Smernica o bezpečnostných opatreniach prevádzkovateľa

(ďalej len „smernica“)
vypracovaná podľa Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe týchto údajov, ktorým sa zrušuje smernica 95/46/ES (ďalej len „Nariadenie GDPR) a v súlade so zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „Zákon č. 18/2018 Z.z.)

PREVÁDZKOVATEĽOM:

Názov: artluk plus, s.r.o.
Právna forma: s.r.o.
Sídlo: Volgogradská 13, Prešov 08001
IČO: 31 737 595
Zapísaný v: Obchodný register Okresného súdu Prešov, Oddiel: Sro , Vložka číslo: 3449/P
V mene ktorého koná: Ľubomír Lukáč, konateľ

/ďalej len „**prevádzkovateľ**“/

ČASŤ I

Základné východiská ochrany osobných údajov podľa Nariadenia GDPR a Zákona č. 18/2018 Z.z.

Pramene práva na ochranu osobných údajov a ich pôsobnosť a základné pojmy

1/Základnými prameňmi práva v oblasti ochrany osobných údajov od 25.05.2018 sú:

- Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe týchto údajov, ktorým sa zrušuje smernica 95/46/ES (ďalej len „Nariadenie GDPR);

- Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „Zákon č. 18/2018 Z.z.).

2/ Predmet úpravy a ciele Nariadenia GDPR podľa Článku 1.:

Nariadením GDPR sa stanovujú pravidlá ochrany fyzických osôb pri spracúvaní osobných údajov a pravidlá týkajúce sa voľného pohybu osobných údajov.

Nariadením GDPR sa chránia základné práva a slobody fyzických osôb, najmä ich právo na ochranu osobných údajov.
Voľný pohyb osobných údajov v rámci Únie sa nesmie obmedziť ani zakázať z dôvodov súvisiacich s ochranou fyzických osôb pri spracúvaní osobných údajov.

3/ Bod 14 recitálu Nariadenia GDPR:

Ochrana, ktorá sa poskytuje Nariadením GDPR, by sa mala vzťahovať na fyzické osoby bez ohľadu na ich štátnu príslušnosť alebo miesto bydliska vo vzťahu ku spracúvaniu ich osobných údajov. Toto nariadenie sa nevzťahuje na spracúvanie osobných údajov, ktoré sa týka právnických osôb, a najmä podnikov založených ako právnické osoby vrátane názvu, formy a kontaktných údajov právnickej osoby.

4/ Vecná pôsobnosťNariadenia GDPR podľa Článku 2.:

Nariadenie GDPR sa vzťahuje na spracúvanie osobných údajov vykonávané úplne alebo čiastočne automatizovanými prostriedkami a na spracúvanie inými než automatizovanými prostriedkami v prípade osobných údajov, ktoré tvoria súčasť informačného systému alebo sú určené na to, aby tvorili súčasť informačného systému.

Nariadenie GDPR sa nevzťahuje na spracúvanie osobných údajov:

a) v rámci činnosti, ktorá nepatrí do pôsobnosti práva Únie;

b) členskými štátmi pri vykonávaní činností patriacich do rozsahu pôsobnosti kapitoly 2 hlavy V ZEÚ;

c) fyzickou osobou v rámci výlučne osobnej alebo domácej činnosti (bod 18 recitálu Nariadenia GDPR: Nariadenie GDPR sa nevzťahuje na spracúvanie osobných údajov fyzickou osobou v priebehu výlučne osobnej alebo domácej činnosti, a teda bez spojenia s profesijnou alebo komerčnou činnosťou. Osobné alebo domáce činnosti by mohli zahŕňať korešpondenciu a uchovávanie adries či využívanie sociálnych sietí a online činnosti vykonávané v kontexte takýchto činností. Toto nariadenie sa však vzťahuje na prevádzkovateľov alebo sprostredkovateľov, ktorí poskytujú prostriedky na spracúvanie osobných údajov na takéto osobné alebo domáce činnosti);

d) príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania, alebo výkonu trestných sankcií vrátane ochrany pred ohrozením verejnej bezpečnosti a jeho predchádzania.

5/ Územná pôsobnosťNariadenia GDPR podľa Článku 3.:

Nariadenie GDPR sa vzťahuje na spracúvanie osobných údajov v rámci činnosti prevádzky prevádzkovateľa alebo sprostredkovateľa v Únii, a to bez ohľadu na to, či sa spracúvanie vykonáva v Únii alebo nie.

Nariadenie GDPR sa vzťahuje na spracúvanie osobných údajov dotknutých osôb, ktoré sa nachádzajú v Únii, prevádzkovateľom alebo sprostredkovateľom, ktorý nie je usadený v Únii, pričom spracovateľská činnosť súvisí:
a) s ponukou tovaru alebo služieb týmto dotknutým osobám v Únii bez ohľadu na to, či sa od dotknutej osoby vyžaduje platba, alebo
b) so sledovaním ich správania, pokiaľ ide o ich správanie na území Únie.

Nariadenie GDPR sa vzťahuje na spracúvanie osobných údajov prevádzkovateľom, ktorý nie je usadený v Únii, ale na mieste, kde sa na základe medzinárodného práva verejného uplatňuje právo členského štátu.

6/ Pôsobnosťzákona č. 18/2018 Z.z. podľa § 3:

Zákon č. 18/2018 Z.z. sa vzťahuje na spracúvanie osobných údajov vykonávané úplne alebo čiastočne automatizovanými prostriedkami a na 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.

Zákon č. 18/2018 Z.z., okrem § 5, druhej a tretej časti tohto zákona, sa vzťahuje na spracúvanie osobných údajov, na ktoré sa vzťahuje osobitný predpis o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (Nariadenie GDPR).

Zákon č. 18/2018 Z.z. sa vzťahuje na spracúvanie osobných údajov Policajným zborom, Vojenskou políciou, Zborom väzenskej a justičnej stráže, Finančnou správou, prokuratúrou a súdmi (ďalej len „príslušný orgán“) na účely predchádzania a odhaľovania trestnej činnosti, zisťovania páchateľov trestných činov, stíhania trestných činov alebo na účely výkonu rozhodnutí v trestnom konaní vrátane ochrany

pred ohrozením verejného poriadku a predchádzania takémuto ohrozeniu (ďalej len „plnenie úloh na účely trestného konania“); z druhej časti tohto zákona sa na spracúvanie osobných údajov podľa predchádzajúcej časti vety vzťahujú len ustanovenia uvedené v § 52, § 59, § 67 a § 73.

Článok I.
Základné ciele smernice

1.1. Táto smernica o bezpečnostných opatreniach prevádzkovateľa predstavuje bezpečnostnú dokumentáciu vypracovanú prevádzkovateľom za účelom preukázania splnenia povinností prevádzkovateľa podľa Nariadenia GDPR a Zákona č. 18/2018 Z.z. prijať vhodné technické a organizačné opatrenia nevyhnutné na zabezpečenie spracúvania osobných údajov dotknutých osôb v súlade s Nariadením GDPR a Zákonom č. 18/2018 Z.z.

1.2. Účelom tejto smernice o bezpečnostných opatreniach prevádzkovateľa, spolu s ďalšími dokumentami, ktoré tvoria jej prílohu, je poskytnúť riešenia, ako zabezpečiť trvalo udržateľný systém spracúvania osobných údajov zodpovedajúci požiadavkám Nariadenia GDPR, Zákona č. 18/2018 Z.z. a ďalších súvisiacich predpisov.

1.3. Cieľom tejto smernice o bezpečnostných opatreniach prevádzkovateľa je stanoviť pravidlá, ktorých dodržiavanie by zamedzilo možným bezpečnostným rizikám a zároveň poskytnúť návod pri riešení prípadných bezpečnostných incidentov.

Článok II.
Základné pojmy

2.1. Podľa Článku 4. ods. 1 Nariadenia GDPR „**osobné údaje**“ sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby (ďalej len „dotknutá osoba“); identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby.

2.2. Podľa Článku 4. ods. 2 Nariadenia GDPR „**spracúvanie**“ je operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov, napríklad získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami.

2.3. Podľa Článku 4. ods. 3 Nariadenia GDPR „**obmedzenie spracúvania**“ je označenie uchovávaných osobných údajov s cieľom obmedziť ich spracúvanie v budúcnosti.

2.4. Podľa Článku 4. ods. 4 Nariadenia GDPR „**profilovanie**“ je akákoľvek forma automatizovaného spracúvania osobných údajov, ktoré pozostáva z použitia týchto osobných údajov na vyhodnotenie určitých osobných aspektov týkajúcich sa fyzickej osoby, predovšetkým analýzy alebo predvídania aspektov dotknutej fyzickej osoby súvisiacich s výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom.

2.5. Podľa Článku 4. ods. 5 Nariadenia GDPR „**pseudonymizácia“** je spracúvanie osobných údajov takým spôsobom, aby osobné údaje už nebolo možné priradiť konkrétnej dotknutej osobe bez použitia dodatočných informácií, pokiaľ sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na ne technické a organizačné opatrenia s cieľom zabezpečiť, aby osobné údaje neboli priradené identifikovanej alebo identifikovateľnej fyzickej osobe.

2.6. Podľa Článku 4. ods. 6 Nariadenia GDPR „**informačný systém**“ je akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe.

2.7. Podľa Článku 4. ods. 7 Nariadenia GDPR „**prevádzkovateľ**“ je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov; v prípade, že sa účely a prostriedky tohto spracúvania stanovujú v práve Únie alebo v práve členského štátu, možno prevádzkovateľa alebo konkrétne kritériá na jeho určenie určiť v práve Únie alebo v práve členského štátu.

2.8. Podľa Článku 4. ods. 8 Nariadenia GDPR „**sprostredkovateľ**“ je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa.

2.9. Podľa Článku 4. ods. 9 Nariadenia GDPR „**príjemca**“ je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorému sa osobné údaje poskytujú bez ohľadu na to, či je treťou stranou. Orgány verejnej moci, ktoré môžu prijať osobné údaje v rámci konkrétneho zisťovania v súlade s právom Únie alebo právom členského štátu, sa však nepovažujú za príjemcov; spracúvanie uvedených údajov uvedenými orgánmi verejnej moci sa uskutočňuje v súlade s uplatniteľnými pravidlami ochrany údajov v závislosti od účelov spracúvania.

2.10. Podľa Článku 4. ods. 10 Nariadenia GDPR „**tretia strana**“ je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt než dotknutá osoba, prevádzkovateľ, sprostredkovateľ a osoby, ktoré sú na základe priameho poverenia prevádzkovateľa alebo sprostredkovateľa poverené spracúvaním osobných údajov.

2.11.Podľa Článku 4. ods. 11 Nariadenia GDPR „**súhlas dotknutej osoby**“ je akýkoľvek slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby, ktorým formou vyhlásenia alebo jednoznačného potvrdzujúceho úkonu vyjadruje súhlas so spracúvaním osobných údajov, ktoré sa jej týka.

2.12. Podľa Článku 4. ods. 12 Nariadenia GDPR „**porušenie ochrany osobných údajov**“ je porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávnený prístup k nim.

2.13. Podľa Článku 4. ods. 13 Nariadenia GDPR „**genetické údaje**“ sú osobné údaje týkajúce sa zdedených alebo nadobudnutých genetických charakteristických znakov fyzickej osoby, ktoré poskytujú jedinečné informácie o fyziológii alebo zdraví tejto fyzickej osoby a ktoré vyplývajú najmä z analýzy biologickej vzorky danej fyzickej osoby.

2.14. Podľa Článku 4. ods. 14 Nariadenia GDPR „**biometrické údaje**“ sú osobné údaje, ktoré sú výsledkom osobitného technického spracúvania, ktoré sa týka fyzických, fyziologických alebo behaviorálnych charakteristických znakov fyzickej osoby a ktoré umožňujú alebo potvrdzujú jedinečnú identifikáciu tejto fyzickej osoby, ako napríklad vyobrazenia tváre alebo daktyloskopické údaje.

2.15. Podľa Článku 4. ods. 15 Nariadenia GDPR „**údaje týkajúce sa zdravia**“ sú osobné údaje týkajúce sa fyzického alebo duševného zdravia fyzickej osoby, vrátane údajov o poskytovaní služieb zdravotnej starostlivosti, ktorými sa odhaľujú informácie o jej zdravotnom stave.

Článok III.
Zásady spracúvania osobných údajov podľa Nariadenia GDPR

3.1. Podľa Článku 5. ods. 1 Nariadenia GDPR osobné údaje musia byť:

a)spracúvané zákonným spôsobom, spravodlivo a transparentne vo vzťahu k dotknutej osobe („**zákonnosť, spravodlivosť a transparentnosť**“);

b) získavané na konkrétne určené, výslovne uvedené a legitímne účely a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmito účelmi; ďalšie spracúvanie na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či štatistické účely sa v súlade s článkom 89 ods. 1 nepovažuje za nezlučiteľné s pôvodnými účelmi („**obmedzenie účelu**“);

c) primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú („**minimalizácia údajov**“);

d) správne a podľa potreby aktualizované; musia sa prijať všetky potrebné opatrenia, aby sa zabezpečilo, že sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bezodkladne vymažú alebo opravia („**správnosť**“);

e) uchovávané vo forme, ktorá umožňuje identifikáciu dotknutých osôb najviac dovtedy, kým je to potrebné na účely, na ktoré sa osobné údaje spracúvajú; osobné údaje sa môžu uchovávať dlhšie, pokiaľ sa budú spracúvať výlučne na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či na štatistické účely v súlade s článkom 89 ods. 1 za predpokladu prijatia primeraných technických a organizačných opatrení vyžadovaných týmto nariadením na ochranu práv a slobôd dotknutých osôb („**minimalizácia uchovávania**“);

f) spracúvané spôsobom, ktorý zaručuje primeranú bezpečnosť osobných údajov, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení („**integrita a dôvernosť**“).

3.2. Podľa Článku 5. ods. 2 Nariadenia GDPRprevádzkovateľ je zodpovedný za súlad s odsekom 1 a musí vedieť tento súlad preukázať („**zodpovednosť**“).

Článok IV.
Zákonnosť spracúvania osobných údajov podľa Nariadenia GDPR – právny základ

4.1. Podľa Článku 6. ods. 1 Nariadenia GDPRspracúvanie je zákonné iba vtedy a iba v tom rozsahu, keď je splnená aspoň jedna z týchto podmienok:

a) dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov na jeden alebo viaceré konkrétne účely;

b) spracúvanie je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo aby sa na základe žiadosti dotknutej osoby vykonali opatrenia pred uzatvorením zmluvy;

c) spracúvanie je nevyhnutné na splnenie zákonnej povinnosti prevádzkovateľa; d) spracúvanie je nevyhnutné, aby sa ochránili životne dôležité záujmy dotknutej osoby alebo inej fyzickej osoby;
e) spracúvanie je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi;

f) spracúvanie je nevyhnutné na účely oprávnených záujmov, ktoré sleduje prevádzkovateľ alebo tretia strana, s výnimkou prípadov, keď nad takýmito záujmami prevažujú záujmy alebo základné práva a slobody dotknutej osoby, ktoré si vyžadujú ochranu osobných údajov, najmä ak je dotknutou osobu dieťa.
Písmeno f) prvého pododseku sa nevzťahuje na spracúvanie vykonávané orgánmi verejnej moci pri výkone ich úloh.

Článok V.
Spracúvanie osobitných kategórií osobných údajov podľa Článku 9 Nariadenia GDPR

5.1. Podľa Článku 9. ods. 1 Nariadenia GDPRzakazuje sa spracúvanie osobných údajov, ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, a spracúvanie genetických údajov, biometrických údajov na individuálnu identifikáciu fyzickej osoby, údajov týkajúcich sa zdravia alebo údajov týkajúcich sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby.

