

Bezpečnostný projekt

Časť:

Bezpečnostná smernica na ochranu osobných údajov v IS prevádzkovaných v pôsobnosti Divadelného ústavu (aktualizácia k 1.9.2018)

Táto bezpečnostná smernica nadobúda platnosť dňom podpisu a účinnosť dňa 1. septembra 2018

Zhrnutie:

Bezpečnostná smernica na ochranu osobných údajov bola vypracovaná v zmysle čl. 25 všeobecného nariadenia o ochrane údajov EÚ č. 2016/679 (GDPR), pričom predstavuje nástroj, ktorým prevádzkovateľ zabezpečuje prijatie primeraných technických a organizačných opatrení na spracúvanie osobných údajov.

Schvaľujem:

Mgr. art. Vladislava FEKETE, ArtD.
riaditeľka
Divadelného ústavu

Autor:	doc. JUDr. Peter VARGA, PhD. Analytik Entry Net, s.r.o.	podpis :	_____	dátum :
Na vedomie	PhDr. Diana SELECKÁ Poverená zodpovedná osoba za Divadelný ústav	podpis :	_____	dátum :
	Poverené osoby	Poverenia o spracúvaní osobných údajov budú uložené u zodpovednej osoby		

© Entry Net, s. r. o.

Bezpečnostná smernica je autorským dielom spracovateľského kolektívu Entry Net, s.r.o. Bratislava (napr. § 16 a 17 zákona č. 185/2015 Z. z., Autorského zákona). Materiál, ani jeho časti nemôžu byť v zmysle platných zákonov použité v iných materiáloch ani odstúpené tretej osobe bez predchádzajúceho písomného súhlasu Entry Net, s.r.o. Bratislava.

Obsah

Výklad základných pojmov a používané skratky	6
1. Dôvod vypracovania Bezpečnostnej smernice	9
2. Podmienky a účel spracúvania osobných údajov	11
2.1 Prevádzkovateľ	11
2.1.1 Zriadenie	11
2.1.2 Pôsobnosť	12
2.1.3 Organizačná štruktúra	13
2.2 Sprostredkovatelia a dodávatelia	13
2.2.1 Ministerstvo kultúry Slovenskej republiky	13
2.2.2 Ďalšie spoločnosti	14
3. Prevádzkované informačné systémy	15
3.1 IS Personalistika a mzdy	15
3.1.1 Opis plánovaného spracúvania osobných údajov v IS Personalistika a mzdy	15
Personálna agenda	15
Mzdová agenda	17
3.1.2 Posúdenie nevyhnutnosti a primeranosti	22
3.1.3 Posúdenie rizika pre práva fyzických osôb v IS Personalistika a mzdy	27
3.1.4 Monitorovanie a preskúmanie podmienok spracúvania osobných údajov v IS Personalistika a mzdy	27
3.2 IS Účtovníctvo	27
3.2.1 Opis plánovaného spracúvania osobných údajov v IS Účtovníctvo	27
3.2.2 Posúdenie nevyhnutnosti a primeranosti	29
3.2.3 Posúdenie rizika pre práva fyzickej osoby v IS Účtovníctvo	30
3.2.4 Monitorovanie a preskúmanie podmienok spracúvania osobných údajov v IS Účtovníctvo 30	30
3.3 IS Zmluvy	30
3.3.1 Opis plánovaného spracúvania osobných údajov v IS Zmluvy	30
3.3.2 Posúdenie nevyhnutnosti a primeranosti	31
3.3.3 Posúdenie rizika pre práva fyzickej osoby v IS Zmluvy	33
3.3.4 Monitorovanie a preskúmanie podmienok spracúvania osobných údajov v IS Zmluvy	33
3.4 IS Registratúra	33
3.4.1 Opis plánovaného spracúvania osobných údajov v IS Registratúra	33
3.4.2 Posúdenie nevyhnutnosti a primeranosti	34
3.4.3 Posúdenie rizika pre práva fyzickej osoby v IS Registratúra	35
3.4.4 Monitorovanie a preskúmanie podmienok spracúvania osobných údajov v IS Registratúra 36	36
3.5 IS Archív DÚ	36
3.5.1 Opis plánovaného spracúvania osobných údajov v IS	36
3.5.2 Posúdenie nevyhnutnosti a primeranosti	37
3.5.3 Posúdenie rizika pre práva fyzickej osoby v IS	38
3.5.4 Monitorovanie a preskúmanie podmienok spracúvania osobných údajov v IS	38
3.6 IS Knižnica	39
3.6.1 Opis plánovaného spracúvania osobných údajov v IS Knižnica	39
3.6.2 Posúdenie nevyhnutnosti a primeranosti	40
3.6.3 Posúdenie rizika pre práva fyzických osôb v IS	41
3.6.4 Monitorovanie a preskúmanie podmienok spracúvania osobných údajov v IS	41
3.7 IS THEATRE.SK	42
3.7.1 Opis plánovaného spracúvania osobných údajov	42
3.7.2 Posúdenie nevyhnutnosti a primeranosti	44

3.7.3	Posúdenie rizika pre práva fyzickej osoby.....	45
3.7.4	Monitorovanie a preskúmanie podmienok spracúvania osobných údajov	45
3.8	IS Kamerový systém	45
3.8.1	Opis plánovaného spracúvania osobných údajov	45
3.8.2	Posúdenie nevyhnutnosti a primeranosti.....	47
3.8.3	Posúdenie rizika pre práva fyzickej osoby.....	48
3.8.4	Monitorovanie a preskúmanie podmienok spracúvania osobných údajov v IS Evidencia návštev.....	49
3.9	IS Podnety.....	49
3.9.1	Opis plánovaného spracúvania osobných údajov v IS Podnety.....	49
3.9.2	Posúdenie nevyhnutnosti a primeranosti.....	50
3.9.3	Posúdenie rizika pre práva fyzickej osoby v IS Podnety	51
3.9.4	Monitorovanie a preskúmanie podmienok spracúvania osobných údajov v IS Podnety.....	51
3.10	IS Sťažnosti.....	51
3.10.1	Opis plánovaného spracúvania osobných údajov v IS Sťažnosti	51
3.10.2	Posúdenie nevyhnutnosti a primeranosti.....	52
3.10.3	Posúdenie rizika pre práva fyzickej osoby v IS Sťažnosti.....	53
3.10.4	Monitorovanie a preskúmanie podmienok spracúvania osobných údajov v IS Sťažnosti	53
3.11	IS Žiadosti podľa infozákona.....	53
3.11.1	Opis plánovaného spracúvania osobných údajov v IS Žiadosti podľa infozákona	53
3.11.2	Posúdenie nevyhnutnosti a primeranosti.....	55
3.11.3	Posúdenie rizika pre práva fyzickej osoby v IS Žiadosti podľa infozákona.....	56
3.11.4	Monitorovanie a preskúmanie podmienok spracúvania osobných údajov v IS Žiadosti podľa infozákona.....	56
3.12	Automatizované spracúvanie prostredníctvom CJES	56
3.12.1	Charakteristika softvéru SOFTIP PROFIT	57
3.12.2	Popis aplikačného prostredia CJES.....	58
3.12.3	Popis databázového prostredia CJES.....	59
3.12.4	Postup a podmienky prístupu do CJES.....	59
3.12.5	Poverená osoba za CJES	60
3.12.6	Určenie poverenej oprávnenej osoby CJES	60
3.12.7	Vytvorenie prístupu do CJES.....	60
3.12.8	Postupy pri poruchových stavoch CJES	61
3.13	Automatizované spracúvanie prostredníctvom NUNTIO ASSR.....	61
3.13.1	Charakteristika elektronického informačného systému NUNTIO ASSR.....	61
3.13.2	Správa registratúry	62
3.13.3	Funkčné vlastnosti NUNTIO ASSR	63
3.13.4	Prínosy riešenia NUNTIO ASSR.....	63
3.13.5	Postup a podmienky prístupu do NUNTIO ASSR.....	64
4.	Podmienky spracúvania osobných údajov	65
5.	Dohľad nad ochranou osobných údajov	67
5.1	Zodpovedná osoba – práva a povinnosti.....	68
6.	Poverenie a povinnosti oprávnenej osoby	69
6.1	Poverenie oprávnenej osoby a spôsob jej poučenia	69
6.2	Práva poverenej osoby	70
6.3	Povinnosti poverenej osoby:	71
6.3.1	Povinnosti poverenej osoby vo vzťahu ku kontrole.....	72
6.4	Zodpovednosť za porušenie práv a povinností	73
6.4.1	Zodpovednosť poverenej osoby za porušenie povinností.....	73
6.4.2	Trestná zodpovednosť poverenej osoby a Prevádzkovateľa.....	73

7. Zásady spracúvania osobných údajov a zákonnosť ich spracúvania.....	75
8. Získavanie osobných údajov.....	79
9. Poskytovanie, sprístupňovanie a zverejňovanie osobných údajov	83
10. Likvidácia osobných údajov a nakladanie s osobnými údajmi po splnení účelu spracúvania, obmedzenie spracúvania	85
11. Prístup k osobným údajom.....	87
12. Sprostredkovateľ	88
13. Ochrana práv dotknutých osôb.....	90
13.1 Práva dotknutých osôb	90
13.2 Oznámenie porušenia práv dotknutých osôb	91
14. Vybavovanie žiadostí dotknutých osôb	93
15. Bezpečnosť osobných údajov pri ich spracúvaní	94
15.1 Posúdenie vplyvu na ochranu osobných údajov	94
15.2 Záznamy o spracovateľských činnostiach	95
15.3 Povinnosti pri spracúvaní osobných údajov v oblasti bezpečnosti	95
16. Cezhraničný prenos osobných údajov	98
16.1 Európska únia.....	98
16.2 Prenos osobných údajov mimo EÚ	98
17. Bezpečnostné opatrenia ochrany osobných údajov.....	100
17.1 Personálne opatrenia	100
17.2 Administratívne opatrenia.....	100
17.2.1 Postup Prevádzkovateľa IS	101
17.2.2 Prioritné úlohy Prevádzkovateľa IS	101
17.3 Opatrenia objektivej a fyzickej bezpečnosti	101
17.4 Technická opatrenia neautomatizovaných prostriedkov	102
17.4.1 Pravidlá používania neautomatizovaných prostriedkov	102
17.5 Technická bezpečnosť automatizovaných prostriedkov	103
17.5.1 Prevádzkovateľ a zodpovednosť za informačnú bezpečnosť.....	103
17.5.2 Funkcie v informačnom systéme	104
17.5.3 Správa infraštruktúry IT	105
17.5.4 Hardvér.....	105
17.5.5 Softvér.....	105
17.5.6 Správa používateľov	106
17.5.7 Identifikácia a autentizácia.....	106
17.5.8 Riadenie prístupu	108
17.5.9 Audit a účtovateľnosť	108
17.5.10 Opakované použitie.....	109
17.5.11 Manipulácia s médiami	109
17.5.12 Používanie elektronickej pošty	110
17.5.13 Používanie počítačovej siete	112
17.5.14 Používanie Internetu	112
17.5.15 Používanie mobilných počítačov a práca doma	113
17.5.16 Používanie ďalších komunikačných kanálov	113
17.5.17 Ochrana počítača počas neprítomnosti užívateľa	114
17.5.18 Depozit hesiel.....	114
17.5.19 Ochrana proti škodlivému kódu	114
17.5.20 Šifrovanie dát	115
17.5.21 Archivácia a zálohovanie	115

17.5.22	Obnova	116
17.5.23	Ochrana proti výpadkom napájania	116
17.5.24	Zodpovednosť používateľov	116
17.5.25	Bezpečnostné riziká v automatizovaných informačných systémoch	117
18.	Spôsob, forma a periodicita výkonu kontrolných činností	119
18.1	Druhy kontrolných mechanizmov	119
18.2	Kontrolný záznam	120
19.	Postupy pri haváriách, poruchách a iných mimoriadnych situáciách	121
19.1	Preventívne opatrenia	121
19.2	Havárie a poruchy	121
19.3	Bezpečnostné incidenty	122
19.3.1	Klasifikácia bezpečnostných incidentov a použitých riešení	122
19.3.2	Odstraňovanie následkov bezpečnostných incidentov	122
20.	Spolupráca s Úradom na ochranu osobných údajov SR	123
20.1	Postavenie Úradu na ochranu osobných údajov	123
21.	Záverečné a prechodné ustanovenia	124
22.	Niektoré zákony upravujúce účel a podmienky spracúvania osobných údajov	125
23.	Špecifikácia príloh	128
24.	Vyhotovovacia doložka	129

Výklad základných pojmov a používané skratky

Základný pojem	Výklad pojmu	Používaná skratka, poznámka, zdroj
Nariadenie 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 (všeobecné nariadenie o ochrane údajov)	Nariadenie 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	GDPR Ú.v. EÚ L 119 zo 4.5.2016, s. 1-88 https://eur-lex.europa.eu/homepage.html
Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov	Zákon upravuje ochranu práv fyzických osôb pred neoprávneným spracúvaním ich osobných údajov, práva, povinnosti a zodpovednosť pri spracúvaní osobných údajov fyzických osôb, postavenie, pôsobnosť a organizáciu Úradu na ochranu osobných údajov SR.	Zákon 18/2018 https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/18/20180525
Vyhláška Úradu na ochranu osobných údajov SR č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov	Vyhláška upravuje postup prevádzkovateľa pri posudzovaní vplyvu plánovaných spracovateľských operácií na ochranu osobných údajov.	Vyhláška 158/2018 https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/158/20180615
Bezpečnostné štandardy	Záväzné bezpečnostné požiadavky a kritériá na kvalitu, rýchlosť a bezpečnosť prenášaných dát, ktoré boli v Slovenskej republike prevzaté zákonným spôsobom alebo adaptované ako ISO norma.	Napr. zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy, Výnos Ministerstva financií Slovenskej republiky č. 55/2014 z 4. marca 2014 o štandardoch pre informačné systémy verejnej správy http://www.informatizacia.sk/standardy-is-vs/596s
Úrad na ochranu osobných údajov Slovenskej republiky	Orgán štátnej správy s celoslovenskou pôsobnosťou, ktorý sa podieľa na ochrane základných práv fyzických osôb pri spracúvaní osobných údajov a ktorý vykonáva dozor nad ochranou osobných údajov vrátane dozoru nad ochranou osobných údajov spracúvaných príslušnými orgánmi pri plnení úloh na účely trestného konania, ak nie je v § 81 ods. 7 a 8 ustanovené inak. Úrad je dozorným orgánom v zmysle GDPR.	Úrad § 80 až 84 Zákona Čl. 4 ods. 21 GDPR, čl. 51 GDPR http://www.dataprotection.gov.sk
Ochrana údajov (Bezpečnostný projekt)	Špecificky navrhnutá a štandardná ochrana osobných údajov, vrátane prijatia primeraných technických a organizačných opatrení.	Čl. 25 GDPR
Posúdenie vplyvu na ochranu údajov	Posúdenie vplyvu plánovaných spracovateľských operácií na ochranu osobných údajov, nevyhnutné vykonať v prípadoch, ak typ spracúvania, najmä s využitím nových technológií a s ohľadom na povahu, rozsah, kontext a účely spracúvania pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb.	ABIS § 5 ods. 3 Vyhlášky 164/2013
Záznamy o spracovateľských činnostiach	Opis spracovateľských operácií s osobnými údajmi	Čl. 30 GDPR
Bezpečnostná smernica	Bezpečnostná smernica upresňuje a aplikuje závery z posúdenia primeraných technických a organizačných opatrení, predstavuje interný akt prevádzkovateľa upravujúci povinnosti pri spracúvaní osobných údajov.	BS §4 Vyhlášky 164/2013
Osobné údaje	Akékolvek 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.	OÚ Čl. 4 ods. 1 GDPR
Osobitné kategórie osobných údajov	Osobné údaje, ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách,	Čl. 9 ods. 1 GDPR

Základný pojem	Výklad pojmu	Používaná skratka, poznámka, zdroj
	a spracúvanie genetických údajov, biometrických údajov na individuálnu identifikáciu fyzickej osoby, údaje týkajúce sa zdravia alebo údaje týkajúce sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby.	
Spracúvanie osobných údajov	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 poskytovaním iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami.	Čl. 4 ods. 2 GDPR
Informačný systém	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.	Čl. 4 ods. 6 GDPR
Profilovanie	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 poskytovaním iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami.	Čl. 4 ods. 4 GDPR
Pseudonymizácia	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.	Čl. 4 ods. 5 GDPR
Klasifikované informácie, údaje a informačné aktíva	Informácie a údaje, ktoré prevádzkovateľ informačného systému označil ako interne dôverné, chráni ich, ich strata, vyzradenie alebo zneužitie môže spôsobiť vážne materiálne alebo nemateriálne škody	KI
Informačný systém	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.	Čl. 4 ods. 6 GDPR
Centrálny jednotný ekonomický systém Softip Profit	Systém založený na technológii klient-server, ktorý tvoria aplikácie zabezpečujúce rýchle a pritom pohodlné riadenie ekonomických, personálnych, mzdových a logistických informácií.	CJES
Ministerstvo kultúry SR	Ministerstvo je ústredným orgánom štátnej správy SR pre štátny jazyk, ochranu pamiatkového fondu, kultúrne dedičstvo a knihovníctvo, umenie, autorské právo a práva súvisiace s autorským právom, osvetovú činnosť a ľudovú umeleckú výrobu, podporu kultúry národnostných menšín, prezentáciu slovenskej kultúry v zahraničí, vzťahy s cirkvami a náboženskými spoločnosťami, médiá a audiovizíu.	MK SR
Datacentrum Ministerstva kultúry SR	Centrum výpočtovej techniky MK SR, v ktorom sú prevádzkované centralizované informačné systémy rezortu kultúry.	Datacentrum
Virtuálna privátna sieť MK SR	VPN (Virtual Private Network) postavená na báze sieťového protokolu MPLS (Multiprotocol Labels Switching), ktorý podporuje aktuálne požiadavky na kvalitu, rýchlosť a bezpečnosť prenášaných dát.	VPN MPLS MK SR
Základné riadiace dokumenty pre oblasť ochrany elektronických informácií MK SR	Základnými riadiacimi dokumentmi v podmienkach a pôsobnosti rezortu kultúry sú Celková bezpečnostná politika MK SR a metodické pokyny na jej aplikáciu u Organizácií, Prevádzkový poriadok VPN MPLS MK SR, Prevádzkový poriadok CJES.	RD MK SR
Organizácia v zriaďovateľskej pôsobnosti MK SR	Organizácia, ktorá v zmysle stanovenej pôsobnosti, s prihliadnutím k osobitným zákonom a v zmysle	Organizácia MK SR alebo iba Organizácia, v skratke O MK SR

Základný pojem	Výklad pojmu	Používaná skratka, poznámka, zdroj
	zriaďovacej listiny vydané MK SR realizuje predmet svojej činnosti.	
Účel spracúvania	Vopred jednoznačne vymedzený alebo ustanovený zámer spracúvania osobných údajov, ktorý sa viaže na určitú činnosť.	
Súhlas dotknutej osoby	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.	Čl. 4 ods. 11 GDPR
Prevádzkovateľ	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 EÚ alebo v práve členského štátu EÚ, možno prevádzkovateľa alebo konkrétne kritériá na jeho určenie určiť v práve EÚ alebo v práve členského štátu EÚ.	Čl. 4 ods. 7 GDPR
Sprostredkovateľ	Fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa.	Čl. 4 ods. 8 GDPR
Príjemca	Fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorému sa osobné údaje poskytujú bez ohľadu na to, či je tretou stranou.	Čl. 4 ods. 9 GDPR
Tretia strana	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.	Čl. 4 ods. 10 GDPR
Poverená osoba	Každá osoba konajúca na základe poverenia prevádzkovateľa alebo sprostredkovateľa, ktorá má prístup k osobným údajom, pričom tieto môže spracúvať len na základe pokynov prevádzkovateľa s výnimkou prípadov, keď sa to vyžaduje podľa práva Únie alebo práva členského štátu.	Čl. 29 GDPR
Zodpovedná osoba	Osoba, ktorá plní úlohy v oblasti dohľadu nad ochranou osobných údajov, pričom má byť riadnym spôsobom a včas zapojená do všetkých záležitostí, ktoré súvisia s ochranou osobných údajov.	Čl. 37 – 39 GDPR
Dotknutá osoba	Každá fyzická osoba, ktorej sa osobné údaje týkajú.	
Práva dotknutej osoby	GDPR upravuje práva dotknutej osoby, najmä právo na informácie a prístup k osobným údajom, pričom tieto práva je možné v nevyhnutnej miere obmedziť iba na základe podmienok uvedených v právnych predpisoch.	Kapitola III GDPR
Porušenie ochrany osobných údajov	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.	Čl. 4 ods. 7 GDPR
Kultúrny objekt	Prírodniny alebo hnuťelné, nehnuteľné, hmotné alebo nehmotné ľudské výtvory, ich artefakty alebo súbory, ktoré sa vyznačujú kultúrnou významnosťou z hľadiska prehistórie, histórie, literatúry, umenia, techniky alebo prírodných a spoločenských vied a spĺňajú kritéria platnej legislatívy (týkajúce sa datovania, proveniencie, charakteru a výnimočnosti), predmety pamiatkového fondu	KO
Digitálny objekt	Digitálna entita obsahujúca údaje (digitálny dokument) a metadáta (popisné údaje, technické dáta)	DO
Digitálny dokument	Zdigitalizovaný kultúrny objekt alebo dokument získaný v digitálnej forme prostredníctvom trvalého prístupového práva.	DD

1. Dôvod vypracovania Bezpečnostnej smernice

1. Bezpečnostná smernica (ďalej len „Smernica“) bola vypracovaná za účelom zabezpečenia primeraných opatrení pre práva fyzických osôb pri spracúvaní osobných údajov a predstavuje záväzný akt pre osoby, ktoré nakladajú s osobnými údajmi pri výkone činností prevádzkovateľa.
2. Smernica predstavuje organizačné opatrenie v zmysle článku 24 ods. 1 Nariadenia GDPR, ktorým Prevádzkovateľ preukazuje, že spracúvanie osobných údajov vykonáva v súlade s nariadením GDPR, zákonom č. 18/2018 Z. z. o ochrane osobných údajov ako aj ďalšou relevantnou právnou úpravou vzťahujúcou sa na spracúvanie osobných údajov a ochranu osobnosti.
3. Základným cieľom aplikácie a následnej implementácie právnej úpravy na ochranu osobných údajov je určiť a implementovať integrované zásady ochrany osobných údajov v podmienkach organizácií v zriaďovateľskej pôsobnosti Ministerstva kultúry SR (ďalej len „Prevádzkovateľ“).
4. Pri vypracovaní Smernice boli využité najmä závery bezpečnostnej dokumentácie na ochranu osobných údajov Ministerstva kultúry SR (ďalej len „MK SR“) ako zriaďovateľa, Bezpečnostnej politiky informačných systémov v rezorte kultúry SR a súvisiacich metodík, Prevádzkového poriadku WAN VPN MK SR a Prevádzkového poriadku Centrálného jednotného ekonomického systému rezortu SOFTIP PROFIT.
5. Pri vypracovaní Smernice boli aplikované zákonným spôsobom prevzaté normy a štandardy na hodnotenie a riadenie bezpečnosti v automatizovaných IS a ostatná aplikovateľná legislatíva Európskej únie a Slovenskej republiky, platná v čase vypracovania a vydania tejto Smernice. Zoznam základnej aplikovateľnej legislatívy je uvedený v čl. 22 tejto Smernice.
6. Smernicami sa aplikujú závery vyplývajúce z analýz bezpečnosti IS, ktoré boli vykonané v jednotlivých miestach ich prevádzkovania u Prevádzkovateľa.
7. Smernica obsahuje najmä:
 - a.) popis prijatých technických, organizačných a personálnych opatrení a spôsob ich využitia v IS,
 - b.) rozsah oprávnení, zodpovednosti a popis povolených činností určených poverených osôb, spôsob ich identifikácie a autentifikácie pri prístupe k IS,
 - c.) rozsah zodpovednosti osôb poverených výkonom dohľadu nad dodržiavaním Zákona v IS,
 - d.) spôsob, formu a periodicitu výkonu kontrolných činností zameraných na držiavanie bezpečnosti v IS,
 - e.) postupy pri haváriách, poruchách a iných mimoriadnych situáciách vrátane preventívnych opatrení na zníženie vzniku mimoriadnych situácií a možnosti efektívnej obnovy stavu pred haváriou.
8. Smernica je výsledkom:
 - a.) Bezpečnostnej politiky informačných systémov v rezorte kultúry SR s požiadavkou jej operatívnej aplikácie do podmienok Prevádzkovateľa, upravených podmienok bezpečnostnej správy a administrácie automatizovaných informačných systémov,
 - b.) vykonanej rizikovej analýzy v prevádzkovaných IS Prevádzkovateľa a opatrení realizovaných na minimalizáciu, predchádzanie a zamedzovanie pôsobenia vyhodnotených bezpečnostných rizík

c.) prijatého bezpečnostného zámeru na splnenie minimálne požadovaných zákonných požiadaviek.

Smernica je neoddeliteľnou súčasťou bezpečnostnej dokumentácie na ochranu osobných údajov Prevádzkovateľa. Jej súčasťou sú aplikačné prílohy, šablóny a vzory písomností, ktorých podrobný zoznam je uvedený v čl. 23 tejto Smernice.

2. Podmienky a účel spracúvania osobných údajov

2.1 Prevádzkovateľ

Prevádzkovateľom v zmysle Zákona a zriaďovacej listiny je Divadelný ústav, štátna príspevková organizácia so sídlom Jakubovo námestie 12, 813 57 Bratislava, IČO: 00164691 (ďalej aj ako „DÚ“ alebo „Prevádzkovateľ“). Informačné systémy, ktoré sú predmetom Analýzy, sú prevádzkované v sídle Prevádzkovateľa.

Okrem všeobecných povinností prevádzkovateľa stanovených Zákonom plní Prevádzkovateľ v zmysle zriaďovacej listiny, predmetu vlastnej činnosti, pôsobnosti, prevádzkového poriadku WAN VPN MK SR a metodických pokynov na realizáciu celkovej bezpečnostnej politiky rezortu kultúry tieto špecifické úlohy:

- je povinný určiť svojho zástupcu (ďalej len „poverená osoba“), ktorý poskytuje súčinnosť poskytovateľovi a slúži ako kontaktná osoba pre poskytovateľa (spravidla ADM CJES, resp. vedúci ekonóm organizácie),
- nahlasuje poruchy CJES,
- poskytuje súčinnosť pri identifikácii zdroja poruchy a odstraňovaní porúch a výpadkov CJES poskytovateľovi podľa jeho pokynov,
- písomne nahlasuje požiadavky na zmeny a rozšírenia ním využívaných služieb alebo požiadavky na nové služby CJES,
- adresuje svoje sťažnosti a reklamácie súvisiace s kvalitou a poruchami služieb CJES určenému zástupcovi Ministerstva kultúry SR (ďalej len „MK SR“),
- poskytuje súčinnosť určenému zástupcovi MK SR pri zabezpečovaní činnosti spadajúcich do pôsobnosti CJES, zabezpečuje ochranu osobných údajov pri ich spracúvaní v CJES. V uvedenom smere s prihliadnutím k príslušným ustanoveniam Zákona, v zmysle prijatého bezpečnostného projektu na ochranu osobných údajov organizácie poveruje zodpovednú osobu za výkon dohľadu nad jeho dodržiavaním v pôsobnosti organizácie, určuje oprávnené osoby organizácie s prístupom k spracúvaným osobným údajom, dotknuté osoby organizácie, ktorých osobné údaje sú v CJES spracúvané v zákonnej lehote informuje o účele a ďalších podmienkach ich spracúvania.

2.1.1 Zriadenie

Prevádzkovateľ bol zriadený v zmysle kompetencií prislúchajúcich Ministerstvu kultúry Slovenskej republiky (ďalej len „MK SR“) podľa zákona NR SR č. 303/1995 Z. z. o rozpočtových pravidlách v znení neskorších predpisov (nahradený zákonom č. 523/2004 o rozpočtových pravidlách verejnej správy a o zmene a doplnení niektorých predpisov, v znení neskorších predpisov).

Prevádzkovateľ je štátna príspevková organizácia, ktorej zriaďovateľom je MK SR. Svojimi príjmami a výdavkami je zapojená na štátny rozpočet Slovenskej republiky prostredníctvom kapitoly MK SR, ktoré garantuje a kontroluje jej činnosť.

Prevádzkovateľ je vedecko-výskumnou, zbierkotvornou, kultúrno-vzdelávacou a informačno-prezentačnou inštitúciou s celoslovenskou pôsobnosťou v oblasti divadelnej kultúry na Slovensku. Bližšie vid' Rozhodnutie MK SR o vydaní zriaďovacej listiny Divadelného ústavu zo dňa 8. decembra 2014 vydané pod č. MK-3055/2014-110/20846.

2.1.2 Pôsobnosť

Divadelný ústav je zbierkotvornou, dokumentačnou, archivačnou, knižničnou, múzejnou vedecko-výskumnou, koncepčnou, edičnou, kultúrno-vzdelávacou, konzultačnou, informačno-prezentačnou a propagačnou inštitúciou s celoslovenskou pôsobnosťou v oblasti profesionálnej divadelnej kultúry na území Slovenskej republiky. Tieto činnosti vykonáva aj smerom do zahraničia.

Základným predmetom činnosti Divadelného ústavu je zhromažďovať, ochraňovať, odborne spracovávať a sprístupňovať dokumentačné, archívne, knižničné, audiovizuálne fondy a zbierky múzejnej a galerijnej hodnoty z oblasti profesionálnej divadelnej kultúry na území Slovenskej republiky, ktoré sú súčasťou národného kultúrneho dedičstva. Divadelný ústav plní úlohy Špecializovaného verejného archívu, Múzea Divadelného ústavu (RM 86/2006) a pracoviska s Akreditáciou o spôsobilosti vykonávať výskum a vývoj.

V rámci svojho predmetu činnosti plní predovšetkým tieto úlohy:

- a) nastoľuje umelecká tvorba a prax,
- b) systematicky zabezpečuje dokumentáciu v oblasti profesionálneho divadelného umenia v Slovenskej republike v celom druhovom a žánrovom zábere, zabezpečuje a koordinuje budovanie centrálnej databázy informácií o profesionálnej divadelnej kultúre v Slovenskej republike v rámci informačného systému THEATRE.SK,
- c) vyžaduje ako poverená osoba vybrané informácie v rozsahu ustanovenom v § 1 vyhlášky Ministerstva kultúry Slovenskej republiky č. 230/2014 Z. z. o rozsahu vybraných informácií požadovaných od divadiel a hudobných inštitúcií, ktorou sa vykonáva zákon č. 103/2014 Z. z. o divadelnej činnosti a hudobnej činnosti a o zmene a doplnení niektorých zákonov,
- d) dokumentuje existenciu a prezentáciu slovenskej profesionálnej divadelnej kultúry v zahraničí,
- e) zabezpečuje zber a spracováva štatistické údaje za zverenú oblasť pre potreby ročného štatistického zisťovania KULT na základe poverenia od zriaďovateľa,
- f) systematicky zhromažďuje, odborne spracováva, ochraňuje, reštauruje, konzervuje, digitalizuje a sprístupňuje fondy a zbierky z oblasti profesionálnej divadelnej kultúry v Slovenskej republike, ktoré sú majetkom štátu a v správe Divadelného ústavu,
- g) sprístupňuje fondy a zbierky formou stálych expozícií, krátkodobých a dlhodobých výstav v Slovenskej republike i v zahraničí,
- h) je hlavným usporiadateľom a koordinátorom slovenských expozícií v rámci Pražského Quadriennale,
- i) vykonáva vedecko-výskumnú činnosť, spolupracuje na vedecko-výskumnej činnosti partnerských inštitúcií v oblasti profesionálnej divadelnej kultúry v Slovenskej republike a v zahraničí,
- j) vykonáva vydavateľskú a publikačnú činnosť, vydáva pôvodnú a prekladovú divadelno-vednú a dramatickú literatúru na všetkých druhoch nosičov, vydáva periodickú tlač a neperiodickú tlač,
- k) produkuje a vydáva zvukovo-obrazové záznamy o osobnostiach a divadelnej činnosti v Slovenskej republike,
- l) koordinuje cielené prieskumy, vykonáva expertízy a dáva podnety pre ďalší rozvoj profesionálnej divadelnej oblasti,
- m) spolupracuje s partnerskými inštitúciami v Slovenskej republike a v zahraničí,
- n) zabezpečuje šírenie informácií o slovenskom profesionálnom divadelnom umení a jeho propagáciu na území Slovenskej republiky a v zahraničí,
- o) je členom medzinárodných mimovládnych organizácií a zúčastňuje sa na ich práci, spolupracuje so slovenskými centrami medzinárodných mimovládnych organizácií, pôsobiach v oblasti profesionálneho divadelného umenia,

- p) organizuje vybrané medzinárodné a domáce profesionálne divadelné podujatia a festivaly, semináre, prednášky, vzdelávacie dielne, sympóziá, konferencie, kolokviá, spolupracuje na rôznych medzinárodných projektoch v oblasti profesionálneho divadelného umenia na území Slovenskej republiky a v zahraničí,
- q) samostatne a na základe poverenia zriaďovateľa zabezpečuje realizáciu vybraných zahraničných podujatí na území Slovenskej republiky a prezentáciu slovenského profesionálneho divadelného umenia v zahraničí,
- r) analyticky, expertízne, informačne a poradensky spolupracuje s inými orgánmi štátnej správy a samosprávy v oblasti profesionálnej divadelnej kultúry, s profesionálnymi divadlami, profesionálnymi divadelnými súbormi, združeniami, nadáciami a ďalšími kultúrnymi inštitúciami tak, aby bolo zabezpečené plnenie úloh zriaďovateľa a predmetu činnosti organizácie,
- s) poskytuje informačné, konzultačné a ďalšie odborné služby verejnosti v súlade so svojím predmetom činnosti prostredníctvom tlačovín, elektronických systémov a webových stránok,
- t) zabezpečuje predaj a distribúciu produktov vlastnej činnosti a produktov partnerských organizácií súvisiacich s predmetom svojej činnosti a charakterom organizácie,
- u) zabezpečuje prevádzku Štúdia 12, v rámci ktorej vytvára a realizuje aj vlastné profesionálne divadelné, vzdelávacie, prezentačné a kultúrne aktivity.

Súčasťou plnenia hlavného predmetu činnosti sú aktivity a to najmä:

- a) sprostredkovateľská a propagačná činnosť v oblasti profesionálnej divadelnej kultúry v rámci napĺňania svojho predmetu činnosti,
- b) ostatné aktivity, podporujúce rozvoj a skvalitnenie plnenia poslania a hlavného predmetu činnosti.

Štatutárnym orgánom Prevádzkovateľa je riaditeľ, ktorého vymenúva a odvoláva minister kultúry Slovenskej republiky.

Štatutárny orgán riadi organizáciu a koná v jej mene v súlade so zriaďovacou listinou a zodpovedá za jej činnosť ministrovi kultúry Slovenskej republiky.

Štatutárny orgán v súlade so zriaďovacou listinou určuje organizačnú štruktúru, vydáva organizačný priadok a pracovný poriadok a ďalšie vnútorné predpisy organizácie.

2.1.3 Organizačná štruktúra

Postavenie, pôsobnosť a vzájomné vzťahy jednotlivých prvkov organizačnej štruktúry Prevádzkovateľa rieši Organizačný poriadok a Pracovný poriadok a ich prílohy.

2.2 Sprostredkovatelia a dodávatelia

2.2.1 Ministerstvo kultúry Slovenskej republiky

Ministerstvo kultúry Slovenskej republiky (ďalej len „MK SR“ alebo „Ministerstvo“) so sídlom na adrese Nám. SNP č. 33, 813 31 Bratislava, ktoré v zmysle zmluvy, ktorou sa Sprostredkovateľ zaväzuje pre Prevádzkovateľa vykonávať činnosti v oblasti vzdialeného automatizovaného spracúvania údajov a to najmä pri realizácii týchto aktivít:

- realizáciu a správu Centrálného jednotného ekonomického systému a dátového skladu pre aplikáciu Softip Profit,
- zabezpečenie bezpečnej a spoľahlivej prevádzky serverov ktoré zabezpečujú komunikačnú infraštruktúru CJES,
- realizáciu a správu centrálnej elektronickej registratúry – NUNTIO – Automatizovaný systém správy registratúry (NUNTIO ASSR),

- zabezpečenie bezpečnej a spoľahlivej prevádzky serverov ktoré zabezpečujú komunikačnú infraštruktúru NUNTIO ASSR,
- zabezpečenia bezpečnej a spoľahlivej prevádzky softvéru potrebného na činnosť CJES a NUNTIO ASSR,
- koncepčné a metodické riadenie rozvoja a prevádzky CJES a NUNTIO ASSR,
- pravidelné prehodnocovanie stavu CJES NUNTIO ASSR, postupov a výsledkov prostredníctvom spoločných stretnutí zástupcov ministerstva a zástupcov poskytovateľa,
- schvaľovanie požiadaviek organizácií na zavedenie, zmenu alebo rozšírenie služieb,
- centrálné zálohovanie dát a priebežnú kontrolu funkčnosti serverov,
- integrovanú ochranu osobných údajov pri ich spracúvaní v CJES a NUNTIO ASSR. V uvedenom smere s prihliadnutím k príslušným ustanoveniam Zákona, v mysle prijatého bezpečnostného projektu na ochranu osobných údajov MK SR poveruje zodpovednú osobu za výkon dohľadu nad jeho dodržiavaním v pôsobnosti MK SR, určuje oprávnené osoby MK SR s prístupom k spracúvaným osobným údajom, dotknuté osoby MK SR, ktorých osobné údaje sú v CJES spracúvané v zákonnej lehote informuje o účele a ďalších podmienkach ich spracúvania.

Účelom poskytovaných služieb je zabezpečenie bezpečnej a spoľahlivej prevádzky softvéru, dátového skladu a serverov, ich údržby a rozvoja, zálohovania údajov Prevádzkovateľa, ich obnovy a poskytnutia Prevádzkovateľovi.

Sprostredkovateľ je oprávnený poveriť údržbou a správou ďalších sprostredkovateľov, v súlade so zákonom.

2.2.2 Ďalšie spoločnosti

Prevádzkovateľ, alebo Ministerstvo má uzatvorené aj ďalšie zmluvy na základe ktorých zabezpečuje činnosti súvisiace s technologickým zabezpečením a pripojením do siete Internet a do VPN MK SR a podobne. Všetky tieto spoločnosti nevykonávajú systematické spracúvanie osobných údajov a nie sú teda sprostredkovateľom v pôsobnosti Zákona.

Jedná sa napríklad o spoločnosť, SWAN, a.s. a pod., ktoré spravidla vystupujú iba ako technologický sprostredkovateľ.

3. Prevádzkované informačné systémy

Vykonanou Analýzou bolo zistené, že Prevádzkovateľ systematicky spracúva osobné údaje dotknutých osôb v nasledovných IS:

3.1 IS Personalistika a mzdy

IS Personalistika a mzdy (ďalej len „IS PAM“) integruje spracúvanie osobných údajov v nasledovných agendách, ktorými sa zabezpečuje pôsobnosť Prevádzkovateľa a podpora operácií pre financovanie (Štátna pokladnica):

- Personálna agenda,
- Mzdová agenda.

3.1.1 Opis plánovaného spracúvania osobných údajov v IS Personalistika a mzdy

Personálna agenda

Personálna agenda je v automatizovanej aj neautomatizovanej forme spracúvaná výhradne v pôsobnosti určených poverených osôb (zamestnancov) Prevádzkovateľa, ktorí majú prístup k osobným údajom v personálnej agende.

Poverená osoba (ide o určených zamestnancov Prevádzkovateľa), ktorá má prístup k osobným údajom v personálnej agende:

- vedie personálnu evidenciu zamestnancov Prevádzkovateľa a zodpovedá za ochranu osobných údajov,
- zabezpečuje pracovnoprávnú agendu zamestnancov Prevádzkovateľa vyplývajúcu z ich pracovného pomeru,
- zabezpečuje úlohy v oblasti sociálnej a zdravotnej starostlivosti zamestnancov,
- vykonáva rozbory a vyhotovuje štatistické výkazy z oblasti personalistiky,
- zabezpečuje výchovu a vzdelávanie pracovníkov, vedie a kontroluje evidenciu študujúcich popri zamestnaní,
- zabezpečuje konkurzy a výberové konania,
- spolupracuje na príprave a hodnotení kolektívnych zmlúv v oblasti odmeňovania a mzdovej politiky,
- zabezpečuje agendu práce a mzdy
- agenda súvisiaca s aplikáciou zákonných podmienok BOZP a PO,
- agenda vstupov, výstupov a hodnotení auditu rizík práce a pracovného prostredia,
- agenda vstupných lekárskeho prehliadok súvisiacich s výkonom zamestnania a poskytovaním pracovnej zdravotnej služby.

Poverené osoby (zamestnanci) Prevádzkovateľa s prístupom k osobným údajom v personálnej agende boli náležitým spôsobom poučené o rozsahu povolených spracovateľských operácií a zásadách ochrany osobných údajov pri ich spracúvaní.

Automatizované spracúvanie sa vykonáva jednak s podporou kancelárskeho balíka MS Office, ako aj s podporou kancelárskeho balíka LibreOffice, ktorými sa zabezpečuje vyhotovenie, tlač a zálohovanie požadovaných dokumentov súvisiacich s uzatvorením, priebehom, ukončením a dokumentáciou pracovného pomeru (pracovná zmluva, platový dekrét, osobný dotazník, súhlas dotknutej osoby na spracúvanie jej osobných údajov, ak sa v zmysle Zákona požaduje, tlačivo poučenia zamestnanca o právach a povinnostiach vyplývajúcich zo Zákona

a zodpovednosti za ich porušenie a pod.). PC, na ktorých sa spracúvanie fyzicky vykonáva, sú pripojené do LAN a majú prístup na internet.

