INTERNÁ POLITIKA OCHRANY OSOBNÝCH ÚDAJOV VILLA BETULA KLUB, O.Z.

Brnice 166

Liptovská Sielnica

§1

ÚVODNÉ USTANOVENIA

(1) V tejto internej politike **VILLA BETULA KLUB** (ďalej len „VB“ „DRE“) vytvára princípy na dodržiavanie zákonného a bezpečného spracúvania osobných údajov podľa článku 5 ods. 1 Nariadenia Európskeho parlamentu a Rady (EÚ) č. 2016/679 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 ako „**GDPR**“), s cieľom efektívne riadiť agendu ochrany osobných údajov vo svojich podmienkach.

(2) Táto interná politika slúži na zabezpečenie súladu s GDPR a zákonom č. 18/2018 Z.z., o ochrane osobných údajov (ďalej len „**Zákon o ochrane osobných údajov**“).

(3) Táto interná politika sa vzťahuje na akékoľvek a všetko spracúvanie osobných údajov, ku ktorému dochádza v DRE vrátane automatizovaného alebo manuálneho spracúvania osobných údajov bez ohľadu na postavenie DRE (prevádzkovateľ alebo sprostredkovateľ) a účel spracúvania osobných údajov.

§ 2

ZÁKLADNÉ POJMY

(1) Táto interná politika používa primárne pojmy definované v čl. 4 GDPR, pričom na účely tejto internej politiky:

„**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;

„**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;

„**obmedzenie spracúvania**“ je označenie uchovávaných osobných údajov s cieľom obmedziť ich spracúvanie v budúcnosti;

„**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;

„**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;

„**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;

„**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;

„**sprostredkovateľ**“ je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa;

„**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;

„**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;

„**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;

„**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;

„**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;

„**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;

„**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;

„**záväzné vnútropodnikové pravidlá**“ je politika ochrany osobných údajov, ktorú dodržiava prevádzkovateľ alebo sprostredkovateľ usadený na území členského štátu na účely prenosu alebo súborov prenosov osobných údajov prevádzkovateľovi alebo sprostredkovateľovi v jednej alebo viacerých tretích krajinách v rámci skupiny podnikov alebo podnikov zapojených do spoločnej hospodárskej činnosti;

„**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;

„**relevantná a odôvodnená námietka**“ je námietka voči návrhu rozhodnutia, či došlo k porušeniu tohto nariadenia, alebo či je plánované opatrenie vo vzťahu k prevádzkovateľovi alebo sprostredkovateľovi v súlade s týmto nariadením, ktoré musí jasne preukázať závažnosť rizík, ktoré predstavuje návrh rozhodnutia, pokiaľ ide o základné práva a slobody dotknutých osôb a prípadne voľný pohyb osobných údajov v rámci Únie;

„**služba informačnej spoločnosti**“ je služba vymedzená v článku 1 bode 1 písm. b) smernice Európskeho parlamentu a Rady (EÚ) 2015/1535;

„**medzinárodná organizácia**“ je organizácia a jej podriadené subjekty, ktoré sa riadia medzinárodným právom verejným, alebo akýkoľvek iný subjekt, ktorý bol zriadený dohodou medzi dvoma alebo viacerými krajinami alebo na základe takejto dohody;

„**Úrad**“ je Úrad na ochranu osobných údajov SR, ktorý je dozorným orgánom v zmysle GDPR a Zákona o ochrane osobných údajov, webové sídlo: www.dataprotection.gov.sk.

(2) Táto interná politika subsidiárne používa aj pojmy definované v § 5 Zákona o ochrane osobných údajov, pričom nasledovnými pojmami sa rozumie:

„**logom**“ záznam o priebehu činnosti používateľa v automatizovanom informačnom systéme;

„**šifrovaním**“ transformácia osobných údajov spôsobom, ktorým opätovné spracúvanie je možné len po zadaní zvoleného parametra, ako je kľúč alebo heslo;

„**online identifikátorom**“ identifikátor poskytnutý aplikáciou, nástrojom alebo protokolom, najmä IP adresa, cookies, prihlasovacie údaje do online služieb, rádiofrekvenčná identifikácia, ktoré môžu zanechávať stopy, ktoré sa najmä v kombinácii s jedinečnými identifikátormi alebo inými informáciami môžu použiť na vytvorenie profilu dotknutej osoby a na jej identifikáciu;

(3) Okrem vyššie uvedeného používa táto interná politika nasledovné definované pojmy:

„**Civilný sporový poriadok**“ znamená zákon č. 160/2015 Z. z., Civilný sporový poriadok, v znení neskorších predpisov;

„**Civilný mimosporový poriadok**“ znamená Zákon č. 161/2015 Z. z., Civilný mimosporový poriadok, v znení neskorších predpisov;

„**Exekučný poriadok**“ znamená zákon č. zákon č. 233/1995 Z. z., o súdnych exekútoroch a exekučnej činnosti (Exekučný poriadok), v znení neskorších predpisov;

„**Občiansky súdny poriadok**“ znamená zákon č. 99/1963 Zb. Občiansky súdny poriadok, v znení neskorších predpisov;

„**Občiansky zákonník**“ znamená zákon č. 40/1964 Zb., Občiansky zákonník, v znení neskorších predpisov;

„**Obchodný zákonník**“ znamená zákon č. 513/1991 Zb., Obchodný zákonník, v znení neskorších predpisov;

„**Podmienky ochrany súkromia**“ znamenajú podmienky ochrany súkromia v aktuálnom znení zverejnené na webovom sídle

„**Vyhláška o požiarnej prevencii**“ znamená vyhláška Ministerstva vnútra Slovenskej republiky č. 121/2002 Z. z. o požiarnej prevencii v znení neskorších predpisov;

„**Zákon o archívoch**“ znamená zákon č. 395/2002 Z. z. o archívoch a registratúrach, v znení neskorších predpisov;

„**Zákon o cenách**“ znamená zákon č. 18/1996 Zb., o cenách, v znení neskorších predpisov;

„**Zákon o dani z príjmov**“ znamená zákon č. 595/2003 Z. z. o dani z príjmov, v znení neskorších predpisov;

„**Zákon o hlásení pobytu**“ znamená zákon č. 253/1998 Z.z., o hlásení pobytu občanov Slovenskej republiky a registri obyvateľov Slovenskej republiky, v znení neskorších predpisov;

„**Zákon o náhrade príjmu**“ znamená zákon č. 462/2003 Z. z. o náhrade príjmu pri dočasnej neschopnosti zamestnanca a o zmene a doplnení niektorých zákonov, v znení neskorších predpisov;

„**Zákon o nájme**“ znamená zákon č. 116/1990 Zb., o nájme a prenájme nebytových priestorov, v znení neskorších predpisov;

„**Zákon o sociálnom fonde**“ znamená zákon č. 152/1994 Z. z. o sociálnom fonde a o zmene a doplnení zákona č. 286/1992 Zb. o daniach z príjmov v znení neskorších predpisov;

„**Zákon o sociálnom poistení**“ znamená zákon č. 461/2003 Z. z. o sociálnom poistení, v znení neskorších predpisov;

„**Zákon o službách zamestnanosti**“ znamená zákon č. 5/2004 Z. z. o službách zamestnanosti a o zmene a doplnení niektorých zákonov, v znení neskorších predpisov;

„**Zákon o ochrane osobných údajov“** znamená zákon č. 18/2018 Z. z. o ochrane osobných údajov;

„**Zákon o účtovníctve**“ znamená zákon č. 431/2002 Z.z., o účtovníctve, v znení neskorších predpisov;

„**Zákon o zdravotnom poistení**“ znamená zákon č. 580/2004 Z. z. o zdravotnom poistení a o zmene a doplnení zákona č. 95/2002 Z. z. o poisťovníctve a o zmene a doplnení niektorých zákonov, v znení neskorších predpisov;

„**Zákonník práce**“ znamená zákon č. 311/2001 Z. z., Zákonník práce v znení neskorších predpisov.

§ 3

ÚČELY SPRACÚVANIA OSOBNÝCH ÚDAJOV

(1) V DRE dochádza k spracúvaniu osobných údajov na nasledovné účely:

	Účel	Právny základ	Režim	Súvisiace právne predpisy	Citlivé OÚ
1	Personalistika a mzdy	Plnenie zákonných povinností (čl. 6 ods. 1 písm. c) GDPR)	GDPR	Zákonník práce; Zákon o odmeňovaní; Zákon o náhrade príjmu; Zákon o dani z príjmov; Zákon o zdravotnom poistení; Zákon o sociálnom poistení; Zákon o službách zamestnanosti; Zákon o sociálnom fonde	Áno
2	Zmluvy	Plnenie zmluvy s dotknutou osobou (čl. 6 ods. 1 písm. b) GDPR)	GDPR	Obchodný zákonník; Občiansky zákonník; Zákon o cenách; Zákon o sociálnom fonde; Zákon o nájme	Nie
3	Súdne spory	Oprávnený záujem DRE (čl. 6 ods. 1 písm. f) GDPR): *preukazovanie, uplatňovanie a obhajovanie právnych nárokov*	GDPR	Občiansky súdny poriadok; Civilný sporový poriadok, Civilný mimosporový poriadok a Správny súdny poriadok	Nie
4	Účtovné doklady	Plnenie zákonných povinností (čl. 6 ods. 1 písm. c) GDPR)	GDPR	Zákon o účtovníctve, Zákon o dani z príjmov;	Nie

(2) Vyššie uvedené účely predstavujú všetky identifikované účely v rámci DRE. DPO je uvedený nižšie

(3) DPO (tak ako sú definované nižšie) je povinný používať jednotné označenie účelov vymedzených v tejto internej politike. Ak sa chce DPO odchýliť od označenia účelu alebo vymedziť nový účel nad rámec uvedený v tejto internej politike, tento krok musí odsúhlasiť Štatutár (tak ako je definovaná nižšie), pričom pred začatím spracúvania musí byť upravený zoznam účelov v tejto internej politike a v Podmienkach ochrany súkromia.

