovateľ je povinný oznámiť úradu porušenie ochrany osobných údajov do 72 hodín po tom, ako sa o ňom dozvedel; to neplatí, ak nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva fyzickej osoby. (4) Oznámenie podľa odseku 1 musí obsahovať najmä ... (5) Prevádzkovateľ je povinný poskytnúť informácie podľa odseku 4 v rozsahu v akom sú mu známe v čase oznámenia podľa odseku 1; ak v čase oznámenia podľa odseku 1 nie sú prevádzkovateľovi známe všetky informácie podľa odseku 4, poskytne ich bezodkladne po tom, čo sa o nich dozvie.	P 4.27.1 Mať k dispozícii nástroje, aby sa prevádzkovateľ dozvedel o prípadnom porušení ochrany osobných údajov skôr ako tretie strany alebo médiá. P 4.27.2 Posúdiť, či narušenie povedie k riziku pre práva fyzickej osoby. P 4.27.3 Zabezpečiť agendu oznámenia a oznámiť do 72 hodín porušenie úradu.	§ 40, ods. (1) ods. (4) ods. (5)
4.28	(2) Ak prevádzkovateľ nespĺní oznamovaciu povinnosť podľa odseku 1, musí zmeškanie lehoty zdôvodniť.	P 4.28.1 Súčasťou agendy oznámenia je aj zdôvodnenie prípadného nesplnenia si oznamovacej povinnosti. P 4.28.2 Zdôvodnenie prípadného zmeškania lehoty.	§ 40, ods. (2)
4.29	(3) Sprostredkovateľ je povinný oznámiť prevádzkovateľovi porušenie ochrany osobných údajov bez zbytočného odkladu po tom, ako sa o ňom dozvedel.	P 4.29.1 Je vhodné v zmluve so sprostredkovateľom mať uvedenú aj túto požiadavku a spôsob jej naplnenia (komu a ako hlásiť). P 4.29.2 Súčasťou agendy oznámenia je aj manažment hlásenia od sprostredkovateľa.	§ 40, ods. (3)



4.30	(6) Prevádzkovateľ je povinný zdokumentovať každý prípad porušenia ochrany osobných údajov podľa odseku 1 vrátane skutočností spojených s porušením ochrany osobných údajov, jeho následky a prijaté opatrenia na nápravu.	P 4.30.1 Zabezpečiť agendu zdokumentovania porušenia a zdokumentovať porušenie. P 4.30.2 V prípade technickej náročnosti zdokumentovania je potrebné zapojiť kvalifikovaný subjekt (napr. súdneho znalca). Je to podstatné najmä pre prípadné následné požiadavky náhrady škody od dotknutých fyzických osôb.	§ 40, ods. (6)
4.31	Oznámenie porušenia ochrany osobných údajov dotknutej osobe - (1) Prevádzkovateľ je povinný bez zbytočného odkladu oznámiť dotknutej osobe porušenie ochrany osobných údajov, ak takéto porušenie ochrany osobných údajov môže viesť k vysokému riziku pre práva fyzickej osoby. (2) Oznámenie podľa odseku 1 musí obsahovať jasne a jednoducho formulovaný opis povahy porušenia ochrany osobných údajov a informácie a opatrenia podľa § 40 ods. 4 písm. b) až d).	P 4.31.1 Posúdiť, či identifikované porušenie ochrany osobných údajov môže viesť k vysokému riziku pre práva fyzickej osoby. Podľa posúdenia postupovať ďalej. P 4.31.2 Zabezpečiť agendu oznámenia a oznámiť porušenie dotknutým osobám bez zbytočného odkladu. P 4.31.3 Uchovať si dokumentáciu k preukázaniu realizácie oznámenia.	§ 41, ods. (1) ods. (2)
4.32	(3) Oznámenie podľa odseku 1 sa nevyžaduje, ak ...	P 4.32.1 Posúdiť, či na identifikované porušenie ochrany osobných údajov možno aplikovať ods. (3) a vyhnúť sa tak povinnosti oznámenia porušenia.	§ 41, ods. (3)
4.33	Posúdenie vplyvu na ochranu osobných údajov - (1) 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.	P 4.33.1 U novo plánovaných, obstarávaných a nasadzovaných IS, u IS s výraznou technologickou zmenou zhodnotiť, či sa na daný systém vzťahuje požiadavka posúdenia vplyvov. <i>V prípade neistoty konzultovať s úradom.</i> P 4.33.2 U prevádzkovaných systémov, ktoré spĺňajú požiadavku vysokého rizika pre práva fyzických osôb, konzultovať s úradom potrebu posúdenia vplyvov. <i>Názor autora tohto dokumentu je, že aj u existujúcich IS s vysokým rizikom je posúdenie vplyvov potrebné vykonať do 25.5.2018.</i>	§ 42, ods. (1)
4.34	(3) 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.	P 4.34.3 Zhodnotiť identifikované IS a posúdiť, či spĺňajú niektorú z požiadaviek ods. (3). V prípade nejasnosti konzultovať s úradom.	§ 42, ods. (3)
4.35	(7) Prevádzkovateľ je povinný posúdiť, či sa spracúvanie osobných údajov uskutočňuje v súlade s posúdením vplyvu na ochranu osobných údajov, a to najmä ak došlo zmene rizika, ktoré predstavuje spracovateľská operácia.	P 4.35.1 Identifikovať zmeny rizika pri spracovateľských operáciách – najmä z dôvodu aplikácie novej technológie alebo formy spracovania, pri nových závažných hrozbách a zraniteľnostiach IS. P 4.35.2 Ak sa týka prevádzkovateľa posúdenie vplyvov (čo musí mať zistené), tak musí následne posúdiť, či sa spracúvanie osobných údajov uskutočňuje v súlade s posúdením vplyvu na ochranu osobných údajov.	§ 42, ods. (7)