5.2. Podľa Článku 9. ods. 2 Nariadenia GDPRodsek 1 sa neuplatňuje, ak platí niektorá z týchto podmienok:
a) dotknutá osoba vyjadrila výslovný súhlas so spracúvaním týchto osobných údajov na jeden alebo viacero určených účelov, s výnimkou prípadov, keď sa v práve Únie alebo v práve členského štátu stanovuje, že zákaz uvedený v odseku 1 nemôže dotknutá osoba zrušiť;

b) spracúvanie je nevyhnutné na účely plnenia povinností a výkonu osobitných práv prevádzkovateľa alebo dotknutej osoby v oblasti pracovného práva a práva sociálneho

zabezpečenia a sociálnej ochrany, pokiaľ je to povolené právom Únie alebo právom členského štátu alebo kolektívnou zmluvou podľa práva členského štátu poskytujúcimi primerané záruky ochrany základných práv a záujmov dotknutej osoby;

c) spracúvanie je nevyhnutné na ochranu životne dôležitých záujmov dotknutej osoby alebo inej fyzickej osoby v prípade, že dotknutá osoba nie je fyzicky alebo právne spôsobilá vyjadriť svoj súhlas;

d) spracúvanie vykonáva v rámci svojej zákonnej činnosti s primeranými zárukami nadácia, združenie alebo akýkoľvek iný neziskový subjekt s politickým, filozofickým, náboženským alebo odborárskym zameraním a pod podmienkou, že spracúvanie sa týka výlučne členov alebo bývalých členov subjektu alebo osôb, ktoré majú pravidelný kontakt s ním v súvislosti s jeho cieľmi, a že bez súhlasu dotknutej osoby sa osobné údaje neposkytnú mimo tohto subjektu;

e) spracúvanie sa týka osobných údajov, ktoré dotknutá osoba preukázateľne zverejnila;

f) spracúvanie je nevyhnutné na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov, alebo kedykoľvek, keď súdy vykonávajú svoju súdnu právomoc;

g) spracúvanie je nevyhnutné z dôvodov významného verejného záujmu na základe práva Únie alebo práva členského štátu, ktoré sú primerané vzhľadom na sledovaný cieľ, rešpektujú podstatu práva na ochranu údajov a stanovujú vhodné a konkrétne opatrenia na zabezpečenie základných práv a záujmov dotknutej osoby;

h) spracúvanie je nevyhnutné na účely preventívneho alebo pracovného lekárstva, posúdenia pracovnej spôsobilosti zamestnanca, lekárskej diagnózy, poskytovania zdravotnej alebo sociálnej starostlivosti alebo liečby, alebo riadenia systémov a služieb zdravotnej alebo sociálnej starostlivosti na základe práva Únie alebo práva členského štátu alebo podľa zmluvy so zdravotníckym pracovníkom, a podlieha podmienkam a zárukám uvedeným v odseku 3;

i) spracúvanie je nevyhnutné z dôvodov verejného záujmu v oblasti verejného zdravia, ako je ochrana proti závažným cezhraničným ohrozeniam zdravia alebo zabezpečenie vysokej úrovne kvality a bezpečnosti zdravotnej starostlivosti a liekov alebo zdravotníckych pomôcok, na základe práva Únie alebo práva členského štátu, ktorým sa stanovujú vhodné a konkrétne opatrenia na ochranu práv a slobôd dotknutej osoby, najmä profesijné tajomstvo;

j) spracúvanie je nevyhnutné na účely archivácie vo verejnom záujme, alebo na účely vedeckého alebo historického výskumu či na štatistické účely podľa článku 89 ods. 1 na základe práva Únie alebo práva členského štátu, ktoré sú primerané vzhľadom na sledovaný cieľ, rešpektujú podstatu práva na ochranu údajov a určujú vhodné a konkrétne opatrenia na zabezpečenie základných práv a záujmov dotknutej osoby.

5.3. Podľa Článku 9. ods. 3 Nariadenia GDPRosobné údaje uvedené v odseku 1 sa môžu spracúvať na účely uvedené v odseku 2 písm. h), ak tieto údaje spracúva odborník, alebo ak sa spracúvajú v rámci zodpovednosti odborníka, ktorý podlieha povinnosti zachovávať profesijné tajomstvo podľa práva Únie alebo práva členského štátu alebo podľa pravidiel, ktoré stanovili príslušné vnútroštátne orgány, alebo ak údaje spracúva iná osoba, ktorá tiež podlieha povinnosti mlčanlivosti podľa práva Únie alebo práva členského štátu alebo pravidiel, ktoré stanovili príslušné vnútroštátne orgány.

5.4. Podľa Článku 9. ods. 4 Nariadenia GDPRčlenské štáty môžu zachovať alebo zaviesť ďalšie podmienky vrátane obmedzení týkajúce sa spracúvania genetických údajov, biometrických údajov alebo údajov týkajúcich sa zdravia.

5.5. Podľa § 78 ods. 5 Zákona č. 18/2018 Z.z. 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.

5.6. Podľa bodu 51 recitálu Nariadenia GDPR spracúvanie fotografií by sa nemalo systematicky považovať za spracúvanie osobitných kategórií osobných údajov, pretože vymedzenie pojmu biometrické údaje sa na ne bude vzťahovať len v prípadoch, keď sa spracúvajú osobitnými technickými prostriedkami, ktoré umožňujú alebo potvrdzujú jedinečnú identifikáciu fyzickej osoby. Takéto osobné údaje by sa nemali spracúvať, pokiaľ spracúvanie nie je povolené v osobitných prípadoch stanovených v tomto nariadení, pričom sa zohľadní, že právo členských štátov môže stanoviť osobitné ustanovenia o ochrane údajov, ktorými prispôsobia uplatňovanie pravidiel tohto nariadenia na účely splnenia zákonnej povinnosti alebo úlohy realizovanej vo verejnom záujme či pri výkone verejnej moci zverenej prevádzkovateľovi. Okrem osobitných požiadaviek na takéto spracúvanie by sa mali uplatňovať všeobecné zásady a iné pravidlá uvedené v tomto nariadení, najmä pokiaľ ide o podmienky pre zákonné spracúvanie. Výnimky zo všeobecného zákazu spracúvania týchto osobitných kategórií osobných údajov by sa mali výslovne uviesť okrem iného vtedy, ak dotknutá osoba poskytla svoj výslovný súhlas alebo v súvislosti s osobitnými potrebami, najmä ak spracúvanie vykonávajú v rámci legitímnych činností určité združenia alebo nadácie, ktorých účelom je umožniť výkon základných slobôd.

Článok VI.
Spracúvanie národného identifikačného čísla podľa Nariadenia GDPR

6.1. Podľa Článku 87 Nariadenia GDPRčlenské štáty môžu stanoviť podrobnejšie osobitné podmienky spracúvania národného identifikačného čísla alebo akéhokoľvek iného identifikátora všeobecného uplatnenia. V uvedenom prípade sa národné identifikačné číslo alebo akýkoľvek iný identifikátor všeobecného uplatnenia používajú len v rámci primeraných záruk v súvislosti s právami a slobodami dotknutej osoby podľa tohto nariadenia.

6.2. Podľa § 78 ods. 4 Zákona č. 18/2018 Z.z. pri spracúvaní osobných údajov možno využiť na účely identifikovania fyzickej osoby všeobecne použiteľný identifikátor podľa osobitného predpisu (Zákon č. 301/1995 Z. z. o rodnom čísle v znení zákona č. 515/2003 Z. z.) 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.

Článok VII.
Cezhraničné spracúvanie osobných údajov a prenos osobných údajov do tretej krajiny podľa Nariadenia GDPR

7.1. Podľa Článku 4 bod 23 Nariadenia GDPR„cezhraničné spracúvanie“ je buď:
a) spracúvanie osobných údajov, ktoré sa uskutočňuje v Únii v kontexte činností prevádzkarní prevádzkovateľa alebo sprostredkovateľa vo viac ako jednom členskom štáte, pričom prevádzkovateľ alebo sprostredkovateľ sú usadení vo viac ako jednom členskom štáte; alebo
b)spracúvanie osobných údajov, ktoré sa uskutočňuje v Únii kontexte činností jedinej prevádzkarne prevádzkovateľa alebo sprostredkovateľa v Únii, ale ktoré podstatne ovplyvňuje alebo pravdepodobne podstatne ovplyvní dotknuté osoby vo viac ako jednom členskom štáte;

Cezhraničným spracúvaním sa rozumie spracúvanie osobných údajov na území EÚ a ich prenos výlučne v rámci členských štátov.

7.2. Cezhraničný prenos osobných údajov mimo územia EÚ podľa Nariadenia GDPR je možné realizovať iba na základe:

- Rozhodnutie o primeranosti – Komisia rozhodla, že tretia krajina, územie, alebo jeden či viaceré určené sektory v danej tretej krajine alebo predmetná medzinárodná organizácia zaručujú primeranú úroveň ochrany. Na takýto prenos nie je nutné žiadne osobitné povolenie (Argentína, Andorrské kniežatstvo, Faerské ostrovy, Guernsey, Izrael, Jersey, Nový Zéland, Kanada – komerčné organizácie, Ostrov Man, Švajčiarsko, Uruguajská východná republika, Spojené štáty americké– spoločnosti certifikované v režime PrivacyShield).

- Prenosy vyžadujúce primerané záruky – v prípade neexistencie rozhodnutia o primeranosti je prenos možný iba vtedy, ak prevádzkovateľ alebo sprostredkovateľ:
a/ poskytol primerané záruky: zákonná povinnosť, záväzné vnútropodnikové pravidlá, štandardné doložky, schválený kódex správania, schválený certifikačný mechanizmus, povoľovací mechanizmus úradu; a zároveň
b/ za podmienky, že dotknuté osoby majú k dispozícii vymožiteľné práva a účinné právne prostriedky nápravy.

- Osobitné situácie – v prípade neexistencie rozhodnutia o primeranosti alebo ak neexistujú primerané záruky, tak prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii sa uskutoční len za podmienok taxatívne uvedených v nariadení (súhlas dotknutej osoby, zmluvný vzťah, dôležité dôvody verejného záujmu, právne nároky, ochrana životne dôležitých záujmov, a iné).

Článok VIII.
Transparentnosť informácií, oznámenia a postupy výkonu práv dotknutej osoby

8.1. Podľa Článku 12. ods. 1 Nariadenia GDPR prevádzkovateľ prijme vhodné opatrenia s cieľom poskytnúť dotknutej osobe všetky informácie uvedené v článkoch 13 a 14 a všetky oznámenia podľa článkov 15 až 22 a článku 34, ktoré sa týkajú spracúvania, a to v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme, formulované jasne a jednoducho, a to najmä v prípade informácií určených osobitne dieťaťu. Informácie sa poskytujú písomne alebo inými prostriedkami, vrátane v prípade potreby elektronickými prostriedkami. Ak o to požiadala dotknutá osoba, informácie sa môžu poskytnúť ústne za predpokladu, že sa preukázala totožnosť dotknutej osoby iným spôsobom.

8.2. Podľa Článku 12. ods. 1 Nariadenia GDPR prevádzkovateľ uľahčuje výkon práv dotknutej osoby podľa článkov 15 až 22. V prípadoch uvedených v článku 11 ods. 2 nemôže prevádzkovateľ odmietnuť konať na základe žiadosti dotknutej osoby pri výkone jej práva podľa článkov 15 až 22, pokiaľ nepreukáže, že dotknutú osobu nie je schopný identifikovať.

8.3. Podľa Článku 12. ods. 3 Nariadenia GDPR prevádzkovateľ poskytne dotknutej osobe informácie o opatreniach, ktoré sa prijalina základe žiadosti podľa článkov 15 až 22, bez zbytočného odkladu a v každom prípade do jedného mesiaca od doručenia žiadosti. Uvedená lehota sa môže v prípade potreby predĺžiť o ďalšie dva mesiace, pričom sa zohľadní komplexnosť žiadosti a počet žiadostí. Prevádzkovateľ informuje o každom takomto predĺžení dotknutú osobu do jedného mesiaca od doručenia žiadosti spolu s dôvodmi zmeškania lehoty. Ak dotknutá osoba podala žiadosť elektronickými prostriedkami, informácie sa podľa možnosti poskytnú elektronickými prostriedkami, pokiaľ dotknutá osoba nepožiadala o iný spôsob.

8.4. Podľa Článku 12. ods. 4 Nariadenia GDPR ak prevádzkovateľ neprijme opatrenia na základe žiadosti dotknutej osoby, bezodkladne a najneskôr do jedného mesiaca od doručenia žiadosti informuje dotknutú osobu o dôvodoch nekonania a o možnosti podať sťažnosť dozornému orgánu a uplatniť súdny prostriedok nápravy.

8.5. Podľa Článku 12. ods. 5 Nariadenia GDPR informácie poskytnuté podľa článkov 13 a 14 a všetky oznámenia a všetky opatrenia prijaté podľa článkov 15 až 22 a článku 34 sa poskytujú bezplatne. Ak sú žiadosti dotknutej osoby zjavne neopodstatnené alebo neprimerané, najmä pre ich opakujúcu sa povahu, prevádzkovateľ môže buď:
a) požadovať primeraný poplatok zohľadňujúci administratívne náklady na poskytnutie informácií alebo na oznámenie alebo na uskutočnenie požadovaného opatrenia, alebo
b) odmietnuť konať na základe žiadosti. Prevádzkovateľ znáša bremeno preukázania zjavnej neopodstatnenosti alebo neprimeranosti žiadosti.

8.6. Podľa Článku 12. ods. 6 Nariadenia GDPR bez toho, aby bol dotknutý článok 11, ak má prevádzkovateľ oprávnené pochybnosti v súvislosti s totožnosťou fyzickej osoby, ktorá podáva žiadosť uvedenú v článkoch 15 až 21, môže požiadať o poskytnutie dodatočných informácií potrebných na potvrdenie totožnosti dotknutej osoby.

8.7. Podľa Článku 12. ods. 7 Nariadenia GDPR informácie, ktoré sa majú poskytnúť dotknutým osobám podľa článkov 13 a 14, možno podať v kombinácii so štandardizovanými ikonami s cieľom poskytnúť dobre viditeľný, jasný a zrozumiteľný prehľad zamýšľaného spracúvania. Ak sú ikony použité v elektronickej podobe, musia byť strojovo čitateľné.

8.8. Podľa Článku 12. ods. 8 Nariadenia GDPR komisia je splnomocnená v súlade s článkom 92 prijímať delegované akty s cieľom bližšie určiť informácie, ktoré sa majú prezentovať vo forme ikon, a postupy určovania štandardizovaných ikon.

Článok IX.
Informácie, ktoré sa majú poskytovať pri získavaní osobných údajov od dotknutej osoby

9.1. Podľa Článku 13. ods. 1 Nariadenia GDPR v prípadoch, keď sa od dotknutej osoby získavajú osobné údaje, ktoré sa jej týkajú, poskytne prevádzkovateľ pri získavaní osobných údajov dotknutej osobe všetky tieto informácie:
a) totožnosť a kontaktné údaje prevádzkovateľa a v príslušných prípadoch zástupcu prevádzkovateľa;
b) kontaktné údaje prípadnej zodpovednej osoby;
c) účely spracúvania, na ktoré sú osobné údaje určené, ako aj právny základ spracúvania;
d) ak sa spracúvanie zakladá na článku 6 ods. 1 písm. f), oprávnené záujmy, ktoré sleduje prevádzkovateľ alebo tretia strana;
e) príjemcovia alebo kategórie príjemcov osobných údajov, ak existujú;
f) v relevantnom prípade informácia o tom, že prevádzkovateľ zamýšľa preniesť osobné údaje do tretej krajiny alebo medzinárodnej organizácii a informácia o existencii alebo neexistencii rozhodnutia Komisie o primeranosti alebo, v prípade prenosov uvedených v článku 46 alebo 47 či v článku 49 ods. 1 druhom pododseku odkaz na primerané alebo vhodné záruky a prostriedky na získanie ich kópie, alebo kde boli poskytnuté.