§ 4

OSOBY ZAHRNUTÉ DO SPRACÚVANIA OSOBNÝCH ÚDAJOV

(1) Táto časť internej politiky vysvetľuje, akým spôsobom DRE organizačno-personálne zabezpečuje súlad s predpismi na ochrany osobných údajov.

Subjekty	**Základne vysvetlenie úloh a zodpovednosti**
Zodpovedná osoba DRE (ďalej len „**DPO“**)	▪ Zodpovedá a poskytuje pravidelné správy o stave ochrany osobných údajov v rámci DRE; ▪ **Metodicky usmerňuje** ▪ **Monitoruje súlad DRE s** GDPR, Zákonom o ochrane osobných údajov a s touto internou politikou; ▪ Zvyšuje povedomie a odbornú prípravy personálu; ▪ Plní úlohy DPO podľa čl. 39 GDPR ▪ Nesie zodpovednosť za plnenie úloh a povinností, ktoré mu ustanovuje táto interná politika ochrany osobných údajov a GDPR;

Kontaktné údaje DPO:	
Paulína Matulániová, **paulina.matulaniova@gmail.com**	
Postavenie:	**Interná** / Externá
Miesto výkonu povinností: Brnice166, 032 21 Liptovská Sielnica	

§ 5

ZÁKLADNÉ ROZDELENIE ÚLOH A ZODPOVEDNOSTI (DPO)

(1) **Nezávislé postavenie**. DRE zabezpečuje a udržiava v rámci celej organizácie také podmienky, ktoré umožňujú postavenie zodpovedných osôb podľa článku 38 GDPR. Z tohto dôvodu má DPO právo byť zapojená do všetkých záležitostí, ktoré súvisia s ochranou osobných údajov a nesmie dostávať žiadne pokyny v súvislosti s plnením svojich úloh a nesmie byť trestaná za výkon svojich úloh. DPO má právo byť zapojená len do tých záležitostí, ktoré súvisia s ochranou osobných údajov a nesmie dostávať žiadne pokyny v súvislosti s plnením svojich úloh a nesmie byť trestaná za výkon svojich úloh.

„Príklad: Za zakázaný pokyn sa považuje napr. pokyn vykonať posúdenie vplyvu s výsledkom nízkeho rizika. Za zakázaný pokyn sa nepovažuje pokyn vedenia poskytnúť poradenstvo v súvislosti s posúdením vplyvu.“

(2) **Poskytovanie informácií a poradenstva**. Na DPO sa môže obrátiť každý zamestnanec alebo partner DRE v otázkach ochrany osobných údajov a žiadať poskytnutie informácií v rámci organizácie.

(3) **Monitorovanie súladu**. DPO monitoruje celkový súlad s GDPR, Zákonom o ochrane osobných údajov (najmä základnými zásadami spracúvania osobných údajov), inými predpismi týkajúcimi sa ochrany súkromia alebo osobných údajov a touto internou politikou minimálne tým, že:

- zvyšuje povedomie a odbornú prípravu personálu ; a
- vykonáva súvisiace audity;

(4) **Zvyšovanie povedomia**. Zodpovedná osoba má právo na kontinuálne prehlbovanie svojich odborných vedomostí v čom ich DRE materiálne podporuje a vytvára pre neho priestor pre absolvovanie vhodného doplnkového tréningu a vzdelávania. Zodpovedná osoba zvyšuje svoje odborné znalosti a vedomosti v oblasti ochrany osobných údajov v prospech DRE účasťou na obdobných kurzoch, seminároch alebo konferenciách zameraných na problematiku ochrany osobných údajov alebo kyber-bezpečnosti . Zodpovedná osoba je povinná kontinuálne sledovať vývoj a trendy v ochrane osobných údajov s dôrazom na: (i) oficiálne právne názory a stanoviská Európskeho výboru pre ochranu osobných údajov (pôvodný názov Pracovná skupina čl. 29); (ii) metodické usmernenia Úradu; (iii) judikatúru Súdneho dvora EÚ vo veciach ochrany osobných údajov. Nadobudnuté znalosti zodpovedná osoba prenášajú do praxe DRE.

„Príklad: DPO sa získava materiály z odborných kurzov, seminárov a konferencií a poskytuje tieto ďalej v rámci DRE, ak je to dovolené.“

(6) **Audity**. Pod vedením DPO sa vykonávajú pravidelné audity ochrany osobných údajov v DRE. Audit sa môže týkať čiastkovej oblasti alebo celej organizácie.

(7) **Spis**. Zodpovedná osoba si vedie ucelený spis o všetkých skutočnostiach a dokumentoch, ktoré súvisia s agendou ochrany osobných. Spis musí byť vždy pripravený pre prípadnú kontrolu alebo konanie zo strany Úradu prípadne súdu vo veci ochrany osobných údajov.

(8) **Posúdenie vplyvu**. Zodpovedná osoba kontinuálne sleduje vznik povinnosti vykonať posúdenie vplyvu podľa článku 35 ods. 1 až 3 GDPR alebo podľa § 42 Zákona o ochrane osobných údajov. Ak sa DPO domnieva, že DRE ako taký má povinnosť vykonať posúdenie vplyvu, okamžite o tom informuje Štatutára, ktorý stanoví ďalší postupu. Odporúčaným postupom je vykonávať posúdenie vplyvu DPO je povinná pri stanovovaní ďalšieho postupu náležite zohľadniť skutočnosť, že ak sa posúdenie vplyvu týka účelov, ktoré sa riadia režimom podľa druhej alebo tretej časti Zákona o ochrane osobných údajov, na vykonávanie posúdenia vplyvu sa vzťahu vyhláška Úradu č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov. Vykonané posúdenie vplyvu je súčasťou Spisu. Povinnosť vykonať posúdenie vplyvu môže spôsobiť napr.:

- využitie modernej technológie, ktorá by mohla viesť k vzniku rizík pre práva a slobody dotknutých osôb;
- systematické a rozsiahle hodnotenie osobných aspektov týkajúcich sa fyzických osôb, ktoré je založené na automatizovanom spracúvaní vrátane profilovania a z ktorého vychádzajú rozhodnutia s právnymi účinkami týkajúcimi sa fyzickej osoby alebo s podobne závažným vplyvom na ňu;
- spracúvanie vo veľkom rozsahu osobitných kategórií údajov alebo osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky;
- systematické monitorovania verejne prístupných miest vo veľkom rozsahu;
- spracúvanie, ktoré za také označí Úrad.

DPO je povinný preskúmať alebo poveriť preskúmaním danú DPO každé už vykonané posúdenie vplyvu na ochranu osobných údajov minimálne raz za 3 roky.

(9) **Kontaktný bod pre Úrad**. Zodpovedná osoba v prípade potreby konzultujú odborné otázky týkajúce sa ochrany osobných údajov s Úradom, prípadne aj s iným dozorným orgánom z iného členského štátu EÚ. Tým nie je dotknutý výkon úlohy zodpovednej osoby pôsobiť samostatne ako kontaktný bod pre Úrad a poskytovať mu v tejto súvislosti základnú koordinačnú a informačnú súčinnosť (napr. viesť komunikáciu, poskytnúť požadované vysvetlenia apod.).Akákoľvek komunikácia s dozornými orgánmi sa uchováva v Spise.

(10) **Riziká pre práva a slobody**. Zodpovedná osoba pri výkone svojich úloh náležite zohľadňuje riziko pre práva a slobody dotknutých osôb, ktoré je spojené alebo môže byť spojené s vykonávanými alebo plánovanými spracovateľskými operáciami, pričom berie na vedomie povahu, rozsah, kontext a účely spracúvania osobných údajov. V prípade vzniku a identifikácie vysokého rizika pre práva a slobody dotknutých osôb

spojeného s vykonávaním spracúvania osobných údajov zodpovedná osoba iniciuje proces vykonania posúdenia vplyvu podľa § 5 ods. 8 vyššie.

(11) **Mlčanlivosť**. Zodpovedná osoba ako aj všetci zamestnanci spracúvajúci osobné údaje alebo majúci prístup k osobným údajom v rámci DRE sú povinní dodržiavať mlčanlivosť o všetkých záležitostiach, o ktorých sa dozvedeli pri výkone svojej funkcie resp. o všetkých osobných údajoch, ktoré spracúvajú alebo ku ktorým majú prístup. Povinnosť zachovávať mlčanlivosť trvá aj po skončení funkcie, pracovného pomeru, alebo obdobného pracovného vzťahu tejto fyzickej osoby s DRE.

(12) **Záznamy o spracovateľských činnostiach**. DPO vedie záznamy o spracovateľských činnostiach.

(15) **Ďalšie úlohy DPO** . Vykonáva DPO taktiež nasledovné činnosti:

- zodpovedá za vypracovanie, aktualizovanie a zverejňovanie Podmienok ochrany súkromia v súlade s §8 nižšie;
- Navrhuje zmeny tejto internej politiky
- ďalšie úlohy, ak tak stanovuje táto interná politika.

§ 6

ZÁKLADNÉ ZÁSADY SPRACÚVANIA OSOBNÝCH ÚDAJOV

(1) Osobné údaje musia byť spracúvané v súlade so základnými zásadami spracúvania podľa čl. 5 GDPR resp. prvej hlavy druhej časti Zákona o ochrane osobných údajov. Za súlad so základnými zásadami zodpovedá DRE, za monitorovanie súladu DRE s nimi zodpovedá DPO.