4.36	Predchádzajúca konzultácia - (1) Prevádzkovateľ je povinný s úradom uskutočniť konzultáciu pred spracúvaním osobných údajov, ak je z posúdenia vplyvu na ochranu osobných údajov podľa § 42 zrejmé, že spracúvanie osobných údajov povedie k vysokému riziku pre práva fyzických osôb, ak prevádzkovateľ neprijme opatrenia na zmiernenie tohto rizika.	P 4.36.1 Mať identifikované IS s posúdením vplyvu a mieru rizika pre práva fyzických osôb. P 4.36.2 Ak je identifikované vysoké riziko, konzultovať s úradom ešte pred spracúvaním osobných údajov (týka sa to nových IS).	§ 43, ods. (1)
4.37	(3) Počas konzultácií s úradom podľa odseku 1 je prevádzkovateľ povinný poskytnúť úradu ...	P 4.37.1 Poskytnúť úradu požadované informácie počas konzultácie.	§ 43, ods. (3)
4.38	Určenie zodpovednej osoby - (1) Prevádzkovateľ a sprostredkovateľ sú povinní určiť zodpovednú osobu, ak a) spracúvanie osobných údajov <u>vykonáva orgán verejnej moci alebo verejnoprávna inštitúcia</u> okrem súdov pri výkone ich súdnej právomoci, b) hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa sú spracovateľské operácie, ktoré si vzhľadom na svoju povahu, rozsah alebo účel vyžadujú pravidelné a systematické monitorovanie dotknutej osoby vo veľkom rozsahu, alebo c) hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa je spracúvanie osobitných kategórií osobných údajov podľa § 16 vo veľkom rozsahu alebo spracúvanie osobných údajov týkajúcich sa uznania viny za spáchanie trestného činu alebo priestupku podľa § 17 vo veľkom rozsahu.	P 4.38.1 Určiť zodpovednú osobu, ak prevádzkovateľ spĺňa zákonné podmienky alebo je to zmysluplné.	§ 44, ods. (1)
4.39	(2) Skupina podnikov môže určiť jednu zodpovednú osobu, ak táto osoba bude spôsobilá plniť úlohy podľa § 46 pre každý podnik zo skupiny podnikov.	P 4.39.1 Rozhodnúť sa, či podnik chce spoločnú zodpovednú osobu. P 4.39.2 Ak áno, vstúpiť do rokovania v rámci skupiny podnikov a určiť zodpovednú osobu.	§ 44, ods. (2)
4.40	(3) Ak je prevádzkovateľom alebo sprostredkovateľom orgán verejnej moci alebo verejnoprávna inštitúcia, môže byť pre viaceré takéto orgány alebo inštitúcie, určená jedna zodpovedná osoba, pričom sa zohľadní ich rozsah a ich organizačná štruktúra.	P 4.40.1 Rozhodnúť sa, či orgán organizácia chce spoločnú zodpovednú osobu. P 4.40.2 Ak áno, vstúpiť do rokovania s ďalšími organizáciami a určiť zodpovednú osobu.	§ 44, ods. (3)
4.41	(4) Okrem prípadov podľa odseku 1 zodpovednú osobu môže určiť prevádzkovateľ alebo sprostredkovateľ alebo združenia a iné subjekty zastupujúce kategórie prevádzkovateľov alebo sprostredkovateľov. Zodpovedná osoba môže konať v mene takýchto združení a iných subjektov zastupujúcich prevádzkovateľov alebo sprostredkovateľov.	P 4.41.1 Rozhodnúť sa, či daný subjekt chce spoločnú zodpovednú osobu. P 4.41.2 Ak áno, vstúpiť do rokovania s ďalšími subjektami a určiť zodpovednú osobu.	§ 44, ods. (4)
4.42	(5) Okrem prípadov podľa odseku 1 je prevádzkovateľ alebo sprostredkovateľ alebo združenia a iné subjekty zastupujúce kategórie prevádzkovateľov alebo sprostredkovateľov povinný určiť zodpovednú osobu, ak sa to vyžaduje v osobitnom predpise alebo medzinárodnej zmluve, ktorou je Slovenská republika viazaná. Zodpovedná osoba môže konať v mene takýchto združení a iných subjektov zastupujúcich prevádzkovateľov alebo sprostredkovateľov.	P 4.42.1 Identifikovať, či je povinnosť určiť zodpovednú osobu v osobitnom predpise alebo medzinárodnej zmluve, ak je to relevantné. P 4.42.2 Ak áno, určiť zodpovednú osobu.	§ 44, ods. (5)
4.43	(6) Zodpovedná osoba sa určí na základe jej odborných kvalít, a to najmä na základe jej odborných znalostí práva a postupov v oblasti ochrany osobných údajov a na základe spôsobilosti plniť úlohy podľa § 46.	P 4.43.1 Zabezpečiť, aby zodpovedná osoba mala adekvátne odborné kvality.	§ 44, ods. (6) ods. (7)