9.2. Podľa Článku 13. ods. 2 Nariadenia GDPR okrem informácií, ktoré sa uvádzajú v odseku 1, prevádzkovateľ poskytne dotknutej osobe pri získavaní osobných údajov tieto ďalšie informácie, ktoré sú potrebné na zabezpečenie spravodlivého a transparentného spracúvania:
a) doba uchovávania osobných údajov alebo, ak to nie je možné, kritériá na jej určenie; b) existencia práva požadovať od prevádzkovateľa prístup k osobným údajom týkajúcim sa dotknutej osoby a práva na ich opravu alebo vymazanie alebo obmedzenie spracúvania, alebo práva namietať proti spracúvaniu, ako aj práva na prenosnosť údajov;
c) ak je spracúvanie založené na článku 6 ods. 1 písm. a) alebo na článku 9 ods. 2 písm. a), existencia práva kedykoľvek svoj súhlas odvolať bez toho, aby to malo vplyv na zákonnosť spracúvania založeného na súhlase udelenom pred jeho odvolaním;
d) právo podať sťažnosť dozornému orgánu;
e) informácia o tom, či je poskytovanie osobných údajov zákonnou alebo zmluvnou požiadavkou, alebo požiadavkou, ktorá je potrebná na uzavretie zmluvy, či je dotknutá osoba povinná poskytnúť osobné údaje, ako aj možné následky neposkytnutia takýchto údajov;
f) existencia automatizovaného rozhodovania vrátane profilovania uvedeného v článku 22 ods. 1 a 4 a aspoň v týchto prípadoch zmysluplné informácie o použitom

postupe, ako aj význame a predpokladaných dôsledkoch takéhoto spracúvania pre dotknutú osobu.

9.3. Podľa Článku 13. ods. 3 Nariadenia GDPR ak má prevádzkovateľ v úmysle ďalej spracúvať osobné údaje na iný účel ako ten, na ktorý boli získané, poskytne dotknutej osobe pred takýmto ďalším spracúvaním informácie o tomto inom účele a ďalšie relevantné informácie uvedené v odseku 2.

9.4. Podľa Článku 13. ods. 4 Nariadenia GDPR odseky 1, 2 a 3 sa neuplatňujú v rozsahu, v akom dotknutá osoba už má dané informácie.

Článok X.
Informácie, ktoré sa majú poskytnúť, ak osobné údaje neboli získané od dotknutej osoby

10.1. Podľa Článku 14. ods. 1 Nariadenia GDPR ak osobné údaje neboli získané od dotknutej osoby, prevádzkovateľ poskytne dotknutej osobe tieto informácie:
a) totožnosť a kontaktné údaje prevádzkovateľa a v príslušných prípadoch zástupcu prevádzkovateľa;
b) kontaktné údaje prípadnej zodpovednej osoby;
c) účely spracúvania, na ktoré sú osobné údaje určené, ako aj právny základ spracúvania; d) kategórie dotknutých osobných údajov;
e) príjemcovia alebo kategórie príjemcov osobných údajov, ak existujú;
f) v relevantnom prípade informácia, že prevádzkovateľ zamýšľa preniesť osobné údaje príjemcovi v tretej krajine alebo medzinárodnej organizácii a informácia o existencii alebo neexistencii rozhodnutia Komisie o primeranosti alebo, v prípade prenosov uvedených v článku 46 alebo 47 či v článku 49 ods. 1 druhom pododseku odkaz na primerané alebo vhodné záruky a prostriedky na získanie ich kópie, alebo kde boli poskytnuté.

10.2. Podľa Článku 14. ods. 2 Nariadenia GDPR okrem informácií uvedených v odseku 1 prevádzkovateľ poskytne dotknutej osobe tieto ďalšie informácie potrebné na zabezpečenie spravodlivého a transparentného spracúvania so zreteľom na dotknutú osobu:
a) doba uchovávania osobných údajov, alebo ak to nie je možné, kritériá na jej určenie; b) ak sa spracúvanie zakladá na článku 6 ods. 1 písm. f), oprávnené záujmy, ktoré sleduje prevádzkovateľ alebo tretia strana;
c) existencia práva požadovať od prevádzkovateľa prístup k osobným údajom týkajúcim sa dotknutej osoby a práva na ich opravu alebo vymazanie alebo obmedzenie spracúvania, a práva namietať proti spracúvaniu, ako aj práva na prenosnosť údajov; d) ak je spracúvanie založené na článku 6 ods. 1 písm. a) alebo na článku 9 ods. 2 písm. a), existencia práva kedykoľvek svoj súhlas odvolať bez toho,

aby to malo vplyv na zákonnosť spracúvania založeného na súhlase udelenom pred jeho odvolaním;
e) právo podať sťažnosť dozornému orgánu;
f) z akého zdroja pochádzajú osobné údaje, prípadne informácie o tom, či údaje pochádzajú z verejne prístupných zdrojov;
g) existencia automatizovaného rozhodovania vrátane profilovania uvedeného v článku 22 ods. 1 a 4 a aspoň v týchto prípadoch zmysluplné informácie o použitom postupe, ako aj význame a predpokladaných dôsledkoch takéhoto spracúvania pre dotknutú osobu.

10.3. Podľa Článku 14. ods. 3 Nariadenia GDPR prevádzkovateľ poskytne informácie uvedené v odsekoch 1 a 2:
a) v primeranej lehote po získaní osobných údajov, najneskôr však do jedného mesiaca, pričom zohľadní konkrétnych okolností, za ktorých sa osobné údaje spracúvajú;
b) ak sa osobné údaje majú použiť na komunikáciu s dotknutou osobou, najneskôr v čase prvej komunikácie s touto dotknutou osobou; alebo
c) ak sa predpokladá poskytnutie osobných údajov ďalšiemu príjemcovi, najneskôr vtedy, keď sa osobné údaje prvýkrát poskytnú.

10.4. Podľa Článku 14. ods. 4 Nariadenia GDPR ak má prevádzkovateľ v úmysle ďalej spracúvať osobné údaje na iný účel ako ten, na ktorý boli osobné údaje získané, poskytne dotknutej osobe pred takýmto ďalším spracúvaním informácie o tomto inom účele a akékoľvek ďalšie relevantné informácie uvedené v odseku 2.

10.5. Podľa Článku 14. ods. 5 Nariadenia GDPR odseky 1 až 4 sa neuplatňujú v rozsahu, v akom:
a) dotknutá osoba má už dané informácie;
b) sa poskytovanie takýchto informácií ukáže ako nemožné alebo by si vyžadovalo neprimerané úsilie, najmä v prípade spracúvania na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či na štatistické účely, na ktoré sa vzťahujú podmienky a záruky podľa článku 89 ods. 1, alebo pokiaľ je pravdepodobné, že povinnosť uvedená v odseku 1 tohto článku znemožní alebo závažným spôsobom sťaží dosiahnutie cieľov takéhoto spracúvania. V takých prípadoch prijme prevádzkovateľ vhodné opatrenia na ochranu práv a slobôd a oprávnených záujmov dotknutej osoby vrátane sprístupnenia daných informácií verejnosti;
c) sa získanie alebo poskytnutie výslovne stanovuje v práve Únie alebo v práve členského štátu, ktorému prevádzkovateľ podlieha, a v ktorom sa stanovujú primerané opatrenia na ochranu oprávnených záujmov dotknutej osoby; alebo

d) v prípade, keď osobné údaje musia zostať dôverné na základe povinnosti zachovávania profesijného tajomstva upravenej právom Únie alebo právom členského štátu vrátane povinnosti zachovávať mlčanlivosť vyplývajúcej zo štatútu.

Článok XI.
Právo dotknutej osoby na prístup k údajom

11.1. Podľa Článku 15. ods.1 a Nariadenia GDPR dotknutá osoba má právo získať od prevádzkovateľa potvrdenie o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú, a ak tomu tak je, má právo získať prístup k týmto osobným údajom a tieto informácie:
a) účely spracúvania;
b) kategórie dotknutých osobných údajov;
c) príjemcovia alebo kategórie príjemcov, ktorým boli alebo budú osobné údaje poskytnuté, najmä príjemcovia v tretích krajinách alebo medzinárodné organizácie;
d) ak je to možné, predpokladaná doba uchovávania osobných údajov alebo, ak to nie je možné, kritériá na jej určenie;
e) existencia práva požadovať od prevádzkovateľa opravu osobných údajov týkajúcich sa dotknutej osoby alebo ich vymazanie alebo obmedzenie spracúvania, alebo práva namietať proti takémuto spracúvaniu;
f) právo podať sťažnosť dozornému orgánu;
g) ak sa osobné údaje nezískali od dotknutej osoby, akékoľvek dostupné informácie, pokiaľ ide o ich zdroj;
h) existencia automatizovaného rozhodovania vrátane profilovania uvedeného v článku 22 ods. 1 a 4 a v týchto prípadoch aspoň zmysluplné informácie o použitom postupe, ako aj význame a predpokladaných dôsledkoch takéhoto spracúvania pre dotknutú osobu.

11.2. Podľa Článku 15. ods. 2 Nariadenia GDPR ak sa osobné údaje prenášajú do tretej krajiny alebo medzinárodnej organizácii, dotknutá osoba má právo byť informovaná o primeraných zárukách podľa článku 46 týkajúcich sa prenosu.

11.3. Podľa Článku 15. ods. 3 Nariadenia GDPR prevádzkovateľ poskytne kópiu osobných údajov, ktoré sa spracúvajú. Za akékoľvek ďalšie kópie, o ktoré dotknutá osoba požiada, môže prevádzkovateľ účtovať primeraný poplatok zodpovedajúci administratívnym nákladom. Ak dotknutá osoba podala žiadosť elektronickými prostriedkami, informácie sa poskytnú v bežne používanej elektronickej podobe, pokiaľ dotknutá osoba nepožiadala o iný spôsob.

11.4. Podľa Článku 15. ods. 4 Nariadenia GDPR právo získať kópiu uvedenú v odseku 3 nesmie mať nepriaznivé dôsledky na práva a slobody iných.

Článok XII.

Právo dotknutej osoby na opravu

12.1. Podľa Článku 16. ods. 1 Nariadenia GDPR dotknutá osoba má právo na to, aby prevádzkovateľ bez zbytočného odkladu opravil nesprávne osobné údaje, ktoré sa jej týkajú. So zreteľom na účely spracúvania má dotknutá osoba právo na doplnenie neúplných osobných údajov, a to aj prostredníctvom poskytnutia doplnkového vyhlásenia.

Článok XIII.
Právo dotknutej osoby na vymazanie (právo „na zabudnutie“)

13.1. Podľa Článku 17. ods. 1 Nariadenia GDPR dotknutá osoba má tiež právo dosiahnuť u prevádzkovateľa bez zbytočného odkladu vymazanie osobných údajov, ktoré sa jej týkajú, a prevádzkovateľ je povinný bez zbytočného odkladu vymazať osobné údaje, ak je splnený niektorý z týchto dôvodov:
a) osobné údaje už nie sú potrebné na účely, na ktoré sa získavali alebo inak spracúvali; b) dotknutá osoba odvolá súhlas, na základe ktorého sa spracúvanie vykonáva, podľa článku 6 ods. 1 písm. a) alebo článku 9 ods. 2 písm. a), a ak neexistuje iný právny základ pre spracúvanie;
c) dotknutá osoba namieta voči spracúvaniu podľa článku 21 ods. 1 a neprevažujú žiadne oprávnené dôvody na spracúvanie alebo dotknutá osoba namieta voči spracúvaniu podľa článku 21 ods. 2;
d) osobné údaje sa spracúvali nezákonne;
e) osobné údaje musia byť vymazané, aby sa splnila zákonná povinnosť podľa práva Únie alebo práva členského štátu, ktorému prevádzkovateľ podlieha;
f) osobné údaje sa získavali v súvislosti s ponukou služieb informačnej spoločnosti podľa článku 8 ods. 1.

13.2. Podľa Článku 17. ods. 2 Nariadenia GDPR ak prevádzkovateľ zverejnil osobné údaje a podľa odseku 1 je povinný vymazať osobné údaje, so zreteľom na dostupnú technológiu a náklady na vykonanie opatrení podnikne primerané opatrenia vrátane technických opatrení, aby informoval prevádzkovateľov, ktorí vykonávajú spracúvanie osobných údajov, že dotknutá osoba ich žiada, aby vymazali všetky odkazy na tieto osobné údaje, ich kópiu alebo repliky.

13.3. Podľa Článku 17. ods. 3 Nariadenia GDPR odseky 1 a 2 sa neuplatňujú, pokiaľ je spracúvanie potrebné:
a) na uplatnenie práva na slobodu prejavu a na informácie;
b) na splnenie zákonnej povinnosti, ktorá si vyžaduje spracúvanie podľa práva Únie alebo práva členského štátu, ktorému prevádzkovateľ podlieha, alebo na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi;

c) z dôvodov verejného záujmu v oblasti verejného zdravia v súlade s článkom 9 ods. 2 písm. h) a i), ako aj článkom 9 ods. 3;
d) na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či na štatistické účely podľa článku 89 ods. 1, pokiaľ je pravdepodobné, že právo uvedené v odseku 1 znemožní alebo závažným spôsobom sťaží dosiahnutie cieľov takéhoto spracúvania, alebo
e) na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov.

Článok XIV.
Právo dotknutej osoby na obmedzenie spracúvania

14.1. Podľa Článku 18. ods. 1 Nariadenia GDPR dotknutá osoba má právo na to, aby prevádzkovateľ obmedzil spracúvanie, pokiaľ ide o jeden z týchto prípadov:
a) dotknutá osoba napadne správnosť osobných údajov, a to počas obdobia umožňujúceho prevádzkovateľovi overiť správnosť osobných údajov;
b) spracúvanie je protizákonné a dotknutá osoba namieta proti vymazaniu osobných údajov a žiada namiesto toho obmedzenie ich použitia;
c) prevádzkovateľ už nepotrebuje osobné údaje na účely spracúvania, ale potrebuje ich dotknutá osoba na preukázanie, uplatňovanie alebo obhajovanie právnych nárokov;
d) dotknutá osoba namietala voči spracúvaniu podľa článku 21 ods. 1, a to až do overenia, či oprávnené dôvody na strane prevádzkovateľa prevažujú nad oprávnenými dôvodmi dotknutej osoby.

14.2. Podľa Článku 18. ods. 2 Nariadenia GDPR ak sa spracúvanie obmedzilo podľa odseku 1, takéto osobné údaje sa s výnimkou uchovávania spracúvajú len so súhlasom dotknutej osoby alebo na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov, alebo na ochranu práv inej fyzickej alebo právnickej osoby, alebo z dôvodov dôležitého verejného záujmu Únie alebo členského štátu.

14.3. Podľa Článku 18. ods. 3 Nariadenia GDPR dotknutú osobu, ktorá dosiahla obmedzenie spracúvania podľa odseku 1, prevádzkovateľ informuje pred tým, ako bude obmedzenie spracúvania zrušené.

Článok XV.
Oznamovacia povinnosť v súvislosti s opravou alebo vymazaním osobných údajov alebo obmedzením spracúvania

15.1. Podľa Článku 19. ods. 1 Nariadenia GDPR prevádzkovateľ oznámi každému príjemcovi, ktorému boli osobné údaje poskytnuté, každú opravu alebo vymazanie osobných údajov alebo obmedzenie spracúvania uskutočnené podľa článku 16, článku 17 ods. 1 a článku 18, pokiaľ sa to neukáže ako nemožné alebo si to nevyžaduje

neprimerané úsilie. Prevádzkovateľ o týchto príjemcoch informuje dotknutú osobu, ak to dotknutá osoba požaduje.

Článok XVI.
Právo na prenosnosť údajov

16.1. Podľa Článku 20. ods. 1 Nariadenia GDPR 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 údaje ďalšiemu prevádzkovateľovi bez toho, aby jej prevádzkovateľ, ktorému sa tieto osobné údaje poskytli, bránil, ak:
a) sa spracúvanie zakladá na súhlase podľa článku 6 ods. 1 písm. a) alebo článku 9 ods. 2 písm. a), alebo na zmluve podľa článku 6 ods. 1 písm. b), a
b) ak sa spracúvanie vykonáva automatizovanými prostriedkami.