(2) **Zákonnosť, spravodlivosť a transparentnosť**. Osobné údaje musia byť spracúvané zákonným spôsobom, spravodlivo a transparentne vo vzťahu k dotknutej osobe. Zákonnosť a spravodlivosť spracúvania napĺňa najmä: (i) vhodným vymedzením účelov a právnych základov spracúvania, ktorú DPO dokumentuje v záznamoch o spracovateľských činnostiach; (ii) používaním jednotných vzorov súhlasov so spracúvaním osobných údajov a zmluvnej dokumentácie, ktorú pripraví DPO ; a (iii) zabezpečením súladu s testom zlučiteľnosti podľa čl. 6 ods. 4 GDPR, ako je bližšie vymedzený v § 7 nižšie. Transparentnosť spracúvania je okrem iného bližšie upravená v §8 nižšie.

(3) **Obmedzenie účelu**. Osobné údaje musia byť získavané na konkrétne určené, výslovne uvedené a legitímne účely a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmito účelmi.

(4) **Minimalizácia údajov**. Osobné údaje musia byť primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú.

(5) **Správnosť**. Osobné údaje musia byť 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. DRE v súvislosti so zásadou správnosti prijal nasledovné opatrenie:

(6) **Minimalizácia uchovávania**. Osobné údaje musia byť 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,

(7) **Integrita a dôvernosť**.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.

(8) **Zodpovednosť**. DRE zodpovedá za súlad s vyššie uvedenými zásadami a musí vedieť kedykoľvek tento súlad preukázať.

(9) **Zákaz zverejňovania rodného čísla**. V zmysle § 78 ods. 4 tretej vety Zákona o ochrane osobných údajov je zakázané zverejňovanie rodného čísla okrem situácie, kedy ho zverejní sama dotknutá osoba.

§ 7

TEST ZLUČITEĽNOSTI NOVÉHO ÚČELU SPRACÚVANIA

(1) Ak majú byť osobné údaje spracúvané na iné účely spracúvania ako na tie, za ktorými boli pôvodne získané, je potrebné pred začatím spracúvania na iné účely vykonať test zlučiteľnosti podľa čl. 6 ods. 4 GDPR. Test zlučiteľnosti vykonáva DPO Výsledkom testu zlučiteľnosti je buď výsledok, že nový účel spracúvania je zlučiteľný (vtedy možno pokračovať v spracúvaní) alebo, že nový účel nie je zlučiteľný (vtedy nemožno pokračovať v spracúvaní). Výsledok testu zlučiteľnosti sa zdokumentuje a uchováva v Spise.

(2) Pri vykonávaní testu compatibility nového účelu s pôvodným účelom, na ktorý boli spracúvané osobné údaje pôvodne získané je DPO povinný zohľadniť požiadavky článku 6 ods. 4 GDPR:

- akékoľvek prepojenie medzi účelmi, na ktoré sa osobné údaje získali, a účelmi zamýšľaného ďalšieho spracúvania;
- okolnosti, za akých sa osobné údaje získali, najmä týkajúce sa vzťahu medzi dotknutými osobami a Prevádzkovateľom;
- možné následky zamýšľaného ďalšieho spracúvania pre dotknuté osoby;
- existenciu primeraných záruk, ktoré môžu zahŕňať šifrovanie alebo pseudonymizáciu.

(3) Test zlučiteľnosti sa nevzťahuje na situácie, kedy DRE vymedzí nové účely spracúvania vo vzťahu k osobným údajom, ktoré ešte neboli získané, napr. ak je viacero účelov od momentu získania osobných údajov vymedzených Podmienkami ochrany súkromia.

(4) Pri vykonávaní testu kompatibility a zohľadňovaní vyššie uvedených požiadaviek DPO prihliada na nižšie uvedenú pomôcku s otázkami. Za každú odpoveď „ÁNO“ je 1 bod. Za každú odpoveď „NIE“ je 0 bodov. Pre úspešné vykonanie testu kompatibility účelov spracúvania osobných údajov je potrebné dosiahnuť výsledok aspoň 7 bodov. Nižšie uvedená tabuľka je len pomôckou pre DPO pre lepšie zabezpečovanie súladu s článkom 6 ods. 4 GDPR.

Otázka	Odpoveď	Bodový zisk
Súvisí po obsahovej stránke nový účel s pôvodným účelom spracúvania (i.e. sleduje dosiahnutie rovnakých alebo podobných cieľov)?	ÁNO / NIE	0-1 bodov
Týka sa nový účel spracúvania osobných údajov rovnakého okruhu dotknutých osôb?	ÁNO / NIE	0-1 bodov
Boli osobné údaje, ktoré už DRE spracúva a ktoré sa týkajú nového účelu spracúvania pôvodne získané v súlade s GDPR (bola splnená informačná povinnosť, bol dostatočný právny základ)?	ÁNO / NIE	0-1 bodov
Môžu dotknuté osoby legitímne očakávať, že DRE by mohol s ohľadom na svoje postavenie a úlohy ktoré plní začať spracúvať osobné údaje na nový účel?	ÁNO / NIE	0-1 bodov
Ak sa týka posudzované spracúvanie osobných údajov z osobitnej kategórie je daný špecifický právny základ podľa článku 9 ods. 2 GDPR na pôvodný účel spracúvania osobných údajov?	ÁNO / NIE	0-1 bodov
Ak sa týka posudzované spracúvanie osobných údajov z osobitnej kategórie je daný špecifický právny základ podľa článku 9 ods. 2 GDPR na nový účel spracúvania osobných údajov?	ÁNO / NIE	0-1 bodov
Ak sa týka posudzované spracúvanie osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky je to v kontexte pôvodného účelu povolené právom EÚ alebo Slovenskej republiky?	ÁNO / NIE	0-1 bodov

Ak sa týka posudzované spracúvanie osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky je to v kontexte nového účelu povolené právom EÚ alebo Slovenskej republiky?	ÁNO / NIE	0-1 bodov
Je dostatočne právne a fakticky garantované, že zamýšľané spracúvanie osobných údajov na nový účel nebude mať žiadne negatívne následky pre práva a slobody dotknutých osôb?	ÁNO / NIE	0-1 bodov
Ak bude súčasťou posudzovaného spracúvania na nový účel spracúvania plne automatizované spracúvanie s právnym účinkom alebo iným podstatným vplyvom na dotknutú osobu budú riadne splnené požiadavky GDPR?	ÁNO / NIE	0-1 bodov
Je zamýšľané spracúvanie osobných údajov na nový účel spracúvania dostatočne zabezpečené organizačnými bezpečnostnými opatreniami prijatými Prevádzkovateľom v súlade s článkom 32 GDPR?	ÁNO / NIE	0-1 bodov
Je zamýšľané spracúvanie osobných údajov na nový účel spracúvania dostatočne zabezpečené technickými bezpečnostnými opatreniami prijatými Prevádzkovateľom v súlade s článkom 32 GDPR?	ÁNO / NIE	0-1 bodov
Výsledok testu zlučiteľnosti:		

§ 8

PLNENIE INFORMAČNÝCH POVINNOSTÍ VOČI DOTKNUTÝM OSOBÁM

(1) **Primárny spôsob**. DRE plní svoje informačné povinnosti podľa článku 13 a 14 GDPR resp. § 19 a § 20 Zákona o ochrane osobných údajov vypracovaním a aktualizovaním jednotných Podmienok ochrany súkromia, ktoré sú dotknutým osobám primárne dostupné na oficiálnom webovom sídle DRE ako aj na všetkých weboch prevádzkovaných DRE. Za vypracovanie a aktualizovanie Podmienok ochrany súkromia zodpovedá DPO.

(2) **Alternatívny spôsob**. V niektorých osobitných prípadoch online sprístupnenie Podmienok ochrany súkromia nemusí byť spravodlivé alebo účelné pre dotknuté osoby. V týchto osobitných prípadoch by mali byť Podmienky ochrany súkromia poskytované aj iným alternatívny spôsobom, a to najmä v tlačenej podobe alebo prenesením tejto povinnosti (zmluvne) na inú osobu.

(3) Ak dochádza k alternatívnemu poskytnutiu Podmienok ochrany súkromia v tlačenej podobe, zamestnanec, ktorý poskytuje Podmienky ochrany súkromia v tlačenej podobe

je povinný zabezpečiť, aby mal vždy k dispozícii minimálne 1 výtlačok Podmienok ochrany súkromia resp. aby vedel kedykoľvek zabezpečiť ich okamžité vytlačenie.

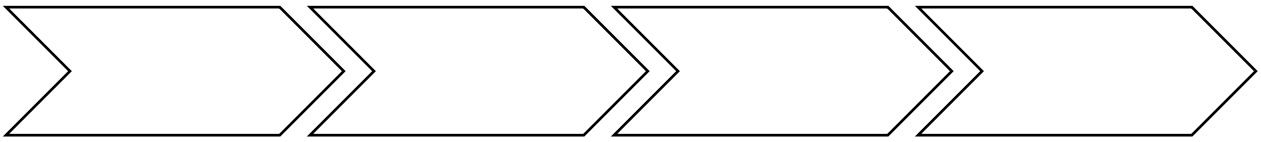
(4) Kedykoľvek dotknutá osoba požiada o základné informácie o spracúvaní osobných údajov v DRE v tlačenej podobe daná DPO poskytne dotknutej osobe Podmienky ochrany súkromia v tlačenej podobe.

(5) V špecifických prípadoch – napr. ak dotknutá osoba nevie čítať – musí daná DPO zabezpečiť, aby dotknutej osobe – ak o to požiada – boli Podmienky ochrany súkromia prečítané ústne alebo iným vhodným spôsobom zohľadňujúcim osobitné potreby dotknutej osoby.