	(7) Zodpovedná osoba môže byť zamestnancom prevádzkovateľa alebo sprostredkovateľa alebo môže plniť úlohy na základe zmluvy.	P 4.43.2 Týchto osôb nie je až tak veľa, takže je potrebné si interné osoby vyškoliť a nechať certifikovať, aby bola potrebná miera istoty o jej odbornosti. Inou možnosťou je prijať na zmluvu novú, drahšiu, kvalifikovanú osobu.	
4.44	(8) Prevádzkovateľ a sprostredkovateľ sú povinní zverejniť, napríklad na ich webovom sídle, kontaktné údaje zodpovednej osoby, ak je určená, a oznámiť ich úradu.	P 4.44.1 Zabezpečiť zverejnenie kontaktných údajov zodpovednej osoby, ak je určená, a oznámiť ich úradu.	§ 44, ods. (8)
4.45	Postavenie zodpovednej osoby - (1) Prevádzkovateľ a sprostredkovateľ sú povinní zabezpečiť, aby zodpovedná osoba riadne a včas vykonávala činnosti súvisiace s ochranou osobných údajov. (2) Prevádzkovateľ a sprostredkovateľ sú povinní poskytnúť zodpovednej osobe pri plnení úloh podľa § 46 potrebnú súčinnosť; najmä sú povinní jej poskytnúť prostriedky potrebné na plnenie týchto úloh a prístup k osobným údajom a spracovateľským operáciám, ako aj zabezpečiť udržiavanie jej odborných znalostí. (3) Prevádzkovateľ a sprostredkovateľ sú povinní zabezpečiť, aby zodpovedná osoba v súvislosti s plnením úloh podľa § 46 nedostávala žiadne pokyny. Prevádzkovateľ ani sprostredkovateľ ju nesmú odvolať alebo postihovať za výkon jej úloh podľa § 46. Zodpovedná osoba je pri plnení úloh podľa § 46 priamo zodpovedná štatutárnemu orgánu prevádzkovateľa alebo štatutárnemu orgánu sprostredkovateľa.	P 4.45.1 Vytvoriť zodpovednej osobe podmienky výkonu práce, podľa § 45 a § 46.	§ 45, ods. (1) ods. (2) ods. (3)
4.46	(1) Zodpovedná osoba najmä a) poskytuje informácie a poradenstvo ... (2) Zodpovedná osoba pri výkone svojich úloh náležite zohľadňuje riziko spojené so spracovateľskými operáciami, pričom berie do úvahy povahu, rozsah, kontext a účel spracúvania osobných údajov.	P 4.46.1 Zabezpečiť adekvátnu kvalifikáciu zodpovednej osoby pre výkon činností podľa § 46. P 4.46.2 Zabezpečiť pre zodpovednú osobu podmienky pre plnenie úloh kontaktného miesta. P 4.46.3 Mať realizovanú analýzu rizík, aby zodpovedná osoba mohla náležite zohľadniť riziko.	§ 46, ods. (1) ods. (2)

5. Povinnosti prevádzkovateľa pri prenose osobných údajov do tretej krajiny

Ide o povinnosti podľa Štvrtej hlavy Druhej časti zákona. Časté sú prenosi osobných údajov jednotlivým inštitúciám EÚ, do USA (napr. ak sa pracuje s cloudovými aplikáciami), do susedných členských krajín.



ID	Text zákona / regulácia	Vyplývajúce povinnosti a úlohy	§
5.1	Všeobecná zásada prenosu - Prenos osobných údajov, ktoré sa spracúvajú alebo sú určené na spracúvanie po prenose do tretej krajiny alebo medzinárodnej organizácii, sa môže uskutočniť len vtedy, ak prevádzkovateľ a sprostredkovateľ dodržiavajú podmienky, vrátane podmienok následného prenosu osobných údajov z predmetnej tretej krajiny alebo od predmetnej medzinárodnej organizácie do inej tretej krajiny alebo inej medzinárodnej organizácii.	P 5.1.1. Mať identifikované všetky IS s prenosom osobných údajov do tretích krajín. P 5.1.2 Ak je sprostredkovateľ alebo spoločný prevádzkovateľ z tretej krajiny, mať identifikované všetky podmienky, ktoré musí dodržiavať pre následný prenos. P 5.1.3 Ak ide o sprostredkovateľa, prevádzkovateľ zmluvne upraví aj náležitosti spojené s prenosom.	§ 47
5.2	Prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii (1) Prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii sa môže uskutočniť, ak Komisia rozhodla, že tretia krajina, územie alebo jeden či viaceré určené odvetvia v danej tretej krajine alebo medzinárodná organizácia, zaručujú primeranú úroveň ochrany osobných údajov. Takýto prenos nevyžaduje osobitné povolenie.	P 5.2.1. Mať identifikované krajiny a medzinárodné organizácie, do ktorých sa prenos uskutočňuje. P 5.2.2. Zistiť na stránkach Komisie, či daná krajina alebo medzinárodná organizácia zaručuje primeranú úroveň ochrany osobných údajov.	§ 48, ods. (1)
5.3	(2) Ak neexistuje rozhodnutie Komisie podľa odseku 1, prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii sa môže uskutočniť len vtedy, ak sa poskytnú primerané záruky ochrany osobných údajov. (3) Primerané záruky podľa odseku 2 sa môžu ustanoviť bez toho, aby bolo potrebné žiadať úrad o osobitné povolenie, prostredníctvom ... (4) Primerané záruky podľa odseku 2 sa môžu tiež zabezpečiť na základe povolenia úradu najmä ...	P 5.3.1. Ak nie je daná krajina alebo medzinárodná organizácia na zozname Komisie, zabezpečiť primerané záruky ochrany osobných údajov a až potom umožniť prenos. P 5.3.2 Ak je to možné, na primerané záruky využiť splnenie niektorého z bodov ods. (3). P 5.3.3 Ak to nie je možné, realizovať primerané záruky na základe povolenia úradu.	§ 48 ods. (2) ods. (3) ods. (4)
5.4	Vnútropodnikové pravidlá - (1) Úrad schváli vnútropodnikové pravidlá, ak a) sa vzťahujú sa na každého člena skupiny podnikov alebo zoskupenia podnikov zapojených do spoločnej hospodárskej činnosti vrátane ich zamestnancov, a títo členovia ich uplatňujú, b) sa nimi upravujú vnútorné postupy pre uplatnenie práv dotknutej osoby, ak ide o spracúvanie osobných údajov, a c) splňajú požiadavky podľa odseku 2.	P 5.4.1. Ak je to relevantné, predložiť na schválenie Úradu vnútropodnikové pravidlá splňajúce požiadavky zákona.	§ 49, ods. (1)
5.5	Prenos alebo poskytnutie osobných údajov, ktoré právny poriadok v Slovenskej republike nepovoľuje - Rozhodnutie súdu, rozhodnutie tribunálu alebo rozhodnutie správneho orgánu tretej krajiny, ktoré od prevádzkovateľa alebo sprostredkovateľa vyžaduje preniesť osobné údaje alebo poskytnúť osobné údaje, môže byť uznané alebo vykonateľné len vtedy, ak je v súlade s medzinárodnou zmluvou uzavretou s treťou krajinou, ktorou je Slovenská republika alebo Európska únia viazaná.	P 5.5.1. Ak vznikne požiadavka na prenos, ktorý právny poriadok SR nedovoľuje, posúdiť, či je v súlade s medzinárodnou zmluvou uzavretou s treťou krajinou, ktorou je Slovenská republika alebo Európska únia viazaná.	§ 50
5.6	Výnimky pre osobitné situácie - (1) Ak neexistuje rozhodnutie o primeranosti podľa § 48 ods. 1 ani primerané záruky podľa § 48 ods. 2 až 4 vrátane vnútropodnikových pravidiel, prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii sa môže uskutočniť len vtedy, ak ...	P 5.6.1. Ak vznikne požiadavka na prenos a neexistuje rozhodnutie o primeranosti ani primerané záruky, zabezpečiť splnenie aspoň jedného z bodov ods. (1) § 48.	§ 48, ods. (1)