16.2. Podľa Článku 20. ods. 2 Nariadenia GDPR dotknutá osoba má pri uplatňovaní svojho práva na prenosnosť údajov podľa odseku 1 právo na prenos osobných údajov priamo od jedného prevádzkovateľa druhému prevádzkovateľovi, pokiaľ je to technicky možné.
16.3. Podľa Článku 20. ods. 3 Nariadenia GDPR uplatňovaním práva uvedeného v odseku 1 tohto článku nie je dotknutý článok 17. Uvedené právo sa nevzťahuje na spracúvanie nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi.

16.4. Podľa Článku 20. ods. 4 Nariadenia GDPR právo uvedené v odseku 1 nesmie mať nepriaznivé dôsledky na práva a slobody iných.

Článok XVII.
Právo namietať

17.1. Podľa Článku 21. ods. 1 Nariadenia GDPRdotknutá osoba má právo kedykoľvek namietať z dôvodov týkajúcich sa jej konkrétnej situácie proti spracúvaniu osobných údajov, ktoré sa jej týka, ktoré je vykonávané na základe článku 6 ods. 1 písm. e) alebo f) vrátane namietania proti profilovaniu založenému na uvedených ustanoveniach. Prevádzkovateľ nesmie ďalej spracúvať osobné údaje, pokiaľ nepreukáže nevyhnutné oprávnené dôvody na spracúvanie, ktoré prevažujú nad záujmami, právami a slobodami dotknutej osoby, alebo dôvody na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov.

17.2. Podľa Článku 21. ods. 2 Nariadenia GDPR ak sa osobné údaje spracúvajú na účely priameho marketingu, dotknutá osoba má právo kedykoľvek namietať proti

spracúvaniu osobných údajov, ktoré sa jej týka, na účely takéhoto marketingu, vrátane profilovania v rozsahu, v akom súvisí s takýmto priamym marketingom.

17.3. Podľa Článku 21. ods. 3 Nariadenia GDPRak dotknutá osoba namieta voči spracúvaniu na účely priameho marketingu, osobné údaje sa už na také účely nesmú spracúvať.

17.4. Podľa Článku 21. ods. 4 Nariadenia GDPRdotknutá osoba sa výslovne upozorní na právo uvedené v odsekoch 1 a 2 najneskôr pri prvej komunikácii s ňou, pričom sa toto právo prezentuje jasne a oddelene od akýchkoľvek iných informácií.

17.5. Podľa Článku 21. ods. 5 Nariadenia GDPRv súvislosti s používaním služieb informačnej spoločnosti a bez ohľadu na smernicu 2002/58/ES môže dotknutá osoba uplatňovať svoje právo namietať automatizovanými prostriedkami s použitím technických špecifikácií.

17.6.Podľa Článku 21. ods. 6 Nariadenia GDPRak sa osobné údaje spracúvajú na účely vedeckého alebo historického výskumu či na štatistické účely podľa článku 89 ods. 1, dotknutá osoba má právo namietať z dôvodov týkajúcich sa jej konkrétnej situácie proti spracúvania osobných údajov, ktoré sa jej týka, s výnimkou prípadov, keď je spracúvanie nevyhnutné na plnenie úlohy z dôvodov verejného záujmu.

Článok XVIII.
Automatizované individuálne rozhodovanie vrátane profilovania

18.1. Podľa Článku 22. ods. 1 Nariadenia GDPRdotknutá osoba má právo na to, aby sa na ňu nevzťahovalo rozhodnutie, ktoré je založené výlučne na automatizovanom spracúvaní, vrátane profilovania, a ktoré má právne účinky, ktoré sa jej týkajú alebo ju podobne významne ovplyvňujú.

18.2. Podľa Článku 22. ods. 2 Nariadenia GDPRodsek 1 sa neuplatňuje, ak je rozhodnutie:
a) nevyhnutné na uzavretie alebo plnenie zmluvy medzi dotknutou osobou a prevádzkovateľom,
b) povolené právom Únie alebo právom členského štátu, ktorému prevádzkovateľ podlieha a ktorým sa zároveň stanovujú aj vhodné opatrenia zaručujúce ochranu práv a slobôd a oprávnených záujmov dotknutej osoby, alebo
c) založené na výslovnom súhlase dotknutej osoby.

18.3. Podľa Článku 22. ods. 3 Nariadenia GDPRv prípadoch uvedených v odseku 2 písm. a) a c) prevádzkovateľ vykoná vhodné opatrenia na ochranu práv a slobôd a

oprávnených záujmov dotknutej osoby, a to aspoň práva na ľudský zásah zo strany prevádzkovateľa, práva vyjadriť svoje stanovisko a práva napadnúť rozhodnutie.

18.4. Podľa Článku 22. ods. 4 Nariadenia GDPRrozhodnutia uvedené v odseku 2 sa nezakladajú na osobitných kategóriách osobných údajov uvedených v článku 9 ods. 1, pokiaľ sa neuplatňuje článok 9 ods. 2 písm. a) alebo g) a nie sú zavedené vhodné opatrenia na zaručenie práv a slobôd a oprávnených záujmov dotknutej osoby.

ČASŤ II
Všeobecné povinnosti prevádzkovateľa a sprostredkovateľa podľa Nariadenia GDPR a Zákona č. 18/2018 Z.z.

Článok I.
Zodpovednosť prevádzkovateľa podľa Nariadenia GDPR

1.1. Za ochranu osobných údajov zodpovedá prevádzkovateľ.

1.2. Podľa Článku 24. ods. 1 Nariadenia GDPRs ohľadom na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre

práva a slobody fyzických osôb prevádzkovateľ prijme vhodné technické a organizačné opatrenia, aby zabezpečil a bol schopný preukázať, že spracúvanie sa vykonáva v súlade s týmto nariadením. Uvedené opatrenia sa podľa potreby preskúmajú a aktualizujú.

1.3. Podľa Článku 24. ods. 2 Nariadenia GDPRak je to primerané vzhľadom na spracovateľské činnosti, opatrenia uvedené v odseku 1 zahŕňajú zavedenie primeraných politík ochrany údajov zo strany prevádzkovateľa.

1.4. Podľa Článku 24. ods. 3 Nariadenia GDPR dodržiavanie schválených kódexov správania uvedených v článku 40 alebo schválených certifikačných mechanizmov uvedených v článku 42 sa môže použiť ako prvok na preukázanie splnenia povinností prevádzkovateľa.

1.5. Prevádzkovateľ je povinný prijať primerané bezpečnostné opatrenia podľa Článku 24 Nariadenia GDPR v nadväznosti na Článok 32 a nasl. Nariadenia GDPR.

1.6. Prevádzkovateľ je najmä povinný prijať primerané a účinné opatrenia na ochranu osobných údajov a mal by vedieť preukázať súlad spracovateľských činností s nariadením GDPR a prijatými opatreniami na ochranu osobných údajov.

1.7. V bezpečnostných opatreniach by sa mala zohľadniť povaha, rozsah, kontext a účel spracúvania a riziko pre práva a slobody fyzických osôb.

Článok II.
Špecificky navrhnutá a štandardná ochrana údajov podľa Nariadenia GDPR

2.1. Podľa Článku 25. ods. 1 Nariadenia GDPR so zreteľom na najnovšie poznatky, náklady na vykonanie opatrení a na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou, ktoré spracúvanie predstavuje pre práva a slobody fyzických osôb, prevádzkovateľ v čase určenia prostriedkov spracúvania aj v čase samotného spracúvania prijme primerané technické a organizačné opatrenia, ako je napríklad pseudonymizácia, ktoré sú určené na účinné zavedenie zásad ochrany údajov, ako je minimalizácia údajov, a začlení do spracúvania nevyhnutné záruky s cieľom splniť požiadavky tohto nariadenia a chrániť práva dotknutých osôb.

2.2. Podľa Článku 25. ods. 2 Nariadenia GDPR prevádzkovateľ vykoná primerané technické a organizačné opatrenia, aby zabezpečil, že štandardne sa spracúvajú len osobné údaje, ktoré sú nevyhnutné pre každý konkrétny účel spracúvania. Uvedená

povinnosť sa vzťahuje na množstvo získaných osobných údajov, rozsah ich spracúvania, dobu ich uchovávania a ich dostupnosť. Konkrétne sa takýmito opatreniami zabezpečí, aby osobné údaje neboli bez zásahu fyzickej osoby štandardne prístupné neobmedzenému počtu fyzických osôb.

2.3. Podľa Článku 25. ods. 3 Nariadenia GDPR schválený certifikačný mechanizmus podľa článku 42 sa môže použiť ako prvok na preukázanie súladu s požiadavkami uvedenými v odsekoch 1 a 2 tohto článku.

Článok III.
Sprostredkovateľ podľa nariadenia GDPR

3.1. Podľa Článku 28. ods. 1 Nariadenia GDPR ak sa má spracúvanie uskutočniť v mene prevádzkovateľa, prevádzkovateľ využíva len sprostredkovateľov poskytujúcich dostatočné záruky na to, že sa prijmú primerané technické a organizačné opatrenia tak, aby spracúvanie spĺňalo požiadavky tohto nariadenia a aby sa zabezpečila ochrana práv dotknutej osoby.

3.2. Podľa Článku 28. ods. 2 Nariadenia GDPR sprostredkovateľ nezapojí ďalšieho sprostredkovateľa bez predchádzajúceho osobitného alebo všeobecného písomného povolenia prevádzkovateľa. V prípade všeobecného písomného povolenia sprostredkovateľ informuje prevádzkovateľa o akýchkoľvek zamýšľaných zmenách v súvislosti s pridaním alebo nahradením ďalších sprostredkovateľov, čím sa prevádzkovateľovi dá možnosť namietať voči takýmto zmenám.

3.3. Podľa Článku 28. ods. 3 Nariadenia GDPR spracúvanie sprostredkovateľom sa riadi zmluvou alebo iným právnym aktom podľa práva Únie alebo práva členského štátu, ktoré zaväzuje sprostredkovateľa voči prevádzkovateľovi a ktorým sa stanovuje predmet a doba spracúvania, povaha a účel spracúvania, typ osobných údajov a kategórie dotknutých osôb a povinnosti a práva prevádzkovateľa.

Uvedená zmluva alebo iný právny akt najmä stanovia, že sprostredkovateľ:
a) spracúva osobné údaje len na základe zdokumentovaných pokynov prevádzkovateľa, a to aj pokiaľ ide o prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii, s výnimkou prípadov, keď si to vyžaduje právo Únie alebo právo členského štátu, ktorému sprostredkovateľ podlieha; v takom prípade sprostredkovateľ oznámi prevádzkovateľovi túto právnu požiadavku pred spracúvaním, pokiaľ dané právo takéto oznámenie nezakazuje zo závažných dôvodov verejného záujmu;

b) zabezpečí, aby sa osoby oprávnené spracúvať osobné údaje zaviazali, že zachovajú dôvernosť informácií, alebo aby boli viazané vhodnou povinnosťou zachovávať dôvernosť informácií vyplývajúcou zo štatútu;

c) vykoná všetky požadované opatrenia podľa článku 32;

d) dodržiava podmienky zapojenia ďalšieho sprostredkovateľa uvedené v odsekoch 2 a 4;

e)po zohľadnení povahy spracúvania v čo najväčšej miere pomáha prevádzkovateľovi vhodnými technickými a organizačnými opatreniami pri plnení jeho povinnosti reagovať na žiadosti o výkon práv dotknutej osoby ustanovených v kapitole III;

f) pomáha prevádzkovateľovi zabezpečiť plnenie povinností podľa článkov 32 až 36 s prihliadnutím na povahu spracúvania a informácie dostupné sprostredkovateľovi;

g) po ukončení poskytovania služieb týkajúcich sa spracúvania na základe rozhodnutia prevádzkovateľa všetky osobné údaje vymaže alebo vráti prevádzkovateľovi a vymaže existujúce kópie, ak právo Únie alebo právo členského štátu nepožaduje uchovávanie týchto osobných údajov;

h) poskytne prevádzkovateľovi všetky informácie potrebné na preukázanie splnenia povinností stanovených v tomto článku a umožní audity, ako aj kontroly vykonávané prevádzkovateľom alebo iným audítorom, ktorého poveril prevádzkovateľ, a prispieva k nim.
So zreteľom na písmeno h) prvého pododseku sprostredkovateľ bezodkladne informuje prevádzkovateľa, ak sa podľa jeho názoru pokynom porušuje toto nariadenie alebo iné právne predpisy Únie alebo členského štátu týkajúce sa ochrany údajov.

3.4. Podľa Článku 28. ods. 4 Nariadenia GDPR ak sprostredkovateľ zapojí do vykonávania osobitných spracovateľských činností v mene prevádzkovateľa ďalšieho sprostredkovateľa, tomuto ďalšiemu sprostredkovateľovi sa prostredníctvom zmluvy alebo iného právneho aktu podľa práva Únie alebo práva členského štátu uložia rovnaké povinnosti ochrany údajov, ako sa stanovujú v zmluve alebo inom právnom akte uzatvorenom medzi prevádzkovateľom a sprostredkovateľom podľa odseku 3, a to predovšetkým poskytnutie dostatočných záruk na vykonanie primeraných technických a organizačných opatrení takým spôsobom, aby spracúvanie spĺňalo požiadavky tohto nariadenia. Ak tento ďalší sprostredkovateľ nesplní svoje povinnosti ochrany údajov, pôvodný sprostredkovateľ zostáva voči prevádzkovateľovi plne zodpovedný za plnenie povinností tohto ďalšieho sprostredkovateľa.

3.5. Podľa Článku 28. ods. 5 Nariadenia GDPR dodržiavanie schváleného kódexu správania uvedeného v článku 40 alebo schváleného certifikačného mechanizmu uvedeného v článku 42 sprostredkovateľom sa môže použiť ako prvok na preukázanie dostatočných záruk uvedených v odsekoch 1 a 4 tohto článku.

3.6. Podľa Článku 28. ods. 6 Nariadenia GDPR bez toho, aby tým bola dotknutá individuálna zmluva medzi prevádzkovateľom a sprostredkovateľom, zmluva alebo iný právny akt uvedené v odsekoch 3 a 4 tohto článku sa môžu vcelku alebo sčasti zakladať na štandardných zmluvných doložkách uvedených v odsekoch 7 a 8 tohto článku, a to aj v prípadoch, keď sú súčasťou certifikácie udelenej prevádzkovateľovi alebo sprostredkovateľovi podľa článkov 42 a 43.

3.7. Podľa Článku 28. ods. 7 Nariadenia GDPR komisia môže stanoviť štandardné zmluvné doložky pre záležitosti uvedené v odsekoch 3 a 4 tohto článku a v súlade s postupom preskúmania uvedeným v článku 93 ods. 2.

3.8. Podľa Článku 28. ods. 8 Nariadenia GDPR dozorný orgán môže prijať štandardné zmluvné doložky pre záležitosti uvedené v odsekoch 3 a 4 tohto článku a v súlade s mechanizmom konzistentnosti uvedeným v článku 63.

3.9. Podľa Článku 28. ods. 9 Nariadenia GDPR zmluva alebo iný právny akt uvedené v odsekoch 3 a 4 sa vypracujú v písomnej podobe vrátane elektronickej podoby.

3.10. Podľa Článku 28. ods. 10 Nariadenia GDPR bez toho, aby boli dotknuté články 82, 83 a 84, ak sprostredkovateľ poruší toto nariadenie tým, že určí účely a prostriedky spracúvania, považuje sa v súvislosti s daným spracúvaním za prevádzkovateľa.