§ 9

POLITIKA VYBAVOVANIA ŽIADOSTÍ DOTKNUTÝCH OSÔB

(1) Proces vybavovania žiadostí dotknutých osôb je možné zobraziť nasledovne, pričom jednotlivé kroky sú vysvetlené nižšie:



(2) Každý krok procesu vybavovania žiadostí dotknutých osôb má všeobecnú lehotu, od ktorej je možné sa odchýliť len ak tak dovoľuje táto interná politika:

(3) S dotknutou osobou sa komunikuje v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme, informácie a odpovede sú formulované jasne a jednoducho, a to najmä v prípade informácií určených osobitne dieťaťu. Vybavovanie žiadosti prebieha zadarmo, pokiaľ sa v tejto internej politike neuvádza inak.

(4) Pri komunikácii s dotknutou osobou sa preferuje spôsob komunikácie používaný alebo preferovaný dotknutou osobou.

„Príklad: Ak dotknutá osoba uplatní žiadosť korešpondenčne (poštou), DRE odpovedá na žiadosť korešpondenčne (poštou), pokiaľ sa v liste neuvádza, že dotknutá osoba si praje odpoveď elektronicky na svoju emailovú adresu. Ak dotknutá osoba uplatní žiadosť emailom, DRE odpovedá emailom, pokiaľ sa v emaily neuvádza, že dotknutá osoba si praje odpovedať korešpondenčne (listom) na uvedenú adresu.“

ZAEVIDOVANIE ŽIADOSTI

(5) DRE uľahčuje výkon práv dotknutých osôb tým, že v Podmienkach ochrany súkromia zriadi jednotné kontaktné body pre dotknuté osoby minimálne vo forme (i) emailu DPO a (ii) korešpondenčnej adresy DPO v rámci DRE. Tieto kontaktné body musia byť určené takým spôsobom, aby bol minimalizovaný počet kanálov, ktorými sa žiadosti dotknutých osôb môžu k DRE dostať.

(6) DRE neprijíma žiadosti dotknutých osôb:

- cez sociálne siete;
- cez SMS;
- telefonicky.

„Príklad: Ak by bol akýkoľvek zamestnanec požiadaný dotknutou osobou o čokoľvek súvisiace s osobnými údajmi, je oprávnený len odkázať na podmienky ochrany súkromia DRE a nesmie žiadnu žiadosť dotknutej osoby prijať v mene DRE, pričom použije nasledovné vysvetlenie:

„OBRÁŤTE SA PROSÍM NA ZODPOVEDNÚ OSOBU DRE, KTOREJ KONTAKTNÉ ÚDAJE NÁJDETE V PODMIENKACH OCHRANY SÚKROMIA NACHÁDZAJÚCICH SA NA WEBOVOM SÍDLE DRE.“

POSÚDENIE OBSAHU ŽIADOSTI

(7) Osoba zodpovedná za žiadosť pri posúdení obsahu žiadosti v prvom rade posúdi:

- Či dotknutá osoba je v žiadosti dostatočne identifikovaná (§ 9 ods. 12 nižšie);
- Či nejde o spracúvanie osobných údajov bez potreby identifikácie podľa čl. 11 GDPR;
- Či nejde o zjavne neopodstatnenú alebo neprimeranú žiadosť podľa čl. 12 ods. 5 GDPR;
- Akého práva sa žiadosť dotknutej osoby týka.

(8) **Pochybnosti o identite dotknutej osoby**. Ak má Osoba zodpovedná za žiadosť oprávnené pochybnosti v súvislosti s totožnosťou fyzickej osoby, ktorá podáva žiadosť, môže požiadať o poskytnutie dodatočných informácií potrebných na potvrdenie totožnosti dotknutej osoby. A následne pripraví odpoveď podľa §9 ods. 20 nižšie.

(9) **Zjavne neopodstatnená alebo neprimeraná žiadosť**. Ak je žiadosť dotknutej osoby zjavne neopodstatnená alebo neprimeraná, najmä pre jej opakujúcu sa povahu, Osoba zodpovedná za vybavenie žiadosti môže ako odpoveď navrhnúť buď:

- požadovať primeraný poplatok zohľadňujúci administratívne náklady na poskytnutie informácií alebo na oznámenie alebo na uskutočnenie požadovaného opatrenia; alebo
- odmietnuť konať na základe žiadosti dotknutej osoby;

(10) **Uplatnené právo dotknutej osoby**.

Dotknutá osoba má tieto práva:

- Právo na prístup k údajom podľa čl. 15 GDPR;
- Právo na opravu podľa čl. 16 GDPR;
- Právo na vymazanie (zabudnutie) podľa čl. 17 GDPR;
- Právo na obmedzenie spracúvania podľa čl. 18 GDPR;
- Právo na oznámenie informácií príjemcom podľa čl. 19 GDPR;
- Právo na prenosnosť podľa čl. 20 GDPR;
- Právo namietať podľa čl. 21 GDPR;
- Právo „namietať“ proti automatizovanému individuálnemu rozhodovaniu podľa čl. 22 GDPR.

(11) **Všeobecné žiadosti**. V praxi môže dochádzať k tomu, že dotknuté osoby žiadajú informácie, ktoré výslovne nevyplývajú z vyššie uvedených práv (napr. dotknutá osoba sa môže pýtať ako je zabezpečená ochrana jej osobných údajov podľa GDPR). Odporúčaným postupom v takom prípade odkazovať na všeobecné informácie v Podmienkach ochrany súkromia, výslovne odpovedať len na žiadosti dotknutých osôb týkajúce sa vyššie uvedených práv.

PRIPRAVENIE ODPOVEDE

(12) Za pripravenie odpovede na žiadosť dotknutej osoby zodpovedá a musí ju zaznamenať **do 12 pracovných dní odo dňa prijatia žiadosti**. Pripravenie odpovede predstavuje len pripravenie návrhu odpovede, ktorá musí byť schválená v nasledovnom kroku. Osoba zodpovedná za žiadosť pri pripravení odpovede postupuje primerane podľa bodov nižšie. Od bodov nižšie sa môže Osoba zodpovedná za žiadosť odchýliť, ak to považuje za potrebné. Nižšie uvedené body predstavujú len návod alebo usmernenie pre Osoby zodpovedné za žiadosti.

(13) Vzorová odpoveď podľa § 9 ods. 12 vyššie (**Pochybnosti o identite dotknutej osoby**) môže znieť nasledovne:

*Z Vašej žiadosti nám nie je dostatočne zrejmá Vaša totožnosť a preto nemôžeme pristúpiť k vybaveniu Vašej žiadosti. Ak máte naďalej záujem o vybavenie Vašej žiadosti, prosíme Vás preto o poskytnutie dodatočných informácií potrebných na potvrdenie Vašej totožnosti (napr.: /**uvedie sa typ informácie alebo informácií, ktoré by v danom kontexte umožnili overiť totožnosť dotknutej osoby**/) alebo si dohodnite osobné stretnutie pre podanie žiadosti na telefónnom čísle /XX/, kde sa preukážete občianskym preukazom. Prosíme Vás o porozumenie, nakoľko poskytnutie niektorých chránených informácií neoprávnenej osobe môže predstavovať porušenie ochrany osobných údajov. Snažíme sa týmto postupom chrániť osobné údaje. **Poučenie**: Postupujeme v súlade s čl. 12 ods. 6 všeobecného nariadenia EÚ o ochrane osobných údajov (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.**“*

(14) Vzorová odpoveď podľa § 9 ods. 13 vyššie (**Zjavne neopodstatnená alebo neprimeraná žiadosť**) môže znieť nasledovne:

Vašu žiadosť považujeme za zjavne neopodstatnenú / neprimeranú z nasledovných dôvodov: /doplnia sa dôvody/. V súlade s čl. 12 ods. 5 všeobecného nariadenia na ochranu osobných údajov (GDPR) sme sa rozhodli:

/dve alternatívy/:

- *konať na základe Vašej žiadosti len po Vašom uhradení administratívnych nákladov spojených s Vašou žiadosťou vo výške XX na účet: XX; alebo*
- *odmietnuť konať na základe Vašej žiadosti.*

Máte možnosť podať sťažnosť Úradu na ochranu osobných údajov SR alebo uplatniť súdny prostriedok nápravy.

(15) PRÁVO NA PRÍSTUP K OSOBNÝM ÚDAJOM (ČLÁNOK 15 GDPR)

Všeobecne. Pri žiadosti o prístup k osobným údajom podľa čl. 15 GDPR Osoba zodpovedná za žiadosť preverí, či o konkrétnej dotknutej osobe sú osobné údaje spracúvané a ak áno, pripraví dotknutej osobe odpoveď s ohľadom na informácie podľa čl. 15 ods. 1 a ods. 2 GDPR. Odporúčaným postupom je vychádzať zo štruktúry a obsahu Podmienok ochrany súkromia, avšak tieto všeobecné informácie je potrebné prispôsobiť žiadosti konkrétnej dotknutej osoby. Ak sa o dotknutej osobe nespracúvajú žiadne osobné údaje, informácie podľa predchádzajúcej vety sa dotknutej osobe neposkytujú (iba informácia, že v rámci DRE sa o nej nespracúvajú žiadne osobné údaje).