Ochrana osobných údajov vedených v automatizovanej časti personálnej agendy sa prioritne zabezpečuje riadeným prístupom do priestorov ich spracúvania, riadeným prístupom k PC, na ktorom sú osobné údaje spracúvané, riadeným prístupom oprávnených užívateľov k aplikácii, diferencovaným riadeným prístupom k jednotlivým modulom aplikácie, centrálnym zálohovaním a internou odbornou podporou poskytovanou poverenými a kompetentnými zamestnancami Prevádzkovateľa.

V neautomatizovanej forme je personálna agenda vedená najmä formou písomných osobných spisov a agend:

- a) zamestnancov pri výkone práce vo verejnom záujme,
- b) agendy evidencie uchádzačov o zamestnanie a realizácie výberových konaní.

Osobné spisy zamestnancov podľa bodu a) tohto článku vedie Ekonomické oddelenie v rozsahu a spôsobom požadovanom osobitnými zákonmi, ktoré stanovujú účel, podmienky, prostriedky a subjekty spracúvania osobných údajov – bližšie viď čl. 3.1.2.1 tejto smernice. Z uvedeného dôvodu sa písomný súhlas dotknutej osoby na spracúvanie jej osobných údajov a údajov blízkych osôb nepožaduje. Súhlas sa požaduje aj na získavanie fotografie, v súvislosti s aplikovanými procedurálnymi opatreniami vydania prístupovej karty do priestorov v správe Prevádzkovateľa. Predmet a rozsah súhlasu dotknutej osoby, informovania dotknutej osoby o účele a podmienkach spracúvania osobných údajov podľa § 15 Zákona a podmienky ich realizácie budú taktiež predmetom implementácie Bezpečnostného projektu na ochranu osobných údajov.

Osobitnou kategóriou osobných údajov spracúvaných v pôsobnosti Ekonomického oddelenia sú údaje z registra trestov. Pre verejnú službu je osobitným zákonom podmienkou preukázania bezúhonnosti predloženie výpisu z registra trestov.

Výpismi z registra trestov preukazujú zamestnanci a uchádzači o zamestnanie svoju bezúhonnosť. S prihliadnutím k ustanoveniam Zákona sa požaduje stanoviť okruh oprávnených osôb, ktoré sa pri posudzovaní bezúhonnosti dotknutej osoby môžu oboznamovať s osobitnou kategóriou osobných údajov o porušení ustanovení trestného práva, priestupkového práva alebo občianskeho práva, ako aj o výkone právoplatných rozsudkov alebo rozhodnutí.

Evidencia uchádzačov o zamestnanie a evidencia súvisiaca s realizáciou výberových konaní podľa bodu b) je vedená v rozsahu potrebnom na plánovanie a rozvoj ľudských zdrojov v pôsobnosti Ekonomického oddelenia Prevádzkovateľa. Evidencie vedú poverené osoby. Po dobu trvania účelu na spracúvanie osobných údajov (napr. výber uchádzačov na uvoľnené alebo novovytvorené pracovné pozície) sa písomný súhlas na spracúvanie osobných údajov nepožaduje, nakoľko v zmysle Zákona ide o opatrenia na zavedenie predzmluvných vzťahov a opatrení na žiadosť dotknutej osoby. Písomný súhlas na spracúvanie osobných údajov je potrebný v prípade, ak Prevádzkovateľ plánuje zaradenie osobných údajov do databázy uchádzačov o zamestnanie, za účelom operatívneho výberu a obsadzovania uvoľnených alebo požadovaných miest.

Prevádzkovateľ prostredníctvom poverených oprávnených osôb vykoná prihlásenie poistencov (zamestnancov pri výkone práce vo verejnom záujme) do Sociálnej poisťovne a príslušnej zdravotnej poisťovne, čo prebieha formou predpísaných tlačív prostredníctvom doporučenej zásielky, výnimočne zabezpečenou elektronickou komunikáciou.

Poverené oprávnené osoby Ekonomického oddelenia taktiež na základe predloženej písomnej žiadosti dotknutej osoby, alebo inštitúcie na to oprávnenej vyhotovujú aj odpisy z osobných údajov dotknutej osoby (napr.: potvrdenie o dobe zamestnania) s tým, že o takýchto odpisoch vedú písomný záznam, ktorý je uložený v osobnom spise a je možné ho dohľadať.

Ochrana osobných údajov vedených v neautomatizovanej časti personálnej agendy sa prioritne zabezpečuje riadeným prístupom do priestorov ich spracúvania, zamedzením prístupu neoprávnených osôb, dôsledným dodržiavaním požiadaviek administratívnej bezpečnosti pri vedení písomných agend ako je ich evidencia, obeh písomností, bezpečné ukladanie písomností v uzamykateľných skrinách a registratúrach, kontrolná činnosť, technicko-organizačné opatrenia na zamedzenie poškodenia alebo zničenia spracúvaných osobných údajov a zabezpečenie zákonných požiadaviek v rozsahu nakladania s osobnými údajmi v personálnej agende po skončení účelu ich spracúvania (registratúra a archivácia písomností, antidiskriminačný zákon a pod.).

Mzdová agenda

Účtovníctvo, výkazníctvo, operatívnu evidenciu, štatistiku, komplexnú mzdovú agendu vrátane zabezpečenia odvodových povinností voči zdravotným poisťovniam, sociálnej poisťovni a daňovému úradu, komplexnú pokladničnú agendu vrátane poskytovania záloh, zúčtovania a finančnej likvidácie cestovných náležitostí, zúčtovania záloh a zabezpečenia odvodov príjmov z činnosti na príjmový účet v mene Prevádzkovateľa vykonávajú oprávnené osoby (zamestnanci) Prevádzkovateľa v zmysle osobitných zákonov, ktoré sú uvedené v čl. 3.1.2.1 tejto smernice. Uvedený popis v plnom rozsahu platí aj pre účtovnú agendu.

Mzdová agenda je v automatizovanej aj neautomatizovanej forme spracovávaná v pôsobnosti poverených a vecne oprávnených osôb (zamestnancov) Prevádzkovateľa, ktoré realizujú komplexné vedenie mzdovej dokumentácie, zúčtovanie miezd, plnenie odvodových povinností vyplývajúcich zo mzdových predpisov a príslušných zákonných ustanovení za interné a externé organizačné jednotky Prevádzkovateľa. Oprávnené osoby s prístupom k osobným údajom v mzdovej agende boli náležitým spôsobom poučené o rozsahu povolených spracovateľských operácií a zásadách ochrany osobných údajov pri ich spracúvaní.

Osobitnou kategóriou osobných údajov vedených v automatizovanej ako aj neautomatizovanej časti mzdovej agendy sú údaje o členstve dotknutých osôb v odborovej organizácii, súvisiace s vykonávaním zrážok členských príspevkov na účet odborovej organizácie. Spracúvanie osobných údajov sa vykonáva v zmysle Zákona, t.j. výhradne po predložení vlastnoručne podpísanej písomnej žiadosti dotknutej osoby o realizáciu zrážok členského príspevku na účet odborovej organizácie.

Ochrana osobných údajov vedených v automatizovanej časti mzdovej agendy sa prioritne zabezpečuje riadeným prístupom do priestorov ich spracúvania, riadeným prístupom k PC, na ktorých sú osobné údaje spracúvané, riadeným prístupom oprávnených užívateľov k aplikácii, diferencovaným riadeným prístupom k jednotlivým modulom aplikácie, centrálnym zálohovaním, centrálnou správou a podporou poskytovanou poverenými a kompetentnými zamestnancami Prevádzkovateľa.

PC, na ktorých sa spracúvanie osobných údajov dotknutých osôb v mzdovej agende vykonáva, sú pripojené k LAN Prevádzkovateľa a prepojené na internet.

Neautomatizované spracúvanie mzdovej agendy je realizované najmä formou mzdových listov.

Poverené oprávnené osoby (zamestnanci) Prevádzkovateľa taktiež vedú a k pracovným účelom využívajú najmä agendu:

- a) pracovnoprávných vzťahov založených dohodou o vykonaní práce,
- b) pracovno-právných vzťahov založených dohodou o brigádnickej práci študentov,
- c) pracovno-právných vzťahov založených dohodou o pracovnej činnosti,
- d) agendu zmlúv uzatvorených podľa zákona č. 185/2015 Z. z. Autorský zákon v platnom znení,

- e) agendu cestovných náležitostí,
- f) agendu fondu pracovného času.

Prevádzkovateľ taktiež prostredníctvom poverených oprávnených osôb (zamestnancov) Prevádzkovateľa vykoná prihlásenie poistencov (okrem zamestnancov pri výkone práce vo verejnom záujme) do Sociálnej poisťovne a príslušnej zdravotnej poisťovne, čo prebieha formou predpísaných tlačív prostredníctvom doporučenej zásielky, výnimočne zabezpečenou elektronickou komunikáciou.

Spracúvanie osobných údajov podľa bodu a) až f) prebieha podľa osobitného zákona, ktorý rieši uvedenú problematiku od návrhu určitej dohody alebo zmluvy cez jej schvaľovací proces až po jej odovzdanie dotknutej osobe. Podľa aplikovaných interných prepisov Prevádzkovateľa a súvisiacich pracovných postupov môže predložiť návrh na uzatvorenie dohody obsahujúci požadované osobné údaje alebo zmluvu ktorýkoľvek organizačný útvar Prevádzkovateľa. Poverené osoby (zamestnanci) Prevádzkovateľa zabezpečujú vedenie a aktualizáciu predmetných agend podľa osobitných zákonov uvedených v čl. 3.1.2.1 tejto smernice. Z tohto dôvodu sa písomný súhlas dotknutej osoby na spracúvanie jej osobných údajov nepožaduje.

Poverené osoby (zamestnanci) Prevádzkovateľa pri spracúvaní mzdovej agendy automatizovaným ako aj neautomatizovaným spôsobom vykonávajú:

- a) výpočet miezd,
- b) výpočet poistného,
- c) vystavovanie a tlač účtovných dokladov,
- d) obeh účtovných dokladov,
- e) evidenciu a archiváciu účtovných dokladov,
- f) evidenciu v oblasti miezd,
- g) vypracovanie výkazov a hlásení pre poisťovne,
- h) prihlasovanie a odhlasovanie zamestnancov v termínoch podľa osobitného zákona,
- i) vedenie agendy dane z príjmu fyzických osôb zo závislej činnosti.

Ochrana osobných údajov vedených v neautomatizovanej časti mzdovej agendy sa prioritne zabezpečuje riadeným prístupom do priestorov ich spracúvania, zamedzením prístupu neoprávnených osôb a dôsledným dodržiavaním požiadaviek administratívnej bezpečnosti pri vedení písomných agend. Ide najmä o ich evidenciu, obeh písomností, bezpečné ukladanie písomností v uzamykateľných skrinách a registratúrach – čo je zabezpečené iba čiastočne – a v iných, odôvodnených prípadoch sa ochrana písomností zabezpečuje uzamykaním priestorov pri každom opustení pracoviska. Je vykonávaná kontrolná činnosť, technicko-organizačné opatrenia na zamedzenie poškodenia alebo zničenia spracúvaných osobných údajov a zabezpečenie zákonných požiadaviek v rozsahu nakladania s osobnými údajmi v mzdovej agende po skončení účelu ich spracúvania (registratúra a archivácia písomností).

Vlastnú realizáciu finančných úhrad mzdových a mimomzdových prostriedkov vykonávajú na základe vystavených účtovných dokladov vecne kompetentní zamestnanci Prevádzkovateľa určení pre styk so Štátnou pokladnicou.

3.1.1.1 Účel spracúvania osobných údajov

Účel spracúvania osobných údajov v IS PAM je vymedzený pôsobnosťou Prevádzkovateľa a najmä osobitnými zákonmi uvedenými v čl. 3.1.2.1 tejto smernice. V medziach stanoveného účelu sú vedené a priebežne aktualizované agendy uvedené v bode 3.1 tejto smernice nasledovne:

- vedenie komplexnej personálnej a mzdovej agendy, podkladov na realizáciu miezd a úhradu mimomzdových prostriedkov súvisiacich s pracovným pomerom, vrátane daňových a odvodových povinností, vrátane ich ročného zúčtovania,
- výplata mzdy zamestnancom (výplatné listiny, výplatné pásky, podklady ku mzdám, rekapitulácia miezd, mzdové listy),
- stravovanie zamestnancov a príspevky zo sociálneho fondu na tento účel,
- bezpečnosť a ochrana zdravia pri práci, vrátane evidencie pracovných úrazov,
- osobné spisy zamestnancov vykonávajúcich prácu pre prevádzkovateľa,
- evidencia pracovného času, vrátane dochádzky, prerušenia pracovného času, čerpania dovolenky ako aj prekážok v práci na strane zamestnanca a zamestnávateľa,
- dohody o hmotnej zodpovednosti,
- služobné preukazy,
- výber zamestnancov (výberové konania, prijímania žiadostí do prijatia pracovného pomeru),
- majetkové priznania,
- kolektívne pracovné právo (kolektívne zmluvy).

3.1.1.2 Zoznam/rozsah osobných údajov spracúvaných

V automatizovanom aj neautomatizovanom IS PAM a jeho agendách sú osobné údaje dotknutých osôb spracúvané diferencovane, v nasledovnom maximálnom rozsahu, ktorý sa aplikuje podľa osobitných zákonov a stanoveného účelu spracúvania osobných údajov:

- priezvisko /aj pôvodné priezvisko a rodné priezvisko/
- meno /aj rodné meno/
- titul
- podpis
- adresa trvalého pobytu, prípadne prechodného pobytu, korešpondenčná adresa
- dátum narodenia
- miesto narodenia
- štát narodenia
- národnosť
- rodné číslo
- osobné číslo
- pohlavie
- rodinný stav
- údaje o rodinných príslušníkoch v rozsahu meno, priezvisko, adresa, dátum narodenia
- rodinný vzťah rodinného príslušníka
- počet detí
- štátna príslušnosť
- absolvované školy a vzdelanie / kvalifikácia/
- výnimky zo vzdelania
- doby v zamestnaní
- dátum uzatvorenia pracovného vzťahu
- dátum nástupu
- doba pracovného vzťahu
- druh vyňatia
- doba vyňatia
- spôsob získania zamestnanca
- skúšobná doba

- dátum skončenia pracovného vzťahu /PV/
- dôvod skončenia PV
- spôsob skončenia PV
- pracovná kategória
- druh pracovného pomeru
- pracovné zaradenie
- organizačný útvar
- fond pracovnej doby
- plat, platové pomery a ďalšie finančné náležitosti priznané za výkon pracovnej činnosti
- dovolenka
- pracovný kalendár
- porušenie pracovnej disciplíny
- nárok na starobný dôchodok
- zmenená pracovná schopnosť
- služobné hodnotenie
- školenia a kurzy
- údaje o zdravotnej spôsobilosti
- údaje o odbornej spôsobilosti
- údaje o odpracovanom čase
- údaje o bankovom účte fyzickej osoby
- číslo telefónu
- predchádzajúci zamestnávateľi
- doba základnej vojenskej služby
- doba civilnej základnej služby
- údaje o priznaní dôchodku, o druhu dôchodku
- údaje o zmenenej pracovnej schopnosti
- údaje o dôležitých osobných prekážkach v práci
- zdravotná poisťovňa zamestnanca
- meno a priezvisko manželky/manžela, druha / družky
- rodné číslo manželky/manžela, druha / družky – dátum narodenia, rodné meno, adresa
- meno a priezvisko dieťaťa
- rodné číslo a dátum narodenia dieťaťa, adresa
- názov a adresa školy, ktorú dieťa nad 16 rokov navštevuje
- údaje o dôchodkovom poistení zamestnanca
- údaje o zákonných zrážkach zamestnanca (výživné, exekúcie)
- údaje o sporení, pôžičkách a zrážkach na poistenie zamestnanca
- údaje o dočasnej práceneschopnosti zamestnanca a o ošetrovaní chorého člena rodiny
- údaje o materskej a rodičovskej dovolenke zamestnanca
- daňové vyhlásenie k dani z príjmu,
- daňový bonus,
- doklad o návšteve školy (16-25 r.),
- doklad o % invalidity
- názov DDS
- údaje zo zamestnaneckej zmluvy doplnkovej dôchodkovej poisťovne
- emailová adresa
- miesto výkonu práce
- podobizeň, obrazové snímky, zvukové záznamy na informatívne účely a účely propagácie zamestnávateľa
- telesné miery za účelom vydania osobných ochranných pracovných pomôcok
- sumy postihnuté výkonom rozhodnutia nariadeným súdom alebo správnym orgánom
- peňažné tresty a pokuty, ako aj náhrady uložené zamestnancovi vykonateľným rozhodnutím príslušných orgánov

- údaje z potvrdenia o zamestnaní
- údaje o vedení zamestnanca v evidencii nezamestnaných občanov
- údaje z dokladu o bezúhonnosti
- údaje o členstve v odborovej organizácii a platbe členského príspevku odborovej organizácii
- osobné údaje z majetkového priznania zamestnancov pri výkone práce vo verejnom záujme
- osobné údaje spracúvané na oprávnení oboznamovať sa s utajovanými skutočnosťami
- osobné údaje spracúvané na potvrdeniach a informačných kartách, na osvedčeniach o absolvovaní skúšok a vzdelávacích aktivít
- údaje uvedené v životopise
- údaje z povolenia o pobyte
- oznámenie a čestné vyhlásenie k dohode o brigádnickej práci študentov na účely uplatnenia práva podľa § 227a zákona o soc. poistení.

Faktory práce a pracovného prostredia (zamestnanecké údaje spracúvané za účelom pracovnej zdravotnej služby),

- názov pracoviska
- druh práce
- dĺžka expozície
- výsledok posúdenia zdravotných rizík
- typ požadovanej prehliadky (pred nástupom, preventívna, periodická...)
- názov a sídlo zamestnávateľa, číslo strediska
- dátum poslednej prehliadky
- meno a kontakt na vedúceho zamestnanca
- záver vyšetrenia (t.j. spôsobilosť/nespôsobilosť na výkon konkrétnej činnosti a dátum jej účinnosti)
- odporúčaný termín ďalšej prehliadky
- termín absolvovania rekondičného pobytu
- miesto rekondičného pobytu
- kategorizácia práce
- názov zdravotnej poisťovne.

3.1.1.3 Zoznam/okruh príjemcov

Osobné údaje môžu byť poskytované nasledujúcim príjemcom: daňový úrad, Sociálna poisťovňa, príslušná zdravotná poisťovňa, inšpektorát práce, Úrad práce, sociálnych vecí a rodiny, Policajný zbor SR, súdy, exekútor.

3.1.1.4 Vymedzenie obdobia uchovávaní osobných údajov

Osobné údaje sú spracúvané po dobu trvania pracovného pomeru, po skončení pracovného pomeru sú naďalej uchovávané v registratúrnom stredisku. Spôsob uchovávaní je určený všeobecne záväznými právnymi predpismi a doba uchovávaní jednotlivých dokumentov je stanovená v registratúrnom poriadku a registratúrnom pláne, pričom závisí od jednotlivých spracovateľských operácií:

Spracovateľská operácia	Doba uchovávaní (v rokoch)
Stravné lístky (mesačné prehľady, príspevky zo sociálneho fondu)	10
Mzdové listy	50
výplata mzdy zamestnancom (výplatné listiny, výplatné pásky, podklady ku mzdám, rekapitulácia miezd)	10
vyhlásenie na zdanenie príjmov fyzických osôb, ročné zúčtovanie daní	10

sociálne poistenie	10
zdravotné poistenie vrátane ročného zúčtovania zdravotného poistenia	10
doplňkové dôchodkové sporenie	10
evidencia úrazov	5
osobné spisy zamestnancov vo verejnom záujme	70
spis osôb vykonávajúcich prácu mimo pracovného pomeru	10
evidencia dochádzky, dovolenky	5
dohody o hmotnej zodpovednosti	5
služobné preukazy	1
výberové konanie	10
žiadosti o prijatie do pracovného pomeru	1
majetkové priznania	5
Kolektívna zmluva	10

3.1.1.5 Dotknuté osoby v IS

Dotknutými osobami v rámci IS PAM sú zamestnanci, uchádzači o zamestnanie, pracovníci na dohodu (dohoda o vykonaní práce, dohoda o brigádnickej práci študentov, dohoda o pracovnej činnosti) a účastníci výberových konaní, ako aj bývalí zamestnanci a rodinní príslušníci, ktorých osobné údaje sú spracúvané pre účely plnenia daňových povinností Prevádzkovateľa.

3.1.2 Posúdenie nevyhnutnosti a primeranosti

3.1.2.1 Zákonnosť spracúvania osobných údajov

Spracúvanie osobných údajov v IS Personalistika a mzdy má zákonný základ v osobitných právnych predpisoch. Právnym základom pre spracúvanie osobných údajov je zmluvný alebo predzmluvný vzťah medzi Prevádzkovateľom a dotknutou osobou.

Účel spracúvania osobných údajov v IS PAM je vymedzený nasledujúcimi osobitnými zákonmi:

Číslo predpisu	Názov predpisu
311/2001 Z. z.	Zákonník práce v znení neskorších predpisov
552/2003 Z. z.	Zákon o výkone práce vo verejnom záujme v znení neskorších predpisov
18/2018 Z. z.	Zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
580/2004 Z. z.	Zákon o zdravotnom poistení o zmene a doplnení zákona č. 95/2002 Z. z. o poisťovníctve a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
461/2003 Z. z.	Zákon o sociálnom poistení v znení neskorších predpisov
595/2003 Z. z.	Zákon o dani z príjmov v znení neskorších predpisov
43/2004 Z. z.	Zákon o starobnom dôchodkovom sporení a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
650/2004 Z. z.	Zákon o doplnkovom dôchodkovom sporení a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
5/2004 Z. z.	Zákon o službách zamestnanosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
462/2003 Z. z.	Zákon o náhrade príjmu pri dočasnej pracovnej neschopnosti zamestnanca a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
152/1994 Z. z.	Zákon o sociálnom fonde a o zmene a doplnení zákona č. 286/1992 Zb. o daniach z príjmov v znení neskorších predpisov

355/2007 Z. z.	Zákon o ochrane, podpore a rozvoji verejného zdravia a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
124/2006 Z. z.	Zákon o bezpečnosti a ochrane zdravia pri práci a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
570/2005 Z. z.	Zákon o brannej povinnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
431/2002 Z. z.	Zákon o účtovníctve v znení neskorších predpisov
553/2003 Z. z.	Zákon o odmeňovaní niektorých zamestnancov pri výkone práce vo verejnom záujme a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
126/2015 Z. z.	Zákon o knižniciach a o zmene a doplnení zákona č. 206/2009 Z. z. o múzeách a o galériách a o ochrane predmetov kultúrnej hodnoty a o zmene zákona Slovenskej národnej rady č. 372/1990 Zb. o priestupkoch v znení neskorších predpisov v znení zákona č. 38/2014 Z. z.
581/2004 Z. z.	Zákon o zdravotných poisťovniach, dohľade nad zdravotnou starostlivosťou a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
663/2007 Z. z.	Zákon o minimálnej mzde v znení neskorších predpisov
404/2011 Z. z.	Zákon o pobyte cudzincov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
215/2004 Z. z.	Zákon o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
395/2002 Z. z.	Zákon o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov

3.1.2.2 Obmedzenie účelu

Prevádzkovateľ zohľadnil zásadu obmedzenia účelu spracúvania osobných údajov prijatím organizačných opatrení, ktorými bolo určené povereným osobám získavať osobné údaje na konkrétny účel súvisiaci s plnením povinností prevádzkovateľa ako zamestnávateľa, pričom osobné údaje v rámci IS nie je možné spracúvať na iné ako vopred vymedzené účely, ktoré majú zákonný základ, táto povinnosť bola uložená všetkým povereným osobám ako základná povinnosť pri spracúvaní osobných údajov. Tieto účely sú legitímne, sú určené všeobecne záväznými právnymi predpismi vzťahujúcimi sa na oblasť zamestnávania.

3.1.2.3 Minimalizácia osobných údajov

Prevádzkovateľ prijal opatrenia, aby sa na každú spracovateľskú operáciu využíval len taký osobný údaj, ktorý je preukázateľne potrebný a nevyhnutný pre plnenie stanoveného účelu spracúvania.

Spracovateľská operácia	Spracúvané osobné údaje v rámci spracovateľskej operácie
stravné lístky (mesačné prehľady, príspevky zo sociálneho fondu)	meno a priezvisko, titul, počet pridelených stravných lístkov, príspevok zo sociálneho fondu, príspevok odborov, zrážka zo mzdy zamestnanca

mzdové listy	meno, priezvisko, rodné priezvisko a titul, rodné číslo, dátum a miesto narodenia, mzda, plat alebo platové pomery a ďalšie finančné náležitosti priznané za výkon funkcie alebo za výkon pracovnej činnosti, údaje o odpracovanom čase, sumy postihnuté výkonom rozhodnutia nariadeným súdom alebo správnym orgánom, peňažné tresty a pokuty, ako aj náhrady uložené zamestnancovi vykonateľným rozhodnutím príslušných orgánov, údaje o pracovnej neschopnosti, údaje o dôležitých osobných prekážkach v práci, údaje o zmenenej pracovnej schopnosti, deň začiatku výkonu štátnej služby alebo pracovnej činnosti, údaje o vyživovaných deťoch v rozsahu meno, priezvisko, rodné číslo, údaje o čerpaní materskej dovolenky a rodičovskej dovolenky, údaje o priznaní dôchodku, o druhu dôchodku, výška príspevku zamestnanca a zamestnávateľa do doplnkovej dôchodkovej poisťovne, platbe členského príspevku odborovej organizácii, rodinný stav, trvalé bydlisko, prechodné bydlisko, údaje o zamestnávateľovi
výplata mzdy zamestnancom (výplatné listiny, výplatné pásky, podklady ku mzdám, rekapitulácia miezd)	meno, priezvisko, rodné priezvisko a titul, rodné číslo, dátum a miesto narodenia, podpis, mzda, plat alebo platové pomery a ďalšie finančné náležitosti priznané za výkon funkcie alebo za výkon pracovnej činnosti, údaje o odpracovanom čase, údaje o bankovom účte fyzickej osoby, sumy postihnuté výkonom rozhodnutia nariadeným súdom alebo správnym orgánom, peňažné tresty a pokuty, ako aj náhrady uložené zamestnancovi vykonateľným rozhodnutím príslušných orgánov, neprávom prijaté sumy dávok sociálneho poistenia a dôchodkov starobného dôchodkového sporenia alebo ich preddavky, štátnych sociálnych dávok, dávok v hmotnej núdzi a príspevkov k dávke v hmotnej núdzi, peňažných príspevkov na kompenzáciu sociálnych dôsledkov ťažkého zdravotného postihnutia, ktoré je zamestnanec povinný vrátiť na základe vykonateľného rozhodnutia podľa osobitného predpisu, údaje o pracovnej neschopnosti, údaje o dôležitých osobných prekážkach v práci, údaje o zmenenej pracovnej schopnosti, pracovné zaradenie a deň začiatku výkonu štátnej služby alebo pracovnej činnosti, údaje o rodinných príslušníkoch v rozsahu meno, priezvisko a dátum narodenia, rodné číslo, údaje o deťoch v rozsahu meno a priezvisko, rodné číslo a údaje o navštevovanej škole, údaje o čerpaní materskej dovolenky a rodičovskej dovolenky, údaje o priznaní dôchodku, o druhu dôchodku, údaje týkajúce sa zrážok pre doplnkové dôchodkové poisťovne, údaje o členstve v odborovej organizácii a platbe členského príspevku odborovej organizácii, rodinný stav, štátna príslušnosť, trvalé bydlisko, prechodné bydlisko, pohlavie, údaje o zamestnávateľovi
vyhlásenie na zdanenie príjmov fyzických osôb, ročné zúčtovanie daní	meno, priezvisko, rodné priezvisko a titul, rodné číslo, dátum a miesto narodenia, podpis, mzda, plat alebo platové pomery a ďalšie finančné náležitosti priznané za výkon funkcie alebo za výkon pracovnej činnosti, údaje o zmenenej pracovnej schopnosti, údaje o zamestnávateľoch, deň začiatku výkonu štátnej služby alebo pracovnej činnosti, údaje o manželovi alebo manželke, deťoch, rodičoch detí v rozsahu meno, priezvisko, dátum a miesto narodenia, rodné číslo, adresa, údaje z potvrdenia o zamestnaní, údaje o vedení zamestnanca v evidencii nezamestnaných občanov, údaje o čerpaní materskej dovolenky a rodičovskej dovolenky, údaje o priznaní dôchodku, o druhu dôchodku, údaje zo zmluvy s doplnkovou dôchodkovou poisťovňou, rodinný stav, trvalé bydlisko, prechodné bydlisko, pohlavie

sociálne poistenie	meno, priezvisko, rodné priezvisko a titul, rodné číslo, dátum a miesto narodenia, podpis, mzda, plat alebo platové pomery a ďalšie finančné náležitosti priznané za výkon funkcie alebo za výkon pracovnej činnosti, údaje o odpracovanom čase, údaje o pracovnej neschopnosti, údaje o dôležitých osobných prekážkach v práci, údaje o zmenenej pracovnej schopnosti, údaje o zamestnávateľoch, deň začiatku výkonu štátnej služby alebo pracovnej činnosti, údaje o rodinných príslušníkoch v rozsahu meno, priezvisko, adresa, dátum narodenia, údaje o manželovi alebo manželke, deťoch, rodičoch detí v rozsahu meno, priezvisko, dátum narodenia, rodné číslo, adresa, údaje o čerpaní materskej dovolenky a rodičovskej dovolenky, údaje o priznaní dôchodku, o druhu dôchodku, rodinný stav, štátna príslušnosť, trvalé bydlisko, prechodné bydlisko, pohlavie
zdravotné poistenie vrátane ročného zúčtovania zdravotného poistenia	meno, priezvisko, rodné priezvisko a titul, rodné číslo, podpis, mzda, plat alebo platové pomery a ďalšie finančné náležitosti priznané za výkon funkcie alebo za výkon pracovnej činnosti, údaje o odpracovanom čase, údaje o pracovnej neschopnosti, údaje o dôležitých osobných prekážkach v práci, údaje o zmenenej pracovnej schopnosti, deň začiatku výkonu štátnej služby alebo pracovnej činnosti, údaje o čerpaní materskej dovolenky a rodičovskej dovolenky, údaje o priznaní dôchodku, o druhu dôchodku, rodinný stav, trvalé bydlisko, prechodné bydlisko, údaje o zamestnávateľovi
doplňkové dôchodkové sporenie	meno, priezvisko, rodné priezvisko a titul, rodné číslo, dátum narodenia, podpis, výška príspevku do DDS, údaje o zamestnávateľovi, údaje o čerpaní materskej dovolenky a rodičovskej dovolenky, trvalé bydlisko, prechodné bydlisko
evidencia úrazov	meno a priezvisko zamestnanca, opis úrazu (čas a miesto zranenia, druh zranenia, zranená časť tela), podpis zraneného, meno, priezvisko a podpis svedka, meno, priezvisko a podpis zapisujúceho, údaje zamestnávateľa
osobné spisy zamestnancov vo verejnom záujme	meno, priezvisko, rodné priezvisko a titul, dátum a miesto narodenia, podpis, mzda, plat alebo platové pomery a ďalšie finančné náležitosti priznané za výkon funkcie alebo za výkon pracovnej činnosti, údaje o odpracovanom rokoch práce vo verejnom záujme, údaje o zamestnávateľoch, pracovné zaradenie a deň začiatku výkonu práce vo verejnom záujme, údaje z potvrdenia o zamestnaní, údaje o čerpaní materskej dovolenky a rodičovskej dovolenky, údaje z dokladu o bezúhonnosti, údaje o priznaní dôchodku, o druhu dôchodku, osobné údaje spracúvané na oprávnení oboznamovať sa s utajovanými skutočnosťami, osobné údaje spracúvané na potvrdeniach, osvedčenia o absolvovaných skúškach a vzdelávacích aktivitách, fotografia na účely identifikácie na služobnom preukaze, výkon služby v služobnom pomere, údaje uvedené v životopise, trvalé bydlisko, prechodné bydlisko, údaje o vzdelaní, spôsobilosť na právne úkony, údaje z menovacích dekrétov, údaje o zdravotnej spôsobilosti, podpis
spis osôb vykonávajúcich prácu mimo pracovného pomeru	meno, priezvisko, rodné priezvisko a titul, dátum a miesto narodenia, podpis, dohodnutá hodinová odmena, údaje o zamestnávateľovi, deň začiatku výkonu práce, potvrdenie od školy o štatúte študenta, osobné údaje spracúvané na potvrdeniach, osvedčenia o absolvovaných skúškach a vzdelávacích aktivitách, trvalé bydlisko, prechodné bydlisko

evidencia dochádzky, dovolenky	meno, priezvisko, rodné priezvisko a titul, rodné číslo, dátum a miesto narodenia, podpis, miesto pobytu na dovolenke, útvár zamestnávateľa, údaje o odpracovanom čase, údaje o pracovnej neschopnosti, údaje o dôležitých osobných prekážkach v práci, údaje o zamestnávateľoch, pracovné zaradenie a deň začiatku výkonu štátnej služby alebo pracovnej činnosti, údaje o rodinných príslušníkoch v rozsahu meno, priezvisko, adresa, dátum narodenia, rodné číslo, údaje o manželovi alebo manželke, deťoch, rodičoch detí v rozsahu meno, priezvisko, dátum narodenia, rodné číslo, adresa, údaje o čerpaní materskej dovolenky a rodičovskej dovolenky, údaje o členstve v odborovej organizácii, osobné údaje spracúvané na potvrdeniach, osvedčenia o absolvovaných skúškach a vzdelávacích aktivitách, rodinný stav, trvalé bydlisko, prechodné bydlisko
dohody o hmotnej zodpovednosti	identifikačné údaje zamestnanca, údaje zamestnávateľa
služobné preukazy	identifikačné údaje, fotografia, podpis, osobné číslo, pracovné zaradenie, údaje zamestnávateľa
výberové konanie	osobné údaje uvedené v životopise, osobné údaje uvedené vo výpise z registra trestov, doklad o dosiahnutom vzdelaní
žiadosti o prijatie do zamestnania mimo výberového konania	osobné údaje uvedené v životopise
majetkové priznanie	identifikačné údaje, údaje týkajúce sa majetku uvedené v majetkovom priznaní, podpis, údaje o zamestnávateľovi
zmluvy	identifikačné a kontaktné údaje zmlúv strán, identifikačné údaje štatutárneho orgánu (fyzickej osoby) alebo inej osoby oprávnenej konať v mene zmluvnej strany, iné údaje nevyhnutné na plnenie zmluvy
evidencia uplatnených práv dotknutých osôb podľa Kapitoly III Nariadenia 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov	titul, meno, priezvisko, adresa a iné osobné údaje, ku ktorým sa vzťahuje uplatňované právo dotknutej osoby
správa registratúry	titul, meno, priezvisko, podpis, adresa, e-mailová adresa, telefónne číslo
spracovanie účtovných dokladov	meno, priezvisko, titul, adresa trvalého pobytu, adresa prechodného pobytu, telefónne číslo, e-mailová adresa, dátum narodenia, druh a číslo dokladu totožnosti, podpis, číslo bankového účtu fyzickej osoby, vyúčtovanie pracovnej cesty
kolektívna zmluva	identifikačné údaje, údaje týkajúce sa služobného voľna čerpaného na základe kolektívnej zmluvy, údaje týkajúce sa nárokov vyplývajúcich z kolektívnej zmluvy

3.1.2.4 Správnosť spracúvaných osobných údajov

Prevádzkovateľ prijal organizačné opatrenie spracúvať len správne a aktualizované osobné údaje, pričom boli prijaté organizačné ako aj technické opatrenia, ktoré umožnia aktualizáciu a prípadne aj výmaz nesprávnych osobných údajov, ktoré sú spracúvané v manuálnej forme, prípadne elektronicky.

3.1.2.5 Minimalizácia uchovávaní

Prevádzkovateľ prijal organizačné a technické opatrenia na zabezpečenie povinnosti spracúvať osobné údaje po dobu, ktorá je nevyhnutná pre účely, pre ktoré sa spracúvajú, pričom následne sú uchovávané v registratúrnom stredisku po dobu, ktorá je určená registratúrnym poriadkom

a registratúrnym plánom. Tieto doby sú vymedzené taktiež v kapitole 3.1.1.4 tejto smernice. Po uplynutí uvedeného času sa zabezpečuje likvidácia osobných údajov (skartácia, pokiaľ sú osobné údaje spracúvané v listinnej forme alebo výmaz, ak sú osobné údaje spracúvané v elektronickej forme).

3.1.2.6 Integrita a dôvernosť spracúvaných osobných údajov

Zásady integrity a dôvernosti, ktorých dodržiavanie je zabezpečené prijatím bezpečnostných opatrení pri práci s osobnými údajmi, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení, vrátane tejto bezpečnostnej smernice. Bližšie sú povinnosti v oblasti integrity a dôvernosti spracúvaných osobných údajov upravené v kapitolách 11 a 17 bezpečnostnej smernice.

3.1.3 Posúdenie rizika pre práva fyzických osôb v IS Personalistika a mzdy

Spracúvanie osobných údajov v IS Personalistika a mzdy má zákonný základ v osobitných právnych predpisoch. V rámci tohto IS dochádza k spracúvaniu bežných osobných údajov, v bežnom rozsahu, ktoré sú potrebné pre riadne plnenie povinností Prevádzkovateľa ako zamestnávateľa.

Spracúvanie osobných údajov v IS nepredstavuje riziko pre práva dotknutých osôb.

Automatizované spracúvanie osobných sa realizuje s využitím aplikačného programového vybavenia CJES podrobne popísaného v kapitole 3.12 Automatizované spracúvanie prostredníctvom CJES a ako záloha a archívne spracovanie sú využité predchádzajúce softvérové riešenia. Bezpečnostné opatrenia sú uvedené v kapitole 17 tejto smernice.

3.1.4 Monitorovanie a preskúvanie podmienok spracúvania osobných údajov v IS Personalistika a mzdy

Opatrenia prijaté na zabezpečenie pravidelného monitorovania podmienok spracúvania osobných údajov, vrátane kontroly zavedených postupov, sú uvedené v kapitole 18 smernice na ochranu osobných údajov.

3.2 IS Účtovníctvo

IS Účtovníctvo predstavuje informačný systém, v ktorom sú osobné údaje spracúvané v automatizovanej aj neautomatizovanej forme v pôsobnosti Ekonomického oddelenia. V rámci spracúvania osobných údajov v účtovnej agende zabezpečujú určené oprávnené osoby vedenie účtovníctva a účtovnej evidencie v predpísanom rozsahu, podľa platnej účtovnej osnovy a v súlade s osobitnými zákonmi.

3.2.1 Opis plánovaného spracúvania osobných údajov v IS Účtovníctvo

Účtovná agenda je v automatizovanej aj neautomatizovanej forme spracúvaná v pôsobnosti poverených a vecne oprávnených osôb (zamestnancov) Prevádzkovateľa (referentov Ekonomického oddelenia), ktorí zabezpečujú vedenie účtovníctva a účtovnej evidencie v predpísanom rozsahu, podľa platnej účtovnej osnovy a v zmysle osobitných zákonov, ktoré sú uvedené v čl. 3.2.2.1 tejto smernice a interných predpisov Prevádzkovateľa. Poverené oprávnené osoby s prístupom k osobným údajom v účtovnej agende boli náležitým spôsobom poučené o rozsahu povolených spracovateľských operácií a zásadách ochrany osobných údajov pri ich spracúvaní.

V rámci výhradne neautomatizovaného spracúvania údajov v účtovnej agende sú oprávneným osobám (zamestnancom) Prevádzkovateľa za účelom automatizovaného zaúčtovania (vedenia účtovníctva) postupované požadované podklady (dohody, zmluvy, účtovné a fakturačné

doklady), ktoré obsahujú alebo môžu obsahovať osobné údaje fyzických osôb v rozsahu potrebnom na ich zaúčtovanie.

Ochrana osobných údajov vedených v neautomatizovanej časti účtovnej agendy sa prioritne zabezpečuje riadeným prístupom do priestorov ich spracúvania, zamedzením prístupu neoprávnených osôb, dôsledným dodržiavaním požiadaviek administratívnej bezpečnosti pri vedení písomnej časti účtovnej agendy, ako je evidencia a obeh písomností, kontrolná činnosť, technicko-organizačné opatrenia na zamedzenie poškodenia alebo zničenia spracúvaných osobných údajov a zabezpečenie zákonných požiadaviek v rozsahu nakladania s osobnými údajmi v účtovnej agende po skončení účelu ich spracúvania (registratúra a archivácia písomností).

3.2.1.1 Účel spracúvania osobných údajov v IS

Účelom spracúvania osobných údajov v IS Účtovníctvo je evidencia fyzických osôb v rámci obchodnej činnosti, realizácie finančných operácií, platieb a vedenie účtovníctva, ktoré súvisí s nákupom alebo predajom tovarov a služieb na základe občianskoprávných, obchodnoprávných prípadne pracovnoprávných vzťahov a ich následné zúčtovanie.

3.2.1.2 Zoznam/rozsah osobných údajov v IS

Osobné údaje v IS Účtovníctvo obsahujú nasledujúce údaje:

- titul/tituly, meno a priezvisko,
- dátum narodenia,
- adresa trvalého bydliska,
- telefónne číslo,
- emailová adresa,
- číslo účtu,
- fakturovaná suma,
- podpis,
- tovar/služba.