Článok IV.
Spracúvanie osobných údajov na základe poverenia prevádzkovateľa alebo sprostredkovateľa

4.1. Podľa Článku 29. Nariadenia GDPR sprostredkovateľ a každá osoba konajúca na základe poverenia prevádzkovateľa alebo sprostredkovateľa, ktorá má prístup k osobným údajom, môže spracúvať tieto údaje len na základe pokynov prevádzkovateľa s výnimkou prípadov, keď sa to vyžaduje podľa práva Únie alebo práva členského štátu.

Článok V.
Bezpečnosť spracúvania osobných údajov podľa Nariadenia GDPR

5.1. Podľa Článku 32. ods. 1 Nariadenia GDPR prevádzkovateľ a sprostredkovateľ prijmú so zreteľom na najnovšie poznatky, náklady na vykonanie opatrení a na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb, primerané technické a organizačné opatrenia s cieľom zaistiť úroveň bezpečnosti primeranú tomuto riziku, pričom uvedené opatrenia prípadne zahŕňajú aj:

a) pseudonymizáciu a šifrovanie osobných údajov;

b) schopnosť zabezpečiť trvalú dôvernosť, integritu, dostupnosť a odolnosť systémov spracúvania a služieb;

c) schopnosť včas obnoviť dostupnosť osobných údajov a prístup k nim v prípade fyzického alebo technického incidentu;

d) proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania.

5.2. Podľa Článku 32. ods. 2 Nariadenia GDPR pri posudzovaní primeranej úrovne bezpečnosti sa prihliada predovšetkým na riziká, ktoré predstavuje spracúvanie, a to najmä v dôsledku náhodného alebo nezákonného zničenia, straty, zmeny, neoprávneného poskytnutia osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávneného prístupu k takýmto údajom.

5.3. Podľa Článku 32. ods. 3 Nariadenia GDPR dodržiavanie schváleného kódexu správania uvedeného v článku 40 alebo schváleného certifikačného mechanizmu uvedeného v článku 42 sa môže použiť ako prvok na preukázanie súladu s požiadavkami uvedenými v odseku 1 tohto článku.

5.4. Podľa Článku 32. ods. 4 Nariadenia GDPR prevádzkovateľ a sprostredkovateľ podniknú kroky na zabezpečenie toho, aby každá fyzická osoba konajúca na základe poverenia prevádzkovateľa alebo sprostredkovateľa, ktorá má prístup k osobným údajom, spracúvala tieto údaje len na základe pokynov prevádzkovateľa s výnimkou prípadov, keď sa to od nej vyžaduje podľa práva Únie alebo práva členského štátu.

5.5. K bezpečnostným opatreniam možno zaradiť najmä prijatie primeraných technických, organizačných a personálnych bezpečnostných opatrení a záruk zo strany prevádzkovateľa, ako aj sprostredkovateľa, ktoré zohľadňujú najmä:

a) zásady spracúvania osobných údajov ako zákonnosť, spravodlivosť a transparentnosť;

b) obmedzenie a kompatibilitu účelov spracúvania;

c) minimalizáciu údajov, pseudonymizáciu alebo šifrovanie údajov a minimalizáciu uchovávania údajov;

d) správnosť údajov;

e) integritu a dôvernosť, dostupnosti údajov;

f) zásady nevyhnutnosti a primeranosti (vzťahuje sa aj na rozsah a množstvo spracúvaných osobných údajov, dobu uchovávania a prístup k týmto osobným údajom) spracúvania s ohľadom na účel spracovateľskej operácie;

g) povahu, rozsah, kontext a účel spracovateľskej operácie;

h) odolnosť a obnovu systémov spracúvania;

i) poverenia oprávnených osôb;

j) prijatie primeraných opatrení, aby sa zabezpečila oprava alebo vymazanie nesprávnych údajov, či iný výkon práv dotknutej osoby;

k) riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb (najmä náhodné alebo nezákonné zničenie osobných údajov, strata alebo zmena osobných údajov, zneužitie osobných údajov – neoprávnený prístup alebo neoprávnené poskytnutie; posúdenie rizík so zreteľom na pôvod, povahu, pravdepodobnosť a závažnosť rizika v súvislosti so spracúvaním, a na identifikáciu najlepších postupov na zmiernenie rizika).

Článok VI.
Ďalšie práva a povinnosti prevádzkovateľa a sprostredkovateľa podľa Zákona č. 18/2018 Z.z.

6.1. Podľa ust. § 78 ods. 1 Zákona č. 18/2018 Z.z. 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.

6.2. Podľa ust. § 78 ods. 2 Zákona č. 18/2018 Z.z. 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.

6.3.Podľa ust. § 78 ods. 3 Zákona č. 18/2018 Z.z. 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 zaradenia, 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.

6.4. Podľa ust. § 78 ods. 4 Zákona č. 18/2018 Z.z. pri spracúvaní osobných údajov možno využiť na účely identifikovania fyzickej osoby všeobecne použiteľný identifikátor podľa osobitného predpisu (Zákon č. 301/1995 Z. z. o rodnom čísle v znení zákona č. 515/2003 Z. z.) 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.

6.5. Podľa ust. § 78 ods. 5 Zákona č. 18/2018 Z.z. 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.

6.6. Podľa ust. § 78 ods. 6 Zákona č. 18/2018 Z.z. 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.

6.7. Podľa ust. § 78 ods. 7 Zákona č. 18/2018 Z.z. ak dotknutá osoba nežije, súhlas vyžadovaný podľa tohto zákona alebo osobitného predpisumôže poskytnúť jej blízka osoba. Súhlas nie je platný, ak čo len jedna blízka osoba písomne vyslovila nesúhlas.

6.8. Podľa ust. § 78 ods. 8 Zákona č. 18/2018 Z.z. 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 účinnýchtechnických a organizačných opatrení najmä na zabezpečenie dodržiavania zásady minimalizácie údajov a pseudonymizácie.

6.9. Podľa ust. § 78 ods. 9 Zákona č. 18/2018 Z.z. ak sa osobné údaje spracúvajú na vedecký účel, účel historického výskumu alebo na štatistický účel, môžu byť práva dotknutej osoby podľa § 21, § 22, § 24 a 27 alebo podľa osobitného predpisu (Čl. 15, 16, 18 a 21 nariadenia GDPR)obmedzené osobitným predpisom alebo medzinárodnou zmluvou, ktorou je Slovenská republika viazaná, ak sú prijaté primerané podmienky a záruky podľa odseku 6, ak by tieto práva dotknutej osoby pravdepodobne znemožnili alebo závažným spôsobom sťažili dosiahnutie týchto účelov, a takéto obmedzenie práv dotknutej osoby je nevyhnutné na dosiahnutie týchto účelov.

6.10. Podľa ust. § 78 ods. 10 Zákona č. 18/2018 Z.z. ak sa osobné údaje spracúvajú na účel archivácie, môžu byť práva dotknutej osoby podľa § 21, § 22 a § 24 až 27 alebo podľa osobitného predpisu (Čl. 15, 16, 18 až 21 nariadenia GDPR) obmedzené osobitným predpisom, ak sú prijaté primerané podmienky a záruky podľa odseku 6, ak by tieto práva dotknutej osoby pravdepodobne znemožnili alebo závažným spôsobom sťažili dosiahnutie týchto účelov, a takéto obmedzenie práv dotknutej osoby je nevyhnutné na dosiahnutie týchto účelov.

6.11. Podľa ust. § 78 ods. 11 Zákona č. 18/2018 Z.z. Prevádzkovateľ a sprostredkovateľ pri prijímaní bezpečnostných opatrení a pri posudzovaní vplyvu na ochranu osobných údajov postupuje primerane podľa medzinárodných noriem a štandardov bezpečnosti.

Článok VII.
Povinnosť mlčanlivosti podľa Zákona č. 18/2018 Z.z.

7.1. Podľa ust. § 79 ods. 1 Zákona č. 18/2018 Z. z. prevádzkovateľ a sprostredkovateľ je povinný zachovávať mlčanlivosť o osobných údajoch, ktoré spracúva. Povinnosť mlčanlivosti trvá aj po ukončení spracúvania osobných údajov.

7.2. Podľa ust. § 79 ods. 2Zákona č. 18/2018 Z. z. prevádzkovateľ a sprostredkovateľ je povinný zaviazať 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.

7.3. Podľa ust. § 79 ods. 3Zákona č. 18/2018 Z. z. povinnosť mlčanlivosti podľa odsekov 1 a 2 neplatí, ak je to nevyhnutné na plnenie úloh súdu a orgánov činných v trestnom konaní podľa osobitného zákona; tým nie sú dotknuté ustanovenia o mlčanlivosti podľa osobitných predpisov (napríklad zákon č. 566/1992 Zb. o Národnej banke Slovenska v znení neskorších predpisov, zákon č. 46/1993 Z. z. v znení neskorších predpisov, zákon Národnej rady Slovenskej republiky č. 171/1993 Z. z. v znení neskorších predpisov, zákon č. 215/2004 Z. z. v znení neskorších predpisov, zákon č. 563/2009 Z. z. o dani z motorových vozidiel a o zmene a doplnení niektorých zákonov v znení neskorších predpisov alebo zákon č. 307/2014 Z. z. o niektorých opatreniach súvisiacich s oznamovaním protispoločenskej činnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov).

7.4. Podľa ust. § 79 ods. 4Zákona č. 18/2018 Z. z. ustanovenia o povinnosti mlčanlivosti podľa odsekov 1 a 2 § 45 ods. 5 sa nepoužijú vo vzťahu k úradu pri plnení jeho úloh podľa tohto zákona alebo osobitného predpisu.

ČASŤ III
Technické a organizačnéopatrenia prevádzkovateľa za účelom zabezpečenia ochrany osobných údajov podľa Nariadenia GDPR a Zákona č. 18/2018 Z.z.

Článok I.
Základné ciele

1.1. Základným cieľom prijatia primeraných technických a organizačných opatrení je zabezpečiť ochranu spracúvaných osobných údajov predich stratou, odcudzením, poškodením, alebo prístupom neoprávnených osôb k týmto údajom.

1.2. Hlavnou úlohou prijatých technických a organizačných opatrení je zamedziť možným negatívnym dopadom na bezpečnosť osobných údajov spracúvaných ako v automatizovanej, tak aj neautomatizovanej podobe.

1.3. Je nevyhnutné prijať také technické a organizačné opatrenia, ktoré zabezpečia, aby riziká, ktorým je vystavený informačný systém, boli znížené na minimum.

Článok II.
Požadované technické opatrenia

2.1. Prevádzkovateľ nesmie pri spracúvaní osobných údajov v automatizovanej podobe používať operačný systém Windows XP a staršie operačné systémy.

2.2.Prevádzkovateľ je povinný zabezpečiť aby prenos osobných údajov, získaných od dotknutej osoby, bol zabezpečený šifrovaním. Za týmto účelom je potrebné použitie SSL certifikátu, HTTPS protokolu, a v prípade programov, ktoré sú na serveroch, je potrebné prenos osobných údajov zabezpečiť kryptovaním(napríklad pomocou VPN, SSH alebo podobných štandardných zabezpečených protokolov).

2.3.Prevádzkovateľ je povinný zabezpečiť, aby prístup k informačným systémom v automatizovanejpodobe bol zabezpečený najnovšími technológiami, napr.: užívateľským menom, heslom, a pod.

2.4. Každá databáza musí byť zabezpečená heslom, aby sa k nej mohli dostať iba oprávnené osoby. Heslá musia spĺňať minimálne požiadavkyzodpovedajúce najnovším štandardom pre bezpečnosť internetového prostredia, napr. minimálny počet znakov a zložitosť,. Heslá musia byť menené v pravidelných intervaloch. Prihlasovacie údaje, ako je ID a heslo nesmú byť v rámci siete nikdy prenášané nezabezpečené.

2.5. V súvislosti s predchádzajúcim bodom je potrebné nastaviť aj proces zablokovania hesla.

2.6.Prístupové oprávnenia musia byť vždy pridelené iba pre také informačné systémy v automatizovanej podobe, ku ktorým daný užívateľ potrebuje prístup za účelom plnenia svojichpovinností. Prístupové identifikačné údaje musia byť prideľované na individuálnom základe a musia byť viazané na osobné údaje užívateľa. Je vylúčené používanie skupinových ID alebo hesiel väčším počtom užívateľov.

2.7.Akékoľvek zariadenia s osobnými údajmi, ako aj vymeniteľné médiá, musia byť vždy zabezpečené proti ich odcudzeniu. Zároveň však musia byť aj zašifrované, aby pre prípad, že by došlo k ich odcudzeniu, nebolo možné skopírovať osobné údaje po ich pripojení k inému počítaču.

2.8.Zabezpečenie osobných údajov na zariadeniach je možné dosiahnuť viacerými spôsobmi, medzi ktoré patrí:

a) použitie hesla na zabezpečenie konkrétneho súboru, ktorý obsahuje osobný údaj, pri jeho uložení na disk (Word/Excel/PDF);

b) použitie programu, ktorý zakryptuje konkrétny súbor na disku;

c) použitie programu, ktorý konkrétny súbor archivuje s heslom a následne ho uloží na disk

d) v prípade novších operačných systémov je možné použiť aj nové programy na zabezpečenie (napr.: bitlocker)

e) je zakázané v rámci lokálnej počítačovej siete zdieľať súbory, ktoré obsahujú osobné údaje, bez toho, aby bolo požadované zadať heslo, aby sa zabránilo automatickému prístupu k týmto údajom.

2.9. Je nevyhnutné trvalé používanie antivírusového programu.

2.10. V prípade prenosu osobných údajov do externých informačných systémov mimo zabezpečených priestorov prevádzkovateľa, je nevyhnutnou podmienkou prenosu šifrovanie týchto údajov.

2.11. Pri automatizovanom spracovaní osobných údajov je nevyhnutné zabezpečiť zálohovanie údajov.

2.12. Osobné údaje fyzických osôb, pri ktorých už netrvá povinnosť ich spracúvať podľa zákona, je potrebné zlikvidovať.

2.13. IT a sieťové systémy, ktoré spracúvajú osobné údaje, musia byť zabezpečené voči neoprávnenému prístupu pomocou najmodernejších opatrení, ktorými sú obvykle firewall.

2.14. Backend systémy musia byť posilnené pomocou moderných technológií, aby boli zabezpečené proti útoku a neoprávneným prístupom.

2.15. Všetky rozhrania s inými IT procesmi musia byť definované a popísané.

2.16. Uchovávanie osobných údajov musí byť realizované v zašifrovanom formáte.

2.17. V prípade likvidácie osobných údajov musia byť použité bezpečné metódy na vymazanie a zničenie osobných údajov. O trvalom vymazaní osobných údajov musia byť vedené záznamy.

2.18. Reprodukcia osobných údajov, dátových nosičov a dokumentov, ktoré obsahujú osobné údaje, je zakázaná, pokiaľ to nie je výslovnou súčasťou plnenia danej úlohy stanovenej sprostredkovateľom.

2.19. K systémom prevádzkovateľa, ktoré slúžia na spracúvanie osobných údajov, je zakázané pripájať externé (odpojiteľné) dátové nosiče (USB, pamäťové karty, CD, DVD), ako aj kopírovať osobné údaje sprístupnené na externé odpojiteľné dátové nosiče, pokiaľ to nie je výslovne súčasťou plnenia zadanej úlohy.

2.20. Všetky materiálne nosiče údajov musia byť zabezpečené proti prístupu neoprávnených osôb.

2.21. Osobnú údaje musia byť pravidelne zálohované tak, aby bolo zabezpečené, že budú dostupné aj v prípade mimoriadnych situácii. Za týmto účelov musí byť vytvorená koncepcia zálohovania dát, vďaka, ktorej budú užívatelia IT systémov, spracúvajúcich osobné údaje môcť využívať všetky dostupné prostriedky na zaistenie obnovy osobných údajov v primeranom čase po vzniku mimoriadnej udalosti.

2.21. Na všetky zdieľané súbory je nutné nastaviť heslá.

2.22. Údaje v el. forme sa ukladajú na databázový server a na prenosné nosiče (CD, DVD), ktoré sú uložené v trezoroch alebo v archíve.