Kópie osobných údajov. V prípade, ak žiadosť dotknutej osoby obsahuje aj výslovnú požiadavku o poskytnutie kópií osobných údajov spracúvaných DRE, Osoba zodpovedná za žiadosť v návrhu odpovedi navrhne spôsob, akým majú byť kópie osobných údajov poskytnuté, pričom sa zohľadní množstvo spracúvaných osobných údajov o dotknutej osobe, ako je uvedené v bode 63 úvodnej časti GDPR:

„Ak prevádzkovateľ spracúva v súvislosti s dotknutou osobou veľké množstvo informácií, mal by môcť požadovať, aby pred doručením informácií dotknutá osoba spresnila, ktorých informácií alebo spracovateľských činností sa žiadosť týka.“

Nepriaznivé dôsledky pre práva a slobody iných. Poskytnutím kópii ale ani celkovo vybavením žiadosti o prístup k osobným údajom nesmie nepriaznivo dotknúť práv a slobôd iných, ako je bližšie uvedené (okrem čl. 15 ods. 4 GDPR) aj v bode 63 úvodnej časti GDPR:

„Uvedené právo by sa nemalo nepriaznivo dotknúť práv alebo slobôd iných osôb, ani obchodného tajomstva alebo práv duševného vlastníctva a najmä autorských práv týkajúcich sa softvéru.“

(16) PRÁVO NA OPRAVU (ČLÁNOK 16 GDPR)

Všeobecne. Pri žiadosti dotknutej osoby podľa článku 16 GDPR Osoba zodpovedná za žiadosť v prvom rade preverí, či dotknutá osoba žiada o opravu nesprávnych osobných údajov alebo o doplnenie neúplných osobných údajov. Právo na opravu nezahŕňa právo na zabezpečenie absolútnej objektívnej pravdivosti osobných údajov, ale len právo na zabezpečenie správnosti údajov z hľadiska účelu spracúvania (viď zásada správnosti).

Informácia príjemcom. Spolu s odpoveďou dotknutej osobe Osoba zodpovedná za žiadosť pripraví návrh informácie, ktorá sa má prípadne zaslať príjemcom osobných údajov v zmysle čl. 19 GDPR.[1]

Doplnkové vyhlásenie. Pre uľahčenie výkonu žiadosti dotknutej osoby je možné dotknutej osobe poskytnúť možnosť vyplnenia doplnkového vyhlásenia:

Doplnkové vyhlásenie k oprave a/alebo aktualizácii osobných údajov	
Meno a priezvisko:	
Adresa elektronickej pošty:	
Právny vzťah dotknutej osoby k prevádzkovateľovi	*Prosím uveďte v akom ste vzťahu k DRE a na aký účel o Vás spracúvame osobné údaje*
Predmet Vašej žiadosti:	*Prosím vysvetlite nám, či požadujete opravu nesprávnych osobných údajov alebo doplnenie neaktuálnych osobných údajov*
Predpokladaná príčina problému:	*Prosím vysvetlite nám prečo si myslíte, že o Vás spracúvame nesprávne alebo neaktuálne osobné údaje*
Žiadosť o opravu	*Prosím presne vymedzte aké osobné údaje požadujete opraviť v tvare nesprávny údaj: xyz, správny údaj: xyz*

(17) PRÁVO NA VYMAZANIE(ZABUDNUTIE) (ČLÁNOK 17 GDPR)

Všeobecne. Osoba zodpovedná za žiadosť v prvom rade preverí, či je splnený aspoň jeden z nižšie uvedených dôvodov podľa čl. 17 ods. 1 GDPR, ktorý oprávňuje dotknutú osobu dosiahnuť vymazanie osobných údajov (ak neexistuje výnimka uvedená nižšie):

[1] Čl. 19 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.“

- osobné údaje už nie sú potrebné na účely, na ktoré sa získavali alebo inak spracúvali;
- dotknutá osoba odvolá súhlas, na základe ktorého sa spracúvanie vykonáva, podľa článku 6 ods. 1 písm. a) alebo článku 9 ods. 2 písm. a) GDPR, a ak neexistuje iný právny základ pre spracúvanie;
- dotknutá osoba namieta voči spracúvaniu podľa článku 21 ods. 1 GDPR (oprávnené alebo verejný záujem) a neprevažujú žiadne oprávnené dôvody na spracúvanie alebo dotknutá osoba namieta voči spracúvaniu podľa článku 21 ods. 2 (priamy marketing);
- osobné údaje sa spracúvali nezákonne;
- osobné údaje musia byť vymazané, aby sa splnila zákonná povinnosť podľa práva Únie alebo práva členského štátu, ktorému DRE podlieha;
- osobné údaje sa získavali v súvislosti s ponukou služieb informačnej spoločnosti podľa článku 8 ods. 1 GDPR.

Výnimky z práva na vymazanie. Osoba zodpovedná za žiadosť následne preverí, či nie sú splnené výnimky uvedené v čl. 17 ods. 3 GDPR, ktoré by odôvodňovali záver, že dotknutá osoba nemá právo na vymazanie jej osobných údajov. Tieto výnimky sú splnené, ak je spracúvanie potrebné:

- na uplatnenie práva na slobodu prejavu a na informácie;
- na splnenie zákonnej povinnosti, ktorá si vyžaduje spracúvanie podľa práva Únie alebo práva členského štátu, ktorému DRE podlieha,
- na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov.

Informácia príjemcom. Spolu s odpoveďou dotknutej osobe Osoba zodpovedná za žiadosť pripraví návrh informácie, ktorá sa má prípadne zaslať príjemcom osobných údajov v zmysle čl. 19 GDPR.

„Príklad: Zo žiadosti dotknutej osoby o vymazanie osobných údajov by malo vyplávať odôvodnenie, z ktorého sa dá vyvodiť, na základe ktorého z dôvodov uvedených v čl. 17 ods. 1 GDPR majú byť osobné údaje vymazané. Na príliš všeobecnú a neodôvodnenú žiadosť ako napr.: „žiadam o vymazanie všetkých osobných údajov, ktoré o mne spracúvate“ je možné odpovedať nasledovne:“

Právo na vymazanie nie je univerzálne alebo absolútne právo (nie vždy je možné dosiahnuť vymazanie osobných údajov u prevádzkovateľa). Dané právo sa uplatňuje len ak sú splnené podmienky podľa čl. 17 ods. 1 GDPR a zároveň len vtedy, ak nie sú dané výnimky podľa čl. 17 ods. 3 GDPR. Keďže z Vašej žiadosti nevyplýva žiadne zdôvodnenie a odkaz na tieto dôvody (Vaša žiadosť je príliš všeobecná), nemôžeme na základe Vašej žiadosti konať. Bez ohľadu na všeobecný charakter Vašej žiadosti si však dovoľujeme uviesť, že ak by neexistovali dôvody na spracúvanie Vašich osobných údajov, Vaše osobné údaje by sme už nespracúvali. Nemyslíme si preto, že existujú dôvody na vymazanie Vašich osobných údajov, čím však nechceme povedať, že by ste nemali právo Vašu žiadosť upresniť uvedením dodatočných informácií. Máte tiež možnosť podať sťažnosť Úradu na ochranu osobných údajov SR alebo uplatniť súdny prostriedok nápravy.

„Príklad: Ak dotknutá osoba žiada vymazanie osobných údajov z dôvodu, že podľa jej názoru sú spracúvané nezákonne, pričom nejde o úplne zjavný prípad nezákonného spracúvania alebo o nezákonnosti nerozhodol ani Úrad ani súd (ide len o osobný právny názor dotknutej osoby alebo jej právneho zástupcu), je možné odpovedať nasledovne:“

Právo na vymazanie nie je univerzálne alebo absolútne právo (nie vždy je možné dosiahnuť vymazanie osobných údajov u prevádzkovateľa). Dané právo sa uplatňuje len ak sú splnené podmienky podľa čl. 17 ods. 1 GDPR a zároveň len vtedy, ak nie sú dané výnimky podľa čl. 17 ods. 3 GDPR. Z Vašej žiadosti vyplýva, že žiadate vymazanie osobných údajov z dôvodu nezákonnosti spracúvania. Nezákonnosť spracúvania môže právoplatne konštatovať len súd alebo Úrad na ochranu osobných údajov SR. Nakoľko k takému konštatovaniu doposiaľ nedošlo, nepovažujeme spracúvanie, ktoré vykonávame na nezákonné. Keďže neexistujú dôvody na vymazanie Vašich osobných údajov, nie sme povinní pristúpiť k vymazaniu Vašich osobných údajov. Máte možnosť podať sťažnosť Úradu na ochranu osobných údajov SR alebo uplatniť súdny prostriedok nápravy.

(18) PRÁVO NA OBMEDZENIE SPRACÚVANIA (ČLÁNOK 18 GDPR)

Všeobecne. Osoba zodpovedná za žiadosť v prvom rade preverí, či je splnený aspoň jeden z nižšie uvedených dôvodov podľa čl. 18 ods. 1 GDPR, ktorý oprávňuje dotknutú osobu účinne uplatniť právo na obmedzenie spracúvania:

- dotknutá osoba napadne správnosť osobných údajov, a to počas obdobia umožňujúceho prevádzkovateľovi overiť správnosť osobných údajov;
- spracúvanie je protizákonné a dotknutá osoba namieta proti vymazaniu osobných údajov a žiada namiesto toho obmedzenie ich použitia;
- prevádzkovateľ už nepotrebuje osobné údaje na účely spracúvania, ale potrebuje ich dotknutá osoba na preukázanie, uplatňovanie alebo obhajovanie právnych nárokov;
- dotknutá osoba namietala voči spracúvaniu podľa článku 21 ods. 1 GDPR, a to až do overenia, či oprávnené dôvody na strane prevádzkovateľa prevažujú nad oprávnenými dôvodmi dotknutej osoby.

Informácia príjemcom. Spolu s odpoveďou dotknutej osobe Osoba zodpovedná za žiadosť pripraví návrh informácie, ktorá sa má prípadne zaslať príjemcom osobných údajov v zmysle čl. 19 GDPR.

Zrušenie obmedzenia. Ak sa po vyhovení žiadosti o obmedzenie spracúvania Ak DPO plánuje obmedzenie spracúvania osobných údajov zrušiť je o tom vopred povinný informovať žiadajúcu dotknutú osobu. DPO je všetky úkony a komunikáciu, ktorú vykonáva pri vybavovaní žiadosti dotknutej osoby povinný uchovávať v osobitnom spise vytvorenom pre agendu vybavovania práv dotknutých osôb.