5.7	(2) Ak prenos nemožno uskutočniť podľa § 48 a nemožno ani uplatniť žiadnu výnimku pre osobitnú situáciu podľa odseku 1, prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii sa môže uskutočniť len vtedy, ak	P 5.7.1. Ak vznikne požiadavka na prenos a nemožno aplikovať žiadnu z predchádzajúcich možností, zabezpečiť splnenie aspoň jedného z bodov ods. (2) § 48.	§ 48 ods. (2)
5.8	(3) Prevádzkovateľ je povinný o prenose podľa odseku 2 vopred informovať úrad. Prevádzkovateľ je okrem poskytnutia informácií podľa § 19 a 20 povinný informovať dotknutú osobu o prenose podľa odseku 2 a o svojich oprávnených záujmoch v lehotách podľa § 19 a 20. Prevádzkovateľ alebo sprostredkovateľ zdokumentujú posúdenie, ako aj vhodné záruky v záznamoch o spracovateľských činnostiach podľa § 37.	P 5.8.1. Ak sa realizuje prenos podľa ods. (2), informovať o prenose Úrad. P 5.8.2. Ak sa realizuje prenos podľa ods. (2), informovať o prenose dotknutú osobu. P 5.8.3. Ak sa realizuje prenos podľa ods. (2), zdokumentovať posúdenie, ako aj vhodné záruky v záznamoch o spracovateľských činnostiach podľa § 37.	§ 48, ods. (3)

6. Možné povinnosti prevádzkovateľa vyplývajúce zo Štvrtej časti zákona

Ide o povinnosti vyplývajúce zo Štvrtej časti zákona týkajúcej sa osobitných situácií. Pre danú osobitnú situáciu je potrebné posúdiť, či sa daného prevádzkovateľa týka.

ID	Text zákona / regulácia	Vyplývajúce povinnosti a úlohy	§
6.1	(1) Prevádzkovateľ môže spracúvať osobné údaje bez súhlasu dotknutej osoby aj vtedy, ak spracúvanie osobných údajov je nevyhnutné na akademický účel, umelecký účel alebo literárny účel; to neplatí, ak spracúvaním osobných údajov na takýto účel prevádzkovateľ porušuje právo dotknutej osoby na ochranu jej osobnosti alebo právo na ochranu súkromia alebo takéto spracúvanie osobných údajov bez súhlasu dotknutej osoby vylučuje osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná.	P 6.1.1. Ak je to relevantné - posúdiť, či dané spracúvanie osobných údajov je nevyhnutné na akademický účel, umelecký účel alebo literárny účel a zároveň sú splnené aj ďalšie podmienky ods. (1) § 78. P 6.1.2. Vedieť Úradu preukázať, že dané spracúvanie osobných údajov je nevyhnutné na akademický účel, umelecký účel alebo literárny účel.	§ 78
6.2	(2) Prevádzkovateľ môže 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; to neplatí, ak spracúvaním osobných údajov na takýto účel prevádzkovateľ porušuje právo dotknutej osoby na ochranu jej osobnosti alebo právo na ochranu súkromia alebo takéto spracúvanie osobných údajov bez súhlasu dotknutej osoby vylučuje osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná.	P 6.2.1. Ak je to relevantné - posúdiť, či dané spracúvanie osobných údajov je nevyhnutné pre potreby informovania verejnosti masovokomunikačnými prostriedkami a ak osobné údaje spracúva prevádzkovateľ, ktorému to vyplýva z predmetu činnosti a zároveň sú splnené aj ďalšie podmienky ods. (2) § 78. P 6.2.2. Vedieť Úradu preukázať, že dané spracúvanie osobných údajov je nevyhnutné pre potreby informovania verejnosti masovokomunikačnými prostriedkami.	§ 78, ods. (2)