2.23 Údaje, ktoré sú na diskoch v PC, sa musia chrániť tak, že : antivírus, zaheslovanie programu, samostatné heslo pre vstup do programu pre každého užívateľa, zálohy disku musia byť uskladnené mimo budovy prevádzkovateľa.

2.23. Každé pamäťové médium musí byť evidované, označené, a musia byť vždy v nevyhnutnom počte.

2.24. Zálohy dát musia byť uložené v oddelenej miestnosti od miesta spracúvania.

2.25. Pri dlhodobom archivovaní je nevyhnutné vykonať kontrolu uloženia a čitateľnosti dát , prípadný prepis na novšie typy nosičov.

2.26. Záložné kapacity informačného systému musia byť umiestnené v sekundárnom zabezpečenom priestore vzdialené od zabezpečeného priestoru.

2.27. Najmenej jeden krát za rok je nevyhnutné vykonať test obnovy informačného systému a údajov z prevádzkovej zálohy.

Článok III.
Požadované organizačné opatrenia

3.1. Prevádzkovateľ stanoví pravidlá spracúvania osobných údajov a určí okruh osôb, ktoré sú oprávnené osobné údaje u prevádzkovateľa spracúvať.

3.2. Spracúvať osobné údaje u prevádzkovateľa môžu iba oprávnené osoby.

3.3. Prevádzkovateľ je povinný zabezpečiť informovanie oprávnených osôb o legislatíve, ktorá sa týka ochrany osobných údajov a o možných negatívnych

dopadoch na bezpečnosť osobných údajov v prípade nedodržania stanovených povinností.

3.4. Prevádzkovateľ je povinný zabezpečiť oboznámenie oprávnených osôb s prijatými technickými a organizačnými opatreniami prevádzkovateľa a zároveň ich poučiť o všetkých povinnostiach súvisiacich s ochranou osobných údajov.

3.5. Priestory, v ktorých sa spracúvajú osobné údaje, sa musia zamykať mimo pracovnej doby, ako aj pri dočasnej neprítomnosti oprávnenej osoby.

3.6.Všetky materiálne nosiče údajov musia byť zabezpečené proti prístupu neoprávnených osôb (uloženie v uzamykateľných skriniach).

3.7. Dokumenty v listinnej podobe sa musia archivovať v uzamknutých skriniach. Dokumenty s prešlou dobou archivácie sa musia bezpečne natrvalo zlikvidovať.

3.8. Dokumenty, ktoré podliehajú archivácii, musia byť uložené v zabezpečenom archíve : uzamykateľná skriňa , trezor, uzamykateľná miestnosť.

3.9.Prevádzkovateľ a oprávnené osoby spracúvajú údaje na takom mieste a takým spôsobom, aby sa znemožnilo ich odcudzeniu.

3.10. Prevádzkovateľ a oprávnené osoby sú povinné zabezpečiť, aby nosiče údajov pri ich prenose medzi miestom uloženia a spracovania neboli sprístupnené neoprávneným osobám.

3.11. Zamestnanci sú oprávnení sa zdržiavať na pracovisku mimo pracovnej doby len so súhlasom prevádzkovateľa.

3.12. Osoby, ktoré nepatria do okruhu oprávnených osôb a sú prizvané na technickú pomoc pri spracovaní osobných údajov (tlačenie, kopírovanie, balenie do obálok a pod.) musia byť poučené zodpovednou osobou o zákaze oboznámiť sa s obsahom informácií a v prípade podvedomého oboznámenia je potrebné ich poučiť o povinnosti mlčanlivosti

3.13. Informačný systém sa musí chrániť pred prístupom nepovolaných osôb.

3.14. Ochranu pred prístupom do priestorov prevádzkovateľa je nevyhnutné zabezpečiť aspoň mechanickými zabezpečovacími systémami, prípadne SBS (nadštandard: kamery, el. zariadenia)

3.15. Pracoviská, kde sa spracúvajú osobné údaje, je nevyhnutné zabezpečiť uzamykateľnými dverami.

3.16. Listinné dokumenty informačného systému musia byť vždy umiestnené mimo dosahu neoprávnených osôb (uzamknuté v skrini), pričom kľúče od uzamknutých skríň majú iba určité osoby podľa rozsahu svojho oprávnenia.

3.17. Tlač a kopírovanie papierových dokumentov, obsahujúcich osobné údaje musí byť fyzicky riadené oprávnenou osobou tak, aby bolo zabezpečené, že žiadne dokumenty nezostanú ponechané v zariadeniach pre tlač, či kopírovanie.

3.18. Dokumenty, obsahujúce osobné údaje, musia byť klasifikované ako dôverné a prenášané musia byť prenášané v uzavretom nosiči (kontajner, obálka), pričom musí obsahovať označenie osoby, ktorej má byť dokument doručený.

3.19. Oprávnená osoba je povinná zabezpečiť aby nedošlo k zneužitiu dokumentov, obsahujúcich osobné údaje, na jej pracovisku a zabezpečiť uloženie dokumentov tak, aby nedošlo k neoprávnenému prístupu k osobným údajom, napr. v uzamykateľnej skrini a priestore.

3.20. Po skončení účelu spracúvania osobných údajov musia byť papierové dokumenty, obsahujúce osobné údaje, odovzdané dotknutej osobe, alebo zničené takým spôsobom, aby nebolo možné tieto údaje z dokumentu obnoviť.

3.21. Prevádzkovateľ je povinný zabezpečiť ochranu osobných údajov proti ich náhodnému zničeniu, či strate (zabezpečenie dostupnosti údajov).

3.22. Osobnú údaje musia byť pravidelne zálohované tak, aby bolo zabezpečené, že budú dostupné aj v prípade mimoriadnych situácii. Za týmto účelov musí byť vytvorená koncepcia zálohovania dát, vďaka, ktorej budú užívatelia IT systémov, spracúvajúcich osobné údaje môcť využívať všetky dostupné prostriedky na zaistenie obnovy osobných údajov v primeranom čase po vzniku mimoriadnej udalosti.

3.23. Osobné údaje sa musia chrániť pred prístupom neoprávnených osôb. Ochranu pred prístupom neoprávnených osôb do priestorov prevádzkovateľa je nevyhnutné zabezpečiť aspoň mechanickými zabezpečovacími systémami, prípadne strážnou službou, alebo kamerovým systémom.

3.24. Pracoviská oprávnených osôb, ktoré spracúvajú osobné údaje, by mali byť vybavené plne uzamykateľnými dverami.

3.25. Neautomatizované prostriedky informačného systému musia byť na pracovisku umiestnené mimo dosahu neoprávnených osôb a v čase neprítomnosti oprávnených osôb na pracovisku musia byť uzamknuté v skrini.

3.26. Písomné, obrazové, zvukové iné záznamy po dátume expiráciemusia byť fyzicky zlikvidované skartovaním, rozložením, spálením, pri čiastočnom likvidovaní prichádza do úvahy začiernenie.

3.27. Prepisovateľné pamäťové médiá sa musia zlikvidovaťvymazaním a naformátovaním, aby nebolo údaje možné obnoviť. Nie obyčajné vymazanie ale prekrytie prázdnymi znakmi alebo iným textom.

3.28. Neprepisovateľné pamäťové médiá sa musia fyzicky zlikvidovať.

Článok IV.
Zodpovedná osoba

4.1. Podľa Článku 37. ods. 1 Nariadenia GDPR prevádzkovateľ a sprostredkovateľ určia zodpovednú osobu v každom prípade, keď:

a) spracúvanie vykonáva orgán verejnej moci alebo verejnoprávny subjekt s výnimkou súdov pri výkone ich súdnej právomoci;

b) hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa sú spracovateľské operácie, ktoré si vzhľadom na svoju povahu, rozsah a/alebo účely vyžadujú pravidelné a systematické monitorovanie dotknutých osôb vo veľkom rozsahu; alebo

c) hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa je spracúvanie osobitných kategórií údajov podľa článku 9 vo veľkom rozsahu alebo spracúvanie osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky podľa článku 10.

4.2. Podľa Článku 37. ods. 2 Nariadenia GDPR skupina podnikov môže určiť jednu zodpovednú osobu, ak je zodpovedná osoba ľahko dostupná z každej prevádzkarne.

4.3. Podľa Článku 37. ods. 3 Nariadenia GDPR ak je prevádzkovateľom alebo sprostredkovateľom orgán verejnej moci alebo verejnoprávny subjekt, pre viaceré takéto orgány alebo subjekty sa môže určiť jedna zodpovedná osoba, pričom sa zohľadní ich organizačná štruktúra a veľkosť.

4.4. Podľa Článku 37. ods. 4 Nariadenia GDPR v iných prípadoch, ako sú prípady uvedené v odseku 1, zodpovednú osobu môže určiť alebo, ak sa to vyžaduje v práve Únie alebo v práve členského štátu, určí 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.

4.5. Podľa Článku 37. ods. 5 Nariadenia GDPR zodpovedná osoba sa určí na základe jej odborných kvalít, a to najmä na základe jej odborných znalostí práva a postupov v oblasti ochrany údajov a na základe spôsobilosti plniť úlohy uvedené v článku 39.

4.6. Podľa Článku 37. ods. 6 Nariadenia GDPR zodpovedná osoba môže byť členom personálu prevádzkovateľa alebo sprostredkovateľa, alebo môže plniť úlohy na základe zmluvy o poskytovaní služieb.

4.7. Podľa Článku 37. ods. 7Nariadenia GDPR prevádzkovateľ alebo sprostredkovateľ zverejnia kontaktné údaje zodpovednej osoby a oznámia ich dozornému orgánu.

4.8. Podľa Článku 38. ods. 1 Nariadenia GDPR Článok prevádzkovateľ a sprostredkovateľ zabezpečia, aby bola zodpovedná osoba riadnym spôsobom a včas zapojená do všetkých záležitostí, ktoré súvisia s ochranou osobných údajov.

4.9. Podľa Článku 38. ods. 2 Nariadenia GDPR prevádzkovateľ a sprostredkovateľ podporujú zodpovednú osobu pri plnení úloh uvedených v článku 39, a to tak, že poskytujú zdroje potrebné na plnenie týchto úloh a prístup k osobným údajom a spracovateľským operáciám, ako aj zdroje na udržiavanie jej odborných znalostí.

4.10. Podľa Článku 38. ods. 3 Nariadenia GDPR prevádzkovateľ a sprostredkovateľ zabezpečia, aby zodpovedná osoba v súvislosti s plnením týchto úloh nedostávala žiadne pokyny. Prevádzkovateľ ani sprostredkovateľ ju nesmú odvolať alebo postihovať za výkon jej úloh. Zodpovedná osoba podlieha priamo najvyššiemu vedeniu prevádzkovateľa alebo sprostredkovateľa.

4.11. Podľa Článku 38. ods. 4 Nariadenia GDPR dotknuté osoby môžu kontaktovať zodpovednú osobu v súvislosti so všetkými otázkami týkajúcimi sa spracúvania ich osobných údajov a uplatňovania ich práv podľa tohto nariadenia.

4.12. Podľa Článku 38. ods. 5 Nariadenia GDPR zodpovedná osoba je v súvislosti s výkonom svojich úloh viazaná povinnosťou zachovávať mlčanlivosť alebo dôvernosť informácií v súlade s právom Únie alebo s právom členského štátu.

4.13. Podľa Článku 38. ods. 6 Nariadenia GDPR zodpovedná osoba môže plniť iné úlohy a povinnosti. Prevádzkovateľ alebo sprostredkovateľ zabezpečia, aby žiadna z takýchto úloh alebo povinností neviedla ku konfliktu záujmov.

4.14. Podľa Článku 39. ods. 1 Nariadenia GDPR zodpovedná osoba má aspoň tieto úlohy:

a) poskytovanie informácií a poradenstva prevádzkovateľovi alebo sprostredkovateľovi a zamestnancom, ktorí vykonávajú spracúvanie, o ich povinnostiach podľa tohto nariadenia a ostatných právnych predpisov Únie alebo členského štátu týkajúcich sa ochrany údajov;

b) monitorovanie súladu s týmto nariadením, s ostatnými právnymi predpismi Únie alebo členského štátu týkajúcimi sa ochrany osobných údajov a s pravidlami

prevádzkovateľa alebo sprostredkovateľa v súvislosti s ochranou osobných údajov vrátane rozdelenia povinností, zvyšovania povedomia a odbornej prípravy personálu, ktorý je zapojený do spracovateľských operácií, a súvisiacich auditov;

c) poskytovanie poradenstva na požiadanie, pokiaľ ide o posúdenie vplyvu na ochranu údajov a monitorovanie jeho vykonávania podľa článku 35;

d) spolupráca s dozorným orgánom;

e) plnenie úlohy kontaktného miesta pre dozorný orgán v súvislosti s otázkami týkajúcimi sa spracúvania vrátane predchádzajúcej konzultácie uvedenej v článku 36 a podľa potreby aj konzultácie v akýchkoľvek iných veciach.

4.15. Podľa Článku 39. ods. 2 Nariadenia GDPR zodpovedná osoba pri výkone svojich úloh náležite zohľadňuje riziko spojené so spracovateľskými operáciami, pričom berie na vedomie povahu, rozsah, kontext a účely spracúvania.

4.16. Podľa Usmernenia pracovanej skupiny WP29 k aplikácii Nariadenia GDPR inštitút zodpovednej osoby nie je ničím novým. Aj keď smernica 95/46/ES3 nevyžadovala, aby spoločnosti menovali zodpovedné osoby, napriek tomu sa v priebehu rokov vo viacerých členských štátoch vyvinula prax ich menovania. Už pred prijatím nariadenia, bola skupina WP29 toho názoru, že zodpovedná osoba je základným kameňom zodpovednosti, že jej menovanie pomáha zabezpečiť súlad s pravidlami ochrany osobných údajov a pre podnikateľov predstavuje konkurenčnú výhodu. Okrem toho že pomáha zabezpečiť súlad s pravidlami ochrany osobných údajov implementáciou nástrojov pre zodpovedné spracúvanie (ako napr. zabezpečením alebo vykonaním posúdenia vplyvov alebo auditov), zodpovedné osoby vystupujú ako prostredníci medzi dôležitými zainteresovanými stranami (dozornými orgánmi, dotknutými osobami a obchodnými oddeleniami spoločností).

4.17. Podľa Usmernenia pracovanej skupiny WP29 k aplikácii Nariadenia GDPR zodpovedné osoby nie sú osobne zodpovedné v prípade výskytu nesúladu s Nariadením. Nariadenie jasne stanovuje, že prevádzkovateľ alebo sprostredkovateľ má zabezpečiť súlad a má byť schopný preukázať, že spracúvanie sa realizuje v súlade s ustanoveniami nariadenia (článok 24 ods. 1). Za súlad v oblasti ochrany osobných údajov je zodpovedný prevádzkovateľ alebo sprostredkovateľ. Prevádzkovateľ a sprostredkovateľ majú taktiež kľúčovú úlohu, pokiaľ ide o poskytnutie súčinnosti zodpovednej osobe, aby sa zabezpečilo účinné vykonávanie jej úloh. Vymenovanie zodpovednej osoby je prvý krok, avšak zodpovedné osoby musia mať dostatočnú mieru autonómie a zdrojov, aby mohli reálne plniť svoje úlohy.

Článok V.