(19)PRÁVO NA PRENOSNOSŤ (ČLÁNOK 20 GDPR)

Všeobecne. Osoba zodpovedná za žiadosť v prvom rade preverí, či sú splnené všetky formálne dôvody podľa čl. 20 GDPR, ktoré oprávňujú dotknutú osobu účinne uplatniť právo na prenosnosť[2] a to či:

- Je spracúvanie založené na právnom základe súhlasu dotknutej osoby alebo plnenia zmluvy;
- Ide o osobné údaje spracúvané výlučne automatizovane (v elektronickej podobe); a
- Ide o osobné údaje poskytnuté priamo dotknutou osobou.

Prenos inému prevádzkovateľovi. Ak sú splnené formálne dôvody podľa čl. 20 GDPR, Osoba zodpovedná za žiadosť následne posúdi, či dotknutá osoba sama žiada o prenos osobných údajov alebo žiada o prenos osobných údajov inému prevádzkovateľovi podľa čl. 20 ods. 2 GDPR.

Formát. Osobné údaje spadajúce pod právo na prenosnosť musia byť poskytované v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte, napr. CSV, XML alebo JSON. Ak je to jednoduchšie a účelnejšie a dotknutá osoba má záujem o dané osobné údaje, môžu sa jej poskytnúť osobné údaje aj vo forme emailového súboru alebo súboru Microsoft Office.

Nepriaznivé dôsledky pre práva a slobody iných. Právo na prenosnosť nesmie mať nepriaznivé dôsledky pre práva a slobody iných (čl. 20 ods. 5 GDPR).

„Príklad: Poskytnutím osobných údajov prostredníctvom práva na prenosnosť nesmie byť napr. vyzradená utajovaná skutočnosť. Na takéto osobné údaje sa právo na prenosnosť nevzťahuje.“

(20)PRÁVO NAMIETAŤ (ČLÁNOK 21 GDPR)

Všeobecne. Osoba zodpovedná za žiadosť v prvom rade preverí, či sú splnené všetky formálne dôvody podľa čl. 21 GDPR, ktoré oprávňujú dotknutú osobu účinne uplatniť právo namietať. Konkrétne, právo namietať existuje len voči takému spracúvaniu osobných údajov, ktoré:

- je založené na právnom základe oprávneného záujmu podľa čl. 6 ods. 1 písm. f) GDPR;
- je založené na právnom základe verejnému záujmu podľa čl. 6 ods. 1 písm. e) GDPR;

- predstavuje spracúvanie na účely priameho marketingu bez ohľadu na právny základ;

vrátane profilovania vo všetkých prípadoch.

Oprávnený záujem.Ak námietka smeruje voči oprávnenému záujmu ako právnemu základu, Osoba zodpovedná za žiadosť v odpovedi poskytne a vysvetlí závery z tzv. testu proporcionality (*legitimate interest assessment alebo „LIA test“)*. Dotknutej osobe nie je nevyhnutné potrebné poskytovať celý LIA test ale len závery z neho v zrozumiteľnej a ľahko čitateľnej podobe vysvetľujúce oprávnené dôvody na také spracúvanie, ktoré prevažujú nad záujmami, právami a slobodami dotknutej osoby alebo dôvody na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov.

Priamy marketing. Pri námietke proti priamemu marketingu nie je možnosť preukazovať oprávnené dôvody na také spracúvanie. Odpoveď je v každom prípade pre dotknutú osobu pozitívna, tzn. z odpovede musí vyplývať, že DRE na základe námietky prestáva spracúvať osobné údaje o danej dotknutej osoby na účely týkajúce sa priameho marketingu.

§ 10

DOBA UCHOVÁVANIA OSOBNÝCH ÚDAJOV

(1) V súlade so zásadou minimalizácie uchovávania osobných údajov DRE spracúva osobné údaje na identifikované účely spracúvania osobných údajov najdlhšie počas všeobecnej doby uchovávania, ktorá je stanovená v tejto tabuľke:

	Účel	Všeobecná doba uchovávania
1	Personalistika a mzdy	Počas trvania pracovného, alebo obdobného pomeru.
2	Zmluvy	10 rokov
3	Súdne spory	Počas trvania súdneho alebo mimosúdneho konania.
4	Účtovné doklady	10 rokov

(2) Vyššie uvedené doby uchovávania predstavujú len všeobecnú dobu uchovávania osobných údajov. Nič v tejto internej politike nebráni uchovávať osobné údaje kratšie ako je vymedzená všeobecná doba uchovávania, ak osobné údaje už nie sú potrebné pre účely, na ktoré sa spracúvajú. Po uplynutí všeobecnej doby uchovávania je možné osobné údaje nachádzajúce sa v registratúrnych záznamoch ďalej uchovávať na archívne účely počas doby uloženia až do vyradenia daných záznamov.

§ 11

ŠPECIFICKY NAVRHNUTÁ A ŠTANDARDNÁ OCHRANA OSOBNÝCH ÚDAJOV

(1) DRE dodržiava základné princípy špecificky navrhnutej a štandardnej ochrany osobných údajov v zmysle čl. 25 GDPR.[3] Medzi všeobecné princípy špecificky navrhnutej ochrany osobných údajov patrí:

- Proaktívny a nie reaktívny prístup k ochrane súkromia;
- Ochrana súkromia je štandardným nastavením IT systémov;
- Ochrana súkromia je štandardným nastavením dizajnovania dátovej architektúry;
- Plná funkcionalita, ktorá umožňuje rešpektovanie súkromia na jednej strane a zároveň bezpečnosť a oprávnené záujmy iných osôb na druhej strane;
- Bezpečnosť dát naprieč ich celým životným cyklom v organizácii (*end-to-end security*);
- Transparentnosť a otvorenosť najmä vo vzťahu k vykonávaným spracovateľským operáciám;
- Jednoduchosť ovládania a centrálne postavenie dotknutej osoby v ochrane súkromia.

(2) Vyššie uvedené všeobecné princípy špecificky navrhnutej ochrany súkromia sú povinné dodržiavať všetky osoby, ktoré v rámci VB dochádzajú do styku s osobnými údajmi alebo ktorých rozhodnutia môžu mať dopad na súkromie fyzických osôb. Týmito princípmi je potrebné sa zaoberať vždy, ak relevantný personál položí základnú otázku uvedenú nižšie.

(3) Základná otázka špecificky navrhnutej ochrany súkromia znie: ***„Aký to bude mať dopad na ochranu súkromia?“***Túto otázku je povinný sa opýtať každý zamestnanec vrátane zodpovednej osoby, ak akýkoľvek nový proces, rozhodnutie alebo projekt v rámci organizácie môže mať dopad na ochranu súkromia resp. ochranu osobných údajov. Ak je táto otázka položená, je povinnosťou najvyššie postaveného personálu zahrnutého do daného procesu, rozhodnutia alebo projektu zohľadniť všeobecné zásady ochrany súkromia a danú otázku a zohľadnenie princípov dostatočne zdokumentovať (napr. v zápisnici zo stretnutia).

---

[3] *„**Špecificky navrhnutá a štandardná ochrana údajov***

1. 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. 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.*

3. Schválený certifikačný mechanizmus podľa článku 42 sa môže použiť ako prvok na preukázanie súladu s požiadavkami uvedenými v odsekoch 1 a 2 tohto článku.“

§ 12

INTERNÁ KONTROLNÁ ČINNOSŤ (INTERNÝ AUDIT)

(1) Kontrolnú činnosť podľa tejto internej politiky ochrany osobných údajov vykonáva DPO

(2) DPO vykonáva kontrolnú činnosť zameranú na dodržiavanie prijatých bezpečnostných a právnych opatrení určených na dosahovanie súladu s GDPR formou interného auditu, ktorý je zameraný najmä na previerku faktickej funkčnosti, spoľahlivosti a aktuálnosti prijatých bezpečnostných opatrení a ich praktického dodržiavania zo strany jednotlivých oprávnených príjemcov osobných údajov, ako aj na ich efektívnosť z hľadiska najnovších poznatkov z oblasti ochrany osobných údajov a kyber-bezpečnosti. DPO rovnako pri výkone auditu kladie dôraz na preverovanie dodržiavania všetkých základných zásad spracúvania osobných údajov.

(3) DPO je pri výkone interného právneho auditu povinný preveriť aj:

- nevyhnutnosť spracúvaného rozsahu osobných údajov pre dosahovanie konkrétnych účelov spracúvania;
- správnosť a aktuálnosť spracúvaných osobných údajov;
- vhodnosť výberu, transparentnosť a ďalšie podmienky (napr. článok 7 GDPR pre vyjadrenie súhlasu) všetkých právnych základov;
- dodržiavanie princípu obmedzenia účelu spracúvania osobných údajov vo vzťahu k spracovateľským operáciám, ktoré sú vykonávané s osobnými údajmi;
- aktuálnosť, správnosť a dostatočnú transparentnosť informácii povinne poskytovaných dotknutým osobám podľa článku 13 a 14 GDPR v rámci Podmienok ochrany súkromia;
- dodržiavanie princípov štandardnej a špecifickej ochrany osobných údajov v zmysle tejto politiky ochrany osobných údajov;
- dodržiavanie preverovania dodávateľov a sprostredkovateľov v zmysle tejto politiky ochrany osobných údajov;
- faktickú existenciu alebo neexistenciu cezhraničných prenosov do tretej krajiny nezaručujúcej primeranú úroveň ochrany osobných údajov a prípadne aj prijatie alebo neprijatie osobitných právnych záruk podľa článku 46 GDPR alebo aplikáciu výnimky pre osobitné situácie podľa článku 49 GDPR.