6.3	(3) Prevádzkovateľ, ktorý je zamestnávateľom dotknutej osoby, je oprávnený poskytovať jej osobné údaje alebo zverejniť jej osobné údaje 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, ak je to potrebné v súvislosti s plnením pracovných povinností, služobných povinností alebo funkčných povinností dotknutej osoby. Poskytovanie osobných údajov alebo zverejnenie osobných údajov nesmie narušiť vážnosť, dôstojnosť a bezpečnosť dotknutej osoby.	P 6.3.1. Posúdiť, či aktuálne poskytované alebo zverejnené osobné údaje zamestnanca sú len v rozsahu uvedenom v ods. (3) § 78. P 6.3.2. Ak nie, zabezpečiť, aby boli poskytované alebo zverejnené osobné údaje zamestnanca len v rozsahu uvedenom v ods. (3) § 78. P 6.3.3 Posúdiť, či poskytovanie alebo zverejnenie týchto osobných údajov nenarušuje vážnosť, dôstojnosť a bezpečnosť dotknutej osoby.	§ 78 ods. (3)
6.4	(4) Pri spracúvaní osobných údajov možno využiť na účely identifikovania fyzickej osoby všeobecne použiteľný identifikátor podľa osobitného predpisu len vtedy, ak jeho využitie je nevyhnutné na dosiahnutie daného účelu spracúvania. Súhlas so spracúvaním všeobecne použiteľného identifikátora musí byť výslovný a nesmie ho vylučovať osobitný predpis, ak ide o jeho spracúvanie na právnom základe súhlasu dotknutej osoby. Zverejňovať všeobecne použiteľný identifikátor sa zakazuje; to neplatí, ak všeobecne použiteľný identifikátor zverejní sama dotknutá osoba.	P 6.4.1. Mať identifikované IS, v ktorých sa používa všeobecne použiteľný identifikátor podľa osobitného predpisu. P 6.4.2. Posúdiť, či je jeho využitie je nevyhnutné na dosiahnutie daného účelu spracúvania. Ak nie, nahradiť ho iným identifikátorom. P 6.4.3. Zabezpečiť, aby súhlas so spracúvaním všeobecne použiteľného identifikátora bol výslovný a pritom ho nesmie vylučovať osobitný predpis, ak ide o jeho spracúvanie na právnom základe súhlasu dotknutej osoby. P 6.4.4. Zabezpečiť, aby nebol všeobecne použiteľný identifikátor zverejnený.	§ 78, ods. (4)
6.5	(5) Prevádzkovateľ môže spracúvať genetické údaje, biometrické údaje a údaje týkajúce sa zdravia aj na právnom základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná.	P 6.5.1. Ak je to relevantné - posúdiť, či existuje právny základ pre spracúvanie genetických údajov, biometrických údajov a údajov týkajúcich sa zdravia v osobitnom predpise, alebo v medzinárodnej zmluve.	§ 78 ods. (5)
6.6	(6) Osobné údaje o dotknutej osobe možno získať od inej fyzickej osoby a spracúvať v informačnom systéme len s predchádzajúcim písomným súhlasom dotknutej osoby; to neplatí, ak poskytnutím osobných údajov o dotknutej osobe do informačného systému iná fyzická osoba chráni svoje práva alebo právom chránené záujmy, oznamuje skutočnosti, ktoré odôvodňujú uplatnenie právnej zodpovednosti dotknutej osoby, alebo sa osobné údaje spracúvajú na základe osobitného zákona podľa § 13 ods. 1 písm. c) a e). Ten, kto takéto osobné údaje spracúva, musí vedieť preukázať úradu na jeho žiadosť, že ich získal v súlade s týmto zákonom.	P 6.6.1. Ak je to relevantné - posúdiť, či na poskytnutie osobných údajov od inej osoby nie je potrebný súhlas dotknutej osoby podľa ods. (6) § 78. P 6.6.2. V tomto prípade prevádzkovateľ zabezpečí preukázanie úradu súladu so zákonom pri ich spracovaní.	§ 78, ods. (6)
6.7	(7) Ak dotknutá osoba nežije, súhlas vyžadovaný podľa tohto zákona alebo osobitného predpisu môže poskytnúť jej blízka osoba. Súhlas nie je platný, ak čo len jedna blízka osoba písomne vyslovila nesúhlas.	P 6.7.1. Ak je to relevantné, identifikovať blízku osobu nežijúcej osoby. P 6.7.2. Získať súhlas od dotýčnej osoby. P 6.7.2. Ak iná blízka osoba vysloví nesúhlas, zabezpečiť zrušenie súhlasu.	§ 78 ods. (7)
6.8	(8) Pri spracúvaní osobných údajov na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel je prevádzkovateľ a sprostredkovateľ povinný prijať primerané záruky pre práva dotknutej osoby. Tieto záruky obsahujú zavedenie primeraných a účinných technických a organizačných	P 6.8.1. Identifikovať IS, kde sú spracovávané osobné údaje na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel. P 6.8.2. Určiť primeranosť technických a organizačných opatrení pre tieto IS na základe analýzy rizík.	§ 78, ods. (8)



	opatrení najmä na zabezpečenie dodržiavania zásady minimalizácie údajov a pseudonymizácie.	P 6.8.3. Ak je to relevantné, prijať primerané technické a organizačné opatrenia.	
6.9	(11) Prevádzkovateľ a sprostredkovateľ pri prijímaní bezpečnostných opatrení a pri posudzovaní vplyvu na ochranu osobných údajov postupuje primerane podľa medzinárodných noriem a štandardov bezpečnosti.	P 6.9.1. Ujasniť si pojem „primeranosti“ a vybrať vhodné normy a štandardy bezpečnosti – najmä z rodiny ISO 27000 a 31000 pre niektoré činnosti manažmentu rizík.	§ 78 ods. (11)
6.10	Mlčanlivosť - (1)Prevádzkovateľ a sprostredkovateľ je povinný zachovávať mlčanlivosť o osobných údajoch, ktoré spracúva. Povinnosť mlčanlivosti trvá aj po ukončení spracúvania osobných údajov.	P 6.10.1. Zabezpečiť povinnosť mlčanlivosti v interných riadiacich aktoch prevádzkovateľa a poučenie dotknutých osôb.	§ 79 ods. (1)
6.11	(2) Prevádzkovateľ a sprostredkovateľ je povinný zaviazat' mlčanlivosťou o osobných údajoch fyzické osoby, ktoré prídu do styku s osobnými údajmi u prevádzkovateľa alebo sprostredkovateľa. Povinnosť mlčanlivosti podľa prvej vety musí trvať aj po skončení pracovného pomeru, štátnozamestnaneckého pomeru, služobného pomeru alebo obdobného pracovného vzťahu tejto fyzickej osoby.	P 6.11.1. Zabezpečiť zaviazanie mlčanlivosťou o osobných údajoch fyzické osoby, ktoré prídu do styku s osobnými údajmi u prevádzkovateľa alebo sprostredkovateľa.	§ 79, ods. (2)

7. Možné povinnosti prevádzkovateľa vyplývajúce zo Piatej časti zákona

Ide o možné povinnosti a úlohy prevádzkovateľa z Piatej časti zákona vyplývajúce činnosti Úradu na ochranu osobných údajov.