3.2.1.3 Zoznam/okruh príjemcov

Osobné údaje môžu byť poskytované nasledujúcim príjemcom: daňový úrad, Policajný zbor SR, súdy, exekútor.

3.2.1.4 Vymedzenie obdobia uchovávania osobných údajov

Spôsob uchovávania je určený všeobecne záväznými právnymi predpismi a doba uchovávania jednotlivých dokumentov je stanovená v registratúrnom poriadku a registratúrnom pláne. Doba uchovávania účtovnej dokumentácie je stanovená v § 35 zákona č. 431/2002 o účtovníctve.

Spracovateľská operácia	Doba uchovávania (v rokoch)
Spracovanie účtovných dokladov	10

3.2.1.5 Dotknuté osoby v IS

Dotknutými osobami v IS Účtovníctvo sú osoby evidované v rámci obchodnej činnosti a realizácie finančných operácií.

3.2.2 Posúdenie nevyhnutnosti a primeranosti

3.2.2.1 Zákonnosť spracúvania osobných údajov

Právny základ a účel spracúvania osobných údajov v IS Účtovníctvo je vymedzený nasledujúcimi osobitnými zákonmi:

Číslo predpisu	Názov predpisu
431/2002 Z. z.	Zákon o účtovníctve v znení neskorších predpisov
222/2004 Z. z.	Zákon o dani z pridanej hodnoty v znení neskorších predpisov
	a ďalšie

3.2.2.2 Obmedzenie účelu

Prevádzkovateľ zohľadnil zásadu obmedzenia účelu spracúvania osobných údajov prijatím organizačných opatrení, ktorými bolo určené povereným osobám získavať osobné údaje na konkrétny účel, ktorým je vedenie účtovníctva a súvisiacich povinností, ktoré vyplývajú z daňových a účtovných zákonov. Osobné údaje nie je možné spracúvať na iné účely, táto povinnosť bola uložená všetkým povereným osobám ako základná povinnosť pri spracúvaní osobných údajov. Tieto účely sú legitímne, sú určené všeobecne záväznými právnymi predpismi vzťahujúcimi sa na oblasť zamestnávania.

3.2.2.3 Minimalizácia osobných údajov

Prevádzkovateľ prijal opatrenia, aby sa na každú spracovateľskú operáciu využíval len taký osobný údaj, ktorý je preukázateľne potrebný a nevyhnutný pre plnenie stanoveného účelu spracúvania.

Spracovateľská operácia	Spracúvané osobné údaje v rámci spracovateľskej operácie
spracovanie účtovných dokladov	meno, priezvisko, titul, adresa trvalého pobytu, adresa prechodného pobytu, telefónne číslo, e-mailová adresa, dátum narodenia, druh a číslo dokladu totožnosti, podpis, číslo bankového účtu fyzickej osoby, vyúčtovanie pracovnej cesty

3.2.2.4 Správnosť spracúvaných osobných údajov

Prevádzkovateľ prijal organizačné opatrenie spracúvať len správne a aktualizované osobné údaje, pričom boli prijaté organizačné ako aj technické opatrenia, ktoré umožnia aktualizáciu a prípadne aj výmaz nesprávnych osobných údajov, ktoré sú spracúvané v manuálnej forme, prípadne elektronicky.

3.2.2.5 Minimalizácia uchovávania

Prevádzkovateľ prijal organizačné a technické opatrenia na zabezpečenie povinnosti spracúvať osobné údaje po dobu, ktorá je nevyhnutná pre účely, pre ktoré sa spracúvajú, pričom následne sú uchovávané v registratúrnom stredisku po dobu, ktorá je určená registratúrnym poriadkom a registratúrnym plánom. Tieto doby sú vymedzené taktiež v bode 3.2.1.4 tejto smernice. Po uplynutí uvedeného času sa zabezpečuje likvidácia osobných údajov (skartácia, pokiaľ sú osobné údaje spracúvané v listinnej forme alebo výmaz, ak sú osobné údaje spracúvané v elektronickej forme).

3.2.2.6 Integrita a dôvernosť spracúvaných osobných údajov

Zásady integrity a dôvernosti, ktorých dodržiavanie je zabezpečené prijatím bezpečnostných opatrení pri práci s osobnými údajmi, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení, vrátane tejto bezpečnostnej smernice.

Bližšie sú povinnosti v oblasti integrity a dôvernosti spracúvaných osobných údajov upravené v kapitolách 11 a 17 bezpečnostnej smernice.

3.2.3 Posúdenie rizika pre práva fyzickej osoby v IS Účtovníctvo

Spracúvanie osobných údajov v IS Účtovníctvo má zákonný základ v osobitných právnych predpisoch. V rámci tohto IS dochádza k spracúvaniu bežných osobných údajov, v bežnom rozsahu, ktoré sú potrebné pre riadne plnenie povinností Prevádzkovateľa vyplývajúcich z daňových právnych predpisov.

Spracúvanie osobných údajov v IS nepredstavuje riziko pre práva dotknutých osôb.

3.2.3.1 Automatizované spracúvanie účtovnej agendy

Automatizované spracúvanie osobných údajov v účtovnej agende sa vykonáva v zmysle stanoveného účelu ich spracúvania, v rozsahu a za podmienok určených Prevádzkovateľom. Pri automatizovanom spracúvaní osobných údajov sú Prevádzkovateľom aplikované požadované technické, organizačné a personálne opatrenia, ktoré sú podrobne popísané v čl. 17 tejto smernice.

Pri automatizovanom spracúvaní údajov v účtovnej agende sa osobné údaje dotknutých osôb nespracúvajú.

3.2.3.2 Neautomatizované spracúvanie účtovnej agendy

V rámci výhradne neautomatizovaného spracúvania údajov v účtovnej agende sú oprávneným osobám (referentom Úseku ekonomiky a referenta pre styk so Štátnou pokladnicou) za účelom automatizovaného zaúčtovania (vedenia účtovníctva) poskytované v písomnej forme požadované podklady (dohody a autorské zmluvy), ktoré obsahujú osobné údaje dotknutých osôb v rozsahu potrebnom na zaúčtovanie.

Ochrana osobných údajov využívaných ako podklady účtovnej agendy sa prioritne zabezpečuje riadeným prístupom do priestorov ich spracúvania, požadovanou evidenciou, obehom a ukladaním písomností obsahujúcich osobné údaje dotknutých osôb.

3.2.4 Monitorovanie a preskúmanie podmienok spracúvania osobných údajov v IS Účtovníctvo

Opatrenia prijaté na zabezpečenie pravidelného monitorovania podmienok spracúvania osobných údajov, vrátane kontroly zavedených postupov, v kapitole 18 smernice na ochranu osobných údajov.

3.3 IS Zmluvy

Informačný systém Zmluvy (ďalej len „IS Zmluvy“) obsahuje databázu zmlúv uzatvorených najmä podľa zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov, zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov, zákona č. 185/2015 Z. z. Autorský zákon. Tieto zmluvy sú základom pre uzatváranie zmluvných záväzkových vzťahov s fyzickými osobami a zároveň sú právnym základom pre spracúvanie účtovných povinností Prevádzkovateľa vyplývajúcich z osobitných daňových predpisov. Zmluvy sú spracúvané elektronicky ako aj manuálne, uložené sú na Oddelení riaditeľky.

3.3.1 Opis plánovaného spracúvania osobných údajov v IS Zmluvy

Prevádzkovateľ pri plnení svojich úloh vstupuje do zmluvných vzťahov, tak s právnickými osobami, ako aj s fyzickými osobami. Za tým účelom dochádza k uzatváraniu zmlúv, ktoré upravujú vzájomné práva a povinnosti zmluvných strán.

V rámci IS Zmluvy sa spracúva databáza uzatvorených zmlúv. Zmluvy sú spracúvané v automatizovanej podobe a vo fyzickej (papierovej) podobe. Podpísané zmluvy sú uchovávané na Oddelení riaditeľky, následne sú presúvané do registratúrneho strediska. Pri elektronickom spracúvaní dochádza k skenovaniu zmlúv a ich nahratiu do Centrálného registra zmlúv v zmysle zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov.

3.3.1.1 Účel spracúvania osobných údajov

Účelom spracúvania osobných údajov v IS Zmluvy je evidencia a spracúvanie zmlúv podľa zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov, zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov, zákona č. 185/2015 Z. z. Autorský zákon. Uzatvorené zmluvy sú právnym podkladom pre plnenie predmetu jednotlivých zmlúv. Zmluvy sú taktiež podkladom pre realizáciu finančných operácií, platieb a vedenie účtovníctva, ktoré súvisí s výplatom v zmysle dohodnutých zmluvných podmienok.

3.3.1.2 Zoznam/rozsah osobných údajov v IS Zmluvy

Zmluvy obsahujú najmä nasledujúce identifikačné údaje zmluvných strán (fyzických osôb – účastníkov zmluvy ako aj osôb konajúcich v mene právnických osôb) ako aj ďalšie údaje:

- titul/tituly, meno a priezvisko,
- dátum narodenia,
- rodné číslo,
- adresa,
- telefónne číslo,
- emailová adresa,
- číslo účtu,
- IBAN,
- SWIFT,
- predmet zmluvy,
- finančné záväzky.

3.3.1.3 Zoznam/okruh príjemcov

Osobné údaje môžu byť poskytované nasledujúcim príjemcom: Policajný zbor SR, súdy, exekútor.

3.3.1.4 Vymedzenie obdobia uchovávania osobných údajov

Spôsob uchovávania je určený všeobecne záväznými právnymi predpismi a doba uchovávania jednotlivých dokumentov je stanovená v zákone č. 395/2002 Z. z. o archívoch a registratúrach ako v Registratúrnom pláne a Registratúrnom poriadku. Táto doba je 10 rokov od uzatvorenia zmluvy, prípadne od jej skončenia, ak ide o rámcové, prípadne zmluvy, ktoré sú uzatvorené na dlhší čas.

3.3.1.5 Dotknuté osoby v IS Zmluvy

Dotknutými osobami v rámci IS Zmluvy sú osoby, ktoré vstupujú do záväzkových vzťahov s Prevádzkovateľom a s ktorými Prevádzkovateľ uzatvára zmluvný vzťah, prípadne osoby, ktoré konajú v mene právnických osôb.

3.3.2 Posúdenie nevyhnutnosti a primeranosti

3.3.2.1 Zákonnosť spracúvania osobných údajov

Právnym základom pre spracúvanie osobných údajov je článok 6 ods. 1 písm.) b) nariadenia GDPR, keďže spracúvanie osobných údajov je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo aby sa na základe žiadosti dotknutej osoby vykonali opatrenia

pred uzatvorením zmluvy, účelom teda je plnenie zmluvy, v ktorej dotknutá osoba vystupuje ako jedna zo zmluvných strán, alebo v predzmluvných vzťahoch s dotknutou osobou alebo pri rokovaní o zmene zmluvy, ktoré sa uskutočňujú na žiadosť dotknutej osoby.

Spracúvanie osobných údajov sa taktiež riadi nasledujúcimi zákonmi:

Číslo predpisu	Názov predpisu
40/1964 Zb.	Občiansky zákonník v znení neskorších predpisov
513/1991 Zb.	Obchodný zákonník v znení neskorších predpisov
185/2015 Z. z.	Autorský zákon
595/2003 Z. z.	Zákon o dani z príjmov v znení neskorších predpisov
563/2009 Z. z.	Zákon o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
431/2002 Z. z.	Zákon o účtovníctve v znení neskorších predpisov
222/2004 Z. z.	Zákon o dani z pridanej hodnoty v znení neskorších predpisov
18/2018 Z. z.	Zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
395/2002 Z. z.	Zákon o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov

3.3.2.2 Obmedzenie účelu

Prevádzkovateľ zohľadnil zásadu obmedzenia účelu spracúvania osobných údajov prijatím organizačných opatrení, ktorými bolo určené povereným osobám získavať osobné údaje od zmluvných strán výhradne na účely uzatvorenia zmluvy a jej realizácie, za podmienok, ktoré samotná zmluva určuje.

Osobné údaje nie je možné spracúvať na iné účely, táto povinnosť bola uložená všetkým povereným osobám ako základná povinnosť pri spracúvaní osobných údajov. Osobné údaje sú spracúvané výhradne poverenými osobami.

V prípade, ak sa zmluva nachádza k registratúrnemu stredisku, prístup k takejto zmluve je obmedzený výhradne pre určené osoby a v súvislosti s plnením zmluvných podmienok a nárokov vyplývajúcich z uzatvorenej zmluvy.

3.3.2.3 Minimalizácia osobných údajov

Prevádzkovateľ prijal opatrenia, aby sa na každú spracovateľskú operáciu využíval len taký osobný údaj, ktorý je preukázateľne potrebný a nevyhnutný pre plnenie stanoveného účelu spracúvania.

Spracovateľská operácia	Spracúvané osobné údaje v rámci spracovateľskej operácie
Vedenie zmluvnej dokumentácie	Rozsah: identifikačné a kontaktné údaje zmlúv strán, identifikačné údaje štatutárneho orgánu (fyzickej osoby) alebo inej osoby oprávnenej konať v mene zmluvnej strany, iné údaje nevyhnutné na plnenie zmluvy

3.3.2.4 Správnosť spracúvaných osobných údajov

Prevádzkovateľ prijal organizačné opatrenie spracúvať len správne a aktualizované osobné údaje, pričom boli prijaté organizačné ako aj technické opatrenia, ktoré umožnia aktualizáciu a prípadne aj výmaz nesprávnych osobných údajov, ktoré sú spracúvané v manuálnej forme, prípadne elektronicky. Osobné údaje poskytujú fyzické osoby, s ktorými sa uzatvára zmluva, v prípade osôb, ktoré konajú za právnické osoby sa správnosť poskytnutých osobných údajov preveruje nahliadnutím do verejne dostupných databáz (Obchodný register, živnostenský register).

3.3.2.5 Minimalizácia uchovávaní

Prevádzkovateľ prijal organizačné a technické opatrenia na zabezpečenie povinnosti spracúvať osobné údaje po dobu, ktorá je nevyhnutná pre účely, pre ktoré sa spracúvajú, pričom tieto doby uchovávaní sú určené právnymi predpismi regulujúcimi spracúvanie archívnych dokumentov. Tieto doby sú vymedzené taktiež v bode 3.3.1.4 tejto smernice. Keďže bádateľský list predstavuje archívny dokument, osobné údaje v ňom uvedené je možné likvidovať len po skončení vyradovacieho konania.

3.3.2.6 Integrita a dôvernosť spracúvaných osobných údajov

Zásady integrity a dôvernosti, ktorých dodržiavanie je zabezpečené prijatím bezpečnostných opatrení pri práci s osobnými údajmi, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení, vrátane tejto bezpečnostnej smernice. Bližšie sú povinnosti v oblasti integrity a dôvernosti spracúvaných osobných údajov upravené v kapitolách 11 a 17 bezpečnostnej smernice na ochranu osobných údajov.

3.3.3 Posúdenie rizika pre práva fyzickej osoby v IS Zmluvy

Spracúvanie osobných údajov v IS Zmluvy má zákonný základ, spracúvanie osobných údajov vyplýva z čl. 6 ods. 1 písm. b) nariadenia GDPR. V rámci tohto IS dochádza k spracúvaniu bežných osobných údajov, v rozsahu, ktorý zodpovedá potrebe identifikácie zmluvných strán a z následných povinností, ktoré vyplývajú pre zmluvné strany, napríklad voči iným subjektom (napr. daňový úrad, súdy, Sociálna poisťovňa a pod.).

Spracúvanie osobných údajov v IS nepredstavuje riziko pre práva dotknutých osôb.

3.3.4 Monitorovanie a preskúmanie podmienok spracúvania osobných údajov v IS Zmluvy

Opatrenia prijaté na zabezpečenie pravidelného monitorovania podmienok spracúvania osobných údajov, vrátane kontroly zavedených postupov, v kapitole 18 bezpečnostnej smernice na ochranu osobných údajov.

3.4 IS Registratúra**3.4.1 Opis plánovaného spracúvania osobných údajov v IS Registratúra**

K spracúvaniu osobných údajov v informačnom systéme IS Registratúra dochádza v rámci všetkých organizačných útvarov Prevádzkovateľa. Účel spracúvania vyplýva zo zákona č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov a je ním úprava práv a povinností Prevádzkovateľa ako pôvodcu registratúry. Registratúrny poriadok a registratúrny plán stanovujú konkrétne práva a povinnosti pôvodcu. Prístup k dokumentom, ktoré sa nachádzajú v budove Prevádzkovateľa, je regulovaný a len pre výhradne určené osoby.

Prevádzkovateľ využíva pri správe registratúr automatizované spracúvanie osobných údajov, ktoré sa vykonáva s využitím NUNTIO ASSR od spoločnosti DIMANO, a. s. Automatizované spracúvanie je bližšie popísané v kapitole 3.13 tejto smernice.

3.4.1.1 Účel spracúvania osobných údajov

Účel spracúvania osobných údajov v IS Registratúra je vymedzený zákonom č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov, ktorý upravuje práva a povinnosti Prevádzkovateľa ako pôvodcu registratúry. Konkrétne práva a povinnosti v oblasti správy registratúry stanovuje Registratúrny poriadok a registratúrny plán Prevádzkovateľa, ktorý určuje pravidlá a postupy pri prijímaní, evidencii, tvorbe a manipulácii

so záznamami (spismi) tak, aby nedošlo k ich poškodeniu, zničeniu, strate alebo zneužitiu. Cieľom Registratúrneho poriadku a plánu je upraviť postup organizačných zložiek Prevádzkovateľa v oblasti správy registratúry (príjem, evidencia, tvorba, vybavovanie, ukladanie, ochrana a prístup k záznamom (spisom), ich odovzdávanie do Registratúrneho strediska a zabezpečovanie pravidelného vyraďovania registratúrnych záznamov bez dokumentárnej hodnoty po uplynutí úložných lehôt).

3.4.1.2 Zoznam/rozsah osobných údajov v IS Registratúra

V IS Registratúra dochádza k spracúvaniu registratúrnych záznamov (spisov) Prevádzkovateľa a k ich prístupu zamestnancami Prevádzkovateľa pre prevádzkové účely. Registratúrne záznamy (spisy) môžu obsahovať osobné údaje v rozsahu uvedenom v predchádzajúcich informačných systémoch, podľa druhu a typu dokumentu.

3.4.1.3 Zoznam/okruh príjemcov

Osobné údaje nie sú poskytované tretím subjektom. Môžu však byť, v prípade potreby, príjemcom podľa osobitných právnych predpisov, ktoré vymedzujú účel spracúvania osobných údajov.

3.4.1.4 Vymedzenie obdobia uchovávanía osobných údajov

Spôsob uchovávanía je určený všeobecne záväznými právnymi predpismi a doba uchovávanía jednotlivých dokumentov je stanovená v zákone č. 395/2002 Z. z. o archívoch a registratúrach ako aj v Registratúrnom pláne a Registratúrnom poriadku Prevádzkovateľa.

Jednotlivé doby uchovávanía sú stanovené nasledovne: 10 rokov (registratúrny denník), 5 rokov (preberacie zoznamy spisov odovzdaných do registratúrneho strediska), 5 rokov (evidencia vypožičaných spisov z registratúrneho strediska), 10 rokov (vyraďovacie konanie), 5 rokov (evidencia obehu registratúrnych záznamov a spisov), 5 rokov (evidencia evidenčných pomôcok).

3.4.1.5 Dotknuté osoby v IS Registratúra

Dotknutými osobami v rámci IS Registratúra sú osoby uvedené na príslušných dokumentoch vznikajúcich pri činnosti Prevádzkovateľa.

3.4.2 Posúdenie nevyhnutnosti a primeranosti

3.4.2.1 Zákonnosť spracúvania osobných údajov

Právnym základom spracúvania osobných údajov v IS Registratúra je zákon č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov.

Spracúvanie osobných údajov v IS Registratúra sa riadi taktiež nasledujúcimi právnymi predpismi:

Číslo predpisu	Názov predpisu
18/2018 Z. z.	Zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
628/2002 Z. z.	Vyhláška MV SR, ktorou sa vykonávajú niektoré ustanovenia zákona o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov

3.4.2.2 Obmedzenie účelu

Prevádzkovateľ zohľadnil zásadu obmedzenia účelu spracúvania osobných údajov prijatím organizačných opatrení, ktorými bolo určené povereným osobám získavať osobné údaje od zmluvných strán výhradne na účely správy registratúry a uchovávanía dokumentov

prostredníctvom elektronickej správy registratúry, v prípade vytlačených dokumentov manuálne v registratúrnom stredisku.

Osobné údaje nie je možné spracúvať na iné účely, než na účely správy registratúry, pričom osobné údaje v uchovávaných dokumentoch sú chránené prostredníctvom obmedzeného prístupu k týmto osobným údajom, ktoré možno využiť výhradne na zákonné účely, prípadne na účely, pre ktoré boli získané. Osobné údaje sú spracúvané výhradne poverenými osobami.

3.4.2.3 Minimalizácia osobných údajov

Prevádzkovateľ prijal opatrenia, aby sa na každú spracovateľskú operáciu využíval len taký osobný údaj, ktorý je preukázateľne potrebný a nevyhnutný pre plnenie stanoveného účelu spracúvania, vrátane rozsahu uchovávaných údajov pre účely správy registratúry.

Spracovateľská operácia	Spracúvané osobné údaje v rámci spracovateľskej operácie
Vedenie registratúry	Rozsah: identifikačné údaje (titul, meno a priezvisko, podpis, adresa, e-mailová adresa, telefónne číslo) + ďalšie údaje na dokumente, ktorý je uchovávaný

3.4.2.4 Správnosť spracúvaných osobných údajov

Prevádzkovateľ prijal organizačné opatrenie spracúvať len správne a aktualizované osobné údaje, pričom boli prijaté organizačné ako aj technické opatrenia, ktoré umožnia aktualizáciu a prípadne aj výmaz nesprávnych osobných údajov, ktoré sú spracúvané elektronicke ako aj manuálne. Osobné údaje poskytujú fyzické osoby, ktoré pričom tieto sa nachádzajú na príslušných dokumentoch.

3.4.2.5 Minimalizácia uchovávania

Prevádzkovateľ prijal organizačné a technické opatrenia na zabezpečenie povinnosti spracúvať osobné údaje po dobu, ktorá je nevyhnutná pre účely, pre ktoré sa spracúvajú, pričom tieto doby sú vymedzené taktiež v bode 3.4.1.4 tejto smernice. Po skončení tejto doby je registratúrny záznam likvidovaný.

3.4.2.6 Integrita a dôvernosť spracúvaných osobných údajov

Zásady integrity a dôvernosti, ktorých dodržiavanie je zabezpečené prijatím bezpečnostných opatrení pri práci s registratúrnymi záznamami, vrátane ochrany pred neoprávneným prístupom k registratúrnym záznamom. Za tým účelom boli najmä vymedzené oprávnenia pre poverené osoby, ktoré vymedzujú prístup k príslušným registratúrnym záznamom – či už ide o registratúrne záznamy uchovávané elektronicke alebo fyzicky v registratúrnom stredisku. Bližšie sú povinnosti v oblasti integrity a dôvernosti spracúvaných osobných údajov upravené v kapitolách 11 a 17 bezpečnostnej smernice na ochranu osobných údajov.

3.4.3 Posúdenie rizika pre práva fyzickej osoby v IS Registratúra

Spracúvanie osobných údajov v IS Registratúra má zákonný základ v osobitných právnych predpisoch. V rámci tohto IS dochádza k spracúvaniu bežných osobných údajov, v rozsahu, ktorý je určený všeobecne záväznými právnymi predpismi vzťahujúcimi sa na oblasť správy registratúry, ktoré sú potrebné pre riadne plnenie povinností Prevádzkovateľa vyplývajúcich z právnych predpisov.

Spracúvanie osobných údajov v IS nepredstavuje riziko pre práva dotknutých osôb.

3.4.4 Monitorovanie a preskúmanie podmienok spracúvania osobných údajov v IS Registratúra

Opatrenia prijaté na zabezpečenie pravidelného monitorovania podmienok spracúvania osobných údajov, vrátane kontroly zavedených postupov, v kapitole 18 bezpečnostnej smernice na ochranu osobných údajov.

3.5 IS Archív DÚ

Informačný systém Archív DÚ integruje spracúvanie osobných údajov v IS, ktorým sa zabezpečuje archívna činnosť vykonávaná DÚ. DÚ vykonáva v rámci tohto IS i evidenciu divadelníkov v zmysle zákona č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov.

3.5.1 Opis plánovaného spracúvania osobných údajov v IS

V IS Archív DÚ dochádza k spracúvaniu archívnych dokumentov získaných akvizičnou činnosťou. Tieto môžu obsahovať osobné údaje podľa druhu dokumentu, ich spracúvanie a sprístupňovanie sa koná v súlade so zákonom č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov. Prístup do priestorov študovne Archívu DÚ (Jakubovo námestie 12, Bratislava) majú výhradne určené osoby ako aj osoby, ktoré požadujú štúdium archívnych dokumentov. Priestory archívu sú zabezpečené proti násilnému vniknutiu, priestory sú chránené elektrozabezpečovacou a požiarou signalizáciou.

V IS Archív DÚ dochádza k spracúvaniu archívnych dokumentov, ktoré môžu obsahovať osobné údaje podľa druhu a typu dokumentu. Pravidlá práce s archívnymi dokumentmi okrem všeobecne záväzných právnych predpisov upravuje aj Bádateľský poriadok Archívu Divadelného ústavu (vydaný dňa 1.1.2018), ktorý je dostupný na webovom sídle DÚ: <http://www.theatre.sk/sk/divadelny-ustav/dokumenty/>

Prístup k archívnym dokumentom využívajú domáci i zahraniční bádatelia na vedecké, študijné a prevádzkové účely. O archívny dokument môže bádateľ požiadať prostredníctvom žiadanky, ktorá je dostupná priamo v študovni Archívu DÚ.

3.5.1.1 Účel spracúvania osobných údajov

Účelom spracúvania osobných údajov v IS Archív DÚ je evidencia bádateľov pre potreby evidencie bádateľských listov a finančných prostriedkov v súlade so zákonom č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov. Spracúvanie osobných údajov v archíve je vymedzené osobitnými zákonmi, ktoré sú ďalej konkretizované v jednotlivých popisoch činností IS.

3.5.1.2 Zoznam/rozsah osobných údajov v IS

Evidencia bádateľov obsahuje osobné údaje v súlade s podmienkami uvedenými v § 12 ods. 4 zákona č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov. Tieto osobné údaje sa nespracovávajú a neposkytujú tretej osobe, len v prípade dôvodného podozrenia z poškodenia, straty alebo zničenia archívneho dokumentu.

Pri prihlasovaní dotknutej osoby za bádateľa sú archívy oprávnené získavať a uchovávať osobné údaje dotknutej osoby – bádateľa v súlade s podmienkami uvedenými v § 12 ods. 4 zákona č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov v rozsahu:

- meno, priezvisko, titul,
- dátum a miesto narodenia,
- rodné číslo,
- adresa trvalého/prechodného pobytu,

- telefónne/faxové číslo, emailová adresa,
- číslo občianskeho preukazu alebo číslo cestovného dokladu.

3.5.1.3 Zoznam/okruh príjemcov

Osobné údaje môžu byť poskytované nasledujúcim príjemcom: Policajný zbor SR, súdy.

3.5.1.4 Vymedzenie obdobia uchovávaní osobných údajov

Spôsob uchovávaní je určený všeobecne záväznými právnymi predpismi a doba uchovávaní jednotlivých dokumentov je stanovená v zákone č. 395/2002 Z. z. o archívoch a registratúrach ako v Bádateľskom poriadku Archívu DÚ.

Spracovateľská operácia	Doba uchovávaní (v rokoch)
Uchovávanie archívnych dokumentov, vrátane bádateľského listu, ktorý je považovaný za archívny dokument	Archívny dokument možno zlikvidovať po skončení vyrad'ovacieho konania

3.5.1.5 Dotknuté osoby v IS

Dotknutými osobami v rámci IS Archív DÚ sú bádатели a používatelia Archívu DÚ.

3.5.2 Posúdenie nevyhnutnosti a primeranosti

3.5.2.1 Zákonnosť spracúvaní osobných údajov

Právnym základom spracúvaní osobných údajov v IS Archív DÚ je zákon č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov.

Spracúvanie osobných údajov v IS Archív DÚ sa riadi taktiež nasledujúcimi právnymi predpismi:

Číslo predpisu	Názov predpisu
18/2018 Z. z.	Zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
628/2002 Z. z.	Vyhláška MV SR, ktorou sa vykonávajú niektoré ustanovenia zákona o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov

3.5.2.2 Obmedzenie účelu

Prevádzkovateľ zohľadnil zásadu obmedzenia účelu spracúvaní osobných údajov prijatím organizačných opatrení, ktorými bolo určené povereným osobám získavať osobné údaje od bádateľov na účel ich evidencie, v zmysle požiadaviek zákona č. 395/2002 Z. z. o archívoch a registratúrach.

Osobné údaje nie je možné spracúvať na iné účely, táto povinnosť bola uložená všetkým povereným osobám ako základná povinnosť pri spracúvaní osobných údajov.

Vo vzťahu k osobným údajom nachádzajúcim sa v archívnych dokumentoch je rešpektovaný zákon o archívoch a registratúrach, ktorý vymedzuje podmienky sprístupnenia osobných údajov v archívnych dokumentoch, vrátane osôb, ktorým takéto dokumenty môžu byť sprístupnené.

3.5.2.3 Minimalizácia osobných údajov

Prevádzkovateľ prijal opatrenia, aby sa na každú spracovateľskú operáciu využíval len taký osobný údaj, ktorý je preukázateľne potrebný a nevyhnutný pre plnenie stanoveného účelu spracúvania.

Spracovateľská operácia	Spracúvané osobné údaje v rámci spracovateľskej operácie
spracúvanie osobných údajov bádateľov	Rozsah spracúvaných osobných údajov bádateľov (žiadateľov o prístup k archívnym dokumentom) je vymedzený § 12 ods. 4 zákona č. 395/2002 Z. z. o archívoch a registratúrach, pričom Prevádzkovateľ nespracúva osobné údaje nad rámec zákonom stanoveného rozsahu
Získavanie údajov bádateľmi	Rozsah osobných údajov je v rozsahu uvedenom na dokumente, ktorý je predmetom výskumnej a bádateľskej činnosti

3.5.2.4 Správnosť spracúvaných osobných údajov

Prevádzkovateľ prijal organizačné opatrenie spracúvať len správne a aktualizované osobné údaje, pričom boli prijaté organizačné ako aj technické opatrenia, ktoré umožnia aktualizáciu a prípadne aj výmaz nesprávnych osobných údajov, ktoré sú spracúvané v manuálnej forme, prípadne elektronicky. Správnosť poskytnutých osobných údajov bádateľov sa preveruje nahliadnutím do preukazu totožnosti osoby žiadajúcej prístup k archívnemu dokumentu. Bádateľský list sa následne stáva archívnym dokumentom, ktorým Prevádzkovateľ uchováva v zmysle právnym predpisov.

3.5.2.5 Minimalizácia uchovávania

Prevádzkovateľ prijal organizačné a technické opatrenia na zabezpečenie povinnosti spracúvať osobné údaje po dobu, ktorá je nevyhnutná pre účely, pre ktoré sa spracúvajú, pričom tieto doby uchovávania sú určené právnymi predpismi regulujúcimi spracúvanie archívnych dokumentov. Tieto doby sú vymedzené taktiež v bode 3.7.1.4 tejto analýzy. Keďže bádateľský list predstavuje archívny dokument, osobné údaje v ňom uvedené je možné likvidovať len po skončení vyradovacieho konania.

3.5.2.6 Integrita a dôvernosť spracúvaných osobných údajov

Zásady integrity a dôvernosti, ktorých dodržiavanie je zabezpečené prijatím bezpečnostných opatrení pri práci s osobnými údajmi, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení, vrátane tejto bezpečnostnej smernice. Bližšie sú povinnosti v oblasti integrity a dôvernosti spracúvaných osobných údajov upravené v kapitolách 11 a 17 bezpečnostnej smernice.

3.5.3 Posúdenie rizika pre práva fyzickej osoby v IS

Spracúvanie osobných údajov v IS Archív DÚ má zákonný základ v osobitných právnych predpisoch (zákon č. 395/2002 Z. z. o archívoch a registratúrach). V rámci tohto IS dochádza k spracúvaniu bežných osobných údajov, v rozsahu, ktorý je určený všeobecne záväznými právnymi predpismi vzťahujúcimi sa na oblasť archívnictva, ktoré sú potrebné pre riadne plnenie povinností Prevádzkovateľa.

Spracúvanie osobných údajov v IS nepredstavuje riziko pre práva dotknutých osôb.

3.5.4 Monitorovanie a preskúmanie podmienok spracúvania osobných údajov v IS

Opatrenia prijaté na zabezpečenie pravidelného monitorovania podmienok spracúvania osobných údajov, vrátane kontroly zavedených postupov, v kapitole 18 bezpečnostnej smernice na ochranu osobných údajov.

3.6 IS Knižnica

3.6.1 Opis plánovaného spracúvania osobných údajov v IS Knižnica

Informačný systém Knižnica je spracovaný na základe zákona č. 126/2015 Z. z. o knižniciach. V uvedenom IS sú osobné údaje spracúvané za účelom evidencie používateľov knižnično-informačných služieb pre potreby ich dosiahnuteľnosti a evidencie finančných prostriedkov a výpožičných listov a ostatných činností, ktoré súvisia s prevádzkou a činnosťou knižnice.

Podmienkou spracúvania osobných údajov vo všetkých súčiastiach KIS je získanie osobných údajov dotknutej osoby. Súhlas dotknutej osoby nie je potrebné získať, keďže dochádza k spracúvaniu osobných údajov pre účely plnenia zmluvy, v ktorej vystupuje dotknutá osoba ako jedna zo zmluvných strán (vypožičiavanie knižničných dokumentov je v zmysle § 16 ods. 6 zákona č. 126/2015 Z. z. o knižniciach záväzkovým právnym vzťahom).

Používateľom knižnice DÚ sa fyzická alebo právnická osoba stáva vystavením preukazu čitateľa. Podpísaním prihlášky čitateľa sa čitateľ zaväzuje, že bude plniť ustanovenia Knižničného poriadku.

Spracúvanie osobných údajov pre potreby vydania čitateľského preukazu a aktivácie do knižničného systému sa vykonáva v zmysle platnej legislatívnej úpravy ochrany osobných údajov – DÚ sa zaväzuje použiť poskytnuté osobné údaje len pre svoju vnútornú potrebu.

V IS Knižnica bol v roku 2011 zavedený integrovaný knižničný systém CLAVIUS, ktorý integruje viacero aplikácií, vrátane evidencie čitateľov a výpožičiek, evidencie poplatkov čitateľov, prolongácií a upomienok. Knižničný systém umožňuje komplexnú správu knižničného fondu, vrátane celkovej evidencie o knihách. Umožňuje zistiť dátumy vrátenia dokumentov, obsahuje informácie o poplatkoch, upomienkach a rezerváciách.

3.6.1.1 Účel spracúvania osobných údajov v IS

Účelom spracúvania osobných údajov je evidencia čitateľov pre potreby ich dosiahnuteľnosti a evidencii finančných prostriedkov a výpožičných listov v súlade so zákonom o knižniciach a činností spojených s bádateľskou činnosťou. Uvedený účel spracúvania osobných údajov je vymedzený osobitnými zákonmi, ktorý je ďalej konkretizovaný v jednotlivých popisoch činností IS.

3.6.1.2 Zoznam/rozsah osobných údajov spracúvaných v IS

V automatizovanom aj neautomatizovanom IS sú spracúvané nasledujúce osobné údaje:

Osobné údaje detského čitateľa:

1. meno
2. priezvisko
3. dátum narodenia
4. miesto narodenia
5. adresa trvalého bydliska
6. adresa prechodného bydliska
7. najvyššie dosiahnuté vzdelanie (základné, stredoškolské, vysokoškolské)
8. telefónne číslo
9. emailová adresa
10. status osoby (žiak, študent, a i., pre účel poskytnutia zľavy alebo zvýhodnenia)

Osobné údaje zákonného zástupcu dieťaťa:

1. meno
2. priezvisko
3. adresa

Osobné údaje čitateľa staršieho ako 15 rokov:

1. titul,
2. meno
3. priezvisko
4. dátum narodenia
5. miesto narodenia
6. adresa trvalého bydliska
7. adresa prechodného bydliska
8. číslo dokladu totožnosti (občianskeho preukazu, cestovného pasu)
9. doba platnosti dokladu totožnosti
10. najvyššie dosiahnuté vzdelanie (základné, stredoškolské, vysokoškolské)
11. telefónne číslo
12. e-mailová adresa
13. status osoby (študent, dôchodca, a i., pre účel poskytnutia zľavy alebo zvýhodnenia)

3.6.1.3 Zoznam/okruh príjemcov

Osobné údaje nie sú poskytované ďalším príjemcom, sú spracúvané výhradne zamestnancami a poverenými osobami Prevádzkovateľa. V osobitných prípadoch (napríklad vymáhanie nedoplatku, nevrátenej výpožičky) môžu byť osobné údaje čitateľa sprístupnené iným subjektom, avšak len za účelom uspokojenia pohľadávky Prevádzkovateľa (súdy, advokátska kancelária).

3.6.1.4 Vymedzenie obdobia uchovávanía osobných údajov

Osobné údaje sú spracúvané po dobu trvania záväzkového vzťahu ako aj dva roky po skončení. V prípade uplatňovania právnych nárokov voči čitateľovi, po dobu uplatňovania týchto nárokov, až do právoplatného vyriešenia.

3.6.1.5 Dotknuté osoby v IS

Dotknutými osobami v rámci IS sú registrovaní čitatelia.

3.6.2 Posúdenie nevyhnutnosti a primeranosti

3.6.2.1 Zákonnosť spracúvania osobných údajov

Právnym základom pre spracúvanie osobných údajov je článok 6 ods. 1 písm.) b) nariadenia GDPR, keďže podľa § 16 ods. 6 zákona o knižniciach je spracúvanie osobných údajov čitateľov a používateľov knižnice záväzkový právny vzťah, ktorý vzniká zapožičaním knižničnej výpožičnej jednotky čitateľom.

Spracúvanie osobných údajov v IS sa riadi taktiež nasledujúcimi zákonmi:

Číslo predpisu	Názov predpisu
126/2015 Z. z.	Zákon o knižniciach v znení neskorších predpisov
40/1964 Zb.	Občiansky zákonník v znení neskorších predpisov
552/2003 Z. z.	Zákon o výkone práce vo verejnom záujme v znení neskorších predpisov
18/2018 Z. z.	Zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
395/2002 Z. z.	Zákon o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov
431/2002 Z. z.	Zákon o účtovníctve v znení neskorších predpisov

3.6.2.2 Obmedzenie účelu

Prevádzkovateľ zohľadnil zásadu obmedzenia účelu spracúvania osobných údajov prijatím organizačných opatrení, ktorými bolo určené povereným osobám získavať osobné údaje na

konkrétny účel, ktorým je vedenie evidencie čitateľov a ich dosiahnuteľnosti a súvisiacich záväzkov, ktoré vyplývajú zo záväzkového čitateľského vzťahu. Osobné údaje nie je možné spracúvať na iné účely, táto povinnosť bola uložená všetkým povereným osobám ako základná povinnosť pri spracúvaní osobných údajov. Osobné údaje sú spracúvané v knižničnom systéme CLAVIUS, prístup k tomuto systému majú výhradne poverené osoby.

3.6.2.3 Minimalizácia osobných údajov

Prevádzkovateľ prijal opatrenia, aby sa na každú spracovateľskú operáciu využíval len taký osobný údaj, ktorý je preukázateľne potrebný a nevyhnutný pre plnenie stanoveného účelu spracúvania.

Spracovateľská operácia	Spracúvané osobné údaje v rámci spracovateľskej operácie
spracovanie údajov používateľov knižnično-informačných služieb	Rozsah spracúvaných osobných údajov je vymedzený v § 18 zákona o knižniciach, pričom Prevádzkovateľ nespracúva osobné údaje nad rámec zákonom stanoveného rozsahu

3.6.2.4 Správnosť spracúvaných osobných údajov

Prevádzkovateľ prijal organizačné opatrenie spracúvať len správne a aktualizované osobné údaje, pričom boli prijaté organizačné ako aj technické opatrenia, ktoré umožnia aktualizáciu a prípadne aj výmaz nesprávnych osobných údajov, ktoré sú spracúvané v manuálnej forme, prípadne elektronicky. K výmazu osobných údajov dochádza po uplynutí dvoch rokov neaktívneho členstva, teda ak nedochádza k využívaniu knižnično-informačných služieb.

3.6.2.5 Minimalizácia uchovávaní

Prevádzkovateľ prijal organizačné a technické opatrenia na zabezpečenie povinnosti spracúvať osobné údaje po dobu, ktorá je nevyhnutná pre účely, pre ktoré sa spracúvajú, pričom následne sú uchovávané v registratúrnom stredisku po dobu, ktorá je určená registratúrnym poriadkom a registratúrnym plánom. Tieto doby sú vymedzené taktiež v bode 3.6.1.4 tejto smernice. Po uplynutí uvedeného času sa zabezpečuje likvidácia osobných údajov (skartácia, pokiaľ sú osobné údaje spracúvané v listinnej forme alebo výmaz, ak sú osobné údaje spracúvané v elektronickej forme).