Záznamy o spracovateľských činnostiach

5.1. Podľa Článku 30. ods. 1 Nariadenia GDPR každý prevádzkovateľ a v príslušnom prípade zástupca prevádzkovateľa vedie záznamy o spracovateľských činnostiach, za ktoré je zodpovedný. Tieto záznamy musia obsahovať všetky tieto informácie:
a) meno/názov a kontaktné údaje prevádzkovateľa a v príslušnom prípade spoločného prevádzkovateľa, zástupcu prevádzkovateľa a zodpovednej osoby;
b) účely spracúvania;
c) opis kategórií dotknutých osôb a kategórií osobných údajov;
d) kategórie príjemcov, ktorým boli alebo budú osobné údaje poskytnuté, vrátane príjemcov v tretích krajinách alebo medzinárodných organizácií;
e) v príslušných prípadoch prenosy osobných údajov do tretej krajiny alebo medzinárodnej organizácii vrátane označenia predmetnej tretej krajiny alebo medzinárodnej organizácie a v prípade prenosov uvedených v článku 49 ods. 1 druhom pododseku dokumentáciu primeraných záruk;
f) podľa možností predpokladané lehoty na vymazanie rôznych kategórií údajov;
g) podľa možností všeobecný opis technických a organizačných bezpečnostných opatrení uvedených v článku 32 ods. 1.

5.2. Podľa Článku 30. ods. 2 Nariadenia GDPR každý sprostredkovateľ a v príslušnom prípadezástupca sprostredkovateľa vedie záznamy o všetkých kategóriách spracovateľských činností, ktoré vykonal v mene prevádzkovateľa, pričom tieto záznamy obsahujú:
a) meno/názov a kontaktné údaje sprostredkovateľa alebo sprostredkovateľov a každého prevádzkovateľa, v mene ktorého sprostredkovateľ koná, a v príslušnom prípade zástupcu prevádzkovateľa alebo sprostredkovateľa a zodpovednej osoby;
b) kategórie spracúvania vykonávaného v mene každého prevádzkovateľa;
c) v príslušných prípadoch prenosy osobných údajov do tretej krajiny alebo medzinárodnej organizácii vrátane označenia predmetnej tretej krajiny alebo medzinárodnej organizácie a v prípade prenosov uvedených v článku 49 ods. 1 druhom pododseku dokumentáciu primeraných záruk;
d) podľa možností všeobecný opis technických a organizačných bezpečnostných opatrení uvedených v článku 32 ods. 1.

5.3. Podľa Článku 30. ods. 3 Nariadenia GDPR záznamy uvedené v odsekoch 1 a 2 sa vedú v písomnej podobe vrátane elektronickej podoby.

5.4. Podľa Článku 30. ods. 4 Nariadenia GDPR prevádzkovateľ alebo sprostredkovateľ a v príslušnom prípade zástupca prevádzkovateľa alebo sprostredkovateľa na požiadanie sprístupnia záznamy dozornému orgánu.

5.5. Podľa Článku 30. ods. 5 Nariadenia GDPR povinnosti uvedené v odsekoch 1 a 2 sa nevzťahujú na podnik alebo organizáciu, ktorá zamestnáva menej ako 250 osôb, pokiaľ nie je pravdepodobné, že spracúvanie, ktoré vykonáva, povedie k riziku pre

práva a slobody dotknutej osoby, pokiaľ je toto spracúvanie príležitostné alebo nezahŕňa osobitné kategórie údajov podľa článku 9 ods. 1 alebo osobných údajov týkajúcich sa uznaní viny za trestné činy a priestupky podľa článku 10.

Článok VI.
Usmernenie k Záznamu o spracovateľských činnostiach prevádzkovateľa alebo zástupcu prevádzkovateľa

6.1. Predmetné usmernenie bolo vydané a zverejnené Úradom na ochranu osobných údajov Slovenskej republiky.

6.2. Každý prevádzkovateľ alebo zástupca prevádzkovateľa (ak takého má prevádzkovateľ povereného) má povinnosť viesť záznam o spracovateľskej činnosti (ďalej len „záznam“) a to buď v papierovej alebo elektronickej podobe, ktorý nemá povinnosť nikam zasielať a ponecháva si ho u seba. Úradom zverejnený záznam je len vzorom a prevádzkovateľ alebo zástupca prevádzkovateľa má možnosť si ho upraviť podľa seba, no musí obsahovať všetky zákonné náležitosti, ktoré sú upravené v § 37 ods. 1 zákona č. 18/2018 Z. z. o ochrane osobných údajov (ďalej len „zákon“), príp. podľa čl. 30 ods. 1 Nariadenia Európskeho parlamentu a Rady (EÚ) 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) (ďalej len „nariadenie“). Na požiadanie úradu je prevádzkovateľ alebo zástupca prevádzkovateľa povinný sprístupniť záznam úradu.

6.3. Výnimky z povinnosti viesť záznam podľa § 37 ods. 5 zákona, resp. podľa čl. 30 ods. 5 nariadenia:
Pre výnimku z povinnosti viesť záznamy platí iba situácia č. 1. V ostatných situáciách sú uvedené možnosti ako má prevádzkovateľ alebo zástupca prevádzkovateľa postupovať, keď nastane niektorá z kombinácii.

6.4. Úrad na ochranu osobných údajov SR dáva do pozornosti, že pracovaná skupina WP29, ktorá vyjadrila svoj názor na to, ako prihliadať na výnimku viesť záznamy tiež uviedla, že prevádzkovateľ alebo zástupca prevádzkovateľa nemusí viesť záznamy len na tie spracovateľské operácie, na ktoré sa samotná výnimka vzťahuje. Teda ak má 10 spracovateľských operácií a na 2 sa vzťahuje výnimka, tak pri ostatných 8 musí viesť záznamy o spracovateľských činnostiach. (Working Party 29 PositionPaper on thederogationsfromtheobligation to maintainrecords of processingactivitiespursuant to Article 30(5) GDPR,
https://www.dataprotection.gov.sk/uoou/sk/content/position-paper-derogations-obligationmaintain-records-processing-activities-pursuant)

6.5. Situácia č. 1: Ak podnik alebo organizácia zamestnáva menej ako 250 osôb a
- pokiaľ nie je pravdepodobné, že spracúvanie osobných údajov, ktoré vykonáva povedie k riziku pre práva a slobody dotknutej osoby a
- spracúvanie osobných údajov je príležitostné a
- spracúvanie nezahŕňa osobitné kategórie osobných údajov podľa § 16 ods. 1 zákona, príp. čl. 9 ods. 1 nariadenia (napr. biometrický údaj, údaj o zdraví a pod.) alebo nezahŕňa osobné údaje týkajúce sa uznania viny za spáchanie trestného činu alebo priestupku podľa § 17 zákona, príp. čl. 10 nariadenia, tak

= prevádzkovateľ alebo zástupca prevádzkovateľa nie je povinný viesť záznamy pre konkrétnu spracovateľskú činnosť, na ktorú sa vzťahuje táto výnimka.
6.6. Situácia č. 2: Ak podnik alebo organizácia zamestnáva menej ako 250 osôb a je pravdepodobné, že spracúvanie osobných údajov, ktoré vykonáva povedie k riziku pre práva a slobody dotknutej osoby, prevádzkovateľ alebo zástupca prevádzkovateľa je povinný viesť záznamy o spracovateľských činnostiach.

6.7. Situácia č. 3: Ak podnik alebo organizácia zamestnáva menej ako 250 osôb a spracúvanie nie je príležitostné, prevádzkovateľ alebo zástupca prevádzkovateľa je povinný viesť záznamy o spracovateľských činnostiach. Situácia č. 4: Ak podnik alebo organizácia zamestnáva menej ako 250 osôb a spracúvanie zahŕňa osobitné kategórie osobných údajov podľa § 16 ods. 1 zákona, príp. čl. 9 ods. 1 nariadenia (napr. biometrický údaj, údaj o zdraví a pod.) alebo osobné údaje týkajúce sa uznania viny za spáchanie trestného činu alebo priestupku podľa § 17 zákona, príp. čl. 10 nariadenia, prevádzkovateľ alebo zástupca prevádzkovateľa je povinný viesť záznamy o spracovateľských činnostiach.

6.8. Záznamy o spracovateľských činnostiach nahrádzajú oznámenia informačných systémov, žiadosti o osobitnú registráciu informačných systémov a evidenčné listy informačných systémov. Oproti predchádzajúcej právnej úprave obsiahnutej v zákone č. 122/2013 Z. z. o ochrane osobných údajov v znení neskorších predpisov nie je táto povinnosť naviazaná na informačný systém, ale na účel spracúvania.

6.9. Prevádzkovateľ alebo zástupca prevádzkovateľa je zodpovedný za to, aby všetky údaje uvedené v zázname boli aktuálne. Napríklad, ak sa zmenila zodpovedná osoba, prevádzkovateľ je povinný tento údaj v zázname ku dňu zmeny aktualizovať.

6.10. Vypĺňanie vzoru záznamu o spracovateľských činnostiach prevádzkovateľa alebo zástupcu prevádzkovateľa:
Prevádzkovateľ alebo zástupca prevádzkovateľa si môže vypracovať vlastný záznam alebo použiť vzor zverejnený úradom. Úradom zverejnený vzor obsahuje všetky povinné náležitosti vyžadované zákonom, príp. nariadením. Ak bude mať

prevádzkovateľ alebo zástupca prevádzkovateľa správne a úplne vypísaný tento vzor bude napĺňať zákon. Samozrejme nie je vylúčené, aby si prevádzkovateľ alebo zástupca prevádzkovateľa v prípade potreby pridal vlastné polia, napr. poznámka a podobne.

6.10.1. Podľa § 37 ods. 1 písm. a) zákona, čl. 30 ods. 1 písm. a) nariadenia:
Prevádzkovateľ alebo zástupca prevádzkovateľa vypíše o sebe identifikačné údaje a kontaktné údaje (obchodné meno/meno a priezvisko, IČO, adresa sídla/trvalého bydliska, telefonický kontakt, mailová adresa), ak nimi disponuje (napr. prevádzkovateľ nemusí mať zriadenú mailovú schránku). Údaje o spoločnom prevádzkovateľovi, zástupcovi prevádzkovateľa a zodpovednej osobe sa vypíšu v prípade, ak boli poverení alebo zodpovedná osoba určená. Pri zodpovednej osobe, ktorá môže byť fyzickou alebo právnickou osobou sa vypíšu všetky identifikačné a kontaktné údaje, ktoré má prevádzkovateľ alebo zástupca prevádzkovateľa k dispozícii. Ak ide o zodpovednú osobu, ktorá je zároveň zamestnancom prevádzkovateľa/zástupcu prevádzkovateľa, nie je potrebné vypĺňať adresu. Ak ide o externú zodpovednú osobu uvedie sa adresa jej sídla alebo trvalého bydliska.

6.10.2. Podľa § 37 ods. 1 písm. b) zákona, čl. 30 ods. 1 písm. b) nariadenia:
Účelom spracúvania osobných údajov (§ 7 zákona, čl. 5 ods. 1 písm. b) nariadenia) sa rozumie konkrétne vymedzený alebo ustanovený zámer, na základe ktorého bude prevádzkovateľ spracúvať osobné údaje viažuce sa na jeho činnosť. Tento účel by si mal prevádzkovateľ stanoviť vopred, jednoznačne a mal by byť oprávnený. Napr. spracúvanie osobných údajov zamestnanca na účel plnenia povinností zamestnávateľa súvisiacich s pracovným pomerom. Každý účel spracúvania musí byť v zázname vymedzený samostatne a ku každému musia byť vyplnené všetky povinné náležitosti. Koľko účelov má prevádzkovateľ, toľko „riadkov“ musí záznam obsahovať.

6.10.3. Podľa § 37 ods. 1 písm. c) zákona, čl. 30 ods. 1 písm. c) nariadenia:
Opis kategórií dotknutých osôb je taký okruh osôb, ktorých osobné údaje sa budú spracúvať. V prípade príkladu na zamestnancoch bude takouto kategóriou práve zamestnanec, manžel/manželka zamestnanca, deti zamestnanca a pod.
Pri kategórii osobných údajov sú tieto možnosti: bežné osobné údaje (§ 2 zákona, čl. 4 bod 1 nariadenia), osobitná kategória osobných údajov (§ 16 zákona, čl. 9 nariadenia) a/alebo osobné údaje týkajúce sa uznania viny za spáchanie trestného činu alebo priestupku (§ 17 zákona, čl. 10 nariadenia). Prevádzkovateľ/zástupca prevádzkovateľa musí uviesť kategóriu, ale nie je vylúčené, aby uviedol menný zoznam všetkých osobných údajov, ktoré spracúva. Je to možnosť, nie povinnosť.

6.10.4. Podľa § 37 ods. 1 písm. d) zákona, čl. 30ods. 1 písm. d) nariadenia:
Ďalšou povinnou náležitosťou je kategória príjemcov. Príjemcom sa podľa § 5 písm. q) zákona (čl. 4 bod 9 nariadenia) rozumie každý, komu sa osobné údaje poskytnú bez

ohľadu na to, či je treťou stranou. Ak prevádzkovateľ vie určiť príjemcu uvedie sa do záznamu konkrétny príjemca, napríklad sociálna poisťovňa, zdravotná poisťovňa v prípade zamestnanca a platenia odvodov za neho. Ak by prevádzkovateľ nevedel určiť príjemcu, uvedie sa kategória, okruh príjemcov, napr. súdy, orgány verejnej moci atď. Príjemcom je aj sprostredkovateľ prevádzkovateľa.
Takýto príjemca sa môže nachádzať aj v tretej krajine, napr. Turecko, Izrael, USA alebo je treťou stranou medzinárodná organizácia (napr. Medzinárodná organizácia práce, Medzinárodná námorná organizácia alebo Svetová zdravotnícka organizácia).

6.10.5. Podľa § 37 ods. 1 písm. e) zákona, čl. 30 ods. 1 písm. e) nariadenia:
V prípade, ak prevádzkovateľ zamýšľa prenos osobných údajov aj do tretích krajín alebo medzinárodných organizácií je povinný vypísať kolónku s touto zákonnou náležitosťou, kam budú údaje prenášané. Je potrebné disponovať dokumentáciou o primeraných zárukách, ktoré tento prenos budú zabezpečovať. Zoznam členských štátov EÚ/EHP a krajín zaručujúcich primeranú úroveň ochrany prikladáme v priamom linku na webové sídlo úradu. V zákone sú tomu venované § 47 – 51 zákona, čl. 44 – 50 nariadenia.

6.10.6. Podľa § 37 ods. 1 písm. f) zákona, čl. 30 ods. 1 písm. f) nariadenia:
Na každú kategóriu osobných údajov je potrebné určiť lehotu, po ktorej majú byť osobné údaje vymazané. Túto lehotu môže stanoviť osobitný právny predpis, napr. zákon o archívoch a registratúrach, prípadne si ju určí prevádzkovateľ sám s ohľadom na zásadu minimalizácie uchovávania osobných údajov (§ 10 zákona, čl. 5 ods. 1 písm. e) nariadenia).
6.10.7. Podľa § 37 ods. 1 písm. g) zákona, čl. 30 ods. 1 písm. g) nariadenia:
Do záznamu o spracovateľských činnostiach je potrebné uviesť aké technické a organizačné bezpečnostné opatrenia prijal prevádzkovateľ, aby zabezpečil, že spracúvanie osobných údajov bude bezpečné, chránené a urobil všetko preto, aby nemohli byť zneužité. Je potrebné vychádzať z § 39 zákona, resp. z čl. 32 nariadenia, ktorý stanovuje najmä tieto opatrenia: pseudonymizácia a šifrovanie osobných údajov, zabezpečenie trvalej dôvernosti, integrity, dostupnosti a odolnosti systémov spracúvania osobných údajov, proces obnovy dostupnosti osobných údajov a prístup k nim v prípade fyzického alebo technického incidentu, proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania osobných údajov.

Inými slovami môže ísť pri technických bezpečnostných opatreniach o zabezpečenie počítača antivírusom, zaheslovanie, v prípade listinnej podoby dokumentu, ktorý obsahuje osobné údaje to môže byť uzamykateľná skriňa, trezor, archív s kódom. Pri organizačných opatreniach je to ľudský faktor, ktorý zabezpečí bezpečnosť spracúvania osobných údajov dotknutých osôb, napr. určená zodpovedná osoba,

poučená oprávnená osoba. V prípade vypracovanej dokumentácie bezpečnosti osobných údajov je možné uviesť odkaz na takýto dokument.