§ 13

POLITIKA OZNAMOVANIA BEZPEČNOSTNÝCH INCIDENTOV

Rozdelenie úloh a zodpovednosti

(1) VB vyvíja všestranné úsilie na predchádzanie vzniku haváriám, poruchám a iným mimoriadnym udalostiam s charakterom bezpečnostného incidentu bez ohľadu na to, či daný bezpečnostný incident má povahu porušenia ochrany osobných údajov alebo nie. Táto časť internej politiky preto pristupuje jednotne k bezpečnostným incidentom

ako takým, bez ohľadu na to, či ide o porušenie ochrany osobných údajov alebo nie, pokiaľ sa v nej neuvádza inak.

Dokumentácia bezpečnostného incidentu

(2) V prípade bezpečnostného incidentu bezodkladne po odstránení alebo maximálnom možnom zmiernení jeho negatívnych následkov sa vykoná:

a. analýza a identifikácia príčiny bezpečnostného incidentu;

b. písomná dokumentácia bezpečnostného incidentu, vrátane zhromažďovania auditných záznamov a podobných dôkazov, v ktorej sa popíše najmä priebeh bezpečnostného incidentu, následky v rovine dopadov na funkčnosť, spoľahlivosť alebo integritu spracúvaných osobných údajov a nadväzné protiopatrenia prijaté na odstránenie alebo zmiernenie dopadov bezpečnostného incidentu;

c. Extrakcia kópie relevantných dát, ktoré obsahujú logovacie záznamy kľúčové pre možné objasnenie a vyšetrenie bezpečnostného incidentu, ak je to možné.

(3) Za dokumentáciu bezpečnostného incidentu zodpovedá DPO.

(4) Vzorová dokumentácia bezpečnostného incidentu, ktorú je povinný vyhotoviť DPO a ktorá je súčasťou Spisu je uvedená v prílohe č. 1 tejto internej smernice.

Oznámenie bezpečnostného incidentu

(5) O oznámení bezpečnostného incidentu s charakterom porušenia ochrany osobných údajov rozhoduje a oznámenie vykonáva DPO.

(6) Porušenie ochrany osobných údajov, ktoré pravdepodobne povedie k vzniku rizík pre práva a slobody dotknutých osôb oznamuje DPO Úradu, pričom sa usiluje vždy stihnúť 72 hodinovú lehotu určenú na splnenie tejto povinnosti. Ak by nebolo možné v rámci 72 hodín od detekcie kvalifikovane zistiť všetky informácie podľa článku 33 ods. 3 GDPR DPO informuje Úrad v rámci 72 hodinovej lehoty o dostupných informáciách. V rozsahu, v akom nie je možné poskytnúť informácie súčasne poskytne DPO ďalšie doplňujúce informácie vo viacerých etapách bez ďalšieho zbytočného odkladu ihneď ako ich získa.

(7) Porušenia ochrany osobných údajov môžu byť oznamované Úradu oficiálne vytvoreným mechanizmom, ktorý je dostupný na webovom sídle Úradu URL: https://dataprotection.gov.sk/uoou/dp/dp-breach

(8) V prípade nedostupnosti vyššie uvedeného oznamovacieho mechanizmu (napr. obmedzenie dostupnosti webového sídla Úradu) DPO zabezpečí alternatívne splnenie oznamovacej povinnosti podľa článku 33 ods. 1 GDPR prostredníctvom jednotného informačného systému kybernetickej bezpečnosti, ktorý prevádzkuje Národný bezpečnostný úrad.

(9) Pri posudzovaní pravdepodobnosti vzniku rizika pre práva a slobody dotknutých osôb Prevádzkovateľ zvažuje najmä pravdepodobnosť vzniku:

- ujmy na zdraví alebo živote dotknutých osôb,

- majetkovej alebo nemajetkovej ujmy dotknutej osoby, a to najmä ak spracúvanie môže viesť k diskriminácii, krádeži totožnosti alebo podvodu, finančnej strate, poškodeniu dobrého mena, strate dôvernosti osobných údajov chránených profesijným tajomstvom, neoprávnenej reverznej pseudonymizácii alebo akémukoľvek inému závažnému hospodárskemu alebo sociálnemu znevýhodneniu či diskriminácii dotknutej osoby;
- špecifických rizík pre práva a slobody hodnotené v posúdení vplyvu na ochranu osobných údajov, ak bezpečnostný incident zasiahol spracúvanie osobných údajov, ktoré podliehalo povinnosti vykonať posúdenie vplyvu podľa článku 35 GDPR.
- či došlo k ohrozeniu alebo kompromitácii osobitnej kategórie osobných údajov (tzv. citlivé údaje);
- či došlo k ohrozeniu alebo kompromitácii osobných údajov jednotlivca, skupiny jednotlivcov, väčšieho datasetu údajov obsahujúcich značné množstvo osobných údajov jednotlivcov alebo všetkých osobných údajov, ktoré sú predmetom spracúvania;
- či došlo k ohrozeniu alebo kompromitácii osobných údajov detí a/alebo iných zraniteľnejších okruhov dotknutých osôb (zamestnanci, ZŤP, maloletí, dôchodcovia, a pod.).

(10) Na základe vyššie uvedeného DPO vyhodnotí úroveň rizika bezpečnostného incidentu s charakterom porušenia ochrany osobných údajov jednou z nasledovných možností:

Úroveň rizika	**Potrebné kroky**
nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb	Neoznamuje sa, dokumentuje sa.
je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb	Oznamuje sa Úradu, dokumentuje sa.
pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb	Oznamuje sa Úradu a dotknutým osobám, dokumentuje sa.

(11)V prípade, ak by povaha porušenia osobných údajov, resp. bezpečnostný incident mal charakter, ktorý môže viesť k vzniku rizika pre práva dotknutých osôb Prevádzkovateľ zabezpečí v oznámení Úradu uvedie:

- 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;

- meno/názov a kontaktné údaje DPO alebo iného kontaktného miesta, kde možno získať viac informácií o porušení ochrany osobných údajov, ktorá je predmetom oznámenia;
- opis pravdepodobných následkov porušenia ochrany osobných údajov;
- opis opatrení prijatých alebo navrhovaných DPO s cieľom napraviť porušenie ochrany osobných údajov vrátane, opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov.

(12) Ak DPO pri hodnotení rizika pre práva a slobody dotknutých osôb dospeje k záveru, že porušenie ochrany údajov vyvolalo vysoké riziko zabezpečí okrem oznámenia bezpečnostného incidentu Úradu aj informovanie každej dotknutej osoby, ktorej osobné údaje boli ohrozené alebo porušené v dôsledku porušenia ochrany údajov spôsobenej bezpečnostným incidentom.

(13) Informovanie dotknutej osoby o porušení ochrany osobných údajov sa usiluje DPO dosiahnuť primárne prostredníctvom elektronickej pošty, sms alebo telefonátom. Ak by neexistovala účinná a uskutočniteľná možnosť ako zabezpečiť informovanie dotknutej osoby, alebo by si to vyžadovalo neprimerané úsilie a náklady (napr. rozosielanie veľmi veľkého počtu poštových zásielok), DPO zváži alternatívnu a účinnú formu informovania dotknutých osôb o porušení ochrany údajov (napr. na svojom webe, medializácia, zapojením sprostredkovateľov apod.).

(14) Okolnosťami, ktoré môžu prispieť k záveru, že porušenie ochrany osobných údajov pravdepodobne nepovedie k rizikám pre práva a slobody môže byť napr.:

- ak by sa podarilo osobné údaje, ktoré sú dotknuté zisteným porušením ochrany údajov zašifrovať tak, že kompromitované osobné údaje sú nečitateľné pre všetky osoby, ktoré nie sú oprávnené mať k nim prístup a použitý prostriedok šifrovacej ochrany informácii je s ohľadom na aktuálny stav poznania spoľahlivým nástrojom pre zabezpečenie dôvernosti dát;
- ak by sa podarilo aplikovať iné následné bezpečnostné a iné následné zmierňovacie opatrenia, ktoré účinne znížia vysoké riziko pre práva a slobody dotknutých osôb, tak že už nebude mať na dotknuté osoby žiadne dôsledky (napr. diaľkové vymazanie strateného notebooku, ktorého pevný disk bol zašifrovaný apod.).

§ 14

ZODPOVEDNOSŤ ZA PORUŠENIE POLITIKY OCHRANY OSOBNÝCH ÚDAJOV

(1) Zavinené porušenie povinnosti ustanovenej osobe, ktorá je v pracovnom alebo inom obdobnom pomere s VB môže byť posúdené ako:

- porušenie pracovnej disciplíny;
- v obzvlášť závažných prípadoch ako závažné porušenie pracovnej disciplíny;
- porušenie zmluvnej povinnosti a môže zakladať zmluvnú zodpovednosť podľa individuálne dohodnutých zmluvných podmienok.

(2) Dôsledkom uplatnenia zodpovednosti vyvodenej v intenciách vyššie uvedeného môže byť ukončenie pracovného alebo obdobného pomeru, uplatňovanie hmotnej zodpovednosti, vyžadovanie nároku na náhradu škody a uplatňovanie iných nárokov spravujúcich sa individuálnymi zmluvnými dojednaniami upravenými konkrétnym zmluvným vzťahom založeným medzi fyzickou osobou povinnou na určité konania upravené v tejto politike ochrany osobných údajov a VB.

§ 15

ZÁVEREČNÉ USTANOVENIA

(1) Táto interná politika sa nezverejňuje, avšak musí byť sprístupnená a kedykoľvek dostupná personálu VB.

(2) Akýkoľvek odkaz na ustanovenie GDPR v tejto internej politike znamená automaticky aj odkaz na príslušné ustanovenie Zákona o ochrane osobných údajov, ak z kontextu daného spracúvania osobných údajov vyplýva alebo neskôr vyplynie, že sa riadi Zákonom o ochrane osobných údajov a nie GDPR.

(3) VB vyškolí na dodržiavanie tejto internej politiky relevantný personál.