3.6.2.6 Integrita a dôvernosť spracúvaných osobných údajov

Zásady integrity a dôvernosti, ktorých dodržiavanie je zabezpečené prijatím bezpečnostných opatrení pri práci s osobnými údajmi, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení, vrátane tejto bezpečnostnej smernice. Bližšie sú povinnosti v oblasti integrity a dôvernosti spracúvaných osobných údajov upravené v kapitolách 11 a 17 bezpečnostnej smernice.

3.6.3 Posúdenie rizika pre práva fyzických osôb v IS

Spracúvanie osobných údajov v IS má zákonný základ v osobitných právnych predpisoch. V rámci tohto IS dochádza k spracúvaniu bežných osobných údajov, v bežnom rozsahu, ktoré sú potrebné pre riadne plnenie povinností Prevádzkovateľa ako knižnice.

Automatizované spracúvanie osobných sa realizuje s využitím knižnično-informačných služieb používateľom prostredníctvom knižnično-informačného systému CLAVIUS.

3.6.4 Monitorovanie a preskúmanie podmienok spracúvania osobných údajov v IS

Opatrenia prijaté na zabezpečenie pravidelného monitorovania podmienok spracúvania osobných údajov, vrátane kontroly zavedených postupov, v kapitole bezpečnostnej smernice na ochranu osobných údajov.

3.7 IS THEATRE.SK

Informačný systém THEATRE.SK (ďalej len „IS THEATRE.SK“). Je integrovaným systémom, ktorý realizuje činnosti súvisiace s tvorbou a vydaním ročenky pod názvom „Divadlá na Slovensku v sezóne ...“, činnosti súvisiace s tvorbou a vydaním „Kalendára jubilantov“, ktoré sú každoročnými publikáciami Divadelného ústavu, činnosti súvisiace s online katalógom fondov a zbierok DÚ (Bach Vademecum), činnosti súvisiace s online katalógom fondov a zbierok DÚ – etheatre.sk a ďalšie činnosti súvisiace s poslaním DÚ.

3.7.1 Opis plánovaného spracúvania osobných údajov

IS THEATRE.SK je informačným systémom, ktorého základným cieľom je dokumentovanie inscenačnej tvorby a osobností divadelníctva na internete a uskutočnenie prípravných krokov na integráciu s digitálnym systémom.

Z dôvodu zachovania kompatibility a archivácie sú ešte implementované aj predchádzajúce automatizované systémy, ktoré sú funkčné a preto tu uvádzame aj ich popis.

Tento IS preberá hlavnú funkcionalitu IS THEISA a dopĺňa ho o ďalšie aspekty funkcionality. IS THEISA bol spracovaný na základe Koncepcie rezortnej časti štátneho informačného systému a v súlade so Zákonom č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov.

Cieľom informačného systému divadelnej dokumentácie THEATRE.SK je:

- vytvorenie kompletnej databázy osobností, divadiel, súborov, inscenácií a podujatí slovenských profesionálnych divadiel od r. 1920;
- vytvorenie a sprístupnenie moderného užívateľského databázového a rešeršného systému pre návštevníkov Divadelného ústavu a ďalších záujemcov s možnosťami rôznych užívateľských výstupov, vrátane výstupov pre odborné publikácie a spracovanie vopred definovaných používateľských výstupov pre odborné publikácie (publikácia Divadlá na Slovensku – ročenka profesionálnych divadiel s ročnou periodicitou a Malý divadelný kalendár) a ďalšie.

Automatizovaný projekt informačného systému THEATRE.SK vytvorila firma Atrian, s.r.o., Podhorská 1, 902 01 Pezinok, IČO: 4554 6711.

K systematickému spracúvaniu osobných údajov v IS THEATRE.SK dochádza v časti databáza osobností a používatelia. V ostatných častiach sa nespracúvajú osobné údaje, avšak sú s databázou osobností úzko späté.

Osobné údaje sú v IS THEATRE.SK spracúvané pre účely tvorby umeleckých alebo literárnych diel, pre potreby informovania verejnosti masovokomunikačnými prostriedkami a osobné údaje spracúva prevádzkovateľ, ktorému to vyplýva z predmetu jeho činnosti. Právnym základom pre spracúvanie osobných údajov je čl. 6 ods. 1 písm. e) nariadenia GDPR (spracúvanie je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme). Pokiaľ ide realizáciu uvedeného účelu, tak v zmysle § 78 ods. 1 zákona č. 18/2018 Z. z. o ochrane osobných údajov, osobné údaje možno spracúvať bez súhlasu dotknutej osoby, keďže spracúvanie osobných údajov je nevyhnutné na akademický účel, umelecký účel alebo literárny účel; to neplatí, ak spracúvaním osobných údajov na taký účel prevádzkovateľ porušuje právo dotknutej osoby na ochranu jej osobnosti alebo právo na ochranu súkromia, čo v tomto prípade nebolo zistené.

Samotné získavanie osobných údajov je ďalej získavané v súlade so zákonom č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov a tiež so Smernicou o odbornej správe fondov a zbierok Divadelného ústavu, ktorá ako činnosť a poslanie definuje aj systematické zhromažďovanie, spracovávanie, uchovávanie a sprístupňovanie dokumentačných materiálov.

Z IS THEATRE.SK sú čerpané osobné údaje do podsystemu **Ročenka**, kedy sú údaje z IS THEATRE.SK zverejnené v publikácii „Divadlá na Slovensku v sezóne ...“, ktorá je dôležitým pramenným materiálom, evidujúcim všetky inscenácie slovenských profesionálnych divadiel v danej sezóne, vrátane menného registra všetkých zúčastnených tvorcov a interpretov.

Z IS THEATRE.SK sú čerpané osobné údaje do podsystemu **Kalendár jubilantov**, kedy sú údaje z IS THEATRE.SK zverejnené v publikácii „Malý divadelný kalendár“, ktorá obsahuje aktuálne jubileá umelcov a slúži ako podkladový materiál pre MK SR aj pre vedenia divadiel k zaslaniu gratulačných listov umelcom, pre spomienkové výstavy a podobne.

Z IS THEATRE.SK sa čerpajú osobné údaje do Katalógu fondov a zbierok Divadelného ústavu (Bach Vademecum). Je to dátový webový prehliadač, prostredníctvom ktorého sa získavajú informácie z fondov a zbierok DÚ. Údaje spracovávané v Divadelnom ústave sú prístupné nielen odbornej, ale aj širokej laickej verejnosti. Návštevník webstránky môže vyhľadávať jednotlivito podľa tematických skupín (Inscenácie, Osobnosti, Divadlá a inštitúcie, Udalosti a podujatia a pod..) alebo fulltextom vo všetkých skupinách naraz, podľa zvoleného hesla (napr. meno herca) alebo skupiny hesiel (napr. meno herca, meno režiséra, divadlo). Súčasťou Katalógu sú aj digitálne kópie archívnych dokumentov (skeny fotografií a iné zdigitalizované objekty), ktorých náhľad bude prístupný aj pre verejnosť. Návštevník tak môže získať komplexnú informáciu o vyhľadávanom subjekte, vrátane osobných údajov ako dátum a miesto narodenia.

Osobné údaje z IS THEATRE.SK sú zverejňované rôznymi formami v uvedených publikáciách a na internete, avšak do systému môžu zasahovať len oprávnené osoby s presne definovanými prístupovými právami.

3.7.1.1 Účel spracúvania osobných údajov

Účelom spracúvania osobných údajov je realizácia činností súvisiacich s predmetom činnosti DÚ a to hlavne s tvorbou a vydaním ročenky pod názvom „Divadlá na Slovensku v sezóne ...“, činností súvisiacich s tvorbou a vydaním „Kalendária divadelných osobností“, ktoré sú každoročnými publikáciami Divadelného ústavu a činností súvisiacich s online Katalógom fondov a zbierok DÚ (Bach Vademecum) a činností súvisiace s online katalógom fondov a zbierok DÚ – etheatre.sk. Uvedený účel spracúvania osobných údajov je vymedzený predmetom činnosti organizácie a je ďalej konkretizovaný v jednotlivých popisoch činností IS.

3.7.1.2 Zoznam/rozsah osobných údajov

V automatizovanej aj neautomatizovanej agende IS THEATRE.SK sú spracúvané nasledovné osobné údaje:

- titul, meno a priezvisko
- dátum a miesto narodenia (príp. úmrtia)
- vzdelanie
- činnosť umelca

3.7.1.3 Zoznam/okruh príjemcov

Osobné údaje môžu byť poskytované tretím subjektom a niektoré osobné údaje sú zverejnené, za účelom dokumentovania divadelného života v SR.

3.7.1.4 Vymedzenie obdobia uchovávaní osobných údajov

K spracúvaniu osobných údajov dochádza na základe súhlasu dotknutých osôb, ktorý možno kedykoľvek odvolať a následne sú osobné údaje zlikvidované.

Spracovateľská operácia	Doba uchovávaní (v rokoch)
-------------------------	----------------------------

Vytvorenie databázy umelcov/umelkýň	V závislosti od spracovateľskej operácie a druhu dokumentu (archívne dokumenty – spracúvané bez časového obmedzenia)
-------------------------------------	--

3.7.1.5 Dotknuté osoby

Dotknutými osobami v rámci IS THEATRE.SK sú fyzické osoby – umelci a umelkyne, ktorí/é vykonávajú alebo vykonávali činnosť v oblasti divadelníctva na Slovensku.

3.7.2 Posúdenie nevyhnutnosti a primeranosti

3.7.2.1 Zákonnosť spracúvania osobných údajov

Právnym základom spracúvania osobných údajov v IS THEATRE.SK je čl. 6 ods. 1 písm. e) nariadenia GDPR (spracúvanie je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme).

Spracúvanie osobných údajov sa taktiež riadi nasledujúcimi zákonmi:

Číslo predpisu	Názov predpisu
185/2015 Z. z.	Autorský zákon
40/1964 Zb.	Občiansky zákonník v znení neskorších predpisov
189/2015 Z. z.	Zákon o kultúrno-osvetovej činnosti
206/2009 Z. z.	Zákon o múzeách a o galériách a o ochrane predmetov kultúrnej hodnoty a o zmene zákona Slovenskej národnej rady č. 372/1990 Zb. o priestupkoch v znení neskorších predpisov
122/2013 Z. z.	Zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
523/2009 Z. z.	Vyhláška MK SR, ktorou sa ustanovujú podrobnosti o základných odborných činnostiach v múzeu alebo v galérii a o evidencii predmetov kultúrnej hodnoty

3.7.2.2 Obmedzenie účelu

Prevádzkovateľ zohľadnil zásadu obmedzenia účelu spracúvania osobných údajov prijatím organizačných opatrení, ktorými bolo určené povereným osobám získavať osobné údaje od výrobcov na vymedzený účel ich evidencie, prípadne aj zverejnenia v databázach DÚ.

Osobné údaje nie je možné spracúvať na iné účely, táto povinnosť bola uložená všetkým povereným osobám ako základná povinnosť pri spracúvaní osobných údajov. Osobné údaje sú spracúvané výhradne poverenými osobami.

3.7.2.3 Minimalizácia osobných údajov

Prevádzkovateľ prijal opatrenia, aby sa na každú spracovateľskú operáciu využíval len taký osobný údaj, ktorý je preukázateľne potrebný a nevyhnutný pre plnenie stanoveného účelu spracúvania.

Spracovateľská operácia	Spracúvané osobné údaje v rámci spracovateľskej operácie
spracúvanie osobných údajov umelcov	Rozsah spracúvaných osobných údajov umelcov je nevyhnutný pre účely dokumentovania divadelného života v SR

Zverejnenie údajov umelcov	Rozsah osobných údajov, ktorý je zverejnený je obmedzený na účely profesijnej dokumentácie a prezentácie divadelnej tvorby
----------------------------	--

3.7.2.4 Správnosť spracúvaných osobných údajov

Prevádzkovateľ prijal organizačné opatrenie spracúvať len správne a aktualizované osobné údaje, pričom boli prijaté organizačné ako aj technické opatrenia, ktoré umožnia aktualizáciu a prípadne aj výmaz nesprávnych osobných údajov, ktoré sú spracúvané v manuálnej forme, prípadne elektronicky. Správnosť osobných údajov umelcov sa preveruje vedeckým bádáním, prípadne komunikáciou s umelcom/umelkyňou.

3.7.2.5 Minimalizácia uchovávaní

Prevádzkovateľ prijal organizačné a technické opatrenia na zabezpečenie povinnosti spracúvať osobné údaje po dobu, ktorá je nevyhnutná pre účely, pre ktoré sa spracúvajú, pričom tieto doby uchovávaní sú určené právnymi predpismi regulujúcimi spracúvanie registratúrnych záznamov. Tieto doby sú vymedzené taktiež v bode 3.7.1.4 tejto smernice.

3.7.2.6 Integrita a dôvernosť spracúvaných osobných údajov

Zásady integrity a dôvernosti, ktorých dodržiavanie je zabezpečené prijatím bezpečnostných opatrení pri práci s osobnými údajmi, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení, vrátane tejto bezpečnostnej smernice. Bližšie sú povinnosti v oblasti integrity a dôvernosti spracúvaných osobných údajov upravené v kapitolách 11 a 17 bezpečnostnej smernice.

3.7.3 Posúdenie rizika pre práva fyzickej osoby

V rámci tohto IS dochádza k spracúvaniu bežných osobných údajov, v rozsahu, ktorý je nevyhnutný pre prezentáciu výrobcu a jeho činnosti v oblasti umeleckej tvorby. Spracúvanie osobných údajov v IS nepredstavuje riziko pre práva dotknutých osôb.

3.7.4 Monitorovanie a preskúmanie podmienok spracúvania osobných údajov

Opatrenia prijaté na zabezpečenie pravidelného monitorovania podmienok spracúvania osobných údajov, vrátane kontroly zavedených postupov, v kapitole 18 bezpečnostnej smernice na ochranu osobných údajov.

3.8 IS Kameraný systém

Informačný systém Kameraný systém je prevádzkovaný výhradne v automatizovanej forme a slúži na monitorovanie a záznam citlivých priestorov na zabezpečenie poriadku, bezpečnosti, ochrany majetku a osôb v priestoroch Prevádzkovateľa, ako aj ochranu knižničných a iných dokumentov, ktoré majú kultúrny a historický význam a značnú spoločenskú hodnotu.

3.8.1 Opis plánovaného spracúvania osobných údajov

Kameraný monitorovací systém v priestoroch Divadelného ústavu je technické zariadenie, ktoré slúži na monitorovanie nasledujúcich priestorov:

- časť verejne prístupných priestorov určených pre návštevníkov a zákazníkov Divadelného ústavu, ktoré sa nachádzajú v zornom poli optiky snímacieho zariadenia – automaticky ovládaných kamier, ktoré sú súčasťou kamerového systému. Konkrétne je monitorovaný (i) priestor predajne a Informačného centra PROSPERO – prízemie a prvé poschodie a (ii) priestor Študovne Divadelného ústavu – prvé poschodie;

- Oddelenia riaditeľky DÚ nainštalovaný kamerový systém pozostávajúci z jednej kamery, ktorá monitoruje priestor vstupných dverí, priestor pred skriňami, v ktorých sa nachádza písomná dokumentácia Prevádzkovateľa a priestor dverí vedúcich do pamätnej Izby manželov Borodáčovcov.

Kamerové záznamy sa vyhotovujú nepretržite, záznamy sa nahrávajú, pričom k automatickému mazaniu nahratých záznamov dochádza po naplnení priestoru na disku do 15 dní od vyhotovenia záznamu. Ku kamerovým záznamom majú prístup výhradne oprávnení zamestnanci Prevádzkovateľa.

Kamerový systém bol zhotovený a inštalovaný firmou Fix, s. r. o. so sídlom na Hlinícka č. 1, 831 05 Bratislava na základe Zmluvy o dielo na projektovanie, dodávku a montáž bezpečnostných systémov elektrickej požiarnej signalizácie (EPS), systému priemyselnej televízie (PTV) a poplachového systému narušenia (PSN) ich záručný a pozáručný servis, ktorá bola uzavretá dňa 28. 8. 2010 na základe verejného obstarávania – prieskumu trhu – zákazky s nízkou hodnotou, na ktorej sa zúčastnili tri spoločnosti.

Kamerový monitorovací systém je dodaný, inštalovaný a zabezpečený servisnými službami uvedenej spoločnosti.

Kamerový monitorovací systém je sprístupnený na Oddelení riaditeľky Divadelného ústavu. Zamestnanci Oddelenia edičnej činnosti a Oddelenia divadelnej dokumentácie, informatiky a digitalizácie Divadelného ústavu si na základe písomnej žiadosti môžu prezrieť záznamy kamerového monitorovacieho systému, samotný záznam môže na základe vyžiadania oprávnených orgánov skopírovať len Oddelenie riaditeľky Divadelného ústavu.

Medzi povinnosti Prevádzkovateľa patrí povinnosť informovať dotknuté osoby o zavedení systému monitorovania, stanoviť zásady prístupu k IS a inštalovaným monitorovacím prostriedkom, lehoty ich uloženia, požiadavky na zamedzenie prístupu neoprávnených osôb k nim, ako aj podmienky sprístupňovania alebo poskytovania vyhotoveného záznamu určenému okruhu oprávnených žiadateľov (napr. orgánov činných v trestnom konaní) pri dokumentovaní a objasňovaní priestupkov a trestnej činnosti.

Upozorňujeme na povinnosť Divadelného ústavu ako prevádzkovateľa IS, že vyhotovené záznamy je potrebné zlikvidovať po skončení účelu spracúvania, teda v primeranom čase. Uvedená povinnosť zlikvidovať vyhotovený záznam neplatí, ak bol záznam použitý na účely trestného konania, priestupkového konania alebo konania o porušení pracovnej disciplíny v pracovnoprávných vzťahoch, prípadne na účely súdneho konania v občianskoprávných vzťahoch.

3.8.1.1 Účel spracúvania osobných údajov

Účelom spracúvania osobných údajov IS KAM je monitorovanie a záznam priestorov za a slúži na ochranu majetku a odhaľovania kriminality, vrátane ochrany knižničných a iných dokumentov, ktoré majú kultúrny a historický význam a značnú spoločenskú hodnotu.

IS neslúži k primárnemu zberu a uchovávaní osobných údajov, ale výhradne na zabezpečenie poriadku, bezpečnosti, ochranu majetku a osôb ako aj ochrany majetku technického zariadenia Prevádzkovateľa.

Opis oprávneného záujmu a jeho vzťah k právam a slobodám dotknutých osôb

a) Účel spracúvania osobných údajov a identifikácia oprávneného záujmu

Účelom spracúvania osobných údajov je ochrana majetku Prevádzkovateľa zamedzením nezákonnej činnosti, ako a odhaľovanie kriminality za účelom ochrany verejného majetku, ktorý má celospoločenskú hodnotu. Ochrana majetku je nevyhnutná, keďže v priestoroch Prevádzkovateľa sa nachádza špecifické vybavenie, ako aj s ohľadom na osobitné činnosti Prevádzkovateľa (archív).

b) Nevyhnutnosť spracúvania osobných údajov

Nevyhnutnosť spracúvania osobných údajov súvisí s efektívnym zabezpečením účelu spracúvania osobných údajov. Prítomnosť kamier pôsobí preventívne, keďže priestor je označený ako monitorovaný, čím má dôjsť k preventívnemu obmedzeniu nezákonnej činnosti. Rovnako pôsobí ako pomoc pre prípadné odhaľovanie nezákonnej činnosti, keďže Prevádzkovateľ dokáže kamerový záznam postúpiť orgánom činným v trestnom konaní pre účely vyšetrovania nezákonnej činnosti a následne aj odhalenie prípadného páchateľa takejto činnosti.

c) *Balančný test: vyváženie oprávnených záujmov proti záujmom jednotlivcov na ochrane ich práv a slobôd*

Vzhľadom na značnú hodnotu majetku a technického vybavenia, ktoré je získané z verejných zdrojov, ako aj na činnosti Prevádzkovateľa, ktoré ako národná knižnica zabezpečuje, Prevádzkovateľ identifikoval potrebu vyhotovovania kamerového záznamu ako preventívne opatrenie a opatrenie uľahčujúce prípadne vyšetrovanie nezákonnej činnosti. Vyhotovovanie kamerového záznamu v spojitosti s výmazom týchto záznamov do 15 dní a obmedzeným prístupom k týmto záznamom predstavuje málo invazívny spôsob do práv a slobôd jednotlivcov, keďže sa týka výhradne označených priestorov Prevádzkovateľa.

3.8.1.2 Zoznam/rozsah osobných údajov

V IS Kamerový systém dochádza k spracúvaniu videozáznamu monitorovaných priestorov formou obrazu nasnímaného kamerami.

3.8.1.3 Zoznam/okruh príjemcov

Osobné údaje nie sú poskytované tretím stranám. V prípade mimoriadnej udalosti však môžu byť poskytnuté orgánom činným v trestnom konaní za účelom prešetrenia zisteného porušenia právnych predpisov a oprávnených záujmov Prevádzkovateľa (napr. Policajný zbor SR, súdy).

3.8.1.4 Vymedzenie obdobia uchovávania osobných údajov

Záznamy sa nahrávajú nepretržite, k automatickému mazaniu nahratých záznamov dochádza v lehote 15 dní odo dňa vzniku záznamu.

3.8.1.5 Dotknuté osoby

Dotknutými osobami v rámci IS Kamerový systém sú osoby pohybujúce sa v priestoroch, ktoré sú monitorované.

3.8.2 Posúdenie nevyhnutnosti a primeranosti

3.8.2.1 Zákonnosť spracúvania osobných údajov

Právnym základom pre spracúvanie osobných údajov je oprávnený záujem Prevádzkovateľa v zmysle čl. 6 ods. 1 písm. f) nariadenia GDPR. Účel a nevyhnutnosť spracúvania osobných údajov sú popísané v texte vyššie.

Účel spracúvania osobných údajov v IS Kamerový systém je upravený nasledujúcimi zákonmi:

Číslo predpisu	Názov predpisu
18/2018 Z. z.	Zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
171/1993 Z. z.	Zákon o Policajnom zbore v znení neskorších predpisov
300/2005 Z. z.	Trestný zákon v znení neskorších predpisov
224/2006 Z. z.	Zákon o občianskych preukazoch a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

3.8.2.2 Obmedzenie účelu

Prevádzkovateľ zohľadnil zásadu obmedzenia účelu spracúvania kamerových záznamov, pričom tieto sú dostupné výhradne oprávneným osobám a ich využitie je možné len pre účely ochrany majetku a odhaľovania kriminality, vrátane efektívneho využívania technických prostriedkov Prevádzkovateľa.

Osobné údaje nie je možné spracúvať na iné účely, táto povinnosť bola uložená všetkým povereným osobám ako základná povinnosť pri spracúvaní osobných údajov. Osobné údaje sú spracúvané výhradne poverenými osobami.

3.8.2.3 Minimalizácia osobných údajov

Prevádzkovateľ prijal opatrenia, aby sa na každú spracovateľskú operáciu využíval len taký osobný údaj, ktorý je preukázateľne potrebný a nevyhnutný pre plnenie stanoveného účelu spracúvania.

Spracovateľská operácia	Spracúvané osobné údaje v rámci spracovateľskej operácie
Vyhotovovanie kamerových záznamov	Rozsah: Obraz nasnímaný kamerami a osoby pohybujúce sa v priestoroch monitorovania

3.8.2.4 Správnosť spracúvaných osobných údajov

Prevádzkovateľ prijal organizačné opatrenie spracúvať len správne a aktualizované osobné údaje, pričom boli prijaté organizačné ako aj technické opatrenia, ktoré umožnia aktualizáciu a prípadne aj výmaz nesprávnych osobných údajov. Predmetom spracúvania sú kamerové záznamy a v nich vyskytujúce sa osoby, ktoré sa pohybujú v priestoroch Prevádzkovateľa.

3.8.2.5 Minimalizácia uchovávania

Prevádzkovateľ prijal organizačné a technické opatrenia na zabezpečenie povinnosti spracúvať osobné údaje po dobu, ktorá je nevyhnutná pre účely, pre ktoré sa spracúvajú, pričom tieto doby sú vymedzené taktiež v bode 3.8.1.4 tejto smernice. Po uplynutí tejto doby sú kamerové záznamy vymazané.

3.8.2.6 Integrita a dôvernosť spracúvaných osobných údajov

Zásady integrity a dôvernosti, ktorých dodržiavanie je zabezpečené prijatím bezpečnostných opatrení pri práci s osobnými údajmi, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení, vrátane tejto bezpečnostnej smernice. Bližšie sú povinnosti v oblasti integrity a dôvernosti spracúvaných osobných údajov upravené v kapitolách 11 a 17 bezpečnostnej smernice na ochranu osobných údajov.

3.8.3 Posúdenie rizika pre práva fyzickej osoby

IS je prevádzkovaný výhradne v automatizovanej forme, pričom Prevádzkovateľ zabezpečil označenie priestorov nálepkou, ktorá informuje, že ide o monitorovaný priestor, stanovil zásady prístupu k IS a inštalovaným monitorovacím prostriedkom, lehoty ich uloženia, požiadavky na zamedzenie prístupu neoprávnených osôb k nim, ako aj podmienky sprístupňovania alebo poskytovania vyhotoveného záznamu určenému okruhu oprávnených žiadateľov (napr. orgánov činných v trestnom konaní) pri dokumentovaní a objasňovaní priestupkov a trestnej činnosti v priestoroch prevádzkovateľa a ich bezprostrednom okolí.

Spracúvanie osobných údajov v IS nepredstavuje riziko pre práva dotknutých osôb.

3.8.4 Monitorovanie a preskúmanie podmienok spracúvania osobných údajov v IS Evidencia návštev

Opatrenia prijaté na zabezpečenie pravidelného monitorovania podmienok spracúvania osobných údajov, vrátane kontroly zavedených postupov, v kapitole 18 bezpečnostnej smernice na ochranu osobných údajov.

3.9 IS Podnety

3.9.1 Opis plánovaného spracúvania osobných údajov v IS Podnety

Informačný systém Podnety je prevádzkovaný pre riešenie podozrení z porušenia právnych predpisov, interných predpisov alebo iného protiprávneho konania. Prevádzkovateľ týmto informačným systémom zabezpečuje plnenie úloh v súvislosti s oznamovaním kriminality alebo inej protispoločenskej činnosti fyzickými osobami, o ktorých sa fyzická osoba dozvedela v súvislosti s výkonom svojho zamestnania, povolania, postavenia alebo funkcie a ktoré môžu významnou mierou prispieť alebo prispeli k objasneniu závažnej protispoločenskej činnosti alebo k zisteniu alebo usvedčeniu jej páchatel'a.

3.9.1.1 Účel spracúvania osobných údajov

Spracúvanie osobných údajov v IS Podnety vyplýva Prevádzkovateľovi zo zákona č. 307/2014 Z. z. o niektorých opatreniach súvisiacich s oznamovaním protispoločenskej činnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. IS Podnety predstavuje spôsob nahlasovania protispoločenskej činnosti zamestnancami Prevádzkovateľ'a, o ktorej sa dozvedeli pri výkone práce, prípadne o ktorej sa dozvedeli inak. Oznámenie je možné podať aj anonymne.

Účel spracúvania osobných údajov je stanovený zákonom NR SR č. 307/2014 Z. z. o niektorých opatreniach súvisiacich s oznamovaním protispoločenskej činnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a je ním vnútorný systém vybavovania podnetov Prevádzkovateľ'a.

3.9.1.2 Zoznam/rozsah osobných údajov v IS Podnety

V IS Podnety dochádza k spracúvaniu nasledujúcich osobných údajov, pričom rozsah spracúvaných osobných údajov je určený príslušnými právnymi predpismi:

- Podľa zákona č. 307/2014 Z. z., § 11 ods. 8 písm. f), Zamestnávateľ spracúva osobné údaje uvedené v podnete.
- Podľa zákona č. 307/2014 Z. z., § 12, Zamestnávateľ je povinný po dobu troch rokov odo dňa doručenia podnetu viesť evidenciu podnetov v rozsahu podľa písm. b): meno, priezvisko a adresa pobytu osoby, ktorá podala podnet
- Zoznam osobných údajov:
 - dátum doručenia podnetu,
 - meno, priezvisko a adresa pobytu osoby, ktorá podala podnet; ak ide o anonymný podnet, uvedie sa iba poznámka, že ide o anonymný podnet,
 - predmet podnetu, ďalšie dotknuté osoby v podnete,
 - výsledok preverenia podnetu,
 - dátum skončenia preverenia podnetu,
 - či je osoba chráneným oznamovateľom,

- ak ide o chráneného oznamovateľa v komunikácii s Inšpektorátom práce aj osobné údaje potrebné na splnenie § 7 ods. 1 zákona č. 307/2014 Z. z. v rozsahu pracovnoprávneho úkonu..

3.9.1.3 Zoznam/okruh príjemcov

Osobné údaje nie sú poskytované tretím subjektom. Môžu však byť, v zmysle zákona č. 307/2014 Z. z., poskytované nasledujúcim príjemcom: inšpektorát práce, prokuratúra, súdy.

3.9.1.4 Vymedzenie obdobia uchovávanía osobných údajov

Spôsob uchovávanía je určený všeobecne záväznými právnymi predpismi a doba uchovávanía jednotlivých dokumentov je stanovená v Registratúrnom pláne a Registratúrnom poriadku, pričom je 5 rokov odo dňa vybavenia podnetu.

3.9.1.5 Dotknuté osoby v IS Podnety

Dotknutými osobami v IS Podnety sú osoby, ktorých sa podnety týkajú ako aj osoby, ktoré podnet podávajú.

3.9.2 Posúdenie nevyhnutnosti a primeranosti

3.9.2.1 Zákonnosť spracúvania osobných údajov

Právny základ pre spracúvanie osobných údajov je zákon NR SR č. 307/2014 Z. z. o niektorých opatreniach súvisiacich s oznamovaním protispoločenskej činnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Účel spracúvanie osobných údajov je taktiež upravený nasledujúcimi zákonmi:

Číslo predpisu	Názov predpisu
18/2018 Z. z.	Zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
307/2014 Z. z.	Zákon o niektorých opatreniach súvisiacich s oznamovaním protispoločenskej činnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
300/2005 Z. z.	Trestný zákon v znení neskorších predpisov
171/1993 Z. z.	Zákon o Policajnom zbore v znení neskorších predpisov
372/1990 Zb.	Zákon o priestupkoch v znení neskorších predpisov

3.9.2.2 Obmedzenie účelu

Prevádzkovateľ zohľadnil zásadu obmedzenia účelu spracúvania osobných údajov výhradne vo vzťahu k prešetreniu podnetu, pričom podnet je adresovaný určenej osobe, ktorá zabezpečí prešetrenie podnetu, v prípade potreby aj s asistenciou príslušných inštitúcií, ktorých právomocou je vyšetrovanie protispoločenskej činnosti.

Osobné údaje nie je možné spracúvať na iné účely, táto povinnosť bola uložená všetkým povereným osobám ako základná povinnosť pri spracúvaní osobných údajov. Osobné údaje sú spracúvané výhradne poverenými osobami.

3.9.2.3 Minimalizácia osobných údajov

Prevádzkovateľ prijal opatrenia, aby sa na každú spracovateľskú operáciu využíval len taký osobný údaj, ktorý je preukázateľne potrebný a nevyhnutný pre plnenie stanoveného účelu spracúvania.

Spracovateľská operácia	Spracúvané osobné údaje v rámci spracovateľskej operácie
-------------------------	--

Prešetrovanie podnetov podľa zákona č. 307/2014 Z. z.	Rozsah: meno, priezvisko, adresa pobytu a ďalšie údaje nevyhnutné na preverenie podnetu
---	--

3.9.2.4 Správnosť spracúvaných osobných údajov

Prevádzkovateľ prijal organizačné opatrenie spracúvať len správne a aktualizované osobné údaje, pričom boli prijaté organizačné ako aj technické opatrenia, ktoré umožnia aktualizáciu a prípadne aj výmaz nesprávnych osobných údajov. Predmetom spracúvania sú údaje osoby, ktorá podnet podala ako aj údaje, ktoré sú v podnete uvedené.

3.9.2.5 Minimalizácia uchovávaní

Prevádzkovateľ prijal organizačné a technické opatrenia na zabezpečenie povinnosti spracúvať osobné údaje po dobu, ktorá je nevyhnutná pre účely, pre ktoré sa spracúvajú, pričom tieto doby súvisia s prešetrením prípadu a následného uchovávaní príslušnej súvisiacej dokumentácie v registratúrnom stredisku až do uskutočnenia vyradovacieho konania.

3.9.2.6 Integrita a dôvernosť spracúvaných osobných údajov

Zásady integrity a dôvernosti, ktorých dodržiavanie je zabezpečené prijatím bezpečnostných opatrení pri práci s osobnými údajmi, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení, vrátane tejto bezpečnostnej smernice. Bližšie sú povinnosti v oblasti integrity a dôvernosti spracúvaných osobných údajov upravené v kapitolách 11 a 17 bezpečnostnej smernice na ochranu osobných údajov.

3.9.3 Posúdenie rizika pre práva fyzickej osoby v IS Podnety

Spracúvanie osobných údajov v IS Podnety má zákonný základ v osobitných právnych predpisoch. V rámci tohto IS dochádza k spracúvaniu bežných osobných údajov, v rozsahu, ktorý je určený všeobecne záväznými právnymi predpismi vzťahujúcimi sa na prešetrovanie podnetov v oblasti odhaľovania protispoločenskej činnosti. Spracúvanie osobných údajov v IS nepredstavuje riziko pre práva dotknutých osôb.

3.9.4 Monitorovanie a preskúmanie podmienok spracúvania osobných údajov v IS Podnety

Opatrenia prijaté na zabezpečenie pravidelného monitorovania podmienok spracúvania osobných údajov, vrátane kontroly zavedených postupov, v kapitole 18 bezpečnostnej smernice na ochranu osobných údajov.

3.10 IS Sťažnosti

3.10.1 Opis plánovaného spracúvania osobných údajov v IS Sťažnosti

Informačný systém Sťažnosti obsahuje databázu osôb, ktoré podávajú sťažnosť, ktorou sa domáhajú ochrany svojich práv alebo právom chránených záujmov, o ktorých sa domnievajú, že boli porušené činnosťou alebo nečinnosťou DÚ, prípadne ktoré poukazujú na konkrétne nedostatky, najmä na porušenie právnych predpisov, ktorých odstránenie je v pôsobnosti DÚ.

3.10.1.1 Účel spracúvania osobných údajov

Účelom spracúvania osobných údajov v IS Sťažnosti je prijímanie, evidovanie, prešetrovanie a písomné oznámenie výsledku prešetrenia sťažnosti alebo prekontrolovania sťažnosti.

3.10.1.2 Zoznam/rozsah osobných údajov v IS Sťažnosti

V IS Sťažnosti dochádza k spracúvaniu nasledujúcich osobných údajov:

- titul, meno a priezvisko, adresa trvalého pobytu alebo prechodného pobytu sťažovateľa,
- názov a sídlo právnickej osoby, meno a priezvisko osoby oprávnenej za ňu konať, ak sťažnosť podáva právnická osoba,
- adresa sťažovateľa na doručovanie v elektronickej forme,
- predmet sťažnosti,
- ďalšie osobné údaje zistené alebo predložené v priebehu vybavovania sťažností.

3.10.1.3 Zoznam/okruh príjemcov

Osobné údaje nie sú poskytované tretím subjektom. Môžu však byť poskytované aj príslušným subjektom, za účelom prešetrenia, ak tak požadujú osobitné zákony.

3.10.1.4 Vymedzenie obdobia uchovávaní osobných údajov

Spôsob uchovávaní ako aj doba uchovávaní jednotlivých dokumentov je stanovená v zmysle zákona č. 395/2002 Z. z. o archívoch a registratúrach ako aj v Registratúrnom pláne a Registratúrnom poriadku. Dokumentácia súvisiaca so sťažnosťami sa uchováva po dobu 5 rokov.

3.10.1.5 Dotknuté osoby v IS Sťažnosti

Dotknutými osobami v IS Sťažnosti sú osoby, ktoré sťažnosť podávajú, prípadne osoby, ktoré sa v podanej sťažnosti uvádzajú.

3.10.2 Posúdenie nevyhnutnosti a primeranosti

3.10.2.1 Zákonnosť spracúvania osobných údajov

Právnym základom pre spracúvanie osobných údajov v IS Sťažnosti je zákon č. 9/2010 Z. z. o sťažnostiach v znení neskorších predpisov.

Účel spracúvania osobných údajov v IS Sťažnosti sa riadi taktiež nasledujúcimi zákonmi:

Číslo predpisu	Názov predpisu
18/2018 Z. z.	Zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
171/1993 Z. z.	Zákon o Policajnom zbore v znení neskorších predpisov
300/2005 Z. z.	Trestný zákon v znení neskorších predpisov

3.10.2.2 Obmedzenie účelu

Prevádzkovateľ zohľadnil zásadu obmedzenia účelu spracúvania osobných údajov výhradne vo vzťahu k prešetreniu sťažnosti a jej vybavenia, v prípade potreby aj s asistenciou príslušných pracovníkov, ktorí majú informácie týkajúce sa sťažnosti.

Osobné údaje nie je možné spracúvať na iné účely, táto povinnosť bola uložená všetkým povereným osobám ako základná povinnosť pri spracúvaní osobných údajov. Osobné údaje sú spracúvané výhradne poverenými osobami.

3.10.2.3 Minimalizácia osobných údajov

Prevádzkovateľ prijal opatrenia, aby sa na každú spracovateľskú operáciu využíval len taký osobný údaj, ktorý je preukázateľne potrebný a nevyhnutný pre plnenie stanoveného účelu spracúvania.

Spracovateľská operácia	Spracúvané osobné údaje v rámci spracovateľskej operácie
Vybavovanie sťažnosti podľa zákona č. 9/2010 Z. z.	Rozsah: meno, priezvisko, adresa trvalého a prechodného pobytu sťažovateľa, adresa na doručovanie v elektronickej forme, ďalšie osobné údaje zistené alebo predložené počas vybavovania sťažnosti

3.10.2.4 Správnosť spracúvaných osobných údajov

Prevádzkovateľ prijal organizačné opatrenie spracúvať len správne a aktualizované osobné údaje, pričom boli prijaté organizačné ako aj technické opatrenia, ktoré umožnia aktualizáciu a prípadne aj výmaz nesprávnych osobných údajov. Predmetom spracúvania sú údaje osoby, ktorá sťažnosť podala ako aj údaje, ktoré sú v sťažnosti uvedené.

3.10.2.5 Minimalizácia uchovávaní

Prevádzkovateľ prijal organizačné a technické opatrenia na zabezpečenie povinnosti spracúvať osobné údaje po dobu, ktorá je nevyhnutná pre účely, pre ktoré sa spracúvajú, pričom tieto doby súvisia s prešetrením sťažnosti a následného uchovávaní príslušnej súvisiacej dokumentácie v registratúrnom stredisku až do uskutočnenia vyradovacieho konania (5 rokov).

3.10.2.6 Integrita a dôvernosť spracúvaných osobných údajov

Zásady integrity a dôvernosti, ktorých dodržiavanie je zabezpečené prijatím bezpečnostných opatrení pri práci s osobnými údajmi, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení, vrátane tejto bezpečnostnej smernice. Bližšie sú povinnosti v oblasti integrity a dôvernosti spracúvaných osobných údajov upravené v kapitolách 11 a 17 bezpečnostnej smernice na ochranu osobných údajov.

3.10.3 Posúdenie rizika pre práva fyzickej osoby v IS Sťažnosti

Spracúvanie osobných údajov v IS Sťažnosti má zákonný základ v osobitných právnych predpisoch. V rámci tohto IS dochádza k spracúvaniu bežných osobných údajov, v rozsahu, ktorý je určený všeobecne záväznými právnymi predpismi vzťahujúcimi sa na prešetrovanie sťažností.

Spracúvanie osobných údajov v IS nepredstavuje riziko pre práva dotknutých osôb.

3.10.4 Monitorovanie a preskúmanie podmienok spracúvania osobných údajov v IS Sťažnosti

Opatrenia prijaté na zabezpečenie pravidelného monitorovania podmienok spracúvania osobných údajov, vrátane kontroly zavedených postupov, v kapitole 18 bezpečnostnej smernice na ochranu osobných údajov.

3.11 IS Žiadosti podľa infozákona

Informačný systém Žiadosti podľa infozákona obsahuje databázu osôb, ktoré podávajú žiadosť podľa zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov ako aj osôb, ktorých sa infožiadosť týka. Keďže Prevádzkovateľ je v zmysle § 2 zákona č. 211/2000 Z. z. povinnou osobou, má povinnosť poskytnúť informácie žiadateľom o informácie, vrátane informácie o dotknutých osobách, v rozsahu stanovenom týmto zákonom.

3.11.1 Opis plánovaného spracúvania osobných údajov v IS Žiadosti podľa infozákona

V rámci informačného systému Žiadosti podľa infozákona dochádza k spracúvaniu osobných údajov prostredníctvom pracovníkov Oddelenia riaditeľky DÚ, prípadne inými zamestnancami určenými riaditeľkou.

IS Žiadosti podľa infozákona predstavuje samostatný informačný systém, v rámci ktorého dochádza k spracúvaniu osobných údajov súvisiacich so sprístupňovaním informácií na žiadosť, ako aj s vybavením žiadosti a vydaním rozhodnutia.