ID	Text zákona / regulácia	Vyplývajúce povinnosti a úlohy	§
7.1	(3) Úrad je pri plnení svojich úloh oprávnený a) nariadiť prevádzkovateľovi a sprostredkovateľovi, prípadne aj zástupcovi prevádzkovateľa alebo sprostredkovateľa, ak bol poverený, aby poskytl informácie, ktoré sú nevyhnutné na plnenie jeho úloh.	P 7.1.1 V prípade požiadavky Úradu poskytnúť mu informácie, ktoré sú nevyhnutné na plnenie jeho úloh.	§ 81 ods. (3)
7.2	3) Úrad je pri plnení svojich úloh oprávnený b) získať od prevádzkovateľa a sprostredkovateľa prístup k osobným údajom a informáciám, ktoré sú nevyhnutné na plnenie jeho úloh; tým nie sú dotknuté ustanovenia o mlčanlivosti podľa osobitných predpisov	P 7.2.1 V prípade požiadavky Úradu umožniť mu prístup k osobným údajom a informáciám.	§ 81, ods. (3)
7.3	3) Úrad je pri plnení svojich úloh oprávnený c) vstupovať do priestorov prevádzkovateľa a sprostredkovateľa, ako aj k akémukoľvek zariadeniu a prostriedkom na spracúvanie osobných údajov, a to v	P 7.3.1 V prípade požiadavky Úradu umožniť mu vstup do priestorov prevádzkovateľa, ako aj k akémukoľvek zariadeniu a prostriedkom na spracúvanie osobných údajov, a to v rozsahu nevyhnutnom na plnenie jeho úloh, ak na to nie je potrebné povolenie podľa osobitného predpisu.	§ 81, ods. (3)



	rozsahu nevyhnutnom na plnenie jeho úloh, ak na to nie je potrebné povolenie podľa osobitného predpisu		
7.4	3) Úrad je pri plnení svojich úloh oprávnený e) uložiť opatrenia na nápravu, pokutu podľa § 104 alebo poriadkovú pokutu podľa § 105, ak prevádzkovateľ, sprostredkovateľ, monitorujúci subjekt alebo certifikačný subjekt porušili ustanovenia tohto zákona alebo osobitného predpisu	P 7.4.1 V prípade uloženia opatrenia na nápravu zo strany Úradu realizovať v zákonných termínoch požadované opatrenia a mať zdokladovanú ich realizáciu.	§ 81, ods. (3)
7.5	3) Úrad je pri plnení svojich úloh oprávnený f) nariadiť prevádzkovateľovi alebo sprostredkovateľovi, aby vyhovel žiadosti dotknutej osoby o uplatnenie jej práv podľa tohto zákona alebo osobitného predpisu	P 7.5.1 V prípade uloženia opatrenia na vyhovieť žiadosti zo strany Úradu v zákonných termínoch vyhovieť danej žiadosti.	§ 81, ods. (3)
7.6	3) Úrad je pri plnení svojich úloh oprávnený g) nariadiť prevádzkovateľovi alebo sprostredkovateľovi, aby svoje spracovateľské operácie zosúladiť podľa potreby určeným spôsobom a v rámci určenej lehoty s ustanoveniami tohto zákona alebo osobitného predpisu	P 7.6.1 V prípade nariadenia na zosúladienie zo strany Úradu realizovať v zákonnej lehote činnosti vedúce k zosúladieniu a mať zdokladovanú ich realizáciu.	§ 81, ods. (3)
7.7	3) Úrad je pri plnení svojich úloh oprávnený h) nariadiť prevádzkovateľovi, aby porušenie ochrany osobných údajov oznámil dotknutej osobe	P 7.7.1 V prípade nariadenia na oznámenie zo strany Úradu realizovať v zákonnej lehote oznámenie mať ho zdokladované.	§ 81, ods. (3)
7.8	3) Úrad je pri plnení svojich úloh oprávnený i) nariadiť dočasné obmedzenie spracúvania osobných údajov alebo trvalé obmedzenie spracúvania osobných údajov	P 7.8.1 V prípade nariadenia na obmedzenie spracúvania osobných údajov zo strany Úradu realizovať v zákonnej lehote obmedzenie a mať ho zdokladované. P 7.8.2 V rámci plánovania kontinuity zabezpečiť náhradné postupy v prípade obmedzenia.	§ 81, ods. (3)
7.9	3) Úrad je pri plnení svojich úloh oprávnený j) predvolať prevádzkovateľa alebo sprostredkovateľa za účelom podania vysvetlenia pri podozrení z porušenia povinností uložených týmto zákonom, osobitným predpisom alebo medzinárodnou zmluvou, ktorou je Slovenská republika viazaná,	P 7.9.1 V prípade nariadenia na obmedzenie spracúvania osobných údajov zo strany Úradu realizovať v zákonnej lehote obmedzenie a mať ho zdokladované.	§ 81, ods. (3)
7.10	3) Úrad je pri plnení svojich úloh oprávnený l) nariadiť pozastavenie prenosu osobných údajov príjemcovi v tretej krajine alebo medzinárodnej organizácii.	P 7.10.1 V prípade nariadenia na pozastavenie prenosu osobných údajov zo strany Úradu realizovať v zákonnej lehote pozastavenie a mať ho zdokladované.	§ 81, ods. (3)
7.11	Kódex správania - (1) Združenie zastupujúce kategóriu prevádzkovateľov alebo sprostredkovateľov alebo iný subjekt zastupujúci kategóriu prevádzkovateľov alebo sprostredkovateľov môže prijať kódex správania, a to najmä na účely spresnenia uplatňovania tohto zákona alebo osobitného predpisu v súvislosti s predmetom kódexu správania podľa osobitného predpisu.	P 7.11.1 Zvážiť možnosť prijať kódex správania ako nástroj preukazovania súladu. P 7.11.2 Identifikovať implementačné požiadavky vyplývajúce z vybraného kódexu. P 7.11.3 V prípade kladného rozhodnutia, pripojiť sa k združeniu s kódexom. P 7.11.5 Pripraviť implementačný plán súladu s kódexom.	§ 85, ods. (1)
7.12	Certifikát - (2) Prevádzkovateľ alebo sprostredkovateľ na účely preukázania súladu spracúvania osobných údajov a existencie primeraných záruk ochrany osobných údajov podľa tohto zákona alebo osobitného predpisu môže požiadať	P 7.12.1 Zvážiť možnosť využiť certifikát na účely preukázania súladu. P 7.12.2 Identifikovať implementačné požiadavky vyplývajúce z certifikačného procesu.	§ 86, ods. (2)