6.10.8. Podľa § 13 zákona, čl. 6 nariadenia:
Vo vzore záznamu o spracovateľských činnostiach prevádzkovateľa alebo zástupcu prevádzkovateľa je vložená fakultatívna náležitosť „právny základ spracovateľskej činnosti“, ktorý je upravený v § 13 zákona, príp. v čl. 6 nariadenia. Nie je to obligatórna náležitosť záznamu o spracovateľských činnostiach, ale vzhľadom na skutočnosť, že na právny základ sa viaže účel spracúvania osobných údajov a v prípade kontroly je prevádzkovateľ/zástupca prevádzkovateľa i tak povinný uviesť právny základ spracúvania, Úrad vidí v tejto náležitosti opodstatnenie.

Povinnosť vyplniť záznam sa vzťahuje aj na každého spoločného prevádzkovateľa ako aj zástupcu prevádzkovateľa a môže sa riadiť týmto návodom na vyplnenie.

Článok VII.
Usmernenie k Záznamu o kategóriách spracovateľských činností sprostredkovateľa alebo zástupcu sprostredkovateľa

7.1. Predmetné usmernenie bolo vydané a zverejnené Úradom na ochranu osobných údajov Slovenskej republiky.

7.2. Každý sprostredkovateľ alebo zástupca sprostredkovateľa (ak takého má sprostredkovateľ povereného) má povinnosť vytvoriť si záznam o kategóriách spracovateľskej činnosti (ďalej len „záznam“) a to buď v papierovej alebo elektronickej podobe, ktorý nemá povinnosť nikam zasielať a ponecháva si ho u seba. Úradom zverejnený záznam je len vzorom a sprostredkovateľ alebo zástupca sprostredkovateľa má možnosť si ho upraviť podľa seba, no musí obsahovať všetky zákonné náležitosti, ktoré sú upravené v § 37 ods. 2 zákona č. 18/2018 Z. z. o ochrane osobných údajov (ďalej len „zákon“), príp. podľa čl. 30 ods. 2 Nariadenia Európskeho parlamentu a Rady (EÚ) 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) (ďalej len „nariadenie“). Na požiadanie úradu je sprostredkovateľ alebo zástupca sprostredkovateľa povinný sprístupniť záznam úradu.

7.3. Výnimky z povinnosti viesť záznam podľa § 37 ods. 5 zákona, resp. podľa čl. 30 ods. 5 nariadenia:

Pre výnimku z povinnosti viesť záznamy platí iba situácia č. 1. V ostatných situáciách sú uvedené možnosti ako má sprostredkovateľ alebo zástupca sprostredkovateľa postupovať, keď nastane niektorá z kombinácií.

7.4. Úrad na ochranu osobných údajov SRdáva do pozornosti, že pracovaná skupina WP29, ktorá vyjadrila svoj názor na to, ako prihliadať na výnimku viesť záznamy tiež uviedla, že sprostredkovateľ alebo zástupca sprostredkovateľa nemusí viesť záznamy len na tie spracovateľské operácie, na ktoré sa samotná výnimka vzťahuje. Teda ak má 10 spracovateľských operácií a na 2 sa vzťahuje výnimka, tak pri ostatných 8 má povinnosť vytvoriť si záznam o kategóriách spracovateľskej činnosti. (Working Party 29 PositionPaper on thederogationsfromtheobligation to maintainrecords of processingactivitiespursuant to Article 30(5) GDPR, https://www.dataprotection.gov.sk/uoou/sk/content/position-paper-derogations-obligationmaintain-records-processing-activities-pursuant)

7.5. Situácia č. 1: Ak podnik alebo organizácia zamestnáva menej ako 250 osôb a
- pokiaľ nie je pravdepodobné, že spracúvanie osobných údajov, ktoré vykonáva povedie k riziku pre práva a slobody dotknutej osoby a
- spracúvanie osobných údajov je príležitostné a
- spracúvanie nezahŕňa osobitné kategórie osobných údajov podľa § 16 ods. 1 zákona, príp. čl. 9 ods. 1 nariadenia (napr. biometrický údaj, údaj o zdraví a pod.) alebo osobné údaje týkajúce sa uznania viny za spáchanie trestného činu alebo priestupku podľa § 17 zákona, príp. čl. 10 nariadenia, tak

= sprostredkovateľ alebo zástupca sprostredkovateľa nie je povinný viesť záznamy pre konkrétnu spracovateľskú činnosť, na ktorú sa vzťahuje táto výnimka.

7.6. Situácia č. 2: Ak podnik alebo organizácia zamestnáva menej ako 250 osôb a je pravdepodobné, že spracúvanie osobných údajov, ktoré vykonáva povedie k riziku pre práva a slobody dotknutej osoby, sprostredkovateľ alebo zástupca sprostredkovateľa je povinný viesť záznamy o kategóriách spracovateľských činností.

7.7. Situácia č. 3: Ak podnik alebo organizácia zamestnáva menej ako 250 osôb a spracúvanie nie je príležitostné, sprostredkovateľ alebo zástupca sprostredkovateľa je povinný viesť záznamy o kategóriách spracovateľských činností.

7.8. Situácia č. 4: Ak podnik alebo organizácia zamestnáva menej ako 250 osôb a spracúvanie zahŕňa osobitné kategórie osobných údajov podľa § 16 ods. 1 zákona, príp. čl. 9 ods. 1 nariadenia (napr. biometrický údaj, údaj o zdraví a pod.) alebo osobné údaje týkajúce sa uznania viny za spáchanie trestného činu alebo priestupku podľa § 17 zákona, príp. čl. 10 nariadenia, sprostredkovateľ alebo zástupca sprostredkovateľa je povinný viesť záznamy o kategóriách spracovateľských činností.

7.9. Sprostredkovateľ alebo zástupca sprostredkovateľa je zodpovedný za to, aby všetky údaje uvedené v zázname boli aktuálne. Napríklad, ak sa zmenila zodpovedná osoba, sprostredkovateľ/zástupca sprostredkovateľa je povinný tento údaj v zázname ku dňu zmeny aktualizovať.

7.10. Vypĺňanie vzoru záznamu o kategóriách spracovateľských činností sprostredkovateľa alebo zástupcu sprostredkovateľa:
Sprostredkovateľ alebo zástupca sprostredkovateľa si môže vypracovať vlastný záznam alebo použiť vzor zverejnený úradom. Úradom zverejnený vzor obsahuje všetky podstatné náležitosti vyžadované zákonom, príp. nariadením. Ak bude mať sprostredkovateľ/zástupca sprostredkovateľa správne a úplne vypísaný tento vzor bude napĺňať zákon. Samozrejme nie je vylúčené, aby si sprostredkovateľ alebo zástupca sprostredkovateľa v prípade potreby pridal vlastné polia, napr. poznámka a podobne.

7.10.1. Podľa § 37 ods. 2 písm. a) zákona, čl. 30 ods. 2 písm. a) nariadenia:
Sprostredkovateľ/zástupca sprostredkovateľa vypíše o sebe identifikačné a kontaktné údaje (obchodné meno/meno a priezvisko, IČO, adresa sídla/trvalého bydliska, telefonický kontakt, mailová adresa), ak nimi disponuje (napr. sprostredkovateľ nemusí mať zriadenú mailovú schránku). Ak má určenú zodpovednú osobu a/alebo zástupcu, obligatórne tieto údaje uvedie. Pri zodpovednej osobe, ktorá môže byť fyzickou alebo právnickou osobou sa vypíšu všetky identifikačné a kontaktné údaje, ktoré má sprostredkovateľa alebo zástupca sprostredkovateľa k dispozícii. Ak ide o zodpovednú osobu, ktorá je zároveň zamestnancom sprostredkovateľa/zástupcu sprostredkovateľa, nie je potrebné vypĺňať adresu. Ak ide o externú zodpovednú osobu uvedie sa adresa jej sídla alebo trvalého bydliska.

Ďalšími náležitosťami sú údaje o všetkých prevádzkovateľoch, v mene ktorých sprostredkovateľ spracúva osobné údaje. Ak má prevádzkovateľ zvoleného svojho zástupcu, príp. ak má sprostredkovateľ sprostredkovateľa (tzv. subdodávateľ alebo subsprostredkovateľ), musí uviesť všetky tieto informácie do záznamu.
V mene koľkých prevádzkovateľov sprostredkovateľ alebo zástupca sprostredkovateľa spracúva osobné údaje, toľkých je sprostredkovateľ/zástupca sprostredkovateľa povinný tam uviesť.

Príklad č. 1: V mene prevádzkovateľa 123, s. r. o. spracúva osobné údaje sprostredkovateľ „AB“, ktorý má určenú zodpovednú osobu „CD“.

Príklad č. 2: Sprostredkovateľ „AB“ spracúva osobné údaje v mene prevádzkovateľa 456, s. r. o., ktorý má svojho zástupcu „EF“ a časť osobných údajov spracúva sprostredkovateľ sprostredkovateľa „GH“.

7.10.2. Podľa § 37 ods. 2 písm. b) zákona, čl. 30 ods. 2 písm. b) nariadenia:
Pri každom prevádzkovateľovi jednotlivo, v mene ktorého sprostredkovateľ alebo zástupca sprostredkovateľa spracúva osobné údaje je potrebné uviesť kategórie spracúvania. Tieto by mali byť predmetom uzatvorenej sprostredkovateľskej zmluvy medzi prevádzkovateľom a sprostredkovateľom alebo zástupcom sprostredkovateľa.

7.10.3. Podľa § 37 ods. 2 písm. c) zákona, čl. 30 ods. 2 písm. c) nariadenia:
V prípade, ak prevádzkovateľ zamýšľa prenos osobných údajov do tretích krajín alebo medzinárodných organizácií sprostredkovateľ alebo zástupca sprostredkovateľa je povinný vypísať aj tieto údaje. Je potrebné disponovať dokumentáciou o primeraných zárukách, ktoré tento prenos budú zabezpečovať. V zákone sú tomu venované § 47 – 51 zákona, v nariadení sú to články 44 – 50.

7.10.4. Podľa § 37 ods. 2 písm. d) zákona, čl. 30 ods. 2 písm. d) nariadenia:
Do záznamu o všetkých kategóriách spracovateľských činností je potrebné uviesť aké technické a organizačné bezpečnostné opatrenia sa prijali, aby sa zabezpečilo, že spracúvanie osobných údajov bude bezpečné, chránené a aby nemohli byť zneužité. Je potrebné vychádzať z § 39 zákona, resp. z čl. 32 nariadenia, ktorý stanovuje najmä tieto opatrenia: pseudonymizácia a šifrovanie osobných údajov, zabezpečenie trvalej dôvernosti, integrity, dostupnosti a odolnosti systémov spracúvania osobných údajov, proces obnovy dostupnosti osobných údajov a prístup k nim v prípade fyzického alebo technického incidentu, proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania osobných údajov.

Inými slovami môže ísť pri technických bezpečnostných opatreniach o zabezpečenie počítača antivírusom, zaheslovanie, v prípade listinnej podoby dokumentu, ktorý obsahuje osobné údaje to môže byť uzamykateľná skriňa, trezor, archív s bezpečnostným kódom. Pri organizačných opatreniach je to ľudský faktor, ktorý zabezpečí bezpečnosť spracúvania osobných údajov dotknutých osôb, napr. určená zodpovedná osoba, poučená oprávnená osoba. V prípade vypracovanej dokumentácie bezpečnosti osobných údajov je možné uviesť odkaz na takýto dokument.

ČASŤ IV

Oznámenie porušenia ochrany osobných údajov

Článok I.
Oznámenie porušenia ochrany osobných údajov dozornému orgánu

1.1. Podľa Článku 33 ods. 1 Nariadenia GDPR v prípade porušenia ochrany osobných údajov prevádzkovateľ bez zbytočného odkladu a podľa možnosti najneskôr do 72 hodín po tom, čo sa o tejto skutočnosti dozvedel, oznámi porušenie ochrany osobných údajov dozornému orgánu príslušnému podľa článku 55 s výnimkou prípadov, keď nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb. Ak oznámenie nebolo dozornému orgánu predložené do 72 hodín, pripojí sa k nemu zdôvodnenie omeškania.

1.2. Podľa Článku 33 ods. 2 Nariadenia GDPR sprostredkovateľ podá prevádzkovateľovi oznámenie bez zbytočného odkladu po tom, čo sa o porušení ochrany osobných údajov dozvedel.

1.3. Podľa Článku 33 ods. 3 Nariadenia GDPR oznámenie uvedené v odseku 1 musí obsahovať aspoň:
a) opis povahy porušenia ochrany osobných údajov vrátane, podľa možnosti, kategórií a približného počtu dotknutých osôb, ktorých sa porušenie týka, a kategórií a približného počtu dotknutých záznamov o osobných údajoch;
b) meno/názov a kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta, kde možno získať viac informácií;
c) opis pravdepodobných následkov porušenia ochrany osobných údajov;
d) opis opatrení prijatých alebo navrhovaných prevádzkovateľom s cieľom napraviť porušenie ochrany osobných údajov vrátane, podľa potreby, opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov.

1.4. Podľa Článku 33 ods. 4 Nariadenia GDPR v rozsahu, v akom nie je možné poskytnúť informácie súčasne, možno informácie poskytnúť vo viacerých etapách bez ďalšieho zbytočného odkladu.

1.5. Podľa Článku 33 ods. 5 Nariadenia GDPR prevádzkovateľ zdokumentuje každý prípad porušenia ochrany osobných údajov vrátane skutočností spojených s porušením ochrany osobných údajov, jeho následky a prijaté opatrenia na nápravu. Uvedená dokumentácia musí umožniť dozorným orgánom overiť súlad s týmto článkom.

Článok II.
Oznámenie porušenia ochrany osobných údajov dotknutej osobe

2.1. Podľa Článku 34 ods. 1 Nariadenia GDPR v prípade porušenia ochrany osobných údajov, ktoré pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, prevádzkovateľ bez zbytočného odkladu oznámi porušenie ochrany osobných údajov dotknutej osobe.

2.2. Podľa Článku 34 ods. 2 Nariadenia GDPR oznámenie dotknutej osobe uvedené v odseku 1 tohto článku obsahuje jasne a jednoducho formulovaný opis povahy porušenia ochrany osobných údajov a aspoň informácie a opatrenia uvedené v článku 33 ods. 3 písm. b), c) a d).

2.3. Podľa Článku 34 ods. 3 Nariadenia GDPR oznámenie dotknutej osobe uvedené v odseku 1 sa nevyžaduje, ak je splnená ktorákoľvek z týchto podmienok:

a) prevádzkovateľ prijal primerané technické a organizačné ochranné opatrenia a tieto opatrenia uplatnil na osobné údaje, ktorých sa porušenie ochrany osobných údajov týka, a to najmä tie opatrenia, na základe ktorých sú osobné údaje nečitateľné pre všetky osoby, ktoré nie sú oprávnené mať k nim prístup, ako je napríklad šifrovanie;
b) prevádzkovateľ prijal následné opatrenia, ktorými sa zabezpečí, že vysoké riziko pre práva a slobody dotknutých osôb uvedené v odseku 1 pravdepodobne už nebude mať dôsledky;
c) by to vyžadovalo neprimerané úsilie. V takom prípade dôjde namiesto toho k informovaniu verejnosti alebo sa prijme podobné opatrenie, čím sa zaručí, že dotknuté osoby budú informované rovnako efektívnym spôsobom.

2.4. Podľa Článku 34 ods. 4 Nariadenia GDPR ak prevádzkovateľ ešte porušenie ochrany osobných údajov neoznámil dotknutej osobe, dozorný orgán môže po zvážení pravdepodobnosti porušenia ochrany osobných údajov vedúceho k vysokému riziku požadovať, aby tak urobil, alebo môže rozhodnúť, že je splnená niektorá z podmienok uvedených v odseku 3.

Táto Smernica o bezpečnostných opatreniach prevádzkovateľa bola prijatá prevádzkovateľom dňa 25.05.2018.

_____

.....
....., konateľ