Žiadosť o sprístupnenie informácií možno podať písomne, ústne, faxom, elektronickou poštou alebo iným technicky vykonateľným spôsobom a musí z nej byť zrejmé, ktorej povinnej osobe je určená, meno, priezvisko, názov alebo obchodné meno žiadateľa, jeho adresa pobytu alebo sídlo, ktorých informácií sa žiadosť týka a aký spôsob sprístupnenia informácií žiadateľ navrhuje. Informácie sa sprístupňujú najmä ústne, nahliadnutím do spisu vrátane možnosti vyhotoviť si odpis alebo výpis, odkopírovaním informácií na technický nosič dát, sprístupnením kópií predlôh s požadovanými informáciami, telefonicky, faxom, poštou, elektronickou poštou. Ak informáciu nemožno sprístupniť spôsobom určeným žiadateľom, dohodne povinná osoba so žiadateľom iný spôsob sprístupnenia informácie.

Proces sprístupnenia žiadosti ako aj jej vybavenia sa riadi zákonom č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií).

V zmysle § 20 zákona č. 211/2000 Z. z. má DÚ povinnosť viesť evidenciu žiadostí tak, aby poskytovala údaje potrebné na kontrolu vybavovania žiadostí a údaje o najčastejšie vyžiadaných informáciách, pričom evidencia musí obsahovať najmä tieto údaje:

- a) dátum podania žiadosti,
- b) vyžiadanú informáciu a navrhovaný spôsob poskytnutia informácie,
- c) výsledok vybavenia žiadosti (poskytnutie informácií, vydanie rozhodnutia alebo postúpenie žiadosti),
- d) podanie opravného prostriedku.

3.11.1.1 Účel spracúvania osobných údajov

Účelom spracúvania osobných údajov v IS Žiadosti podľa infozákona je vybavovanie žiadostí o sprístupnenie informácií v zmysle zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov.

3.11.1.2 Zoznam/rozsah osobných údajov v IS Žiadosti podľa infozákona

V IS Žiadosti podľa infozákona dochádza k spracúvaniu nasledujúcich osobných údajov:

- titul, meno, priezvisko, adresa trvalého pobytu alebo prechodného pobytu a ďalšie osobné údaje žiadateľa,
- predmet žiadosti,
- osobné údaje o dotknutej osobe sprístupnené povinnou osobou na základe zákona alebo predchádzajúceho písomného súhlasu.

3.11.1.3 Zoznam/okruh príjemcov

Osobné údaje nie sú poskytované tretím subjektom. Môžu však byť poskytované aj príslušným subjektom, za účelom prešetrovania, ak tak požadujú osobitné zákony.

3.11.1.4 Vymedzenie obdobia uchovávania osobných údajov

Spôsob uchovávania ako aj doba uchovávania jednotlivých dokumentov je stanovená v zákone č. 395/2002 Z. z. o archívoch a registratúrach ako aj v Registratúrnom pláne a Registratúrnom poriadku a je 5 rokov odo dňa vybavenia infožiadosti.

3.11.1.5 Dotknuté osoby v IS Žiadosti podľa infozákona

Dotknutými osobami v IS Žiadosti podľa infozákona sú osoby, ktoré žiadosť o sprístupnenie informácií podávajú, prípadne osoby, ktorých sa žiadosť týka.

3.11.2 Posúdenie nevyhnutnosti a primeranosti

3.11.2.1 Zákonnosť spracúvania osobných údajov

Právnym základom pre spracúvanie osobných údajov v IS Žiadosti podľa infozákona je zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov.

Účel spracúvania osobných údajov v IS Žiadosti podľa infozákona sa riadi taktiež nasledujúcimi zákonmi:

Číslo predpisu	Názov predpisu
18/2018 Z. z.	Zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
40/1964 Zb.	Občiansky zákonník v znení neskorších predpisov
311/2001 Z. z.	Zákonník práce v znení neskorších predpisov
552/2003 Z. z.	Zákon o výkone práce vo verejnom záujme v znení neskorších predpisov

3.11.2.2 Obmedzenie účelu

Prevádzkovateľ zohľadnil zásadu obmedzenia účelu spracúvania osobných údajov výhradne vo vzťahu k žiadosti o informácie a jej vybavenia, v prípade potreby aj s asistenciou príslušných pracovníkov, ktorí majú informácie týkajúce sa žiadosti.

Osobné údaje je možné spracúvať len v súvislosti so žiadosťou, pričom rozsah osobných údajov, ktoré je možné sprístupniť, je uvedený v zákone č. 211/2000 Z. z. Osobné údaje sú spracúvané výhradne poverenými osobami.

3.11.2.3 Minimalizácia osobných údajov

Prevádzkovateľ prijal opatrenia, aby sa na každú spracovateľskú operáciu využíval len taký osobný údaj, ktorý je preukázateľne potrebný a nevyhnutný pre plnenie stanoveného účelu spracúvania.

Spracovateľská operácia	Spracúvané osobné údaje v rámci spracovateľskej operácie
Vybavovanie žiadostí o sprístupnenie informácií podľa zákona č. 211/2000 Z. z.	Rozsah: titul, meno, priezvisko, adresa trvalého a prechodného pobytu, prípadne ďalšie osobné údaje žiadateľa a osobné údaje o dotknutej osobe sprístupnené povinnou osobou na základe zákona alebo predchádzajúceho písomného súhlasu

3.11.2.4 Správnosť spracúvaných osobných údajov

Prevádzkovateľ prijal organizačné opatrenie spracúvať len správne a aktualizované osobné údaje, pričom boli prijaté organizačné ako aj technické opatrenia, ktoré umožnia aktualizáciu a prípadne aj výmaz nesprávnych osobných údajov. Predmetom spracúvania sú údaje osoby, ktorá žiadosť podala ako aj údaje, ktoré sú v žiadosti požadované.

3.11.2.5 Minimalizácia uchovávania

Prevádzkovateľ prijal organizačné a technické opatrenia na zabezpečenie povinnosti spracúvať osobné údaje po dobu, ktorá je nevyhnutná pre účely, pre ktoré sa spracúvajú, pričom tieto doby súvisia s vybavením žiadosti a následného uchovávania príslušnej súvisiacej dokumentácie v registratúrnom stredisku až do uskutočnenia vyradovacieho konania (3 roky).

3.11.2.6 Integrita a dôvernosť spracúvaných osobných údajov

Zásady integrity a dôvernosti, ktorých dodržiavanie je zabezpečené prijatím bezpečnostných opatrení pri práci s osobnými údajmi, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom

primeraných technických alebo organizačných opatrení, vrátane tejto bezpečnostnej smernice. Bližšie sú povinnosti v oblasti integrity a dôvernosti spracúvaných osobných údajov upravené v kapitolách 11 a 17 bezpečnostnej smernice na ochranu osobných údajov.

3.11.3 Posúdenie rizika pre práva fyzickej osoby v IS Žiadosti podľa infozákona

Spracúvanie osobných údajov v IS žiadosti podľa infozákona má zákonný základ v osobitných právnych predpisoch. V rámci tohto IS dochádza k spracúvaniu bežných osobných údajov, v rozsahu, ktorý je určený všeobecne záväznými právnymi predpismi vzťahujúcimi sa na vybavenie žiadosti.

Spracúvanie osobných údajov v IS nepredstavuje riziko pre práva dotknutých osôb.

3.11.3.1 Automatizované spracúvanie

IS Žiadosti podľa infozákona predstavuje internú databázu, ktorá sa fyzicky nachádza na pracovnej stanici poverenej oprávnenej osoby. Táto pracovná stanica je súčasťou siete pozostávajúcej z pracovných staníc LAN, prepojených na verejnú počítačovú sieť.

3.11.3.2 Neautomatizované spracúvanie

Kartotéka s agendou je v správe poverenej oprávnenej osoby z úseku generálneho riaditeľa. Všetky písomné dokumenty obsahujúce osobné údaje sa po ukončení účelu ich spracúvania sa odovzdávajú do Registratúrneho strediska. Zverejňovanie osobných údajov nesmie byť v rozpore s oprávnenými záujmami dotknutej osoby, pričom zverejnenie všeobecne použiteľného identifikátora je zakázané.

3.11.4 Monitorovanie a preskúvanie podmienok spracúvania osobných údajov v IS Žiadosti podľa infozákona

Opatrenia prijaté na zabezpečenie pravidelného monitorovania podmienok spracúvania osobných údajov, vrátane kontroly zavedených postupov, v kapitole 18 bezpečnostnej smernice na ochranu osobných údajov.

3.12 Automatizované spracúvanie prostredníctvom CJES

Pre zabezpečenie automatizovaných činností v IS CJES bol na základe zmluvy č. MK 132/07/M zo dňa 10.12.2007, uzatvorenej medzi MK SR a spoločnosťou SOFTIP, a.s. Banská Bystrica obstaraný softvérový produkt SOFTIP PROFIT.

Spoločnosť SOFTIP, a.s. na základe uvedenej zmluvy je povinná:

- poskytovať technickú podporu aplikačnému programovému vybaveniu (ďalej len „APV“) SOFTIP PROFIT
- vykonávať údržbu APV SOFTIP PROFIT pre MK SR a organizácie v zriaďovateľskej pôsobnosti MK SR

SOFTIP, a.s. ako dodávateľ bude vykonávať technickú podporu systému formou podpory prevádzky APV SOFTIP PROFIT a servisných zásahov v prípade nefunkčnosti systému alebo jeho komponentov.

Podpora prevádzky bude poskytovaná formou prevádzkových zásahov a preventívnych zásahov.

Údržba APV SOFTIP PROFIT zahŕňa:

Hot - line

- poskytnutie odpovede cez Call centrum na otázky týkajúce sa problémových situácií vzniknutých pri používaní APV, tzn. k obsluhu APV, k problémovým stavom APV, k správaniu sa APV v rozpore s opisom v programovej dokumentácii v časovom priestore približne 15 minút,
- prijatie nahlásených chýb APV,
- prijatie námetov na zlepšenie APV.

Udržiavanie APV

- poskytnutie legislatívnych verzií so zapracovanými legislatívnymi zmenami do APV,
- poskytnutie verzií APV s jeho optimalizovanými funkciami,
- poskytnutie verzií APV s rozšírenou funkcionalitou všeobecného charakteru,
- poskytnutie aktualizovaných verzií APV v dôsledku zmien v informačných technológiách.

Služby Centra podpory zákazníkom (ďalej len „CPZ“)

Podrobnosti spôsobu poskytovania údržby sú popísané vo všeobecných obchodných podmienkach spoločnosti SOFTIP, a.s.

Komplexný popis systému je uvedený v dodanej dokumentácii k APV SOFTIP PROFIT, ktorý je prílohou a súčasťou dodaného softvéru a je prístupný priamo z aplikácie.

3.12.1 Charakteristika softvéru SOFTIP PROFIT

SOFTIP PROFIT je moderný systém založený na technológii klient-server. Tvoria ho aplikácie zabezpečujúce rýchle a pritom pohodlné riadenie podniku v sekciách:

- Riadenie ekonomických informácií,
- Riadenie logistických informácií,
- Personálne a mzdové riadenie.

Správu systému a spúšťanie jednotlivých aplikácií zabezpečujú aplikácie Administrátor, Centrál a Číselníky sústredené v sekcii Správa systému Softip Profit.

V sekcii **Riadenie ekonomických informácií** sú sústredené funkcie zabezpečujúce spracovanie evidencií legislatívne upravených zákonom o účtovníctve a daňovými zákonmi. Pozostáva z aplikácií: Účtovníctvo, DPH, Saldokonto, Pokladňa, Dodávatelia, Financovanie, IMA, DIM a Inventúry.

Aplikácie v sekcii **Riadenie logistických informácií** sú určené na riadenie obchodnej činnosti obchodných a výrobných organizácií a tiež na evidenciu a riadenie toku materiálových zásob podnikov.

V sekcii **Personálne a mzdové riadenie** sú komplexne riešené všetky okruhy riadenia ľudských zdrojov – od definovania organizačnej schémy cez personálnu evidenciu, automatizované spracovanie miezd a plátov, sociálnu starostlivosť o zamestnancov až po ďalšie vzdelávanie zamestnancov. Sekciu tvoria aplikácie: Personalistika, Mzdy a Dochádzka.

3.12.1.1 Základné vlastnosti programového balíka SOFTIP PROFIT

- Je založený na technológii klient/server a pracuje v prostredí MS Windows.
- Pracuje s databázou MS SQL.
- Prepojenie na kancelárske systémy Microsoft Office, údaje z modulov Softip Profit sú exportovateľné do aplikácií Microsoft Word a Microsoft Excel. Programy kancelárskeho systému Microsoft Office sú priamo spustiteľné z programového balíka Softip Profit.
- Prepojenie a spolupráca s Internetom a Intranetom – systém je schopný získať z Internetu niektoré vybrané informácie pre svoju činnosť.
- Integrovanosť – úzka prepojenosť všetkých sekcií a aplikácií systému umožňuje prepojenie na vonkajší WorkFlow cez Microsoft Exchange a iné groupwarové aplikácie.

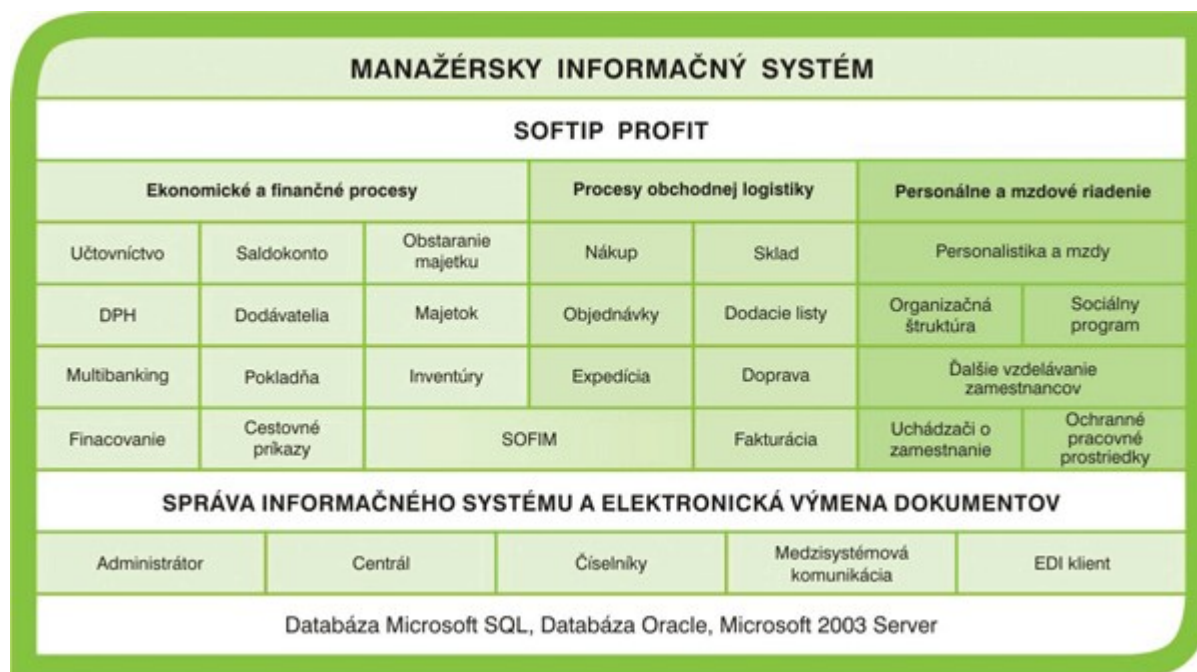
- Bezpečnosť – systém je integrovaný s bezpečnostnými mechanizmami databázového servera a operačného systému. S údajmi môže pracovať iba riadne autorizovaný užívateľ s pridelenými právami na nevyhnutné objekty databázy a aplikačné služby.
- Spôľahlivosť – využíva transakčné vlastnosti databázového servera s možnosťou zálohovania a obnovy až do posledne potvrdenej transakcie.

3.12.1.2 Základné sekcie

Aplikačné programové vybavenie Softip Profit tvoria aplikácie zabezpečujúce spracovanie sociálnych a ekonomických informácií v štyroch základných sekciách:

- Správa informačného systému:
 - Administrátor – poskytuje administrátorovi systému možnosť spravovať užívateľov informačného systému, prideľovať práva pre jednotlivých užívateľov a zabezpečiť komunikáciu systému s okolím, zabezpečuje aj upgrade databázy.
 - Centrál – na spúšťanie jednotlivých aplikácií informačného systému, zjednodušuje spustenie programov a zabezpečuje automatické pripojenie klienta na server.
 - Číselníky – umožňuje centrálnu administráciu všetkých číselníkov pre všetky sekcie informačného systému.
- Ekonomika,
- Personálne a mzdové riadenie,
- Logistika,
- doplnjúca sekcia – Sekcia odvetvových aplikácií.

SOFTIP PROFIT tvoria aplikácie, ktoré poskytujú plne integrované riešenie pre riadenie ekonomicko–finančných procesov, pre riadenie procesov obchodnej a materiálnej logistiky a komplexné riešenie pre riadenie ľudských zdrojov. Aplikácie sú integrované nad jednou databázou a zákazník si z nich môže vybrať takú zostavu, ktorá najviac vyhovuje jeho potrebám:



3.12.2 Popis aplikačného prostredia CJES

APV SOFTIP PROFIT je nasadené do terminálového prostredia CITRIX farmy. Používatelia prihlasujúci sa do farmy serverov sú overovaní v Active directory domény culture.gov.sk, kde má každý používateľ vytvorené konto s parametrami popísanými v analýze účtov.

Na všetkých serveroch vo farme je nainštalovaný CITRIX Web Interface na ktorý sa používateľ prihlasuje cez internetový prehliadač (napr.: IE) na ktorúkoľvek z adries servera CJES.

Ak používateľ nemá nainštalovaného CITRIX klienta, je informovaný o nutnosti inštalácie klienta a zároveň sú mu poskytnuté dva odkazy na inštaláciu CITRIX klienta.

„Download the ICA Client for Windows“ odkazuje na upravený bez obslužný inštalátor, ktorý je uložený na všetkých serveroch farmy, alebo „the Citrix client download site“ je presmerovaním na stiahnutie CITRIX klientov priamo zo stránok <http://www.citrix.com/download/>.

Inštalácia prebieha intuitívne a na jej realizáciu sú vypracované pracovné postupy.

Ak je CITRIX Web klient nainštalovaný, po otvorení okna prehliadača už nie sú zobrazované odkazy na inštaláciu CITRIX klientov.

Po zadaní prihlasovacieho mena a prihlasovacieho hesla dostane používateľ zoznam pre neho publikovaných aplikácií.

Kliknutím na odkaz požadovanej aplikácie sa spustí CITRIX klient, ktorý zabezpečí pripojenie na server v CITRIX farme CJES a v novom okne sa spustí samotná aplikácia APV SOFTIP PROFIT.

Po prvom prihlásení sa do CITRIX farmy je nastavené vynútenie zmeny hesla používateľa.

3.12.3 Popis databázového prostredia CJES

Microsoft SQL 2005 Standard Edition je nainštalovaný na serveroch PROFIT-CL1 až PROFIT-CL4.

Servery PROFIT-CL1 a PROFIT-CL2 sú nainštalované v 2node clusteri. Je použitá technológia Microsoft cluster. Nad Microsoft clusterom je nainštalovaný SQL cluster.

Druhý node v clusteri je neaktívny, v prípade výpadku sa stáva aktívny. Ak sa obnoví funkčnosť prvého nodu je nastavený Immediately failback – aktívnym sa stáva prvý node.

Na serveri PROFIT-CL1 a PROFIT-CL2 je nainštalovaná inštancia PROFIT-SQLCLS1\I01

Na serveri PROFIT-CL3 a PROFIT-CL4 je nainštalovaná inštancia PROFIT-SQLCLS1\I02

Databázy pre APV SOFTIP PROFIT sú vytvorené v inštancii PROFIT-SQLCLS1\I01. Pre každú organizáciu bola vytvorená samostatná databáza (S:\MSSQL\MSSQL.1\MSSQL\Data). Databázy sú umiestnené na diskovom poli IBM System Storage DS3400.

3.12.4 Postup a podmienky prístupu do CJES

Základné pravidlá prevádzky, zásady bezpečnej a spoľahlivej prevádzky, správy, podpory a využívania služieb CJES sú riešené prostredníctvom „Prevádzkového poriadku Centrálného ekonomického systému rezortu Ministerstva kultúry Slovenskej republiky“ v platnom znení.

Základné pravidlá prevádzky WAN VPN siete (rezortná sieť) a určenie zásad jej bezpečnej a spoľahlivej prevádzky sú riešené prostredníctvom „Prevádzkového poriadku WAN VPN siete rezortu MK SR“ v platnom znení.

V nasledovných bodoch tejto Smernice sú ďalej uvedené zjednodušené pracovné postupy a jednotlivé kroky pred samotným povolením práce s informačným systémom Prevádzkovateľa prostredníctvom CJES.

3.12.5 Poverená osoba za CJES

Z dôvodu presného a jednoznačného určenia postupu pri aplikácii požadovaných technických, organizačných a personálnych opatrení na ochranu osobných údajov štatutárny orgán Organizácie určí poverenú osobu vecne zodpovednú za CJES (ďalej len „PO“), ktorá v mene Organizácie a v súčinnosti s poverenou zodpovednou osobou za ochranu osobných údajov Organizácie (ďalej len „ZO“) zabezpečuje zriaďovanie a zrušenie prístupových oprávnení v CJES. Touto osobou je spravidla ekonomický námestník, vedúci ekonomického oddelenia, alebo samotný štatutárny orgán.

Každú zmenu PO musí štatutárny orgán Organizácie písomne nahlásiť Projektovému manažérovi CJES na MK SR (ďalej len „PM“) s nasledujúcimi údajmi:

- názov organizácie,
- titul, meno, priezvisko, funkcia, telefón, e-mail PO
- titul, meno, priezvisko, funkcia, telefón, e-mail lokálneho administrátora CJES (ak bol v organizácii určený)

3.12.6 Určenie poverenej oprávnenej osoby CJES

Spracúvať osobné údaje môže podľa Zákona výlučne poverená oprávnená osoba, ktorou je každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovnoprávneho vzťahu, štátnozamestnaneckého pomeru, služobného pomeru, členského vzťahu, na základe poverenia, zvolenia alebo vymenovania alebo v rámci výkonu verejnej funkcie.

Osobné údaje môže oprávnená osoba spracúvať len na základe poverenia Prevádzkovateľa, ktorý ju pred vydaním prvého pokynu na vykonanie akejkoľvek spracovateľskej operácie s osobnými údajmi poučí o právach a povinnostiach ustanovených Zákonom, o zodpovednosti za ich porušenie a o povinnosti mlčanlivosti, o čom vedie písomný záznam.

Poučenie poverenej oprávnenej osoby je vykonané prostredníctvom ZO, záznam o podmienkach poverenia, vrátane poučenia (podpísaný Oprávnenou osobou) je uložený v dokumentácii Bezpečnostného projektu, alebo v osobnom spise.

3.12.7 Vytvorenie prístupu do CJES

Pre vytvorenie konta a vygenerovanie prístupových oprávnení je postup nasledovný:

3.12.7.1 Požiadavka na vytvorenie prístupu do CJES

PO požiada formou e-mailovej správy z presne určeného konta (nahláseného PM) o zriadenie prístupu podľa platnej prílohy Prevádzkového poriadku CJES na adresu softip@culture.gov.sk, následne po zriadení konta je na určené e-mailové konto organizácie oznámené zriadenie konta, kde sú prvotné prístupové oprávnenia.

3.12.7.2 Inštalácia CITRIX klienta

Následne po vygenerovaní prístupových oprávnení je možné pripraviť pracovnú stanicu na zabezpečenú komunikáciu prostredníctvom CITRIX klienta.

Inštaláciu CITRIX klienta zabezpečí PO prostredníctvom určeného administrátora Organizácie alebo prostredníctvom PM.

3.12.7.3 Zmena a zrušenie prístupu do CJES

Pre zmenu prístupových oprávnení do CJES (zmena pracovnej pozície, zastupiteľnosť a pod.) PO požiada formou e-mailovej správy z presne určeného konta (nahláseného PM) o zriadenie prístupu podľa platnej prílohy Prevádzkového poriadku CJES svojho lokálneho administrátora, alebo na určenej adrese softip@culture.gov.sk.

3.12.8 Postupy pri poruchových stavoch CJES

V prípade poruchových stavov so sieťou VPN MK SR alebo s aplikáciou SOFTIP Profit postupovať podľa aktuálneho „Informačného listu k VPN MK SR a SOFTIP Profit – riešenie a postup pri poruchových stavoch“.

3.13 Automatizované spracúvanie prostredníctvom NUNTIO ASSR

V tejto kapitole popisujeme samostatne automatizovaný systém NUNTIO ASSR, nakoľko sú v ňom spracúvané osobné údaje z viacerých IS Prevádzkovateľa.

Softvérové riešenie NUNTIO Automatizovaný systém správy registratúry (ďalej len „NUNTIO ASSR“) pre Ministerstvo kultúry SR bolo dodané na základe zmluvy o dielo č. 17/2004 (MK-38/2004-M).

NUNTIO® Správa registratúry je komplexným riešením elektronickej správy registratúry v súlade s platnou legislatívou, ktorú vyvinula spoločnosť DIMANO, a. s. Spoločnosť DIMANO, a. s., je držiteľom certifikátu MV SR o posúdení zhody s požiadavkami Výnosu MV SR č. 525/2011 Z. z. o štandardoch pre elektronické informačné systémy na správu registratúry na úrovni vysoká úroveň zhody pre tento systém. NUNTIO® zavádza korektný postup pri prijímaní aj odosielaní fyzických aj elektronických záznamov, podporuje zamestnancov pri udržiavaní záznamov v spisoch. Pomáha pri dodržiavaní zákonných lehôt, archivácii a vyradovanom procese záznamov.

Zavedenie elektronickej správy registratúry neprináša výhodu len v splnení legislatívnej povinnosti. Aplikácia zavedie poriadok v dokumentácii organizácie, sprístupní dokumenty zamestnancom v elektronickej podobe, pričom originál môže byť bezpečne uložený v príručnej registratúre zodpovednej osoby. Tým sa predchádza riziku straty originálneho dokumentu. Systém stráži lehoty spracovania, automatizuje tvorbu zoznamov záznamov na vyradenie.

3.13.1 Charakteristika elektronického informačného systému NUNTIO ASSR

Elektronický informačný systém NUNTIO ASSR je určený pre správu a riadenie informačného toku, elektronické ukladanie dokumentov, ale aj pre správu registratúry v organizácii. Zabezpečuje správu dokumentov počas ich životného cyklu od vzniku, cez triedenie, sledovanie obehu, spracovanie, schvaľovanie, vybavenie, monitorovanie stavu a miesta spracovania, uloženie, až po odoslanie z organizácie.

NUNTIO ASSR ponúka a podporuje:

- a) prehľadnú správu dokumentov prostredníctvom modulov;
- b) elektronicky riadený obeh záznamov v rámci organizácie;
- c) vkladanie dokumentov zo súborového systému alebo zo skenovacieho pracoviska;
- d) vkladanie preddefinovaných elektronických formulárov;
- e) verzionovanie príloh;
- f) monitorovanie obehu a kontrolu stavu spracovania záznamov;
- g) bezpečné uloženie záznamov;
- h) okamžité sprístupnenie uložených dokumentov pre iných používateľov na podporu a urýchlenie toku informácií;
- i) správu registratúry v organizáciách;
- j) komunikáciu s eDesk schránkami na ÚPVS;
- k) komunikáciu so systémom CEP cez elektronickú podateľňu;
- l) podpisovanie zaručeným elektronickým podpisom;
- m) zaručenú elektronickú konverziu dokumentov.

Aplikácia je postavená tak, aby v rôznych situáciách dovoľovala používateľovi použiť len tie nástroje, ktoré sú v danom okamihu pre neho povolené. Taktiež práva na zobrazenie záznamov, spisov a úložných jednotiek sú riadené prístupom. Nosným prvkom aplikácie sú jednoznačne určené procesy vytvorené pre rôzne typy záznamov, ktoré aplikácia povoľuje vygenerovať. Proces pre každý typ záznamu je vytvorený unikátne s prihliadnutím na jeho funkciu a účel. Niektoré typy záznamov sú podporené schvaľovacím procesom, ktorý je napasovaný na vnútorné procesy konkrétnej organizácie. Je snaha o minimalizáciu obehu papierovej podoby dokumentu, keďže aplikácia NUNTIO ASSR zabezpečuje možnosť obehu dokumentu aj v elektronickej forme.

Celý informačný systém je rozdelený do jednotlivých modulov, ktoré riešia správu dokumentov a týkajú sa určitej problematiky. Zobrazenie modulov je dané prístupovými právami používateľa.

Elektronický informačný systém NUNTIO ASSR obsahuje nasledovné moduly:

Denník

Slúži na evidenciu záznamov a sledovanie ich stavu.

Spisy

Slúži na prehliadanie vytvorených spisov a prácu s nimi.

Príručná registratúra

Modul slúži na tvorbu úložných jednotiek (ďalej ÚJ) a prácu s nimi.

Registratúrne stredisko

Poskytuje možnosti archivácie a vyradenia úložných jednotiek.

Registratúrny plán

Zobrazuje samotný registratúrny plán organizácie a povoľuje prácu s kategóriami vecných skupín a vecnými skupinami.

Podateľňa

Eviduje prichádzajúcu poštu do organizácie a rozposiela ju na útvary.

Expedovanie

Slúži na odoslanie vybavených záznamov z organizácie.

Vyhľadávanie

Slúži na vyhľadávanie záznamov, spisov, úložných jednotiek podľa rôznych atribútov.

Adresár

Modul poskytuje adresár fyzických a právnických osôb, s ktorými prichádza organizácia do styku, v ktorom je umožnené prehľadávanie.

Zastupovanie

Modul poskytuje vedúcemu pracovníkovi nastaviť zastupovanie pre referentov na svojom útvare alebo podriadenom útvare pre prácu v elektronickom informačnom systéme NUNTIO ASSR.

Organizačná štruktúra

Modul poskytuje správcovi možnosť úpravy organizačnej štruktúry organizácie.

Správa aplikácie

Modul je prístupný len pre administrátora a obsahuje systémové nástroje.

Aplikačné oznámenia

Slúži na spracovanie asynchrónnych funkcií.

Pomoc

Poskytuje link na používateľskú príručku a iné zdieľané dokumenty.

3.13.2 Správa registratúry

Správu registratúry upravuje:

- Zákon Národnej rady Slovenskej republiky č. 395/2002 Z. z. o archívoch a registratúrach a doplnení niektorých zákonov v znení neskorších predpisov;
- Vyhláška MV SR č. 628/2002 Z. z., ktorou sa vykonávajú niektoré ustanovenia zákona o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov;
- výnos MV SR č. 525/2011 Z. z. o štandardoch pre elektronické systémy na správu registratúry;

ako zabezpečovanie evidovania, tvorby, ukladania, ochrany registratúrnych záznamov, prístupu k nim a zabezpečovanie ich vyradovania.

Predmetom správy registratúry je zabezpečenie manipulácie s registratúrnymi záznamami, komplexná starostlivosť o ochranu a uloženie registratúrnych záznamov do uplynutia ich prevádzkovej potreby.

Registratúrny záznam je informácia evidovaná pôvodcom registratúry. V príručke sa tento pojem identifikuje termínom **záznam**.

Spis je registratúrny záznam alebo súbor registratúrnych záznamov, ktoré vznikli v súvislosti s vybavovaním tej istej veci. V príručke aj aplikácii sa tento pojem identifikuje rovnako termínom **spis**.

Systém NUNTIO ASSR kopíruje procesy správy registratúry v dohodnutom rozsahu, ktorého zmyslom je spravovať čoraz väčšie množstvo registratúrnych záznamov v organizácii a poskytovať rýchlo a v požadovanom rozsahu kvalitné informácie.

3.13.3 Funkčné vlastnosti NUNTIO ASSR

Podateľňa	Spisy	Príručná registratúra	Reg. stredisko
Evidencia prijatých záznamov	Spracovanie záznamov	Tvorba ukladacích jednotiek	Preberanie ukladacích jednotiek z útvarov
Spracovanie odosielaných záznamov	Vytvorenie spisu, zakladanie záznamov do spisov	Uzamykanie spisov	Lokalizácia fyzických spisov
Evidencia a správa adresátov	Používanie preddefinovaných šablón	Zaraďovanie spisov do ukladacích jednotiek	Podpora vyradovacieho konania
Pripojenie naskenovaného dokumentu	Kontrola termínov vybavenia	Podpora vyradovacieho procesu spisov	Správa výpožičiek
Pridelenie pošty na vybavenie, tlačové zostavy	Uzatvorenie spisu, ročná uzávierka	Tlač odovzdávacieho protokolu do RS	Rôzne tlačové zostavy

3.13.4 Prínosy riešenia NUNTIO ASSR

- podporuje legislatívne korektnú správu registratúry
- podporí úplnú evidenciu záznamov prichádzajúcich do a odchádzajúcich z organizácie
- sprehľadní a zjednotí správu záznamov
- upozorní na dôležité termíny
- poskytne prehľad o stave spracovania záznamov
- podporí používanie záväzných podnikových štandardov pre písanie dokumentov
- zjednoduší vyradovacie procesy v zmysle platnej legislatívy
- so systémom získate aj odborné poradenstvo pri tvorbe internej predpisovej dokumentácie v oblasti správy registratúry (registratúrne poriadky, plány...)
- má „user friendly“ používateľské prostredie s jednoduchým ovládaním
- rešpektuje špecifiká a požiadavky organizácie

3.13.5 Postup a podmienky prístupu do NUNTIO ASSR

Základné pravidlá prevádzky, zásady bezpečnej a spoľahlivej prevádzky, správy, podpory a využívania služieb sú riešené prostredníctvom „Prevádzkového poriadku NUNTIO ASSR rezortu Ministerstva kultúry Slovenskej republiky“ v platnom znení.

Základné pravidlá prevádzky WAN VPN siete (rezortná sieť) a určenie zásad jej bezpečnej a spoľahlivej prevádzky sú riešené prostredníctvom „Prevádzkového poriadku WAN VPN siete rezortu MK SR“ v platnom znení.

4. Podmienky spracúvania osobných údajov

1. Účel a prostriedky spracúvania osobných údajov stanovuje Prevádzkovateľ pre tie IS, ktorých je Prevádzkovateľom, pokiaľ tento nie je stanovený osobitným zákonom.
2. Ak účel spracúvania osobných údajov stanovuje osobitný zákon, v takom prípade zabezpečí Prevádzkovateľ jeho primeranú aplikáciu do vlastných podmienok.
3. Účelom spracúvania osobných údajov je vopred jednoznačne vymedzený zámer spracúvania osobných údajov, ktorý sa viaže na určitú činnosť.
4. Spôsob a podmienky spracúvania osobných údajov musí vždy zodpovedať stanovenému účelu ich spracúvania a musí byť v súlade so zákonmi.
5. Pred začatím každého spracúvania osobných údajov musia byť vopred stanovené:
 - a.) identifikácia IS, v ktorom budú údaje spracúvané,
 - b.) účel spracúvania osobných údajov,
 - c.) zoznam spracúvaných údajov,
 - d.) okruh dotknutých osôb,
 - e.) právny základ IS,¹
 - f.) dátum začatia spracúvania osobných údajov,
 - g.) organizačná zložka, ktorá riadi spracúvanie osobných údajov,
 - h.) ďalšie organizačné zložky alebo zamestnanci, ktorí sa podieľajú na spracúvaní údajov² s uvedením povolených činností pri spracúvaní osobných údajov,
 - i.) spôsob získavania osobných údajov,
 - j.) spôsob nakladania s údajmi po splnení a skončení účelu ich spracúvania,
 - k.) doba uchovávania osobných údajov po skončení účelu ich spracúvania,
 - l.) okruh príjemcov, ktorým sú osobné údaje sprístupnené,
 - m.) tretie strany, ktorým sú osobné údaje poskytnuté,
 - n.) forma zverejnenia osobných údajov a právny základ ich zverejnenia,³
 - o.) tretie krajiny do ktorých je uskutočňovaný cezhraničný prenos osobných údajov a právny základ cezhraničného toku.
6. Navrhované podmienky spracúvania osobných údajov uvedené v bode č. 5. tohto článku Smernice posúdi pred začatím ich spracúvania určená osoba z pohľadu zaistenia ich súladu s právnymi predpismi.
7. V prípade kladného posúdenia podľa predchádzajúceho bodu a zabezpečenia zákonných podmienok pri spracúvaní osobných údajov povolí spracúvanie osobných údajov štatutárny zástupca Prevádzkovateľa.

¹ spracúvanie sa vykonáva na základe právneho základu, ktorý je uvedený v článku 6 ods. 1 nariadenia GDPR: .

² do tejto kategórie spadajú napr. zamestnanci, ktorí k osobným údajom pristupujú v rámci ich pracovného zaradenia a stanovených pracovných povinností.

³ Zverejnenie osobných údajov dotknutých osôb je možné vykonávať iba v zmysle osobitného alebo na základe predchádzajúceho písomného súhlasu dotknutej osoby so zverejnením poskytnutých osobných údajov.

8. Ak v priebehu spracúvania osobných údajov príde k zmene niektorej zo skutočností uvedených v bode 5. tohto článku Smernice, posúdenie uvedené v predchádzajúcich bodoch sa zopakuje.
9. Účel spracúvania osobných údajov v informačnom systéme musí byť v súlade s pôsobnosťou určenou právnymi predpismi. Spracúvanie osobných údajov za iným účelom sa zakazuje.
10. Preukázateľne poveriť a poučiť osoby v zamestnaneckom alebo obdobnom pracovnom vzťahu o právach a povinnostiach ustanovených Zákomom a zodpovednosti za ich porušenie (povinnosť mlčanlivosti), ktorými sa budú riadiť pri vykonávaní spracovateľských operácií v automatizovanom a neautomatizovanom IS. Vzor Záznamu o poverení oprávnenej osoby s prístupom k IS – príloha č. 4 tejto Smernice.
11. Schváliť aktuálny zoznam poverených oprávnených osôb, určených na spracúvanie osobných údajov v IS s vymedzením rozsahu ich oprávnení.
12. V odôvodnených prípadoch poveriť a poučiť iné fyzické osoby, ktoré prídu do styku s osobnými údajmi u prevádzkovateľa, majú alebo môžu mať prístup k IS o právach a povinnostiach ustanovených Zákomom a o zodpovednosti za ich porušenie. Vzor Záznamu o poučení inej fyzickej osoby – príloha č. 4 tejto Smernice.
13. Spracúvanie osobných údajov iným spôsobom, ako stanovuje táto Smernica sa zakazuje.

5. Dohľad nad ochranou osobných údajov

1. Za výkon dohľadu nad ochranou osobných údajov spracúvaných podľa tohto zákona zodpovedá Prevádzkovateľ.
2. Prevádzkovateľ prijme s ohľadom na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb vhodné technické a organizačné opatrenia, aby zabezpečil a bol schopný preukázať, že spracúvanie sa vykonáva v súlade s nariadením GDPR a zákonom o ochrane osobných údajov. Tieto opatrenia podľa potreby preskúma a aktualizuje.
3. Prevádzkovateľ 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 nariadenia GDPR a chrániť práva dotknutých osôb, pričom prihliadne 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.
4. 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 uchovávaní a ich dostupnosť. Konkrétne sa takýmito opatreniami zabezpečí, aby osobné údaje neboli bez zásahu fyzickej osoby štandardne prístupné neobmedzenému počtu fyzických osôb.
5. Prevádzkovateľ, ktorý je orgán verejnej moci alebo verejnoprávny subjekt s výnimkou súdov pri výkone ich súdnej právomoci, alebo ak hlavnými činnosťami Prevádzkovateľa sú spracovateľské operácie, ktoré si vzhľadom na svoju povahu, rozsah a/alebo účely vyžadujú pravidelné a systematické monitorovanie dotknutých osôb vo veľkom rozsahu; alebo ak hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa je spracúvanie osobitných kategórií údajov (podľa článku 9 GDPR) vo veľkom rozsahu alebo spracúvanie osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky (podľa článku 10 GDPR), je povinný určiť zodpovednú osobu a jej určenie nahlásiť na Úrad na ochranu osobných údajov (prostredníctvom webového formulára, ktorý je dostupný na webovom sídle Úradu).
6. Písomné poverenie zodpovednej osoby vykonáva štatutárny zástupca Prevádzkovateľa, pritom postupuje podľa GDPR a Zákona⁴.
7. Vzor písomného poverenia zodpovednej osoby je uvedený v prílohe č. 2a tejto Smernice. Zakladá sa do osobného spisu zamestnanca, jeho kópia sa zakladá do bezpečnostnej dokumentácie (Bezpečnostného projektu) na ochranu osobných údajov Prevádzkovateľa.
8. Prevádzkovateľ písomne informuje Úrad o poverení zodpovednej osoby za Prevádzkovateľa prostredníctvom webového formulára na stránke Úradu: <https://dataprotection.gov.sk/uouu/zo/register-zo>
9. Zodpovedná osoba poverená výkonom dohľadu nad ochranou osobných údajov 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, ktoré má v zmysle GDPR a Zákona..

⁴ Článok 37 až 39 GDPR a § 44 až 46 Zákona.

5.1 Zodpovedná osoba – práva a povinnosti

Zodpovedná osoba poverená k výkonu dohľadu nad ochranou osobných údajov v podmienkach Prevádzkovateľa má najmä nasledovné povinnosti zodpovednej osoby, ktoré sú vymedzené v článku 39 GDPR ako aj v § 46 Zákona a zahŕňajú nasledujúce činnosti:

- a.) poskytovanie informácií a poradenstva prevádzkovateľovi alebo sprostredkovateľovi a zamestnancom, ktorí vykonávajú spracúvanie, o ich povinnostiach podľa nariadenia GDPR a ostatných právnych predpisov EÚ alebo podľa Zákona, osobitných predpisov alebo medzinárodných zmlúv, ktorými je Slovenská republika viazaná, týkajúcich sa ochrany osobných údajov,⁵
- b.) monitorovanie súladu s nariadením GDPR, s ostatnými právnymi predpismi EÚ Zákonom, osobitnými predpismi alebo medzinárodnými zmluvami, ktorými je Slovenská republika viazaná, 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 GDPR a/alebo § 42 Zákona,
- d.) spolupráca s dozorným orgánom, ktorým je Úrad na ochranu osobných údajov SR,
- e.) plnenie úlohy kontaktného miesta pre dozorný orgán v súvislosti s otázkami týkajúcimi sa spracúvania vrátane predchádzajúcej konzultácie uvedenej v článku 36 GDPR a/alebo § 43 Zákona a podľa potreby aj konzultácie v akýchkoľvek iných veciach,
- f.) náležite zohľadňuje riziko spojené so spracovateľskými operáciami, pričom berie na vedomie povahu, rozsah, kontext a účely spracúvania.