	úrad alebo certifikačný subjekt o vydanie certifikátu alebo obnovenie certifikátu. Certifikát sa vydá alebo obnoví najviac na obdobie troch rokov.	P 7.12.3 V prípade kladného rozhodnutia pripraviť implementačný plán certifikácie. P 7.12.4 Vybrať certifikačný subjekt a koordinovať s ním jednotlivé aktivity.	
7.13	Monitorujúci subjekt (4) Monitorujúci subjekt je oprávnený a) monitorovať súlad spracúvania osobných údajov podľa tohto zákona alebo osobitného predpisu prevádzkovateľom alebo sprostredkovateľom, ktorý je členom združenia, ktorý sa zaviazal dodržiavať schválený kódex správania ...	P 7.13.1 V prípade využitia kódexu správania umožniť monitorujúcemu subjektu monitorovať súlad spracúvania osobných údajov.	§ 87, ods. (4)
7.14	Povinnosti certifikačného subjektu (1) Certifikačný subjekt je oprávnený v rozsahu osvedčenia o udelení akreditácie vydať certifikát alebo obnoviť certifikát prevádzkovateľovi alebo sprostredkovateľovi na obdobie troch rokov.	P 7.14.1 V prípade využitia certifikátu na účely preukázania súladu zabezpečiť si akreditovaný certifikačný subjekt. P 7.14.2 Zabezpečiť si vydanie certifikátu a jeho následnú obnovu po splnení podmienok certifikácie.	§ 89, ods. (1)
7.15	Začatie kontroly - (6) Kontrola je začatá dňom doručenia oznámenia o kontrole prevádzkovateľovi alebo sprostredkovateľovi, zástupcovi prevádzkovateľa alebo zástupcovi sprostredkovateľa, ak bol poverený, alebo monitorujúcemu subjektu podľa § 87 alebo certifikačnému subjektu podľa § 88 (ďalej len „kontrolovaná osoba“).	P 7.15.1 V prípade začatia kontroly zabezpečiť prijatie oznámenia a následné informovanie vedenia.	§ 90, ods. (3)
7.16	Zaujatost' kontrolného orgánu - (2) Ak má kontrolovaná osoba pochybnosti o nezaujatosti kontrolného orgánu alebo jeho člena so zreteľom na jeho vzťah k predmetu kontroly alebo ku kontrolovanej osobe, je oprávnená podať písomné námietky s uvedením dôvodu najneskôr do 15 dní odo dňa, keď sa o tejto skutočnosti dozvedela. Podanie námietok nemá odkladný účinok; kontrolný orgán je podľa prvej vety oprávnený vykonať pri kontrole len také úkony, ktoré nezniesú odklad.	P 7.16.1 V prípade začatia kontroly posúdiť nezaujatost' kontrolného orgánu alebo jeho člena a rozhodnúť o podaní námietky. P 7.16.2 V prípade rozhodnutia o námietke zabezpečiť jej podanie.	§ 91, ods. (2)
7.17	Povinnosti kontrolovanej osoby - Kontrolovaná osoba je povinná a) strpieť výkon kontroly a vytvoriť kontrolnému orgánu primerané podmienky na výkon kontroly a spracovanie kontrolných zistení, b) poskytnúť kontrolnému orgánu súčinnosť nevyhnutnú pre riadny výkon kontroly, najmä pri dokumentovaní primeranej úrovne bezpečnosti s ohľadom na riziká, ktoré predstavuje spracúvanie osobných údajov v podmienkach prevádzkovateľa a sprostredkovateľa, c) v čase výkonu kontroly zabezpečiť kontrolnému orgánu dostupný a bezpečný prístup k zariadeniam, prostriedkom a k informačným systémom, d) poskytnúť kontrolnému orgánu požadovanú súčinnosť v súlade s jeho oprávneniami podľa § 93 a zdržať sa konania, ktoré by mohlo mariť výkon kontroly, e) dostaviť sa na predvolanie kontrolného orgánu s cieľom podať vysvetlenia k predmetu kontroly, f) v určenej lehote poskytnúť kontrolnému orgánu originál alebo kópiu dokladov, iných písomností, vyjadrenia a informácie, osobné údaje spracúvané na	P 7.17.1 Vytvoriť primerané podmienky a zabezpečiť požadovanú zákonnú súčinnosť kontrolnému orgánu. P 7.17.2 Mať pripravené a ľahko dostupné doklady, ktoré môžu byť v rámci kontroly požadované. <i>Napr. aby neboli podklady u jednej osoby, ktoré môžu byť na dovolenke alebo PN.</i> P 7.17.3 Zabezpečiť kontrolnému orgánu dostupný a bezpečný prístup k zariadeniam, prostriedkom a k informačným systémom. P 7.17.4 Dostaviť sa na predvolanie kontrolného orgánu. P 7.17.5 Poskytnúť požadované podklady podľa písm. f). P 7.17.6 Dostaviť sa na prerokovanie protokolu.	§ 94