(4) Táto interná politika nadobúda účinnosť dňa 25.8.2018.

V Liptovskom Mikuláši

Dňa 25.5.2018

Príloha č. 1
Vzorový formulár na zdokumentovanie porušenia ochrany osobných údajov

Tento záznam o porušení ochrany osobných údajov bol vypracovaný v súlade s čl. 33 ods. 5 GDPR[4] a slúži na zdokumentovanie porušenia a evidenciu o prijatých bezpečnostných opatreniach a postupoch na zmiernenie rizika pre práva a slobody pre fyzické osoby (ďalej len ako „**Záznam**“).

---

[4] Čl. 33 ods. 5 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.“*

Villa Betula KLUB
Brnice 166
032 21 Liptovská Sielnica
(ďalej len ako „**Prevádzkovateľ**“)

Keďže:

(A) V zmysle čl. 4 bod 12 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* (ďalej len „**Porušenie**“).

(B) V zmysle čl. 33 ods. 5 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.*“

Prevádzkovateľ sa rozhodol zdokumentovať Porušenie nasledovne:

1.	**Dátum, miesto a čas zistenia Porušenia a jeho interné označenie:**	*/uvedie sa dátum, miesto a presný čas zistenia Porušenia, odporúča sa číslovať záznamy o Porušení alebo inak označovať/*
2.	**Kontaktné údaje zodpovednej osoby ak je vymenovaná:**	*/uvedie sa titul, meno, priezvisko, email a telefónne číslo zodpovednej osoby, ako bola vymenovaná/*
3.	**Kontaktné údaje na iné osoby disponujúce dôležitými poznatkami o Porušení:**	*/napr. interný zamestnanec, ktorý zistil alebo oznámil DPOovi Porušenie/*
4.	**Základný opis Porušenia:**	*/DPO vlastnými slovami opíše čo sa stalo/*

5.	**Spôsob zistenia Porušenia:**	*/napr. chýbajúce dokumenty alebo súbory, prijatie automatickej notifikácie z bezpečnostného softvéru, notifikácia neobvyklých javov v sieťovej činnosti, notifikácia analýzy logovacích údajov, hlásenie zamestnanca, hlásenie IT poradcu, oznámenie od sprostredkovateľa, činnosť zodpovednej osoby, medializácia, prijatie podozrivej elektronickej pošty, prijatie žiadosti kyber zločinca pri ransomvérovom útoku, výpadok funkcií online služieb v dôsledku Ddos útoku, poznatky získané v dôsledku aplikácie kontrolných mechanizmov zamestnávateľa voči zamestnancom a pod./*
7.	**Popis povahy Porušenia:**	*/charakterizuje sa konkrétna udalosť, ktorá bola zistená a ktorá má potenciál ohroziť alebo porušiť integritu, dôvernosť, či dostupnosť dát, ktoré obsahujú osobné údaje. Rovnako sa vždy presne charakterizuje udalosť, ktorá viedla k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov alebo neoprávnenému prístupu k dátam obsahujúcich osobné údaje. Zároveň sa uvedie okruh dotknutých osôb zasiahnutých Bezpečnostným incidentom a ich (približný) počet, zoznam potenciálne kompromitovaných osobných údajov, ktorý je predmetom spracúvania a kvantifikácia počtu ohrozených alebo porušených dát (napr. počtom záznamov a veľkosťou dát v MB, GB, TB)./*
8.	**Identifikácia prijatých bezpečnostných opatrení, ktoré boli určené na prevenciu pred vznikom Porušenia:**	*/ uvedú sa bezpečnostné opatrenia a postupy, ktoré boli v zmysle interných politík, smerníc alebo bezpečnostných projektov určené na ochranu pred vznikom zisteného Porušenia/*

9.	**Pravdepodobné príčiny vzniku Porušenia:**	*/v prípade Porušenia s reálnym vplyvom na vznik rizika a/alebo vysokého rizika pre práva a slobody dotknutých osôb sa interné vyšetrovanie a kontrolná činnosť Spoločnosti zameria aj na identifikáciu príčin vzniku Porušenia, pričom sa popíšu všetky relevantné skutočnosti, ktoré mali vplyv na vznik, priebeh a dopady zisteného Porušenia/* */tiež sa odporúča uviesť chronologický opis priebehu incidentu, opis hrozieb, ktoré sa realizovali, identifikáciu zraniteľností, ktoré boli využité a spôsob akým to celé prebehlo, ďalej sa odporúča tiež uviesť zoznam dotknutých aktív, ktoré boli zasiahnuté Porušením, identifikovať a vymedziť prekonané bezpečnostné opatrenia, ak Porušenie vzniklo aj napriek prijatiu adekvátneho bezpečnostého opatrenia a uviesť predpokladaný dôvod prekonania takéhoto bezpečnostného opatrenia/* */tiež sa odporúča uviesť záznam o tom, ktoré konkrétne bezpečnostné opatrenia alebo postupy prijaté boli porušené, ak je medzi vznikom Porušenia a porušením príčinná súvislosť ako aj pokúsiť sa identifikovať osobu alebo osoby zodpovedné za porušenie povinnosti a interných pravidiel a s tým súvisiaci vznik Porušenia/*
10.	**Vzťah Porušenia a zostatkového rizika pre práva a slobody fyzických osôb:**	*/osobitne sa posúdi povaha Porušenia vo vzťahu k zostatkovým rizikám a nepokrytým rizikám, ktoré DPO zdokumentovala napr. vo svojom bezpečnostnom projekte podľa predchádzajúcej legislatívy/*
11.	**Opis pravdepodobných následkov Porušenia:**	*/popíšu sa zistené a pravdepodobné negatívne dopady Porušenia nie len na aktíva, ale aj napr. na povinnosť zachovávať mlčanlivosť, na osoby ktorých sa inkriminované osobné údaje týkali, na oprávnené záujmy klienta/*
12.	**Opis opatrení prijatých alebo navrhovaných s cieľom napraviť Porušenie:**	*/uvedú sa všetky úkony, ktoré boli vykonané alebo ktoré sa navrhujú vykonať v konkrétnych termínoch konkrétnymi poverencami s cieľom napraviť Porušenie /*
13.	**Opis opatrení určených na zmiernenie nepriaznivých dôsledkov Porušenia:**	*/DPO uvedie všetky úkony, ktoré boli vykonané alebo ktoré sa navrhujú vykonať v konkrétnych termínoch, konkrétnymi poverencami s cieľom zmierniť nepriaznivé dôsledky Porušenia/*

14.	**Navrhované doplnenie bezpečnostných opatrení:**	*/DPO zdokumentuje aké opatrenia sa prijali na predchádzanie obdobným incidentom ako je Porušenie v budúcnosti./*
15.	**Posúdenie vzniku povinnosti oznámiť Porušenie Úradu na ochranu osobných údajov podľa článku 33 GDPR:**	*/DPO odpovedá na otázku: je pravdepodobné, že Porušenie povedie k riziku pre práva a slobody fyzických osôb? DPO uvedenie zdôvodnenie odpovede. /*
16.	**Posúdenie vzniku povinnosti oznámiť Porušenie dotknutej osobe podľa článku 34 GDPR:**	*/DPO odpovedá na otázku: je pravdepodobné, že Porušenie povedie k vysokému riziku pre práva a slobody fyzických osôb spolu so zdôvodnení. /*
17.	**Dátum a čas oznámenia Porušenia Úradu na ochranu osobných údajov:**	*/uvedie sa presný dátum a čas oznámenia a priloží sa písomný dôkaz o vykonaní tohto úkonu - vypĺňa sa iba v prípade pozitívneho záveru o oznámení/*
18.	**Dôvody zmeškania lehoty na oznámenie Porušenia Úradu na ochranu osobných údajov:**	*/odôvodnenie pre nedodržanie predmetnej lehoty 72 hodín (3 dní) – vypĺňa sa iba v prípade pozitívneho záveru o oznámení a zmeškaní lehoty/*
19.	**Dátum, čas a spôsobom oznámenia Porušenia dotknutým osobám**	*/uvedie sa presný dátum a čas oznámenia ako aj spôsob oznámenia Porušenia vo vzťahu k dotknutým osobám./*
20.	**Vyjadrenie štatutárneho orgánu Prevádzkovateľa k Porušeniu a ďalšiemu postupu:**	*/štatutárny orgán sa vyjadrí k vyššie uvedenému obsahu a schváli ďalší postup (najmä rozhodnutie o oznámení / neoznámení Porušenia/*

Na základe vyššie uvedeného zdokumentovania Prevádzkovateľ prijal rozhodnutie:

□	neoznámiť Porušenie Úradu na ochranu osobných údajov SR podľa čl. 33 GDPR (v takom prípade sa Porušenie iba zdokumentuje týmto záznamom);	*„pretože Porušenie pravdepodobne* ***nepovedie k rizikám*** *pre práva a slobody fyzických osôb“*

□	oznámiť Porušenie Úradu na ochranu osobných údajov SR podľa čl. 33 GDPR (v takom prípade oznámenie porušenia sa priloží k tomuto záznamu).	*„pretože Porušenie pravdepodobne **povedie k rizikám** pre práva a slobody fyzických osôb“*
□	oznámiť Porušenie aj dotknutým osobám podľa čl. 34 GDPR	*„pretože Porušenie pravdepodobne **povedie k vysokým rizikám** pre práva a slobody fyzických osôb“*
□	neoznámiť Porušenie dotknutým osobám podľa čl. 34 GDPR	*„pretože Porušenie pravdepodobne **nepovedie k vysokým rizikám** pre práva a slobody fyzických osôb“*

Vypracoval:

Schválil:

Dňa:

Prílohy (ak sú relevantné):

- Kópia oznámenia Porušenia Úradu na ochranu osobných údajov;
- Kópia oznámenia Porušenia dotknutým osobám.