⁵ Článok 39 ods. 1 písm. a) GDPR a § 46 ods. 1 písm. a) Zákona.

6. Poverenie a povinnosti oprávnenej osoby

6.1 Poverenie oprávnenej osoby a spôsob jej poučenia

V zmysle článku 29 GDPR ako aj § 36 Zákona, 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 EÚ, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná⁶.

Poverená osoba je oprávnenou osobou, ktorá môže prichádzať do styku s osobnými údajmi a na predmetné činnosti bola náležite určená.⁷

Fyzická osoba, (prípadne aj spolupracujúca právnická osoba, ktorá nemá postavenie sprostredkovateľa) navrhovaná na oboznamovanie sa s osobnými údajmi v rámci jej pracovného zaradenia je poverená ako aj poučená o svojich povinnostiach spravidla ku dňu vzniku pracovného pomeru avšak vždy pred vydaním prvého pokynu k spracovateľskej operácii.

Prevzatie poverenia ako aj poučenie o svojich povinnostiach potvrdí poverená osoba vlastnoručným podpisom. Evidenciu písomného poučenia poverenej osoby zabezpečuje osoba určená osoba. Poverenie sa vyhotovuje v jednom výtlačku, ktorý sa zakladá do osobného spisu. Poverenie sa vyhotovuje podľa vzoru vedeného v prílohe č. 4 tejto Smernice.

Písomný zoznam poverených osôb s prístupom k osobným údajom vedie a aktualizuje písomne poverená zodpovedná osoba na základe požiadaviek predkladaných vedúcimi interných organizačných zložiek Prevádzkovateľa. Zoznam je uložený v dokumentácii Bezpečnostného projektu na ochranu osobných údajov Prevádzkovateľa a vyhotovuje sa podľa vzoru vedeného v prílohe č. 3 tejto Smernice.

Písomný zoznam určených poverených osôb s prístupom k osobným údajom je platný po jeho schválení štatutárnym zástupcom Prevádzkovateľa.

Poverenie oprávnenej osoby vykonáva štatutárny zástupca, prípadne ním poverená osoba, pričom môže ísť aj o zodpovednú osobu, ktorá je kompetentná podať všetky nasledovné informácie v rozsahu:

- a) o právach a povinnostiach ustanovených GDPR, Zákonom, inými právnymi predpismi a o zodpovednosti za ich porušenie,
- b) o rozsahu oprávnení,
- c) o rozsahu a popise povolených činností pri prístupe k osobným údajom,
- d) o podmienkach spracúvania osobných údajov,
- e) o spôsobe výkonu uložených činností pri práci s informačným systémom,
- f) o pravidlách a spôsobe ochrany osobných údajov pred ich stratou, poškodením alebo neautorizovaným prístupom,
- g) o povinnosti mlčanlivosti o osobných údajov v súlade s § 79 Zákona, ktoré trvá aj po skončení pracovného pomeru, štátnozamestnaneckého pomeru, služobného pomeru alebo obdobného pracovného vzťahu tejto fyzickej osoby.

Poverená osoba musí byť informovaná o zodpovednej osobe písomne poverenej dohľadom nad ochranou osobných údajov u Prevádzkovateľa. Prevádzkovateľ rovnako zabezpečí adekvátne školenie, prípadne poučenie poverenej osoby o jej právach a povinnostiach vyplývajúcich z právnych predpisov na ochranu osobných údajov.

⁶ Články 29, 32 ods. 4 GDPR.

⁷ vzor poverenia: viď príloha č. 3 tejto Smernice.

Poučenie potvrdí poverená osoba vlastnoručným podpisom. Evidenciu písomného poučenia poverenej osoby zabezpečuje zodpovedná osoba, ktorá poučenie vykonala, prípadne iná určená osoba. Poučenie sa vyhotovuje v jednom výtlačku, ktorý sa zakladá do osobného spisu, alebo priamo do dokumentácie Bezpečnostného projektu na ochranu osobných údajov, ktorú vedie a aktualizuje Zodpovedná osoba za IS.

V prípade zmeny spôsobu spracúvania osobných údajov v IS je poverená osoba, ktorá tieto zmeny vykonala, povinná toto bezodkladne ohlásiť písomne poverenej zodpovednej osobe za IS.

Každá iná fyzická osoba a pracovník tretej strany (subdodávateľa) ktorému budú sprístupnené osobné údaje spracúvané Prevádzkovateľom musí byť informovaný o:

- a) rozsahu oprávnení a povolených činností pri prístupe k osobným údajom,
- b) spôsobe výkonu uložených činností pri práci s informačným systémom,
- c) pravidlách a spôsobe ochrany osobných údajov pred ich stratou, poškodením alebo neautorizovaným prístupom,
- d) poučení o mlčanlivosti v súlade s § 79 Zákona.

6.2 Práva poverenej osoby

Poverená osoba má právo vykonávať spracovateľské operácie s osobnými údajmi spracúvanými v informačných systémoch v ktorom bola určená ako poverená osoba na základe pokynu Prevádzkovateľa výlučne v súlade s právnym základom, od ktorého Prevádzkovateľ odvodzuje oprávnenie spracúvať osobné údaje, a to len v rozsahu a spôsobom, ktorý je nevyhnutný na dosiahnutie ustanoveného alebo vymedzeného účelu spracúvania a je v súlade s právnymi predpismi na ochranu osobných údajov a internými riadiacimi aktmi Prevádzkovateľa.

Poverená osoba má právo najmä na:

- a) pridelenie prístupových práv do určených informačných systémov osobných údajov Prevádzkovateľa v rozsahu nevyhnutnom na plnenie jej úloh; nevyhnutnosť priamo determinuje pracovné zaradenie poverenej osoby v rozsahu opisu činností jej pracovného miesta,
- b) opätovné poučenie, ak došlo k podstatnej zmene jej pracovného alebo funkčného zaradenia, a tým sa významne zmenil obsah náplne jej pracovných činností, alebo sa podstatne zmenili podmienky spracúvania osobných údajov alebo rozsah spracúvaných osobných údajov v rámci jej pracovného alebo funkčného zaradenia,
- c) povinnosť mlčanlivosti podľa § 78 ods. 1 a 2 Zákona 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,
- d) vykonávanie spracovateľských operácií s osobnými údajmi v mene Prevádzkovateľa, vrátane osobitnej kategórie osobných údajov, v rozsahu nevyhnutnom na plnenie pracovných úloh určených opisom pracovného miesta poverenej osoby,
- e) odmietnutie vykonať pokyn k spracúvaniu osobných údajov, ktorý je v rozpore so všeobecne záväznými právnymi predpismi alebo dobrými mravmi,
- f) na vydanie dokladu (poverenia), ktorým bude preukazovať svoju pracovnú príslušnosť k zamestnávateľovi v prípade, že získava osobné údaje mimo sídla Prevádzkovateľa.

Vo vzťahu ku kontrole vykonávanej podľa Zákona poverená osoba má právo najmä:

- a) na profesionálny prístup kontrolného orgánu pri výkone kontroly,
- b) vyžadovať od kontrolného orgánu preukázať sa poverením na vykonanie kontroly a svojou príslušnosťou k úradu, ak je oprávnenou osobou štatutárny orgán, alebo osoba oprávnená konať v mene štatutárneho orgánu; to platí aj v prípade, ak sa na kontrole zúčastňuje aj prizvaná osoba,

- c) oboznamovať sa s kontrolnými zisteniami a písomne sa k nim vyjadrovať, ak je oprávnenou osobou štatutárny orgán alebo osoba oprávnená konať v mene štatutárneho orgánu,
- d) podávať písomné námietky po oboznámení sa s kontrolnými zisteniami, ak je oprávnenou osobou štatutárny orgán alebo osoba oprávnená konať v mene štatutárneho orgánu,
- e) vyžadovať plnenie povinností kontrolného orgánu pri výkone kontroly podľa § 90 a nasl. Zákona, ak je oprávnenou osobou štatutárny orgán alebo osoba oprávnená konať v mene štatutárneho orgánu.

Rozsah konkrétnych spracovateľských operácií, ktorý bude poverená osoba vykonávať, je definovaný úrovňou prístupu k jednotlivým informačným systémom osobných údajov v poverení osoby (ďalej len „poverenie“).

6.3 Povinnosti poverenej osoby:

- a) Poverená osoba je v súvislosti so spracúvaním osobných údajov povinná rešpektovať príslušné povinnosti formulované Prevádzkovateľom najmä v rámci:
 - a. bezpečnostnej dokumentácie informačných systémov osobných údajov,
 - b. interných predpisov ktoré súvisia s výkonom pracovnej pozície a s ktorými bola oboznámená pred prvým pokynom k spracovateľskej operácii.
 - c. spracúvať osobné údaje len na základe pokynu Prevádzkovateľa IS prostredníctvom svojho priameho nadriadeného, ktorý je povinný poverenú osobu oboznámiť aj s rozsahom spracovateľských operácií. V zmysle Zákona sa spracúvaním osobných údajov rozumie vykonávanie operácií alebo súboru operácií s osobnými údajmi, napr. ich:
 - získavanie, zhromažďovanie, zaznamenávanie,
 - usporadúvanie, prepracúvanie alebo zmena,
 - vyhľadávanie, prehliadanie,
 - preskupovanie, kombinovanie, premiestňovanie,
 - využívanie, uchovávanie, likvidácia,
 - prenos, poskytovanie, sprístupňovanie alebo zverejňovanie.
- b) Poverená osoba nesmie osobné údaje spracúvané prevádzkovateľom využiť pre osobnú potrebu, či potrebu inej osoby alebo na iné, než služobné účely podľa tohto poverenia.
- c) Pri uchovávaní osobných údajov poverená osoba je povinná rešpektovať úschovné lehoty záznamov v súlade s Registratúrnym poriadkom a plánom a u záznamov, ktoré sú zaradené do predarchívnej starostlivosti stanovovať len dobu nevyhnutnú na uplatnenie práv alebo povinností ustanovených osobitným zákonom.
- d) Zakazuje sa poskytovať alebo sprístupňovať osobné údaje dotknutých osôb iným osobám ako oprávneným alebo subjektom určeným osobitným zákonom, poskytovať osobné údaje a dôverné informácie k nim prostredníctvom telefónu, kedy nie je možné overiť totožnosť prijímateľa a jeho faktické oprávnenie na oboznamovanie sa so spracúvanými osobnými údajmi. V prípade pochybnosti o správnosti postupu je poverená osoba povinná vopred informovať poverenú zodpovednú osobu a vyžiadať si jej stanovisko.
- e) Poznať zodpovednú osobu za Prevádzkovateľa.
- f) V prípade zistenia, že spracúvanie osobných údajov nezodpovedá prijatým interným normám, právnym predpisom na ochranu osobných údajov alebo ním vzniká podozrenie z porušenia práv dotknutých osôb, prípadne, že došlo k bezpečnostnému incidentu oprávnená osoba je povinná bezodkladne oznámiť túto skutočnosť písomne zodpovednej osobe, alebo štatutárnemu orgánu.

Ďalšie povinnosti poverenej osoby:

- a) získavať na základe svojho pracovného zaradenia pre Prevádzkovateľa len nevyhnutné osobné údaje výlučne na zákonom ustanovený alebo vymedzený účel; je neprípustné, aby poverená osoba získavala osobné údaje pod zámienkou iného účelu spracúvania alebo inej činnosti,
- b) vykonávať povolené spracovateľské operácie len so správnymi, úplnými a podľa potreby aktualizovanými osobnými údajmi vo vzťahu k účelu spracúvania,
- c) nesprávne a neúplné osobné údaje je bez zbytočného odkladu povinná opraviť alebo doplniť; nesprávne a neúplné osobné údaje, ktoré nemožno opraviť alebo doplniť tak, aby boli správne a úplné je povinná blokovat', kým sa rozhodne o ich likvidácii v súlade s Registratúrnym poriadkom a registratúrnym plánom Prevádzkovateľa,
- d) pred získavaním osobných údajov od dotknutej osoby ju oboznámiť s názvom a sídlom Prevádzkovateľa, účelom spracúvania osobných údajov, rozsahom spracúvania osobných údajov, predpokladanom okruhu tretích strán pri poskytovaní osobných údajov alebo príjemcov pri sprístupňovaní osobných údajov, forme zverejnenia, ak sa osobné údaje zverejňujú a tretie krajiny, ak sa predpokladá, alebo je zrejmé, že sa do týchto krajín uskutoční cezhraničný prenos osobných údajov a ďalšími informáciami v súlade s článkom 13 nariadenia GDPR, vrátane poučenia o jej právach,
- e) zabezpečiť preukázateľný súhlas na spracúvanie osobných údajov dotknutej osoby v informačnom systéme osobných údajov prevádzkovateľa, ak sa osobné údaje spracúvajú na základe súhlasu dotknutej osoby, ,
- f) preukázať príslušnosť oprávnenej osoby k prevádzkovateľovi hodnoverným dokladom (napr. služobným preukazom, alebo poverením na získavanie),
- g) postupovať výlučne v súlade s technickými, organizačnými a personálnymi opatreniami prijatými prevádzkovateľom podľa článkov 24 a 25 nariadenia GDPR a ostatnými riadiacimi aktmi Prevádzkovateľa,
- h) vykonať likvidáciu osobných údajov, ktoré sú súčasťou už nepotrebných pracovných dokumentov (napr. rôzne pracovné súbory, pracovné verzie dokumentov v listinnej podobe) rozložením, vymazaním alebo fyzickým zničením hmotných nosičov tak, aby sa z nich osobné údaje nedali reprodukovať; to neplatí vo vzťahu k osobným údajom, ktoré sú súčasťou obsahu registratúrnych záznamov Prevádzkovateľa,
- i) v prípade nejasností pri spracúvaní osobných údajov sa obrátiť na Prevádzkovateľa alebo zodpovednú osobu (ak bola poverená),
- j) chrániť prijaté dokumenty a súbory pred stratou, poškodením, zneužitím, odcudzením, neoprávneným sprístupnením, poskytnutím alebo inými neprípustnými formami spracúvania,
- k) dodržiavať mlčanlivosť o osobných údajoch podľa § 79 Zákona, s ktorými poverená osoba v rámci svojho pracovného pomeru prichádza do styku, a to aj po zániku jej pracovného pomeru, okrem zákonom priznaných výnimiek podľa § 79 ods. 3 Zákona,
- l) dodržiavať všetky povinnosti, o ktorých bola poverená osoba poučená.

6.3.1 Povinnosti poverenej osoby vo vzťahu ku kontrole

Vo vzťahu ku kontrole vykonávanej podľa § 94 Zákona oprávnená osoba kontrolovanej osoby je povinná najmä:

- a) strpieť výkon kontroly a vytvoriť kontrolnému orgánu primerané podmienky na výkon kontroly a spracovanie kontrolných zistení,
- b) poskytnúť kontrolnému orgánu súčinnosť nevyhnutnú na riadny výkon kontroly, najmä pri dokumentovaní primeranej úrovne bezpečnosti s ohľadom na riziká, ktoré predstavuje spracúvanie osobných údajov v podmienkach prevádzkovateľa a sprostredkovateľa,
- c) v čase výkonu kontroly zabezpečiť kontrolnému orgánu dostupný a bezpečný prístup k zariadeniam, prostriedkom a k informačným systémom,
- d) poskytnúť kontrolnému orgánu požadovanú súčinnosť v súlade s jeho oprávneniami podľa § 93 a zdržať sa konania, ktoré by mohlo mariť výkon kontroly,

- e) dostaviť sa na predvolanie kontrolného orgánu s cieľom podať vysvetlenia k predmetu kontroly,
- f) v určenej lehote poskytnúť kontrolnému orgánu originál alebo kópiu dokladov, iných písomností, vyjadrenia a informácie, osobné údaje spracúvané na pamäťových médiách vrátane technických nosičov osobných údajov, výpisy a zdrojové kódy programov, ak ich vlastní alebo má k dispozícii, a ďalšie materiály alebo podklady potrebné na výkon kontroly a v odôvodnených prípadoch umožniť odoberať originály alebo kópie aj mimo priestorov kontrolovanej osoby,
- g) poskytnúť kontrolnému orgánu úplné a pravdivé ústne a písomné informácie, vyjadrenia a vysvetlenia ku kontrolovaným a s kontrolou súvisiacim skutočnostiam,
- h) na požiadanie kontrolného orgánu sa dostaviť na prerokovanie protokolu.

6.4 Zodpovednosť za porušenie práv a povinností

6.4.1 Zodpovednosť poverenej osoby za porušenie povinností

Poverená osoba je v zmysle § 79 Zákona povinná zachovávať mlčanlivosť o osobných údajoch, ktoré spracúva a s ktorými príde do styku. Povinnosť mlčanlivosti trvá aj po skončení spracúvania osobných údajov. Povinnosť mlčanlivosti 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.

- a) Porušením povinností alebo zneužitím oprávnení pri spracúvaní osobných údajov môže poverená osoba naplniť skutkovú podstatu občianskoprávných, administratívno-právných deliktov, pričom takéto konanie môže zamestnávateľ vyhodnotiť ako porušenie pracovnej disciplíny, prípadne závažné porušenie pracovnej disciplíny, ktorej dôsledok môže byť okamžité skončenie pracovného pomeru.

6.4.2 Trestná zodpovednosť poverenej osoby a Prevádzkovateľa

Poverená osoba môže v súvislosti s protiprávnym nakladaním s osobnými údajmi čeliť aj trestnému stíhaniu za trestné činy podľa § 247 (neoprávnený prístup do počítačového systému), § 247a (neoprávnený zásah do počítačového systému), § 247b (neoprávnený zásah do počítačového údaj), § 247c (neoprávnené zachytávanie počítačových údajov), § 247d (výroba a držba prístupového zariadenia, hesla do počítačového systému alebo iných údajov) a § 374 (neoprávnené nakladanie s osobnými údajmi) zákona č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov alebo môže voči nej byť vedené administratívne konanie.

V zmysle zákona NR SR č. 91/2016 Z. z. o trestnej zodpovednosti právnických osôb a o zmene a doplnení niektorých zákonov môže dôjsť v súvislosti s trestnými činmi podľa § 247 (neoprávnený prístup do počítačového systému), § 247a (neoprávnený zásah do počítačového systému), § 247b (neoprávnený zásah do počítačového údaj), § 247c (neoprávnené zachytávanie počítačových údajov), § 247d (výroba a držba prístupového zariadenia, hesla do počítačového systému alebo iných údajov) k založeniu trestnoprávnej zodpovednosti Prevádzkovateľa.

K založeniu trestnoprávnej zodpovednosti Prevádzkovateľa môže dôjsť ak je trestný čin spáchaný v prospech, alebo v mene Prevádzkovateľa, alebo v rámci jeho činnosti, alebo prostredníctvom konania:

- a) štatutárneho orgánu alebo člena štatutárneho orgánu,
- b) toho, kto vykonáva kontrolnú činnosť alebo dohľad v rámci právnickej osoby, alebo
- c) inou osobou, ktorá je oprávnená zastupovať právnickú osobu alebo za ňu rozhodovať.

Trestný čin je spáchaný Prevádzkovateľom aj vtedy, ak osoba uvedená v odsekoch a), b) a c) nedostatočným dohľadom alebo kontrolou, ktoré boli jej povinnosťou, hoci z nedbanlivosti

umožnila spáchať trestný čin osobou, ktorá konala v rámci oprávnení, ktoré jej boli zverené právnickou osobou, napríklad v rámci plnenia pracovných úloh.

Trestná zodpovednosť právnickej osoby nie je podmienená vyodením trestnej zodpovednosti voči fyzickej osobe uvedenej v odsekoch a), b) a c) tohto bodu a nie je podmienená ani zistením, ktorá konkrétna fyzická osoba sa dopustila konania, ktoré zakladá trestnú zodpovednosť Prevádzkovateľa.

Trestná zodpovednosť fyzickej osoby, ktorá konala spôsobom, ktorým bola založená trestná zodpovednosť Prevádzkovateľa nie je založením trestnoprávnej zodpovednosti Prevádzkovateľa nijako dotknutá.

7. Zásady spracúvania osobných údajov a zákonnosť ich spracúvania

1. Prevádzkovateľ zabezpečí, aby osobné údaje boli spracúvané v súlade s nasledujúcimi zásadami⁸:

- a) *zákonnosť, spravodlivosť a transparentnosť*, ktorá zahŕňa povinnosť spracúvať osobné údaje na základe zákonného základu, spravodlivo a transparentne vo vzťahu k dotknutej osobe;

Každé spracúvanie osobných údajov by malo byť zákonné a spravodlivé. Pre fyzické osoby by malo byť transparentné, že sa získavajú, používajú, konzultujú alebo inak spracúvajú osobné údaje, ktoré sa ich týkajú, ako aj to, v akom rozsahu sa tieto osobné údaje spracúvajú alebo budú spracúvať. Zásada transparentnosti si vyžaduje, aby všetky informácie a komunikácia súvisiace so spracúvaním týchto osobných údajov boli ľahko prístupné a ľahko pochopiteľné a formulované jasne a jednoducho. Uvedená zásada sa týka najmä informácií pre dotknuté osoby o identite prevádzkovateľa a účeloch spracúvania, a ďalších informácií na zabezpečenie spravodlivého a transparentného spracúvania, pokiaľ ide o dotknuté fyzické osoby a ich právo získať potvrdenie a oznámenie spracúvaných osobných údajov, ktoré sa ich týkajú. Fyzické osoby by mali byť upozornené na riziká, pravidlá, záruky a práva pri spracúvaní osobných údajov, ako aj na to, ako uplatňovať svoje práva pri takomto spracúvaní.

- b) *obmedzenie účelu*, ktoré spočíva v povinnosti, aby osobné údaje boli získavané na konkrétne určené, výslovne uvedené a legitímne účely a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmito účelmi (výnimka: archivácia, vedecký alebo historický výskum či štatistický účel).

Každé spracúvanie osobných údajov je potrebné na konkrétne účely, na ktoré sa osobné údaje spracúvajú. Tieto by mali byť výslovne uvedené a legitímne a stanovené v čase získavania osobných údajov.

- c) *minimalizácia údajov*, ktorá spočíva v povinnosti spracúvať osobné údaje primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú

Osobné údaje by mali byť primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú. To si vyžaduje najmä zabezpečenie toho, aby obdobie, počas ktorého sa tieto osobné údaje uchovávajú, bolo obmedzené na nevyhnutný rozsah. Rovnako je potrebné rešpektovať potrebu spracúvať osobné údaje len vtedy, ak účel spracúvania nebolo možné za primeraných podmienok dosiahnuť inými prostriedkami.

- d) *správnosť*, ktorá spočíva v povinnosti spracúvať správne a podľa potreby aktualizované osobné údaje, pričom je nevyhnutné zabezpečiť, aby sa prijali všetky potrebné opatrenia, že sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bezodkladne vymažú alebo opravia.

Uvedená zásada predpokladá prijatie všetkých primeraných opatrení, aby sa zabezpečila oprava alebo vymazanie nesprávnych údajov.

⁸ Článok 5 ods. 1 GDPR.

- e) *minimalizácia uchovávaní*, ktorá spočíva, že 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, pokiaľ sa budú spracúvať výlučne na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či na štatistické účely za predpokladu prijatia primeraných technických a organizačných opatrení vyžadovaných nariadením GDPR na ochranu práv a slobôd dotknutých osôb.

S cieľom zabezpečiť, aby sa osobné údaje neuchovávali dlhšie, než je to nevyhnutné, by mal prevádzkovateľ stanoviť lehoty na vymazanie alebo pravidelné preskúmanie.

- f) *integrita a dôvernosť*, ktorá spočíva v povinnosti spracúvať osobné údaje 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.

Osobné údaje by sa mali spracúvať tak, aby sa zabezpečila primeraná bezpečnosť a dôvernosť osobných údajov vrátane predchádzania neoprávnenému prístupu k osobným údajom a zariadeniu používanému na spracúvanie, alebo neoprávnenému využitiu týchto údajov a zariadení.

2. Za dodržiavanie uvedených zásad zodpovedá prevádzkovateľ, ktorý je povinný preukázať ich dodržiavať a súlad pri spracúvaní osobných údajov. Prevádzkovateľ stanovil, že dodržiavanie týchto zásad sleduje zodpovedná osoba, ktorá v prípade zistenia nesúladu spracúvania osobných údajov s týmito zásadami bezodkladne informuje štatutárneho zástupcu Prevádzkovateľa.
3. Aby bolo spracúvanie zákonné, osobné údaje by sa mali spracúvať na právnom základe, ktorý je vyjadrený v GDPR. Podmienka zákonnosti spracúvania je splnená, ak je naplnená aspoň jedna z nižšie uvedených podmienok:

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

Ak je spracúvanie založené na súhlase dotknutej osoby, prevádzkovateľ by mal vedieť preukázať, že dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov, pričom dotknutá osoba si musí byť vedomá, že dáva súhlas a v akom rozsahu ho udeľuje. Súhlas, ktorý vopred naformuloval Prevádzkovateľ, musí byť v zrozumiteľnej a ľahko dostupnej forme a formulované jasne a jednoducho a nemal by obsahovať nekalé podmienky. Aby sa zaistilo, že súhlas bude informovaný, dotknutá osoba by si mala byť vedomá aspoň identity prevádzkovateľa a zamýšľaných účelov spracúvania osobných údajov. Súhlas by sa nemal považovať za slobodný, ak dotknutá osoba nemá skutočnú alebo slobodnú voľbu alebo nemôže odmietnuť či odvolať súhlas bez nepriaznivých následkov.

Súhlas sa nepovažuje za poskytnutý slobodne, ak nie je možné dať samostatný súhlas na jednotlivé spracovateľské operácie osobných údajov napriek tomu, že by to bolo v konkrétnom prípade vhodné, alebo ak sa plnenie zmluvy vrátane poskytnutia služby podmieňuje takýmto súhlasom, aj keď to na takéto plnenie nie je takýto súhlas nevyhnutný.

Ak je spracúvanie založené na súhlase, prevádzkovateľ musí vedieť preukázať, že dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov, pričom dotknutá osoba má právo kedykoľvek odvolať svoj súhlas. Odvolanie súhlasu nemá vplyv na zákonnosť spracúvania vychádzajúceho zo súhlasu pred jeho odvolaním.

Pred poskytnutím súhlasu musí byť dotknutá osoba o tejto skutočnosti informovaná. Odvolanie súhlasu musí byť také jednoduché ako jeho poskytnutie.

V súvislosti s ponukou služieb informačnej spoločnosti adresovanou priamo dieťaťu je spracúvanie osobných údajov dieťaťa zákonné, len ak má dieťa aspoň 16 rokov. Ak má dieťa menej než 16 rokov, takéto spracúvanie je zákonné iba za podmienky a v rozsahu, v akom takýto súhlas vyjadril alebo schválil zákonný zástupca.

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

Spracúvanie by sa malo považovať za zákonné, ak je potrebné v súvislosti so zmluvou alebo s úmyslom uzatvoriť zmluvu.

- c) spracúvanie je nevyhnutné na *splnenie zákonnej povinnosti prevádzkovateľa*;

Ak sa spracúvanie vykonáva v súlade so zákonnými povinnosťami, ktoré má prevádzkovateľ, alebo ak je spracúvanie potrebné na splnenie úlohy realizovanej vo verejnom záujme alebo z úradnej moci, základ pre spracúvanie by mal existovať v práve EÚ alebo v práve SR. Za dostatočný právny základ možno považovať právny predpis, ktorý je základom pre viaceré spracovateľské operácie založené na zákonnej povinnosti, ktorá sa vzťahuje na prevádzkovateľa, alebo ak je spracúvanie nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci, pričom právny predpis by mal rozhodovať o účele spracúvania.

- d) spracúvanie je nevyhnutné, aby sa *ochránili životne dôležité záujmy dotknutej osoby alebo inej fyzickej osoby*;

Spracúvanie osobných údajov by sa malo rovnako považovať za zákonné, ak je potrebné na účely ochrany záujmu, ktorý je zásadný pre život dotknutej alebo inej fyzickej osoby. Spracúvanie osobných údajov na základe životne dôležitého záujmu inej fyzickej osoby by sa malo uskutočniť v zásade len vtedy, keď sa takéto spracúvanie zjavne nemôže zakladať na inom právnom základe. Niektoré typy spracúvania môžu slúžiť na dôležité účely verejného záujmu aj životne dôležité záujmy dotknutej osoby, napríklad ak je spracúvanie nevyhnutné na humanitárne účely vrátane monitorovania epidémií a ich šírenia alebo v humanitárnych núdzových situáciách, najmä v prípade prírodných katastrof a katastrof spôsobených ľudskou činnosťou.

- e) spracúvanie je nevyhnutné na *splnenie úlohy realizovanej vo verejnom záujme* alebo pri *výkone verejnej moci zverenej prevádzkovateľovi*;

Právny základ na spracúvanie osobných údajov musí byť ustanovený v právnych predpisoch, ktoré stanovujú účel spracúvania osobných údajov, kategóriu dotknutých osôb a zoznam spracúvaných osobných údajov alebo rozsah spracúvaných osobných údajov.

- 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 osobou dieťa

Oprávnené záujmy prevádzkovateľa vrátane prevádzkovateľa, ktorému môžu byť tieto osobné údaje poskytnuté, alebo tretej strany môžu poskytnúť právny základ pre spracúvanie, ak nad nimi neprevažujú záujmy alebo základné práva a slobody dotknutej osoby, pričom sa zohľadnia primerané očakávania dotknutých osôb na základe ich vzťahu k prevádzkovateľovi. Takýto oprávnený záujem by mohol existovať napríklad vtedy, keby medzi dotknutou osobou a prevádzkovateľom

existoval relevantný a primeraný vzťah, napríklad keby bola dotknutá osoba voči prevádzkovateľovi v postavení klienta alebo v jeho službách. Existencia oprávneného záujmu by si v každom prípade vyžadovala dôkladné posúdenie vrátane posúdenia toho, či dotknutá osoba môže v danom čase a kontexte získavania osobných údajov primerane očakávať, že sa spracúvanie na tento účel môže uskutočniť. Záujmy a základné práva dotknutej osoby by mohli prevážiť nad záujmami prevádzkovateľa údajov najmä vtedy, ak sa osobné údaje spracúvajú za okolností, keď dotknuté osoby primerane neočakávajú ďalšie spracúvanie.

Tento právny základ by sa nemal vzťahovať na spracúvanie osobných údajov orgánmi verejnej moci pri plnení ich úloh.

Spracúvanie osobných údajov nevyhnutne potrebné na účely predchádzania podvodom tiež predstavuje oprávnený záujem príslušného prevádzkovateľa údajov.

Spracúvanie osobných údajov na účely priameho marketingu možno považovať za oprávnený záujem.

8. Získavanie osobných údajov

1. Získavanie osobných údajov je vykonávanie akýchkoľvek operácií, ktoré vedú k nadobudnutiu osobných údajov o dotknutej osobe na ich systematické spracúvanie v IS, ktoré sa vykonávajú v zmysle vopred stanoveného účelu ich spracúvania.
2. Dotknutá osoba musí byť pred poskytnutím svojich osobných údajov vopred oboznámená s podmienkami ich spracúvania v IS a to v rozsahu stanovenom nariadením GDPR.⁹ Takéto oboznámenie nie je potrebné v rozsahu, v akom dotknutá osoba už má dané informácie.
3. Pri získavaní osobných údajov priamo od dotknutej osoby, ktorej sa osobné údaje týkajú, je potrebné poskytnúť nasledujúce 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 dôvode nevyhnutnosti na účely oprávneného záujmu, ktorý sleduje prevádzkovateľ alebo tretia strana (článok 6 ods. 1 písm. f) GDPR), 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 odkaz na primerané alebo vhodné záruky (záväzné vnútropodnikové pravidlá).

Okrem týchto informácií je taktiež potrebné poskytnúť tieto ďalšie informácie:

- 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 namietat' proti spracúvaniu, ako aj práva na prenosnosť údajov;
- c) ak je spracúvanie založené na súhlase dotknutej osoby (článok 6 ods. 1 písm. a) GDPR) alebo na súhlase dotknutej osoby so spracúvaním osobitných kategórií osobných údajov (článok 9 ods. 2 písm. a) GDPR), 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, ktorým je Úrad na ochranu osobných údajov SR;
- 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 použití

⁹ Článok 13 GDPR.

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

4. Pri úmysle spracúvať získané osobné údaje na iný účel ako ten, na ktorý boli získané, poskytnúť dotknutej osobe pred takýmto ďalším spracúvaním informácie o tomto inom účele a ďalšie relevantné informácie uvedené v predchádzajúcom bode.¹⁰
5. 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 prípadne ak sa realizuje splnenie úlohy vo verejnom záujme (podľa § 13 ods. 1 písm. c) a e) Zákona). Ten, kto také osobné údaje spracúva, musí vedieť preukázať úradu na jeho žiadosť, že ich získal v súlade s týmto Zákomom.
6. V prípade, ak Prevádzkovateľ nezíska osobné údaje priamo od dotknutej osoby, poskytne (i) v primeranej lehote po získaní osobných údajov, najneskôr však do jedného mesiaca, pričom zohľadní konkrétne okolnosti, za ktorých sa osobné údaje spracúvajú, (ii) ak sa osobné údaje majú použiť na komunikáciu s dotknutou osobou, najneskôr v čase prvej komunikácie s touto dotknutou osobou; alebo (iii) ak sa predpokladá poskytnutie osobných údajov ďalšiemu príjemcovi, najneskôr vtedy, keď sa osobné údaje prvýkrát poskytnú. Informácia musí byť poskytnutá v rozsahu uvedenom v bode 3, vrátane informácie, z akého zdroja pochádzajú osobné údaje, prípadne o tom, či osobné údaje pochádzajú z verejne prístupných zdrojov.¹¹
7. Do IS možno poskytnúť len pravdivé osobné údaje. Za nepravdivosť osobných údajov zodpovedá ten, kto ich do informačného systému poskytol. Prevádzkovateľ považuje poskytnutý osobný údaj za pravdivý, kým sa nepreukáže opak.
8. Pri získavaní osobných údajov musí byť vždy zachovaná ich diskretnosť.
9. Spracúvať osobné údaje možno len ak Prevádzkovateľ disponuje relevantným právnym základom pre spracúvanie osobných údajov (podmienka zákonnosti spracúvania osobných údajov)¹². Takýmto právnym základom je:
 - a) súhlas dotknutej osoby 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 osobou dieťa.

To sa nevzťahuje na spracúvanie vykonávané orgánmi verejnej moci pri výkone ich úloh.

¹⁰ Článok 13 ods. 3 GDPR.

¹¹ Článok 14 GDPR.

¹² Článok 6 GDPR.

10. Zákon špecifikuje osobitné situácie zákonného spracúvania osobných údajov, ktoré predpokladá spracúvanie osobných údajov bez potreby získavania súhlasu dotknutej osoby, avšak pri rešpektovaní práva na ochranu osobnosti a ochranu súkromia. Spracúvanie osobných údajov je považované za zákonné, ak sú splnené nasledujúce podmienky:
- a) spracúvanie osobných údajov je nevyhnutné na akademický účel, umelecký účel alebo literárny účel; to neplatí, ak spracúvaním osobných údajov na taký účel prevádzkovateľ porušuje právo dotknutej osoby na ochranu jej osobnosti alebo právo na ochranu súkromia alebo také spracúvanie osobných údajov bez súhlasu dotknutej osoby vylučuje osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná¹³;
 - b) 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 taký účel prevádzkovateľ porušuje právo dotknutej osoby na ochranu jej osobnosti alebo právo na ochranu súkromia alebo také spracúvanie osobných údajov bez súhlasu dotknutej osoby vylučuje osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná¹⁴;
 - c) prevádzkovateľ je zamestnávateľom dotknutej osoby, je oprávnený poskytovať jej osobné údaje alebo zverejniť jej osobné údaje v rozsahu titul, meno, priezvisko, pracovné zaradenie, služobné zaradenie, funkčné zaradenie, osobné číslo zamestnanca alebo zamestnanecké číslo zamestnanca, odborný útvar, miesto výkonu práce, telefónne číslo, faxové číslo, adresa 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 osoby¹⁵;
11. Súhlas za neživé osoby môže poskytnúť jej blízka osoba. Súhlas nie je platný, ak čo len jedna blízka osoba písomne vyslovila nesúhlas.
12. Pri spracúvaní osobných údajov možno využiť na účely identifikovania fyzickej osoby všeobecne použiteľný identifikátor podľa osobitného predpisu (takýmto je rodné číslo) 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.
13. Pri spracúvaní osobných údajov na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel je prevádzkovateľ a sprostredkovateľ povinný prijať primerané záruky pre práva dotknutej osoby. Tieto záruky obsahujú zavedenie primeraných a účinných technických a organizačných opatrení najmä na zabezpečenie dodržiavania zásady minimalizácie údajov a pseudonymizácie.
14. Ak sa osobné údaje spracúvajú na vedecký účel, účel historického výskumu alebo na štatistický účel, môžu byť práva dotknutej osoby 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 také obmedzenie práv dotknutej osoby je nevyhnutné na dosiahnutie týchto účelov.

¹³ § 78 ods. 1 Zákona.

¹⁴ § 78 ods. 2 Zákona.

¹⁵ § 78 ods. 3 Zákona.

15. Ak sa osobné údaje spracúvajú na účel archivácie, môžu byť práva dotknutej osoby obmedzené osobitným predpisom, ak sú prijaté primerané podmienky a záruky, ak by tieto práva dotknutej osoby pravdepodobne znemožnili alebo závažným spôsobom sťažili dosiahnutie týchto účelov a také obmedzenie práv dotknutej osoby je nevyhnutné na dosiahnutie týchto účelov.
16. Získavanie osobných údajov dotknutých osôb iným, ako vyššie uvedeným spôsobom sa zakazuje.

9. Poskytovanie, sprístupňovanie a zverejňovanie osobných údajov

1. Prevádzkovateľ¹⁶ 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. Sprostredkovateľ¹⁷ je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa.
3. Prijemca¹⁸ 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 prijemcov; spracúvanie uvedených údajov uvedenými orgánmi verejnej moci sa uskutočňuje v súlade s uplatniteľnými pravidlami ochrany údajov v závislosti od účelov spracúvania.
4. Tretia strana¹⁹ 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.
5. Prevádzkovateľ umožní sprístupnenie, poskytnutie alebo zverejnenie osobných údajov iba za podmienok a v rozsahu stanovenom právnymi predpismi, ktoré stanovujú účel, podmienky, prostriedky a subjekty spracúvania osobných údajov.
6. Zákonnosť sprístupnenia, poskytnutia alebo zverejnenia osobných údajov musí byť preskúmaná ešte v čase pred ich vykonaním.
7. Ten, kto sprístupnenie alebo poskytnutie osobných údajov od Prevádzkovateľa požaduje, je povinný vopred doložiť odkazom na konkrétne ustanovenia právnych predpisov, účel, rozsah a prípadné ďalšie podmienky spracúvania údajov, ktoré mu majú byť sprístupnené alebo poskytnuté. O každom takomto sprístupnení alebo poskytnutí osobných údajov musí byť informovaná zodpovedná osoba poverená dohľadom nad ochranou osobných údajov za Prevádzkovateľa.
8. Pri každom zverejnení osobných údajov Prevádzkovateľ spolu s údajmi uvedie odkaz na konkrétne ustanovenie právnych predpisov, ktoré toto zverejnenie umožňuje alebo ukladá, vrátane účelu, spôsobu, doby, miesta, obsahu a rozsahu zverejnenia osobných údajov.
9. K IS spracúvajúcej osobné údaje alebo do priestorov, kde je IS prevádzkovaný môžu mať v odôvodnených prípadoch prístup aj pracovníci tretích strán, plniaci úlohy vyplývajúce im zo zmluvného vzťahu medzi Prevádzkovateľom a treťou stranou (napr. subdodávateľ, technický alebo upratovací servis, havarijné zásahy a pod.).
10. Oprávnenie prístupu do miesta spracúvania osobných údajov pre zamestnancov tretích strán, ktoré neboli určené ako oprávnené osoby podľa predchádzajúceho bodu posúdi zodpovedná osoba za Prevádzkovateľa, ktorá taktiež vykoná ich poučenie o zásadách ochrany osobných údajov.

¹⁶ Článok 4 ods. 7 GDPR.

¹⁷ Článok 4 ods. 8 GDPR.

¹⁸ Článok 4 ods. 9 GDPR.

¹⁹ Článok 4 ods. 10 GDPR.

11. V prípade, ak dôvodom prístupu do miesta spracúvania osobných údajov je aj sprístupnenie osobných údajov podľa bodu 9 tohto článku Smernice, musí tretia strana (subdodávateľ) spĺňať rovnaké požiadavky ako sprostredkovateľ. V zmluve uzatvorenej medzi Prevádzkovateľom a treťou stranou musí byť tretej strane stanovená povinnosť poučiť svojich zamestnancov, ktorí budú prichádzať do styku s osobnými údajmi ako aj povinnosť prijať technické, organizačné a personálne opatrenia na ochranu osobných údajov, ktoré budú primerané účelu, podmienkam a prostriedkom ich spracúvania.