	pamäťových médiách vrátane technických nosičov osobných údajov, výpisy a zdrojové kódy programov, ak ich vlastní alebo má k dispozícii, a ďalšie materiály alebo podklady potrebné na výkon kontroly, a v odôvodnených prípadoch umožniť odoberať originály alebo kópie aj mimo priestorov kontrolovanej osoby, g) poskytnúť kontrolnému orgánu úplné a pravdivé ústne a písomné informácie, vyjadrenia a vysvetlenia ku kontrolovaným a s kontrolou súvisiacim skutočnostiam, h) na požiadanie kontrolného orgánu sa dostaviť na prerokovanie protokolu.		
7.18	Ukončenie kontroly - (4) Kontrolovaná osoba je po oboznámení sa s kontrolnými zisteniami v protokole oprávnená podať písomné námietky v lehote 21 dní odo dňa doručenia protokolu. Na neskôr podané námietky kontrolný orgán neprihliada.	P 7.18.1 Posúdiť kontrolné zistenia a rozhodnúť o podaní námietku. P 7.18.2 V prípade rozhodnutia o námietke zabezpečiť jej podanie.	§ 97, ods. (4)
7.19	Konanie o ochrane osobných údajov - (1) Účelom konania o ochrane osobných údajov (ďalej len „konanie“) je zistiť, či došlo k porušeniu práv fyzických osôb pri spracúvaní ich osobných údajov alebo došlo k porušeniu tohto zákona alebo osobitného predpisu v oblasti ochrany osobných údajov, a v prípade zistenia nedostatkov, ak je to dôvodné a účelné, uložiť opatrenia na nápravu, prípadne pokutu za porušenie tohto zákona alebo osobitného predpisu pre oblasť ochrany osobných údajov. ... (3) Účastníkom konania môže byť a) dotknutá osoba, ktorá podala návrh na začatie konania podľa § 100, b) <u>prevádzkovateľ</u> , c) sprostredkovateľ, d) certifikačný subjekt, e) monitorujúci subjekt.	P 7.19.1 Aktívne sa zúčastniť konania.	§ 99, ods. (3)
7.20	Rozhodnutie - (3) Úrad je oprávnený <u>uložiť povinnosť prevádzkovateľovi</u> alebo sprostredkovateľovi, najmä nariadiť a) odstránenie zistených nedostatkov a príčin ich vzniku v úrade určenej lehote, b) prijatie technických a organizačných opatrení s cieľom zaistiť úroveň bezpečnosti primeranú rizikám pre práva fyzických osôb, c) posúdenie vplyv spracovateľských operácií na ochranu osobných údajov v súlade s týmto zákonom alebo osobitným predpisom. (5) <u>Prevádzkovateľ</u> alebo sprostredkovateľ <u>je povinný</u> písomne informovať úrad o splnení uložených opatrení v úrade určenej lehote.	P 7.20.1 Splniť uloženú povinnosť v určenej lehote. P 7.20.2 Písomne informovať úrad o splnení uložených opatrení v úrade určenej lehote.	§ 102, ods. (3)
7.21	(1) Proti rozhodnutiu podľa § 102 možno podať rozklad, o ktorom rozhodne predseda úradu. (2) Podávateľ rozkladu môže rozšíriť podaný rozklad alebo doplniť podaný rozklad o ďalší návrh alebo o ďalšie body len v lehote určenej na podanie rozkladu.	P 7.18.1 Posúdiť rozhodnutie o uloženej povinnosti a rozhodnúť sa o podaní rozkladu. P 7.18.1 V prípade kladného rozhodnutia podať rozklad.	§ 103, ods. (1) ods. (2)



Práva fyzických osôb

Prehľad nových práv fyzických osôb, ktoré zakladajú povinnosti prevádzkovateľom.

- ✓ Napĺňanie práv fyzických osôb (1- 17) zakladá prevádzkovateľom moci nové, samostatné agendy.
- ✓ Práva 18 – 22 sú vážnym rizikom pre prevádzkovateľov.

Dotknutá osoba má právo:

1. Kedykoľvek odvolať súhlas so spracovaním osobných údajov, ktoré sa jej týkajú (§ 14).
2. Získať od prevádzkovateľa informácie súvisiace so získavaním osobných údajov (§ 19, § 20).
3. Získať od prevádzkovateľa potvrdenie o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú (§ 21).
4. Získať od prevádzkovateľa informácie súvisiace so spracúvaním osobných údajov (§ 21).
5. Na prístup k osobným údajom (§21).
6. Na poskytnutie osobných údajov (§ 21).
7. Na opravu osobných údajov (§ 22).
8. Na doplnenie neúplných osobných údajov (§ 22).
9. Na výmaz osobných údajov (§ 23).
10. Na obmedzenie spracúvania osobných údajov (§ 24)
11. Na oznámenie opravy osobných údajov, vymazanie osobných údajov alebo obmedzenie spracúvania (§ 25).
12. Právo na prenosnosť osobných údajov (§ 26).
13. Právo namietat' spracúvanie osobných údajov (§ 27)
14. Na to, aby sa na ňu nevzťahovalo rozhodnutie, ktoré je založené výlučne na automatizovanom spracúvaní osobných údajov (§ 28).
15. Právo na informácie o opatreniach, ktoré sa prijali na základe žiadosti osoby (§ 29).
16. Na poskytnutie súčinnosti pri uplatňovaní práv podľa § 21 až 28 (§ 29).
17. Právo na informácie o dôvodoch nekonania poskytovateľa (§ 29).
18. Právo na náhradu škody a zodpovednosť (§ 38, Článok 82 GDPR).
19. Právo podať sťažnosť dozornému orgánu (Článok 77, GDPR).
20. Právo na účinný súdny prostriedok nápravy voči rozhodnutiu dozorného orgánu (Článok 78, GDPR).
21. Právo na účinný súdny prostriedok nápravy voči prevádzkovateľovi alebo sprostredkovateľovi (Článok 79, GDPR).
22. Právo na zastupovanie – právo fyzickej osoby poveriť neziskový subjekt, organizáciu alebo združenie, aby podali sťažnosť v jej mene, aby v jej mene uplatnili práva podľa článkov 77, 78 a 79 a **aby v jej mene uplatnili právo na náhradu škody podľa článku 82**, ak to umožňuje právo členského štátu. (Článok 80, GDPR).