10. Likvidácia osobných údajov a nakladanie s osobnými údajmi po splnení účelu spracúvania, obmedzenie spracúvania

1. Prevádzkovateľ je po splnení účelu spracúvania povinný bez zbytočného odkladu zabezpečiť likvidáciu osobných údajov.
2. Odsek 1 sa nepoužije, ak osobné údaje sú súčasťou registrátorného záznamu podľa osobitného zákona.²⁰
3. Po splnení účelu spracúvania sú osobné údaje uchovávané a neskôr vyradované podľa platných predpisov Prevádzkovateľa.²¹
4. Úschovné lehoty písomných, obrazových, zvukových a iných záznamov, ktoré obsahujú osobné údaje a sú zaradené do predarchívnej starostlivosti, možno stanoviť len na dobu nevyhnutnú na uplatnenie práv alebo povinností ustanovených Zákomom.
5. Prevádzkovateľ zabezpečuje likvidáciu registrátorného záznamu podľa osobitného predpisu.
6. Prevádzkovateľ zabezpečí bez zbytočného odkladu likvidáciu osobných údajov, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú.
7. Dotknutá osoba má právo na vymazanie svojich osobných údajov (právo na zabudnutie) 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 a neexistuje iný právny základ pre spracúvanie;
 - c) dotknutá osoba namieta voči spracúvaniu a neprevažujú žiadne oprávnené dôvody na spracúvanie alebo dotknutá osoba namieta voči spracúvaniu pre účely priameho marketingu;
 - d) osobné údaje sa spracúvali nezákonne;
 - e) osobné údaje musia byť vymazané, aby sa splnila zákonná povinnosť podľa práva EÚ alebo práva členského štátu, ktorému prevádzkovateľ podlieha;
 - f) osobné údaje sa získavali v súvislosti s ponukou služieb informačnej spoločnosti.
8. Ak prevádzkovateľ zverejnil osobné údaje a podľa je povinný ich vymazať, 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.
9. Právo na vymazanie osobných údajov sa neuplatní, pokiaľ je spracúvanie potrebné na:
 - a) na uplatnenie práva na slobodu prejavu a na informácie;
 - b) na splnenie zákonnej povinnosti, ktorá si vyžaduje spracúvanie podľa práva EÚ alebo práva SR, alebo na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi;

²⁰ Zákon č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov.

²¹ Registratúrny poriadok a Registratúrny plán.

- 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 GDPR);
 - d) na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či na štatistické účely podľa, pokiaľ je pravdepodobné, že právo na vymazanie osobných údajov znemožní alebo závažným spôsobom sťaží dosiahnutie cieľov takéhoto spracúvania, alebo;
 - e) na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov.
10. 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, a to až do overenia, či oprávnené dôvody na strane prevádzkovateľa prevažujú nad oprávnenými dôvodmi dotknutej osoby.
11. Ak sa spracúvanie obmedzilo, 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 EÚ alebo SR. Dotknutú osobu, ktorá dosiahla obmedzenie spracúvania, prevádzkovateľ informuje pred tým, ako bude obmedzenie spracúvania zrušené.
12. Prevádzkovateľ oznámi každému príjemcovi, ktorému boli osobné údaje poskytnuté, každú opravu alebo vymazanie osobných údajov alebo obmedzenie spracúvania, pokiaľ sa to neukáže ako nemožné alebo si to nevyžaduje neprimerané úsilie. Prevádzkovateľ o týchto príjemcoch informuje dotknutú osobu, ak to dotknutá osoba požaduje.

11. Prístup k osobným údajom

1. Prístup zamestnancov Prevádzkovateľa k spracúvaným osobným údajom dotknutých osôb je možný len za účelom plnenia určených pracovných povinností. Prístup nad uvedený rámec sa zakazuje.
2. Uložené pracovné povinnosti musia byť vždy v súlade s účelom spracúvania osobných údajov vymedzenom Bezpečnostným projektom na ochranu osobných údajov a v súlade s legislatívnymi normami vzťahujúcimi sa na daný účel spracúvania osobných údajov, najmä so Zákonom.
3. Pre každý účel spracúvania osobných údajov musí byť určené a zrejmé, ktorá organizačná zložka Prevádzkovateľa takéto spracúvanie zabezpečuje.
4. Prístup k osobným údajom majú iba určení zamestnanci organizačných zložiek Prevádzkovateľa, ktoré spracúvanie osobných údajov za daným účelom zabezpečujú.
5. Podmienkou určenia poverenej osoby s prístupom k osobným údajom dotknutých osôb je jej poučenie o právach a zodpovednosti za ochranu osobných údajov, ktorého súčasťou je poučenie o rozsahu povolených spracovateľských operácií a zásadách prístupu k IS, v ktorom sa spracúvanie osobných údajov vykonáva.
6. Sprístupnenie osobných údajov ďalším zamestnancom Prevádzkovateľa schvaľuje štatutárny zástupca Prevádzkovateľa na základe žiadosti vedúceho organizačnej zložky, ktorý prístup k osobným údajom pre podriadeného zamestnanca požaduje. Súčasťou žiadosti o vytvorenie prístupu k osobným údajom je stanovisko vedúceho organizačnej zložky, v pôsobnosti ktorej sa spracúvanie osobných údajov vykonáva a vyjadrenie poverenej zodpovednej osoby za výkon dohľadu nad dodržiavaním Zákona u Prevádzkovateľa. Poverená zodpovedná osoba za Prevádzkovateľa vedie agendu žiadostí o prístup k osobným údajom, zoznam poverených osôb s prístupom k osobným údajom a na základe predložených požiadaviek vykonáva jeho aktualizáciu podľa vzoru uvedeného v prílohe č. 3 tejto Smernice.
7. Interné zložky Prevádzkovateľa vykonávajú spracúvanie osobných údajov v zmysle, rozsahu a za podmienok stanovených zákonmi, zriaďovacou listinou, organizačným poriadkom alebo štatútom Prevádzkovateľa.
8. Prístup k spracúvaným osobným údajom nad vymedzený rámec sa zakazuje.

12. Sprostredkovateľ

1. Sprostredkovateľom²² je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa. Ak sa má spracúvanie uskutočniť v mene prevádzkovateľa, prevádzkovateľ využíva len sprostredkovateľov poskytujúcich dostatočné záruky na to, že sa prijímú primerané technické a organizačné opatrenia tak, aby spracúvanie spĺňalo požiadavky nariadenia GDPR a aby sa zabezpečila ochrana práv dotknutej osoby .
2. Sprostredkovateľ je povinný spracúvať osobné údaje osobne a nezapojiť ďalšieho sprostredkovateľa bez predchádzajúceho osobitného alebo všeobecného písomného povolenia prevádzkovateľa.²³
3. Spracúvanie sprostredkovateľom sa riadi zmluvou alebo iným právnym aktom podľa práva EÚ alebo práva SR, 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 stanoví, 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 zachovávajú dôvernú informáciu, alebo aby boli viazané vhodnou povinnosťou zachovávať dôvernú informáciu 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 povinností 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.
4. 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.

²² Článok 4 ods. 8 GDPR.

²³ vzor písomnej zmluvy o spracúvaní osobných údajov sprostredkovateľom v mene prevádzkovateľa je uvedený v prílohe č. 13 tejto Smernice.

5. 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 EÚ alebo práva SR uložia rovnaké povinnosti ochrany údajov, ako sa stanovujú v zmluve alebo inom právnom akte uzatvorenom medzi prevádzkovateľom a sprostredkovateľom, 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.
6. Zmluva so sprostredkovateľom, uvedená v odseku 3 tohto článku, sa vypracujú v písomnej podobe vrátane elektronickej podoby.

13. Ochrana práv dotknutých osôb

13.1 Práva dotknutých osôb

Ochrana práv dotknutých osôb upravuje kapitola III nariadenia GDPR (články 12 až 23). V zmysle právnej úpravy má fyzická osoba nárok získať transparentné informácie týkajúce sa spracúvania jej osobných údajov (pozri vyššie kapitolu 8 tejto smernice).

Dotknuté osoby majú nasledujúce práva, ktorých podmienky sú stanovené v Nariadení GDPR ako aj v Zákone. Dotknuté osoby majú právo požadovať od Prevádzkovateľa prístup k osobným údajom, právo na ich opravu alebo vymazanie alebo obmedzenie spracúvania, alebo právo namietat' proti spracúvaniu, ako aj právo na prenosnosť údajov. Podrobnejšie sú tieto práva upravené v článkoch 15 až 23 Nariadenia GDPR ako aj nižšie:

a.) Právo na prístup²⁴

Dotknutá osoba má právo na poskytnutie informácií o tom, či sa spracúvajú jej osobné údaje a ak tomu tak je, má právo získať prístup k týmto osobným údajom, vrátane kópie osobných údajov, ktoré sa jej týkajú a ktoré sú spracúvané, vrátane informácií, ktoré sa spracúvania týkajú.

Vo väčšine prípadov budú tieto informácie poskytnuté v písomnej listinnej forme, pokiaľ dotknutá osoba nepožaduje iný spôsob ich poskytnutia.

b.) Právo na opravu²⁵

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.

c.) Právo na vymazanie (právo na „zabudnutie“)²⁶

Dotknutá osoba má právo požiadať o vymazanie svojich osobných údajov, pričom prevádzkovateľ je povinný bez zbytočného odkladu osobné údaje vymazať, ak sú splnené podmienky podľa GDPR, napríklad v prípade, (i) ak osobné údaje, ktoré sú spracúvané, už viac nie sú viac potrebné na naplnenie pôvodného účelu spracúvania, prípadne ak (ii) dotknutá osoba súhlas odvolala a neexistuje iný právny základ pre ich ďalšie spracúvanie, (iii) dotknutá osoba namieta voči spracúvaniu a neprevažujú žiadne oprávnené dôvody na spracúvanie, (iv) osobné údaje sa spracúvali nezákonne, (v) osobné údaje musia byť vymazané, aby sa splnila zákonná povinnosť podľa práva EÚ alebo práva SR, (vi) osobné údaje sa získavali v súvislosti s ponukou služieb informačnej spoločnosti.

Právo dotknutej osoby na vymazanie osobných údajov je potrebné posúdiť z pohľadu všetkých relevantných okolností, napríklad z pohľadu právnych a regulačných povinností, čo môže mať za následok, že nebude možné žiadosti vyhovieť.

d.) Právo na obmedzenie spracúvania²⁷

Dotknutá osoba má právo na obmedzenie spracúvania jej osobných údajov, napríklad vtedy, ak sa domnieva, že spracúvané osobné údaje sú nepresné alebo už ďalej nie je dôvod pre ich spracúvanie.

²⁴ Článok 15 GDPR.

²⁵ Článok 16 GDPR.

²⁶ Článok 17 GDPR.

²⁷ Článok 18 GDPR.

e.) Právo na prenosnosť údajov²⁸

Dotknutá osoba má za určitých okolností právo požiadať o prenos osobných údajov na inú tretiu stranu podľa výberu dotknutej osoby. Právo na prenosnosť sa však týka len osobných údajov, ktoré boli získané na základe súhlasu alebo na základe zmluvy, ktorej je dotknutá osoba jednou zo zmluvných strán.

f.) Právo namietat'²⁹

Dotknutá osoba má právo namietat' voči spracúvaniu osobných údajov, ktoré je založené na legitímnych oprávnených záujmoch Prevádzkovateľa, prípadne na realizovaní úlohy vo verejnom záujme. 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.

Ak sa osobné údaje spracúvajú na účely priameho marketingu, dotknutá osoba má právo kedykoľvek namietat' proti spracúvaniu osobných údajov, ktoré sa jej týka, na účely takéhoto marketingu, vrátane profilovania v rozsahu, v akom súvisí s takýmto priamym marketingom. V takom prípade sa ďalej osobné údaje na také účely nesmú spracúvať. Ak sa osobné údaje spracúvajú na účely vedeckého alebo historického výskumu či na štatistické účely, dotknutá osoba má právo namietat' z dôvodov týkajúcich sa jej konkrétnej situácie proti spracúvaniu osobných údajov, ktoré sa jej týka, s výnimkou prípadov, keď je spracúvanie nevyhnutné na plnenie úlohy z dôvodov verejného záujmu.

g.) Práva súvisiace s automatizovaným rozhodovaním³⁰

Dotknutá osoba má právo odmietnuť automatizované rozhodovanie, vrátane profilovania, z ktorého pre ňu vyplynie právny alebo podobný významný dôsledok.

h.) Právo podať sťažnosť

Dotknutú osobu je potrebné informovať o práve podať sťažnosť a spôsobe, akým sú osobné údaje spracúvané, vrátane uplatnenia vyššie uvedených práv, ako aj možnosti obrátiť sa na našu zodpovednú osobu.

Rovnako je potrebné dotknutú osobu informovať o možnosti podať sťažnosť na dozorný orgán, ktorým je Úrad na ochranu osobných údajov Slovenskej republiky, <https://dataprotection.gov.sk>, Hraničná 12, 820 07 Bratislava 27; tel. číslo: +421 /2/ 3231 3214; E-mail: statny.dozor@pdp.gov.sk.

13.2 Oznámenie porušenia práv dotknutých osôb

Z dôvodu, že porušenie ochrany osobných údajov je spôsobilé spôsobiť fyzickým osobám ujmu na zdraví, majetkovú alebo nemajetkovú ujmu, ako je napríklad strata kontroly nad svojimi osobnými údajmi alebo obmedzenie práv týchto osôb, diskriminácia, krádež totožnosti alebo podvod, finančná strata, neoprávnená reverzná pseudonymizácia, poškodenie dobrého mena, strata dôvernosti osobných údajov chránených profesijným tajomstvom, alebo akékoľvek iné závažné hospodárske či sociálne znevýhodnenie dotknutej fyzickej osoby, má prevádzkovateľ povinnosť, ihneď, ako sa dozvie, že došlo k porušeniu ochrany osobných údajov, bez zbytočného odkladu a podľa možnosti najneskôr do 72 hodín od okamihu, ako sa dozvedel, že došlo k porušeniu ochrany osobných údajov, toto porušenie oznámiť Úradu na ochranu osobných údajov SR s výnimkou prípadov, keď vie prevádzkovateľ v súlade so zásadou

²⁸ Článok 20 GDPR.

²⁹ Článok 21 GDPR.

³⁰ Článok 22 GDPR.

zodpovednosti preukázať, že nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb. Ak nie je možné oznámenie podať do 72 hodín, malo by sa k oznámeniu pripojiť odôvodnenie omeškania, pričom informácie možno poskytnúť vo viacerých etapách bez ďalšieho zbytočného odkladu³¹.

Prevádzkovateľ by mal taktiež bezodkladne poskytnúť dotknutej osobe informáciu o porušení ochrany osobných údajov, ak toto porušenie ochrany osobných údajov pravdepodobne povedie k vysokému riziku pre práva a slobody fyzickej osoby, aby mohla prijať potrebné preventívne opatrenia. V oznámení by sa mala uviesť povaha porušenia ochrany osobných údajov, ako aj odporúčania pre dotknutú fyzickú osobu o tom, zmierniť potenciálne nepriaznivé dôsledky. Takéto informovanie dotknutých osôb by sa malo vykonať čo najskôr je to možné, a v úzkej spolupráci s Úradom na ochranu osobných údajov SR³².

³¹ Bližšie článok 33 GDPR.

³² Bližšie článok 34 GDPR.

14. Vybavovanie žiadostí dotknutých osôb

Prevádzkovateľ poskytne dotknutej osobe informácie o opatreniach, ktoré sa prijali na 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.

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.

Informácie ohľadom spracúvania osobných údajov ako aj všetky oznámenia a všetky opatrenia prijaté podľa článkov 15 až 22 a článku 34 GDPR (ochrana práv dotknutých osôb) 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. Ak existujú oprávnené pochybnosti v súvislosti s totožnosťou fyzickej osoby, ktorá podáva žiadosť vo veci ochrany práv dotknutej osoby, môže prevádzkovateľ požiadať o poskytnutie dodatočných informácií potrebných na potvrdenie totožnosti dotknutej osoby.

Agendu o písomnom vybavovaní žiadostí dotknutých osôb vedie poverená zodpovedná osoba.

15. Bezpečnosť osobných údajov pri ich spracúvaní

1. Prevádzkovateľ prijme, 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.
2. Prevádzkovateľ pri posudzovaní primeranej úrovne bezpečnosti 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 údajom³³.
3. Prevádzkovateľ zabezpečí, 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 EÚ alebo práva členského štátu EÚ.

15.1 Posúdenie vplyvu na ochranu osobných údajov

1. Posúdenie vplyvu na ochranu osobných údajov je Prevádzkovateľ povinný vykonať v prípade, ak spracovateľské operácie pravdepodobne povedú k vysokému riziku pre práva a slobody fyzických osôb z dôvodu ich povahy, rozsahu, kontextu a účelu. Takýmito typmi spracovateľských operácií môžu byť najmä tie, ktoré používajú nové technológie, alebo tie, ktoré sú nového druhu a v súvislosti s ktorými prevádzkovateľ ešte nevykonával posúdenie vplyvu na ochranu údajov, alebo ak sa stanú nevyhnutnými vzhľadom na čas, ktorý uplynul od prvotného spracúvania.
2. Prevádzkovateľ sa počas vykonávania posúdenia radí so zodpovednou osobou.
3. Posúdenie vplyvu na ochranu osobných údajov je potrebné vykonať pred spracúvaním, aby posúdil osobitnú pravdepodobnosť a závažnosť vysokého rizika, pričom zohľadní povahu, rozsah, kontext a účely spracúvania a zdroje rizika. Uvedené posúdenie vplyvu by malo zahŕňať najmä plánované opatrenia, záruky a mechanizmy na zmiernenie daného rizika, na zabezpečenie ochrany osobných údajov a na preukázanie súladu s nariadením GDPR.
4. Posúdenie vplyvu na ochranu osobných údajov sa vyžaduje najmä v prípadoch:
 - a) systematického a rozsiahleho hodnotenia 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;

³³ Článok 32 ods. 2 GDPR.

- b) spracúvania vo veľkom rozsahu osobitných kategórií údajov alebo osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky, alebo
 - c) systematického monitorovania verejne prístupných miest vo veľkom rozsahu.
5. Ak z posúdenia vplyvu na ochranu údajov vyplýva, že spracúvanie by v prípade neexistencie záruk, bezpečnostných opatrení a mechanizmov na zmiernenie rizika viedlo k vysokému riziku pre práva a slobody fyzických osôb, a prevádzkovateľ sa domnieva, že riziko sa nedá zmierniť primeranými prostriedkami, pokiaľ ide o dostupné technológie a náklady na vykonanie opatrení, je potrebné uskutočniť konzultáciu s Úradom na ochranu osobných údajov SR, a to ešte pred začiatkom spracovateľskej činnosti. Takéto vysoké riziko pravdepodobne vyplýva z určitého typu spracúvania a rozsahu a frekvencie spracúvania, v dôsledku ktorých môže tiež vzniknúť škoda alebo zásah do práv a slobôd fyzickej osoby.

15.2 Záznamy o spracovateľských činnostiach

1. Prevádzkovateľ je povinný viesť záznamy o spracovateľských činnostiach, za ktoré je zodpovedný, pričom tieto záznamy musia obsahovať údaje o prevádzkovateľovi, účele spracúvania osobných údajov, opis kategórií dotknutých osôb a kategórií osobných údajov, kategórie príjemcov, prenosy osobných údajov do tretej krajiny, lehoty na vymazanie osobných údajov, opis technických a organizačných bezpečnostných opatrení.
2. Tieto záznamy by mal byť prevádzkovateľ povinný na požiadanie poskytnúť tieto záznamy Úradu na ochranu osobných údajov SR, keďže slúžia na monitorovanie spracovateľských operácií
3. Vzor záznamu o spracovateľských činnostiach je dostupný na nasledujúcej stránke Úradu na ochranu osobných údajov SR:
<https://dataprotection.gov.sk/uouu/sk/content/vzor-zaznamov-o-spracovatel'skych-cinnostiach>
4. Povinnosť vyhotovovať záznamy o spracovateľských činnostiach sa nevzťahuje na prevádzkovateľovo, ktorí zamestnávajú 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 osobných údajov alebo osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky.

15.3 Povinnosti pri spracúvaní osobných údajov v oblasti bezpečnosti

1. Prevádzkovateľ zodpovedá za bezpečnosť spracúvaných osobných údajov tým, že ich chráni pred poškodením, zničením, stratou, zmenou, neoprávneným prístupom a sprístupnením, poskytnutím alebo zverejnením, ako aj pred akýmkoľvek inými neprípustnými spôsobmi spracúvania.
2. Prevádzkovateľ zabezpečuje rovnakú úroveň bezpečnosti osobných údajov spracúvaných v listinnej forme ako aj osobných údajov spracúvaných s využitím automatizovaných prostriedkov ich spracúvania (informačno-komunikačných technológií).
3. Základné zásady bezpečnosti pri práci s písomnosťami obsahujúcimi osobné údaje sú nasledovné:
 - a) vytváranie, evidencia, ukladanie, obeh, prenos, archivácia, likvidácia prípadne ďalšie činnosti s písomnosťami prebiehajú podľa platného Registratúrneho poriadku

- a Registratúrneho plánu Prevádzkovateľa a schválených zásad tvorby a obehu písomností,
- b) písomnosti obsahujúce osobné údaje môžu byť uložené iba v priestoroch, ktoré sú primerane chránené pred prístupom alebo násilným vniknutím neoprávnenej osoby, pred ich zničením alebo poškodením ako následku vzniku mimoriadnej situácie. Ochrana priestoru sa zabezpečuje primeranými technickými, organizačnými a personálnymi opatreniami Prevádzkovateľa a ich vzájomnou kombináciou,³⁴
 - c) vynášanie písomností obsahujúcich osobné údaje mimo priestorov Prevádzkovateľa podlieha schváleniu vedúceho príslušného organizačnej zložky Prevádzkovateľa, prípadne stanovisku poverenej zodpovednej osoby za Prevádzkovateľa,
 - d) pri prenose písomností v rámci priestorov Prevádzkovateľa ako aj pri schválenom prenose písomností mimo priestorov Prevádzkovateľa je potrebné dbať na primeranú ochranu dôvernosti prenášaných písomností (uzavreté a nepriehľadné transportné obaly),
 - e) prístup k písomnostiam obsahujúcim osobné údaje majú iba na to určení zamestnanci v postavení poverenej osoby,
 - f) v prítomnosti neoprávnených osôb sa práca s písomnosťami obsahujúcimi osobné údaje zakazuje,
 - g) vyhotovené písomnosti obsahujúce osobné údaje sú po ich vyradení z evidencií likvidované skartáciou, znemožňujúcou spätnú rekonštrukciu písomností,
 - h) dátové nosiče sú po skončení životnosti fyzicky likvidované,
 - i) nepretržitá prítomnosť poverenej osoby v chránenom priestore (v miestnostiach, v ktorých sú osobné údaje spracúvané), ak sa v ňom nachádzajú aj iné ako poverené osoby, ak oprávnená osoba odchádza, je povinná písomnosti obsahujúce osobné údaje uzamknúť, alebo uložiť do chráneného priestoru,
 - j) spracúvanie citlivých údajov mimo priestory a infraštruktúru Prevádzkovateľa je zakázané,
 - k) dodržiavanie politiky čistého stola, t.j. uloženie dokumentov s obsahom osobných údajov do určených uzamykateľných úschovných objektov (skriň),
4. Základné zásady bezpečnosti pri spracúvaní osobných údajov v elektronickej forme sú nasledovné:
- a) každý počítač musí byť vybavený aplikáciou na antivírusovú kontrolu, táto aplikácia musí byť pravidelne aktualizovaná,
 - b) pri prístupe k počítaču je vždy vyžadovaná identifikácia a autentifikácia používateľa,
 - c) fyzický prístup k počítaču a jeho vstupno-výstupným zariadeniam má iba určený zamestnanec, výpočtové zariadenia musia byť umiestnené v zamykaných priestoroch,
 - d) používateľské a prístupové heslá musia byť zvolené tak, aby boli ťažko uhádnuteľné, musia byť pravidelne obmieňané a držané v tajnosti,

³⁴ mechanické zábranné prostriedky požadovanej úrovne odolnosti, uzamykateľné bezpečnostné uzávery, poplachové systémy na hlásenie narušenia s vyvedením poplachového signálu do miesta výkonu strážnej služby alebo regionálnych stredísk registrácie poplachov, prístupové, prepúšťacie a dochádzkové automatizované systémy, videomonitorovacie systémy, elektronické protipožiarne systémy s vyvedením poplachového signálu do miesta výkonu strážnej služby alebo regionálneho strediska požiarneho zboru, vymedzenie bezpečnostných zón a pravidiel prístupu do nich, zavedenie a kontrola režimu ukladania kľúčov, procedurálne zásady prítomnosti na pracoviskách v pracovnej a mimopracovnej dobe, režim návštev a pod.

- e) prenosné médiá, ktoré obsahujú osobné údaje musia byť chránené pred stratou, poškodením a neoprávneným prístupom,
 - f) v aplikáciách je používané riadenie prístupu, rozsah povoleného prístupu k osobným údajom je iba v miere nevyhnutnej na výkon pracovných činností používateľa,
 - g) spracúvané osobné údaje musia byť pravidelne zálohované, zálohovanie je zabezpečované centrálnou správou alebo lokálnym zálohovaním, podľa podmienok, obsahu a rozsahu spracúvaných osobných údajov,
 - h) používateľ dodržiava stanovené pravidlá práce s počítačom, aplikáciou a počítačovou sieťou,
 - i) voľné vystavenie osobných údajov na WWW stránkach Prevádzkovateľa je považované za zverejnenie osobných údajov
 - j) monitor pracovnej stanice a tlačiareň umiestniť vždy tak, aby bolo zamedzené prístupu k osobným údajom náhodným okoloidúcim.
5. Každý zamestnanec Prevádzkovateľa pri podozrení z narušenia bezpečnosti osobných údajov spracúvaných v elektronickej forme, alebo pri podozrení z narušenia bezpečnosti zvereného počítača upovedomí o tejto skutočnosti bezodkladne najbližšieho nadriadeného a poverenú zodpovednú osobu za Prevádzkovateľa.
6. Kontrolu zamestnancov pri dodržiavaní týchto pravidiel vykonáva ich priamy nadriadený, osoba poverená výkonom dohľadu nad ochranou osobných údajov v danej organizačnej zložke a zodpovedná osoba poverená za Prevádzkovateľa. K záznamu o priebehu a výsledku kontroly dodržiavania stanovených zásad ochrany osobných údajov sa využíva vzor uvedený v prílohe č. 11 tejto Smernice.
7. Kontrolu dodržiavania zavedených bezpečnostných mechanizmov pri práci s počítačom, s aplikáciami obsahujúcimi osobné údaje a počítačovou sieťou zabezpečuje poverený bezpečnostný správca IS.

16. Cezhraničný prenos osobných údajov

1. Pre každý účel spracúvania osobných údajov Prevádzkovateľom musí byť formálne rozhodnuté, či je vykonávaný ich cezhraničný prenos.
2. Prevádzkovateľ môže vykonávať prenos osobných údajov iba do krajín, ktoré zabezpečujú primeranú úroveň ochrany osobných údajov.
3. Prevádzkovateľ nepoverí spracúvaním osobných údajov subjekt v cudzine.
4. Ochrana osobných údajov spracúvaných Prevádzkovateľom, prenesených na územie Slovenskej republiky od subjektov so sídlom alebo s trvalým pobytom v cudzine, sa vykonáva v súlade s nariadením GDPR, Zákonom a touto Smernicou.

16.1 Európska únia

1. Voľný pohyb osobných údajov medzi Slovenskou republikou a členskými štátmi EÚ a štátmi Európskeho hospodárskeho priestoru sa zaručuje; voľný pohyb osobných údajov v rámci EÚ sa nesmie obmedziť ani zakázať z dôvodov súvisiacich s ochranou fyzických osôb pri spracúvaní osobných údajov.
2. Nariadenie GDPR sa vzťahuje na spracúvanie osobných údajov v rámci činnosti prevádzky prevádzkovateľa alebo sprostredkovateľa v EÚ, a to bez ohľadu na to, či sa spracúvanie vykonáva v EÚ alebo nie.
3. Toto nariadenie 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.
4. Nariadenie sa vzťahuje na spracúvanie osobných údajov prevádzkovateľom, ktorý nie je usadený v EÚ, ale na mieste, kde sa na základe medzinárodného práva verejného uplatňuje právo členského štátu EÚ.

16.2 Prenos osobných údajov mimo EÚ

1. Všeobecným pravidlom, ktorý sa uplatňuje pre prenos osobných údajov do tretích krajín (krajiny, ktoré nie sú členskými štátmi EÚ alebo štátmi Európskeho hospodárskeho priestoru), je že akýkoľvek prenos osobných údajov, ktoré sa spracúvajú alebo sú určené na spracúvanie po prenose do tretej krajiny alebo medzinárodnej organizácii, sa uskutoční len vtedy, ak prevádzkovateľ a sprostredkovateľ dodržiavajú podmienky stanovené v GDPR, vrátane podmienok následných prenosov osobných údajov z predmetnej tretej krajiny alebo od predmetnej medzinárodnej organizácie do inej tretej krajiny, alebo inej medzinárodnej organizácii.
2. Nariadenie GDPR umožňuje prenos osobných údajov do tretích krajín, pričom špecifikuje nasledujúce nástroje na prenos osobných údajov do tretích krajín:
 - a) rozhodnutia o primeranosti
 - b) štandardné zmluvné doložky prijaté Komisiou
 - c) štandardné doložky prijaté dozorným orgánom
 - d) zmluvné doložky povolené dozorným orgánom

- e) záväzné vnútropodnikové pravidlá
 - f) schválený kódex správania
 - g) schválený certifikačný mechanizmus
3. Vo veci akýchkoľvek prenosov osobných údajov do tretích krajín je nevyhnutné informovať zodpovednú osobu, ktorá dohliadne na zákonné požiadavky prenosu.

17. Bezpečnostné opatrenia ochrany osobných údajov

Prevádzkovateľ má v zmysle nariadenia GDPR, zákona č. 18/2018 Z. z. o ochrane osobných údajov ako aj vyhlášky Úradu na ochranu osobných údajov SR č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov, povinnosť prijať primerané technické, organizačné a personálne opatrenia na ochranu osobných údajov. Tieto sú vykonávané súborom bezpečnostných opatrení v oblasti:

- a) personálnej,
- b) administratívnej,
- c) objektovej a fyzickej,
- d) neautomatizovaných technických prostriedkov,
- e) automatizovaných technických prostriedkov,
- f) určením postupov na odvrátenie rizík narušenia IS,
- g) zavedením požadovaných kontrolných mechanizmov.

17.1 Personálne opatrenia

Nižšie popísané opatrenia súvisia s výberom, určením, odbornou prípravou a kontrolou osôb, ktoré sa môžu v stanovenom rozsahu oboznamovať s osobnými údajmi, spracúvanými v IS.

Prevádzkovateľ:

- a) V súčinnosti s riešiteľom technickej infraštruktúry IS vykoná typológiu personálnych aspektov IS. Tými sú jeho prvky, úlohy, role, aktíva a pasíva personálnej bezpečnosti, personálne bezpečnostné riziká, požiadavky na technickú a odbornú úroveň užívateľov IS.
- b) Ak je to potrebné, písomne poverí osobu zodpovednú za výkon dohľadu nad ochranou osobných údajov v IS a oznámi túto skutočnosť Úradu.
- c) S prihliadnutím na plánovaný obsah a rozsah spracúvaných osobných údajov, plánovanej infraštruktúry a prvkom IS zabezpečí vypracovanie oprávnení, povinností a zodpovednosti za ochranu osobných údajov v jednotlivých funkciách a rolách IS.
- d) Vydá úlohy k vypracovaniu, aktualizácii, alebo dopracovaniu bezpečnostnej dokumentácie na ochranu osobných údajov.
- e) Prostredníctvom určenej osoby za Prevádzkovateľa zabezpečí zavedenie záznamov o spracovateľských činnostiach, prípadne posúdenia vplyvu na ochranu osobných údajov, ak je to požadované právnymi predpismi.
- f) Vykoná zaradenie zamestnancov s postavením poverenej osoby s vymedzením rozsahu ich oprávnení, povolených činností a spôsobu identifikácie a autentizácie pri prístupe k IS. Určenie poverených osôb s prístupom k osobným údajom – vzor vid' príloha č. 3 tejto Smernice.
- g) V odôvodnených prípadoch poučí iné fyzické osoby, ktoré prídu do styku s osobnými údajmi u prevádzkovateľa, majú alebo môžu mať prístup k IS o právach a povinnostiach ustanovených Zákonom a o zodpovednosti za ich porušenie. Vzor poverenia – príloha č. 4 tejto Smernice.

17.2 Administratívne opatrenia

Opatrenia administratívnej bezpečnosti súvisia s realizáciou opatrení, využitých k ochrane osobných údajov pri administratívnych činnostiach.

17.2.1 Postup Prevádzkovateľa IS

Prevádzkovateľ je povinný zaviesť účinné organizačné, technické a personálne opatrenia k zamedzeniu neoprávnenej manipulácie s osobnými údajmi pri administratívnych činnostiach, ktorými sú ich získavanie, zhromažďovanie, zaznamenávanie, príjem, evidencia, odosielanie, poskytovanie, preprava, ukladanie, uchovávanie, rozmnožovanie, vyradovanie, skartácia a ďalšia manipulácia.

Skutočnosti obsahujúce zákonom chránené osobné údaje môžu mať formu písomnosti alebo iného záznamu, môžu byť taktiež obsahom elektrického, elektromagnetického, elektronického alebo iného fyzikálneho transportného média.

17.2.2 Prioritné úlohy Prevádzkovateľa IS

Pri aplikácii organizačných, technických a personálnych opatrení v oblasti administratívnej bezpečnosti osobných údajov dôraz zamerať na:

- a) určenie osoby alebo viacerých osôb zodpovedných za chod administratívnych činností,
- b) ich zaškolenie k činnostiam v predmetnej oblasti,
- c) stanovenie a aktualizáciu princípov vnútorného a vonkajšieho informačného toku,
- d) prípravu oprávnených osôb k dodržiavaniu základných noriem pri realizácii a zdieľaní administratívnych činností,
- e) stanovenie základných princípov administratívnej činnosti, ktorými sú:
 - zásady príjmu, zasielania a doručovania písomností obsahujúcich osobné údaje,
 - vzory administratívnych pomôcok,
 - pravidlá evidencie a označovania písomností obsahujúcich osobné údaje,
 - zásady kopírovania a iného rozmnožovania písomností obsahujúcich osobné údaje,
 - podmienky ukladania, vypožičiavania a obehu písomností obsahujúcich osobné údaje,
 - pravidlá archivácie, vyradovania a skartácie písomností obsahujúcich osobné údaje,
- f) kontrolu dodržiavania stanovených administratívnych opatrení. Záznam o vykonanej kontrole v IS – vzor. vid' príloha č. 11 tejto Smernice,

Pri vykonávaní a zdieľaní administratívnych činností nariaďujem dôsledne dodržiavať registratúrny poriadok a registratúrny plán v zmysle platných právnych predpisov, čím zabezpečiť jednotný, racionálny a kvalitný výkon správy registratúry.

17.3 Opatrenia objektivej a fyzickej bezpečnosti

Opatrenia sú vykonávané na ochranu osobných údajov pred nepovolanými osobami a zabránenie neoprávnenej manipulácie s nimi na pracoviskách Prevádzkovateľa IS.

Postup Prevádzkovateľa IS

Prevádzkovateľ je povinný:

- a) Zaviesť účinné organizačné, technické a personálne opatrenia k zamedzeniu vstupu nepovolaných osôb do miest, kde sú spracúvané osobné údaje a pred neoprávnenou manipuláciou s nimi v prevádzkových a zabezpečovacích priestoroch.
- b) Obsah, rozsah a spôsob zabezpečenia objektivej a fyzickej bezpečnosti je nutné prispôbiť významu chráneného záujmu, ktorým je zabezpečenie zákonných podmienok ochrany osobných údajov.
- c) Predmetné opatrenia vykonať s použitím mechanických zábranných prostriedkov, poplachových systémov na hlásenie narušenia, prístupových a dochádzkových systémov, monitorovacích systémov, protipožiarnych zabezpečovacích systémov, fyzickou ochranou

priestorov, zavedením doplnkových organizačných a režimových opatrení a ich vzájomnou kombináciou.

- d) Opatrenia objektovej a fyzickej bezpečnosti úzko súvisia s výberom, určením a odbornou prípravou osôb k správneému používaniu inštalovaných prostriedkov a systémov, prevenciou, ako aj opatreniami prijímanými na odvrátenie vzniknutých bezpečnostných incidentov.
- e) Uvedené opatrenia nariaďujem realizovať v zmysle interných predpisov, rutín, procedúr, bezpečnostných a pracovných postupov.

17.4 Technická opatrenia neautomatizovaných prostriedkov

Technické bezpečnostné opatrenia neautomatizovaných prostriedkov je tvorená systémom manažérsko-technických a logistických opatrení zabezpečujúcich elimináciu a minimalizáciu hrozieb a rizík pôsobiacich na technické prostriedky pri spracúvaní osobných údajov.

Technická bezpečnosť musí byť zameraná najmä na:

- riadenie ochrany osobných údajov v systéme celkovej bezpečnostnej politiky, hodnotenie a riadenie technických bezpečnostných rizík, interný a externý audit bezpečnosti, kontrolnú činnosť zameranú na aktuálnosť a dodržiavanie prijatých noriem, ktorými sa u prevádzkovateľa vykonáva ochrana osobných údajov pri ich spracúvaní,
- správnosť a bezpečnosť pri používaní technických prostriedkov na realizáciu administratívnych činností, ktorými je kopírovanie a tlač písomností obsahujúcich osobné údaje, ich reprodukcia, prepisovanie na mechanických a elektronických písacích strojoch, príjem a odosielanie faxových správ obsahujúcich osobné údaje,
- správnosť postupov pri ničení vyradených písomností obsahujúcich osobné údaje na určených zariadeniach (skartačné zariadenia),
- účinnosť použitých mechanických zábranných prostriedkov na vytváranie dostatočných prekážok k zamedzeniu neoprávneného prístupu a násilného vniknutia do miest spracúvania a ukladania osobných údajov,
- splnenie požiadavky na ukladanie písomností a dátových nosičov v uzamykateľných uzáveroch za účelom zamedzenia prístupu neoprávnených osôb alebo zamestnancov Prevádzkovateľa, ktorí neboli určení ako oprávnené osoby na oboznamovanie sa s osobnými údajmi dotknutých osôb.

17.4.1 Pravidlá používania neautomatizovaných prostriedkov

Pri ničení vyradených písomností musia byť používané inštalované zariadenia na ich skartáciu, ktoré primerane zamedzujú rekonštrukcii skartovaných písomností. Pre oblasť osobitnej kategórie osobných údajov a citlivé údaje je potrebné používať minimálne triedu P4 (6mm x max. 20mm) alebo vyššiu. Aj napriek tomu že pre bežné osobné údaje je postačujúca trieda P3 (odpad so šírkou prúžku max. 2 mm s neobmedzenou dĺžkou) odporúčame obstarávať len skartovacie zariadenia s vyššou triedou bezpečnosti. (v prípade označenia DIN sa jedná sa o DIN 4 a vyššie).

Vo vyhodnotených miestach koncentrácie osobných údajov v pôsobnosti Prevádzkovateľa musí byť zistené používanie základných mechanických zábranných prostriedkov a používanie primeraných zariadení na uzamykanie dokumentov obsahujúcich osobné údaje, ktoré sú pozitívne primerane koncentracii a rozsahu spracúvania osobných údajov od trezorov, cez plechové skrine až po uzamykateľné skrinky.

Každá návšteva musí byť evidovaná na vrátnici v medziach zákona pre jednorazové vstupy. Príchod návštevy je vrátnikom telefonicky oznamovaný navštevovanému zamestnancovi, ktorý je od momentu oznámenia vrátnikom zodpovedný za jeho pobyt u Prevádzkovateľa.

Kancelárske priestory sú v prípade neprítomnosti zamestnancov uzamykané. Vstup do jednotlivých miestností majú okrem zamestnancov aj upratovačky, ktoré zabezpečujú ich upratovanie po skončení pracovného času. Upratovanie je zabezpečené zmluvou s externou spoločnosťou, ktorá obsahuje podmienky a správanie sa upratovačiek a zodpovednosti za ich porušenie.

17.5 Technická bezpečnosť automatizovaných prostriedkov

Všeobecné požiadavky na bezpečnosť počítačových systémov musia byť riešené v súlade s technickými bezpečnostnými opatreniami podľa odsekov 2.18 až 2.31 Európskeho štandardu pre hodnotenie bezpečnosti informačných systémov ITSEC zaradené do nasledujúcich skupín opatrení:

- Úlohy, funkcie a zodpovednosti osôb v IS
- Identifikácia a autentifikácia
- Riadenie prístupu
- Účtovateľnosť
- Opakované použitie
- Výmena dát

Tieto sa v pôsobnosti Prevádzkovateľa realizujú v zmysle metodických pokynov MK SR, ktorými sa v podmienkach MK SR a organizácií v jeho zriaďovateľskej pôsobnosti aplikujú štandardy pre informačné systémy verejnej správy:

Metodický pokyn MK SR pre klasifikáciu a riadenie aktív informačných systémov
Metodický pokyn MK SR pre nákup, vývoj a údržbu informačných systémov
Metodický pokyn MK SR pre organizáciu a riadenie bezpečnosti informačných systémov
Metodický pokyn MK SR pre analýzu a riadenie rizík informačných systémov

Metodické pokyny MK SR sú priebežne rozpracované do základných riadiacich dokumentov Prevádzkovateľa.

17.5.1 Prevádzkovateľ a zodpovednosť za informačnú bezpečnosť

V pôsobnosti Prevádzkovateľa je informačná bezpečnosť riadená prostredníctvom generálneho riaditeľa, ktorý určuje primárnu Bezpečnostnú politiku v rámci informačných technológií a stanovuje bezpečnostného manažéra.

Za implementáciu a riadenie informačných pravidiel zodpovedá bezpečnostný manažér, ktorý musí v zmysle celkovej bezpečnostnej politiky plniť a určovať funkciu administrátora a správcu systémov.

Na riadení a kontrole informačnej bezpečnosti sa taktiež podieľajú:

- Ministerstvo kultúry SR, ktoré riadi Organizácie „Metodickými pokynmi ...“ v oblasti IT
- externí špecialisti na informačnú bezpečnosť,
- externí audítori.

Každý zamestnanec je náležite poučený a má počas trvania pracovnoprávného resp. zmluvného vzťahu nasledovné povinnosti:

- dodržiavať bezpečnostnú politiku IS rezortu kultúry, metodické pokyny rezortu kultúry a vnútorné predpisy organizácie a to najmä „Prevádzkový poriadok počítačovej siete“
- dodržiavať pokyny a usmernenia vedúceho zamestnanca, bezpečnostného správcu IS a osoby poverenej výkonom dohľadu nad ochranou osobných údajov,

- dodržiavať pravidlá ochrany údajov a služieb IS pred stratou, poškodením alebo neoprávneným prístupom,
- využívať služby IS v súlade so svojim pracovným zaradením / zmluvou a podľa pokynov vedúceho zamestnanca,
- dodržiavať povinnosť mlčanlivosti o skutočnostiach dôvernej povahy, s ktorými sa oboznámila, a to aj po ukončení pracovnoprávneho alebo obdobného vzťahu s organizáciou.

17.5.2 Funkcie v informačnom systéme

Používatelia	Takmer každý zamestnanec Prevádzkovateľa je používateľom niektorého z počítačových informačných systémov, a preto musí rozumieť základným pravidlám počítačovej bezpečnosti. Používatelia sú prvým stupňom ochrany a musia aktívne spolupracovať s bezpečnostným správcom a administrátorom IS pri tvorbe a aktualizácii bezpečnostných postupov a pravidiel.
Správcovia systémov	Zodpovedajú za každodennú, rutinnú implementáciu bezpečnostných pravidiel a štandardov. Spoločne s vedúcimi zamestnancami aktívne navrhujú najúčinnnejšie bezpečnostné riešenia a striktné dodržiavajú odsúhlasené postupy a pravidlá. Sú povinní dokonale poznať systémy, ktoré spravujú. Snažia sa minimalizovať svoj vlastný prístup k skutočnému obsahu údajov na systémoch, ktoré spravujú.
Riaditeľ	Rozhoduje o potrebe a obsahu informačných systémov, oprávňuje organizačné útvary a jednotlivcov k prístupu do informačných systémov. Rozhoduje o investíciách do bezpečnosti a posudzuje strategické bezpečnostné zámery.

17.5.2.1 Bezpečnostný manažér

Bezpečnostný manažér zaisťuje odborné úlohy a riadenie informačnej bezpečnosti. Jeho povinnosťami sú hlavne:

- pripravovať hodnotenie stavu informačnej bezpečnosti,
- pôsobiť v oblasti operatívneho riadenia informačnej bezpečnosti, napríklad v nevyhnutných prípadoch povoľovať výnimky z Bezpečnostnej politiky a Bezpečnostných smerníc,
- podieľať sa na hodnotení nových produktov a systémov z hľadiska informačnej bezpečnosti,
- sústreďovať informácie, evidovať a vyhodnocovať riešenie bezpečnostných incidentov a bezpečnostných nedostatkov,
- riadiť a vykonávať vyšetrovanie bezpečnostných incidentov a nadväzujúce činnosti, navrhovať a prijímať bezpečnostné opatrenia v oblasti informačnej bezpečnosti,
- kontrolovať dodržiavanie Bezpečnostných smerníc, vykonávať kontroly prijatých bezpečnostných opatrení vrátane kontrol na pracoviskách jednotlivých užívateľov,
- spolupracovať pri vykonávaní externého, prípadne interného auditu,
- spolupracovať s externými špecialistami na informačnú bezpečnosť.

17.5.2.2 Správca počítačovej siete

Správca počítačovej siete plní funkciu bezpečnostného správcu aj administrátora informačného systému a je zodpovedný za:

- konfiguráciu operačného systému
- zálohovanie centrálnych systémov
- správu prístupových práv (zakladanie, zmeny a rušenie užívateľov)

- nastavenie bezpečnostnej politiky na pracovných staniciach
- aktualizáciu operačného systému a programového aplikačného vybavenia
- udržiavanie predpísaného programového vybavenia jednotlivých staníc
- pridávanie (registráciu) sieťových objektov v doméne
- **Správcom počítačovej siete je:**
 - Správca počítačovej siete:**
 - *Sadloň Michal, Mgr.*
- **Bezpečnostným správcom CJES je MK SR**

17.5.3 Správa infraštruktúry IT

Za správu infraštruktúry IT zodpovedajú určení administrátori.

Administrátori musia byť v dobe neprítomnosti navzájom zastupiteľní. Podmienkou pre zastupovanie je, že administrátor musí pracovať pod samostatným užívateľským menom, zdieľanie mena a hesla administrátora je prísne zakázané.

Administrátori vedú dokumentáciu o nastaveniach parametrov systému. Táto dokumentácia obsahuje najmä:

- konfiguráciu serverov,
- konfiguráciu pracovných staníc (typové nastavenie),
- zoznam aktívnych a pasívnych prvkov siete,
- konfigurácia aktívnych prvkov (router, firewall),
- schémy zapojenia.

17.5.4 Hardvér

Základné pravidlá práce s pracovnými stanicami spolu s právami a povinnosťami používateľov sú používateľom oznamované prostredníctvom školenia, o čom nevedie správca písomný záznam. Používateľ je povinný dodržiavať bezpečnostné pravidlá prevádzky počítačovej siete na základe uvedeného poučenia.

Všetky dôležité prvky, ktoré zabezpečujú činnosť systémov a serveri zabezpečujúce a podporujúce jednotlivé informačné systémy musia byť uložené a spravované v zabezpečenej serverovni, ktorá spĺňa požiadavky na kontinuitu prevádzky.

Pevné disky, na ktorých sa môžu nachádzať osobné údaje musia byť vyberané z PC alebo údaje na nich musia byť znehodnotené pred ich odovzdaním do zberu alebo na recykláciu a zatiaľ fyzicky uložené v uzamykateľných skrinách.

17.5.5 Softvér

Na zariadeniach môže byť inštalovaný len legálny softvér, t.j. taký, ktorý bol získaný a je používaný v súlade so zákonmi (vrátane rešpektovania autorských práv) a v súlade s licenčnými podmienkami.

Tiež je zakázané kopírovať a distribuovať časti operačného systému a inštalovaných programov bez vedomia správcu siete.

Užívateľ nesmie svojvoľne meniť konfiguráciu pracovných staníc a počítačov v sieti, čo by negatívne vplývalo na prevádzku siete.

Zmeny konfigurácie predmetných prostriedkov výpočtovej techniky môžu byť vykonané len so súhlasom správcu siete.

Všetky operačné systémy počítačov, serverov a aplikácie prevádzkované na nich je nutné udržiavať v aktuálnom stave. Každým dňom sa objavujú nové a nové bezpečnostné diery v softvéri, ktoré predstavujú reálne riziko ukradnutia údajov alebo identity používateľov.

Správca siete zodpovedá aj za nasledovné úlohy:

- Identifikácia úrovne rýchlej opravy a servisných balíkov
- Testovanie rýchlej opravy na pilotnej skupine počítačov
- Distribúcia rýchlej opravy na vybrané skupiny počítačov
- Kontrola úspešnosti inštalácie záplat
- Návrat k pôvodnému stavu v prípade problematických rýchlych opráv

17.5.6 Správa používateľov

Vytváranie, rušenie a správu používateľských účtov v sieti je riešená v zmysle odporúčaných štandardov a noriem s parametrami popísanými v nasledujúcich bodoch.

Vytváranie, rušenie a zmena používateľských účtov sa rieši v pôsobnosti administrátora siete, tieto vykonáva výhradne na základe písomných požiadaviek nadriadeného vedúceho osoby, na ktorú je požadované zriadenie, zmena alebo zrušenie používateľského účtu (okrem generovania nového hesla, kedy sa súhlas nadriadeného vedúceho nevyžaduje).

Administrátor je povinný uvedené písomné požiadavky evidovať.

Vytvárať, rušiť a spravovať užívateľské účty prostredníctvom inej osoby než na to určenej je zakázané.

17.5.7 Identifikácia a autentizácia

Identifikácia a autentizácia zahŕňa jednoznačné zistenie identity užívateľa a overenie, že identita užívateľa je správna.

Identifikácia a autentizácia pokrýva všetky funkcie, ktoré súvisia so správou užívateľov, t.j. ich pridávanie, rušenie a úprava užívateľov.

Systém jednoznačne identifikuje a autentizuje oprávnených užívateľov. Táto identifikácia a autentizácia predchádza všetkým interakciám medzi systémom a užívateľom. Iné aktivity sú možné len po úspešnej identifikácii a autentizácii. Pri identifikácii a autentizácii musí užívateľ zadať svoju jednoznačnú užívateľskú identifikáciu a dodatočnú autentizačnú informáciu, v tomto prípade heslo.

17.5.7.1 Účty a autentifikácia

Z hľadiska práv a privilégií delíme účty na:

- *Privilegované – pre správu systému („root“, „administrator“)*
- *Neprivilegované – pre koncového používateľa.*

Z hľadiska typu účtu sú tieto rozdelené na:

- *Užívateľsky jedinečné*
- *Hosťovské*
- *Otvorené – bez požiadavky preukázať dôvernú znalosť (t.j. heslo)*
- *Skupinové – účty, ktorých dôverná znalosť (t.j. heslo) je zdieľaná medzi viacerými osobami.*

Z hľadiska spôsobu prihlasovania sa účty delia na:

- *Interaktívne – autentifikácia prebieha na základe aktívneho vstupu používateľa*
- *Neinteraktívne – autentifikácia prebieha automatizovane (skript, aplikácia)*

Všetky informačné systémy Prevádzkovateľa musia byť konfigurované tak, aby sa ľubovoľné operácie s klasifikovanými údajmi dali priradiť jednoznačne unikátnej osobe a to znamená, že je zakázané používať hosťovské, otvorené a skupinové účty.

Základnou požiadavkou na každého používateľa je zákaz poskytovať dôvernú znalosť k účtu (heslo) ľubovoľnej inej osobe alebo funkcii v informačnom systéme, t.j. ani správcovi systému a generálnemu riaditeľovi.

Všetky heslá sú definované ako citlivé a dôverné informácie.

Zoznam zakázaných činností:

- Neposkytni nikomu heslo cez telefón
- Neposkytni heslo prostredníctvom emailovej správy
- Neposkytni heslo vedúcemu
- Nehovor o hesle pred niekým iným
- Neposkytujte heslo na dotazníkoch, alebo bezpečnostných formulároch
- Neposkytni heslo rodinným príslušníkom.
- Neposkytni heslo spolupracovníkom ani počas neprítomnosti
- Nepoužívajte „Zapamätať heslo“ do aplikácií

Nezapisujte svoje heslá nikam a neskladujte ich niekde vo vašej kancelárii. Neskladujte heslá v súboroch na nejakom počítačovom systéme (vrátane pocket PC alebo podobných zariadeniach) bez zakódovania, alebo šifrovania.

Ak máte podozrenie, že váš účet, alebo heslo bolo kompromitované oznámte tento nadriadenému (bezpečnostnému správcovi IS) a zmeňte všetky prístupové heslá.

Každý užívateľ nesie zodpovednosť za svoje autentifikačné údaje a tým aj za činnosť vykonanú pod jemu prideleným účtom.

17.5.7.2 Identifikácia a autentizácia na úrovni pracovnej stanice

Systém po každom užívateľovi požaduje, aby mu oznámil svoju identitu a túto identitu rovnako preukázal, t.j. aby sa autentizoval. Pre oznámenie identity používateľ používa meno používateľa, ktoré zavádza správca. Pre preukázanie identity (autentizáciu) používateľ používa heslo. Prvotné heslo stanovuje správca, ktoré používateľ po prvom prihlásení musí zmeniť.

Všetky heslá užívateľskej úrovne (email, web, desktop, atď. – zavedené v Active directory – Domain controller) by mali byť zmenené minimálne jedenkrát za 90 dní. Odporúčaný interval je však 60 dní.

Silné heslá majú nasledovné charakteristiky:

- Musia obsahovať malé aj veľké písmeno (a-z, A-Z)
- Musia obsahovať číslicu alebo nealfanumerické znaky (0-9, !@#\$%^&*()_+|~-=\{}[]:;'\<>?.,/))
- Musia byť minimálne 8 znakov dlhé
- Nesmú byť slovom zo slovníku ani inej reči, slangu, dialektu, žargónu a pod.
- Nesmú byť založené na osobných informáciách, mien členov rodiny a pod.
- Heslo by nemalo byť nikdy napísané ani inak zaznamenané. Snažte sa tvoriť heslá, ktoré sú ľahko zapamätateľné avšak ťažko uhádnuteľné.

Heslo nesmie byť počas zadávania nikdy užívateľovi zobrazované.

Uvedený spôsob identifikácie a autentizácie platí pre všetky pracovné stanice v pôsobnosti Prevádzkovateľa okrem staníc, ktoré slúžia verejnosti ako prístupový bod na Internet. Tieto stanice sú však na sieti bezpečne oddelené od produkčného prostredia Prevádzkovateľa.

17.5.7.3 Identifikácia a autentizácia na úrovni OS servera

Pre identifikáciu a autentizáciu na úrovni OS servera sú využité prostriedky konkrétneho operačného systému. Vo všetkých lokálnych sieťach je vyžadované povinné zadávanie hesla pre všetkých užívateľov. Pre všetky servery v pôsobnosti a správe Prevádzkovateľa platia rovnaké požiadavky na silu a bezpečnosť ako v predchádzajúcej časti.

17.5.7.4 Identifikácia a autentizácia na úrovni aplikácie

Po identifikácii a autentizácii užívateľov do siete je používateľ povinný sa identifikovať a autentizovať aj do aplikácie.

17.5.8 Riadenie prístupu

V pôsobnosti Prevádzkovateľa je realizované riadenie prístupu k jednotlivým objektom v súlade s bezpečnostnými štandardami a odporučeniami. Pokrýva všetky funkcie, ktoré riadia tok informácií a použitia zdrojov medzi užívateľmi, procesmi a objektmi. Správa (t.j. udeľovanie a odvolávanie) prístupových práv a ich verifikácia je realizovaná aj na úrovni aplikácie, aj na úrovni jednotlivých modulov.

Systém zaisťuje, že užívatelia a procesy, bežiacie pod ich menom, nemôžu získať prístup k dátam alebo prostriedkom, pre ktorý nie sú autorizované. Systém je schopný pridelovať prístupové práva až na úrovni jednotlivých užívateľov. Identifikácia a autentizácia predchádza akejkolvek interakcii medzi systémom a užívateľom.

17.5.8.1 Riadenie prístupu tretích strán

Rozličné dôvody, požiadavky a výhody, pre ktoré sa prístup tretej strany požaduje, sa môže vykonať len pri splnení všetkých bezpečnostných opatrení ustanovených v bezpečnostnej smernici.

Tretia strana predloží požiadavky na realizáciu vzdialeného prístupu, prípadne zoznamov zamestnancov spoločnosti s rozličnými typmi autorizácii v IS s uvedením práv a privilégií.

Administrátor po prijatí stanoviska, že prístup je oprávnený zavedie užívateľov do systému, alebo vytvorí zabezpečený vzdialený prístup.

17.5.8.2 Vzdialený prístup

Vzdialený prístup k prostriedkom spoločnosti je možný výhradne po schválení štatutárnym orgánom a môže ho vytvoriť výhradne IT manažér za nasledovných podmienok.

Dátové spojenie je počas celej relácie šifrované prostredníctvom minimálne algoritmu AES (štandard U.S. FIPS PUB 197) s použitím 256 bitového kľúča, negociovaného pomocou algoritmu RSA. Integrita a dôveryhodnosť prípadnej špecializovanej aplikácie spustenej na počítači musí byť zabezpečená elektronickým podpisom overenej certifikačnej autority.

17.5.9 Audit a účtovateľnosť

Zabezpečené štandardnými prostriedkami OS, resp. aplikačného programového vybavenia.

17.5.9.1 Účtovateľnosť a audit na úrovni pracovnej stanice

Účtovateľnosť a audit na úrovni pracovnej stanice je riešený štandardnými prostriedkami operačného systému Windows.

17.5.9.2 Účtovateľnosť a audit na úrovni aplikácie

Základom riešenia účtovateľnosti je protokolovanie všetkých, z hľadiska bezpečnosti podstatných udalostí. Základom auditu je funkcia preverujúca stav informačného systému a databáz.

17.5.9.3 Účtovateľnosť a audit na úrovni serverov

Účtovateľnosť a audit na úrovni serverov je riešený štandardnými prostriedkami použitého operačného systému. Použité auditné záznamy a ich vyhodnocovanie na jednotlivých serveroch sú popísané v jednotlivej dokumentácii k danému serveru a ich aplikácia je v súlade so štandardmi.

17.5.10 Opakované použitie

Je zabezpečené opakované použitie zdrojov, ako sú operačná pamäť, oblasti diskovej pamäti, kriticky dôležitých pracovných staníc a pod., pri zachovaní požadovanej úrovne bezpečnosti, t.j. prostriedkami pridelovanými pri činnosti IS jednotlivým užívateľom neobsahujú žiadne informácie ich predchádzajúceho vlastníka.

Pre implementáciu bezpečnostných funkcií riadenia opakovaného použitia na úrovni systémových zdrojov (operačná pamäť, disková pamäť) sa využívajú štandardné funkcie použitého operačného systému.

Na úrovni aplikácie je treba zaistiť riadenie opakovaného použitia pre displeje pracovných staníc. Na úrovni aplikácie je treba konkrétne použiť šetrič obrazovky a autentizované zamykanie klávesnice heslom.

Pre implementáciu šetriča obrazovky a autentizovaného zamykania klávesnice heslom sú použité štandardné prostriedky operačného systému Windows 7 na pracovných staniciach. Odporúča sa od všetkých užívateľov povinné používanie šetriča obrazovky so zamykaním heslom, čo v čase analýzy nebolo zabezpečené centrálnou správou.

17.5.11 Manipulácia s médiami

Medzi médiá priradíme všetky papierové médiá, ako tlačové výstupy, písomné dokumenty a rôzne koncepty a elektronické médiá, ako USB kľúče, diskety, disky a ďalšie médiá slúžiace na zaznamenávanie a zálohovanie dát. Všetky typy týchto médií je potrebné chrániť rovnako dôsledne ako dáta v automatizovanom informačnom systéme.

Pre bezpečné používanie všetkých záznamových médií platia tieto pravidlá:

- médiá, ktoré obsahujú osobné údaje musia byť označené, evidované a zverené konkrétnej osobe,
- používatelia sú povinní chrániť zverené záznamové médiá a údaje, ktoré sa na nich nachádzajú, pred neoprávneným prístupom, modifikáciou, stratou alebo poškodením,
- používatelia sú povinní zverené médiá používať len na pracovné účely,
- médiá je možné vynášať mimo priestorov Prevádzkovateľa alebo pripájať do zariadení, ktoré nie sú vo vlastníctve Prevádzkovateľa, iba v prípade, že sú na tento účel určené,
- ukladanie údajov na médiá, ktoré nie sú vo vlastníctve Prevádzkovateľa sa pokladá za poskytnutie údajov mimo priestorov Prevádzkovateľa, na ktoré je potrebný súhlas vlastníka údajov,
- v operačných systémoch zariadení Prevádzkovateľa je štandardne zablokovávaná možnosť automatického spustenia obsahu média po jeho vložení.

Pri používaní príručných médií sú používatelia povinní riadiť sa týmito pravidlami:

- používať príručné médiá iba na prenos informácií, nie na ich dlhodobé ukladanie,
- priebežne vymazávať údaje z príručných médií tak, aby sa na médiu vždy nachádzali iba tie údaje, ktoré sú nevyhnutné na momentálne realizovaný prenos,

- ukladať zverené príručné médiá najmä počas svojej neprítomnosti na bezpečné miesto, ku ktorému nemajú prístup ďalšie osoby (napr. uzamknutá zásuvka alebo miestnosť),
- všetky príručné médiá musia byť pred sprístupnením používateľovi skontrolované na prítomnosť škodlivého softvéru.

Pri používaní archívnych médií je potrebné riadiť sa týmito pravidlami:

- na archiváciu dát môžu byť používané len médiá určené na tento účel (napr. zálohovacie pásky, pevné disky alebo DVD),
- pri ukladaní údajov na archíve médiá je ako súčasť označenia média potrebné aj uvedenie krátkej charakteristiky uložených údajov a ich typu z hľadiska dôvernosti,
- archívne médiá musia byť bezpečne fyzicky uložené (napr. uzamykateľná protipožiarna skriňa, trezor).

Pri preprave médií za hranice fyzických priestorov Prevádzkovateľa je potrebné, aby boli chránené pred neautorizovaným prístupom, zneužitím alebo poškodením. Na ochranu prenášaných záznamových médií slúžia tieto opatrenia:

- pri preprave médií mimo priestorov Prevádzkovateľa používať len médiá, ktoré sú na tento účel určené,
- neponechávať pri preprave médiá bez dozoru v rizikových priestoroch ako sú napr. autá, hotelové izby, zasadacie miestnosti alebo iné verejne prístupné priestory a viditeľné miesta,
- zabezpečiť médiá voči fyzickému poškodeniu a vplyvom prostredia (teplota, vlhkosť a pod.) zvolením vhodného ochranného obalu v súlade so špecifikáciou výrobcu média,
- v prípade potreby využívať na prepravu spoľahlivú tretiu stranu (napr. kuriér),
- doručiť adresátovi sprievodné informácie o zasielanom médiu (napr. údaje o prepravcovi, očakávaný termín doručenia, popis média, štruktúra zasielaných údajov) odlišným kanálom (napr. telefonicky alebo elektronickou poštou),
- v prípade, že sú na médiách uložené citlivé údaje, je vhodné chrániť ich dôvernosť a integritu prostredníctvom:
 - fyzických prostriedkov – použitím prenosných uzamykateľných skriniek, obalom, ktorý je pre prístup k médiu nutné porušiť, vlastnoručným doručením,
 - kryptografických prostriedkov – šifrovanie a elektronický podpis, aby sa v prípade odcudzenia alebo straty média nedostali citlivé údaje Prevádzkovateľa k neoprávneným osobám a aby bol prijímateľ uistený o identite odosielateľa a nezmenenej podobe údajov.

V prípade, že sú záznamové médiá pre Prevádzkovateľa ďalej nepotrebné alebo nepoužiteľné, je potrebné dodržiavať tieto opatrenia pre bezpečnú likvidáciu médií:

- všetky nepotrebné médiá u Prevádzkovateľa musia byť bezpečne a spoľahlivo zlikvidované,
- každé médium je pred likvidáciou potrebné vyradiť z evidencie médií,
- likvidácia médií obsahujúcich citlivé informácie musí byť realizovaná fyzickým zničením (napr. spálením, rozdrvením, skartovaním),
- o likvidácii médií s citlivými informáciami musí byť vytvorený záznam,
- pre likvidáciu údajov na prepisovateľných médiách nie je nevyhnutná fyzická likvidácia média, pred akýmkoľvek ďalším použitím média je však nevyhnutné vykonať bezpečné vymazanie údajov na médiu využitím špecializovaného softvéru určeného na tento účel (fungujúceho na princípe viacnásobného prepisovania média náhodnými dátami),
- je potrebné zabrániť hromadeniu médií alebo údajov určených k likvidácii, veľké množstvo neklasifikovaných údajov môže spôsobiť citlivosť jednotlivých údajov.

17.5.12 Používanie elektronickej pošty

Na zníženie rizík vyplývajúcich z používania elektronickej pošty sú implementované technické aj organizačné opatrenia.

Technické opatrenia zabezpečuje správca počítačovej siete Prevádzkovateľa a zahŕňajú:

- testovanie prichádzajúcich aj odchádzajúcich správ elektronickej pošty na prítomnosť škodlivého kódu (napr. vírus) a automatické rozpoznávanie a separovanie nevyžiadaných správ,
- blokovanie správ prichádzajúcich z prostredia mimo Prevádzkovateľa, ak je ako adresa odosielateľa uvedená interná adresa Prevádzkovateľa,
- monitorovanie parametrov správ s cieľom overiť dodržiavanie zásad komunikácie používateľmi,
- priebežná aktualizácia programového vybavenia na doručovanie a čítanie správ elektronickej pošty (u používateľa, ako aj na serveroch),
- údržba systémov na doručovanie pošty a pravidelná kontrola ich funkčnosti.

Pri používaní elektronickej pošty sa aplikujú nasledovné zásady:

- používateľ je zodpovedný za obsah a údržbu svojej poštovej schránky, je preto povinný pravidelne kontrolovať jej obsah a mazať nepotrebné správy. Preplnenie poštovej schránky používateľa na poštovom serveri môže spôsobiť zablokovanie príjmu pošty,
- elektronická pošta prijatá a odoslaná zo systému elektronickej pošty Prevádzkovateľa je považovaná za pracovnú komunikáciu (nie je považovaná za súkromnú komunikáciu), ktorá môže byť Prevádzkovateľom archivovaná, kontrolovaná a ostáva jej majetkom,
- neodosielať nevyžiadajú elektronickú poštu alebo reťazovú poštu (správy typu „...pošli ďalej“), ak to priamo nesúvisí s pracovnou činnosťou zamestnanca,
- prijaté správy obsahujúce výzvy a varovania zasielať ďalej, iba ak súvisia s pracovnou náplňou zamestnanca alebo po konzultácii so správcom IT,
- neotvárať nevyžiadané správy (spam), alebo emaily s pochybným obsahom, najmä od neznámych odosielateľov,
- neotvárať prílohy z nevyžiadanej elektronickej pošty alebo prílohy nesúvisiace s pracovnou náplňou zamestnanca,
- v prípade opakovaného doručenia nevyžiadanej elektronickej pošty od iného zamestnanca túto skutočnosť oznámiť správcovi IT,
- za žiadnych okolností neposielať formou elektronickej pošty svoje prihlasovacie údaje (predchádzanie phishingu – vymámenia prístupových údajov od používateľov),
- neodosielať adresy elektronickej pošty iných zamestnancov mimo Prevádzkovateľa bez ich vedomia a súhlasu, pri odosielaní hromadnej pošty využívať funkciu skrytej kópie (Bcc), do kolónky adresáta zapísať vlastnú adresu a ostatných adresátov uviesť do skrytej kópie,
- neposielať elektronickou poštou dokumenty s citlivými informáciami bez dodatočného zabezpečenia dôvernosti (napr. šifrovanie),
- používateľ je povinný pri odosielaní elektronickej pošty súvisiacej s pracovnou náplňou používať pridelenú pracovnú adresu,
- elektronickú poštu je možné používať iba na účely súvisiace s pracovnou náplňou zamestnanca,
- obsah odosielaných správ musí byť v súlade s legislatívou a dobrými mravmi,
- pri registrácii do externých systémov vyžadujúcich overenie prostredníctvom elektronickej pošty používať pracovnú adresu iba pri dôveryhodných systémoch a iba na účely súvisiace s pracovnou činnosťou (zníži sa tým objem nevyžiadaných správ zasielaných na túto adresu),
- posielanie elektronickej pošty s falošnou identitou (uvedením inej ako pridelennej adresy odosielateľa) a anonymný prístup k elektronickej pošte je zakázaný,
- zabezpečiť informovanie odosielateľa správy elektronickej pošty, ktorá bola očividne zaslaná omylom, o prijatí správy. V prípade, ak takáto elektronická pošta bola zaslaná viacerým adresátom, treba informovať iba odosielateľa, nie všetkých adresátov uvedených v zozname.

17.5.13 Používanie počítačovej siete

Pri používaní počítačovej siete sú používatelia povinní dodržiavať nasledovné pravidlá:

- počítačovú sieť a jej služby využívať iba na plnenie pracovných povinností,
- pri práci v sieti dodržiavať zákony, bezpečnostnú politiku IS rezortu kultúry, metodické pokyny ministerstva, riadiace akty Prevádzkovateľa,
- používať všetky inštalované bezpečnostné mechanizmy a nemeniť ich nastavenie,
- v prípade identifikácie problémov, kompromitácie bezpečnosti alebo zneužitia zariadení siete alebo poskytovaných služieb tieto skutočnosti ihneď oznámiť bezpečnostnému správcovi IS alebo poverenej osobe správy IT,
- zdroje dostupné v sieti sú zdieľané všetkými používateľmi, preto je potrebné využívať ich hospodárne.

Používatelia majú zakázané nasledovné činnosti:

- meniť informácie slúžiace na určenie totožnosti používateľa alebo na určenie prístupových práv,
- akýmkoľvek spôsobom pristupovať k údajom iných používateľov alebo používať inú než skutočnú identitu, meniť identitu iných používateľov vrátane takýchto pokusov,
- používať akékoľvek spôsoby na zisťovanie komunikácie (odpočúvanie) v počítačovej sieti,
- používať akékoľvek spôsoby na zisťovanie a vstupovanie do hardvérovej a softvérovej konfigurácie sieťového pripojenia zariadení alebo meniť tieto parametre,
- umožňovať prístup k službám počítačovej siete ďalším zamestnancom alebo osobám, iným ako schváleným spôsobom alebo ak to priamo nevyplýva z ich pracovných povinností,
- pripájať do siete ďalšie zariadenia okrem určených situácií (napr. pripájanie notebookov) a vytvárať nové prepojenia medzi sieťami,
- vytvárať v sieti nové služby (napr. zdieľanie údajov, zasielanie krátkych správ) bez súhlasu správy IKT,
- manipulovať s aktívnymi alebo pasívnymi prvkami počítačovej siete,
- narúšať činnosť siete alebo zariadení v nej pripojených,
- snažiť sa získať alebo využívať prístup k službám na ktoré nemá oprávnenie.

Aktivity používateľa v počítačovej sieti môžu byť monitorované.

O zásadách používania počítačovej siete musia byť používatelia poučení pred prvým umožnením prístupu k sieti.

17.5.14 Používanie Internetu

Na zníženie rizík vyplývajúcich z používania internetu musia byť u Prevádzkovateľa implementované technické aj organizačné opatrenia.

Technické opatrenia zabezpečuje správca IT Prevádzkovateľa a zahŕňajú:

- filtrovanie komunikácie do siete internet blokovaním určených stránok, alebo naopak povolením prístupu iba k určitým stránkam,
- monitorovanie stránok, ku ktorým používatelia pristupujú a objemu prenesenej komunikácie s cieľom overiť dodržiavanie stanovených pravidiel používateľmi,
- pri prístupe k zabezpečeným WWW stránkam (protokolom HTTPS) automatické overenie identity zdroja, ak je toto overenie neúspešné, blokovanie prístupu,
- priebežná aktualizácia programového vybavenia na prístup k sieti internet (u používateľa prehliadač WWW, na serveroch najmä proxy server).

Za nevhodné a neprijateľné využívanie prístupu k sieti internet sa považuje najmä:

- využívanie iného ako oficiálneho pripojenia do siete (napr. neznáme wi-fi siete, prostredníctvom súkromného mobilného zariadenia),

- používanie služieb internetu na osobné účely a na činnosti zamerané na dosiahnutie osobného prospechu,
- aktivity a vystupovanie v rozpore so zákonmi, riadiacimi aktmi Prevádzkovateľa a dobrými mravmi,
- prístup k autorským dielam (hudba, obrázky, film, softvér) v rozpore s licenčnými podmienkami autora,
- vystupovať na internete oficiálne a prezentovať svoje názory ako názory Prevádzkovateľa (pokiaľ to nie je obsiahnuté v pracovnej náplni zamestnanca),
- publikovať interné materiály a informácie (pokiaľ to nie je obsiahnuté v pracovnej náplni zamestnanca),
- využívať služby na internete, ktoré by viedli k neúmernej záťaži alebo narušeniu činnosti prostriedkov Prevádzkovateľa, k nemožnosti použitia prostriedkov inými používateľmi alebo k obmedzeniu používateľských práv iných používateľov,
- umožňovať prácu v internete ostatným zamestnancom alebo iným osobám, ktoré to nemajú povolené,
- hrať hry na internete, spúšťať programy a otvárať súbory pornografického a rasistického charakteru ako aj pristupovať k týmto údajom cez internet,
- používať pracovnom čase verejné sociálne siete (napr. facebook, twitter) a iné prostriedky nechránenej komunikácie (napr. ICQ) na súkromné účely,
- akákoľvek aktivita, ktorá by mohla poškodiť dobré meno Prevádzkovateľa,
- používať na prístup k službám siete internet programy a nástroje, ktoré boli schválené a povolené správcom IT.

17.5.15 Používanie mobilných počítačov a práca doma

Prevádzkové informácie môžu byť spracúvané na mobilných počítačoch za týchto podmienok:

- môžu sa používať iba autorizované mobilné počítače Prevádzkovateľa, ktoré sú primeraným spôsobom chránené pred prístupom neoprávnenej osoby,
- používatelia sú poučení o rizikách používania mobilných počítačov,
- na mobilnom počítači je nainštalovaný aktuálny antivírusový program.

V prípade, ak sa na mobilnom počítači spracúvajú a ukladajú dôverné informácie alebo osobné údaje, musí byť použité šifrovanie dát na disku.

Práca na domácich a iných počítačoch nepatriacich Prevádzkovateľovi je zakázaná.

Prístup z iných sietí je možné zabezpečiť výhradne zabezpečeným spojením prostredníctvom IT Administrátora cez Cisco VPN Client cez určený komunikačný kanál, prípadne aj Open VPN klient alebo iný zabezpečený protokol.

17.5.16 Používanie ďalších komunikačných kanálov

Medzi ďalšie komunikačné kanály patria:

- listové zásielky,
- fax,
- telefón, mobilný telefón,
- osobný styk.

Pre zasielanie osobných údajov formou listovej zásielky sa môže používať:

- doporučená listová zásielka,
- dôveryhodná kuriérna služba.

Zasielanie osobných údajov faxom je povolené len za predpokladu, že je zaistená prítomnosť adresáta ako obsluhy faxového prístroja prijímateľa.

Odobzdávanie osobných údajov telefónom a mobilným telefónom sa ako významné riziko zakazuje.

Ukladanie osobných údajov v záznamníkoch a hlasových schránkach je ako významné riziko zakázané.

Pri osobnom styku je rozhovor o osobných údajoch dotknutých osôb možný len v prípade, že tento nemôže vypočuť nepovolaná osoba. Je zakázané hovoriť o osobných údajoch v dopravných prostriedkoch, vo verejných miestnostiach, na pracoviskách Prevádzkovateľa a sprostredkovateľov pokiaľ ich okná sú orientované do verejne prístupných miest a v čase rozhovoru sa využívajú na vetranie a podobne.

17.5.17 Ochrana počítača počas neprítomnosti užívateľa

Používateľ je povinný primerane chrániť pridelené automatizované prostriedky na spracúvanie osobných údajov pred neoprávnenou manipuláciou s nimi v čase jeho neprítomnosti.

Predtým, ako používateľ opustí pracovisko, je povinný:

- a) ak odchádza na dlhší čas – vypnúť počítač (pracovnú stanicu),
- b) ak odchádza na kratšiu dobu – odhlásiť sa, alebo zamknúť stanicu.

Toto je Používateľ povinný vykonať aj napriek tomu, že je nastavené uzamykanie centrálnou politikou.

17.5.18 Depozit hesiel

V podmienkach Prevádzkovateľa neexistuje depozit správcovských (administračných) hesiel. To môže priniesť značné komplikácie v prípade absolútnej nedostupnosti správcu siete. Ak by bol nutný servisný zásah v čase nedostupnosti správcu siete na serveroch, nebolo by ho možné vykonať aj keby bola prítomná iná, odborne spôsobilá osoba.

Deponované heslá by mali byť umiestnené v zapečatenej nepriesvitnej obálke. Musia byť stále umiestnené v trezore, ku ktorému má kľúč len zodpovedný pracovník. O každej manipulácii s deponovanými heslami je potrebné spísať záznam do protokolu, ktorý podpíše vlastník hesla a zodpovedný pracovník.

Bežní užívatelia neukladajú heslá do depozitu. V prípade potreby prístupu na užívateľský účet, ku ktorému nie je známe heslo, je kontaktovaný pracovník sprostredkovateľa, ktorý po overení oprávnenosti takej požiadavky zmení heslo požadovaného užívateľa na heslo prvé. Týmto postupom užívateľ nemusí nikdy nikomu svoje heslo oznámiť (ani ho nemusí uložiť do depozitu) a súčasne sa dozvie o tom, že iná osoba pristupovala na jeho účet (správca IS mu zmenil heslo). Potom si užívateľ znovu zmení heslo tak, aby ho nikto nepoznal.

17.5.19 Ochrana proti škodlivému kódu

Musí byť aplikovaná antivírusová ochrana ako na serveri, tak aj na pracovných staniach.

Pri nasadenom antivírusovom systéme musia platiť nasledovné požiadavky:

- musí byť nainštalovaný na všetkých pracovných staniach, serveroch a prenosných počítačoch,
- musí byť nainštalovaná jeho aktuálna verzia,
- musí umožňovať nepretržitú kontrolu kritických častí disku, súborov a správ elektronickej pošty na pozadí,
- musí umožňovať periodické vykonanie antivírusovej kontroly celého systému,
- musí umožňovať používateľom antivírusovú kontrolu zvolených médií, adresárov a súborov.

Za inštaláciu, aktualizáciu a aktiváciu antivírusového systému zodpovedá správca IT.

Pri práci s prijatými správami elektronickej pošty sú aplikované nasledovné pravidlá pre používateľov (vo väčšine prípadov sú uvedené pravidlá už aplikované priamo na filtroch k elektronickej pošte):

- zákaz otvárať prílohy správ, ktoré pochádzajú z neznámych alebo podozrivých adries v Internete,
- zákaz otvárať spustiteľné súbory (obsahujú koncovky .exe, .com, .bat, .vbs, .scr). Správy, ktoré obsahujú takéto súbory okamžite zmažte. Informujte odosielateľa a informujte určenú osobu,
- v žiadnom prípade nevykonávajte sami odstraňovanie počítačových vírusov. V prípade zistenia vírusu prostredníctvom antivírusového programu, alebo ak sami máte podozrenie na prítomnosť vírusu, okamžite to oznámte zodpovednej osobe.

Užívatelia majú zakázané vypínať antivírusovú ochranu. V prípade výskytu a detekcie počítačového vírusu sú povinní informovať správcu, ktorý rozhodne o ďalšom postupe.

17.5.20 Šifrovanie dát

Šifrovacie (kryptografické) prostriedky sú určené pre:

- ochranu dôvernosti dát pri prenose,
- ochranu dôvernosti dát uložených na elektronických médiách,
- autentizáciu pomocou digitálnych certifikátov a elektronický podpis.

U Prevádzkovateľa nie sú stanovené pravidlá pre šifrovanie, ale odporúča sa, že sa môžu používať len šifrovacie prostriedky, ktoré sú schválené a používajú dĺžku kľúča najmenej 128 bitov pre symetrickú šifru a 1024 bitov pre asymetrickú šifru.

Digitálne certifikáty určené pre šifrovanú komunikáciu a autentizáciu komunikujúcich strán vydá certifikačná autorita schválená Prevádzkovateľom.

Pre zabezpečenie ochrany šifrovacích prostriedkov musia platiť nasledovné pravidlá:

- nesmú byť prenášané rovnakým komunikačným kanálom, ktorým sú prenášané šifrované informácie,
- šifrovacie kľúče sa musia periodicky meniť, ich maximálna doba platnosti je jeden rok,
- kópie šifrovacích kľúčov a prístupové kódy k nim sa musia bezpečným spôsobom deponovať u zodpovednej osoby, toto umožní získať späť zašifrovanú informáciu v prípade chyby systému, ľudského výpadku, deponovanie vykonať vloženíím do zalepenej obálky, ktorá je zapečatená a podpísaná majiteľom kľúča,
- tajné šifrovacie kľúče, ktoré slúžia pre elektronický podpis sa nesmú v žiadnom prípade deponovať, tieto sú po celú dobu ich platnosti pod kontrolou ich vlastníkov.

17.5.21 Archivácia a zálohovanie

Archiváciou a zálohovaním rozumieme uloženie celého alebo vybraného dátového priestoru a prostredia do súboru na jednu alebo viac diskiet, na pevný disk, alebo iné pamäťové médium.

Záloha všetkých dôležitých aktív je vykonávaná v pravidelných časových intervaloch.

17.5.21.1 Test funkcionality dátového nosiča

U kritických záloh je nevyhnutné vykonávať test funkčnosti vytvorenej zálohy a test samotného dátového nosiča.

17.5.21.2 Určenie doby uchovávanía záloh a kontrola jej dodržiavania

Dĺžka uchovávanía osobných údajov závisí od účelu, pre ktorý boli získané ako aj ich povaha. Ak je nevyhnutné uchovávať údaje z dôvodu existencie zákonnej požiadavky, tie treba uchovávať dovtedy, kým takáto zákonná požiadavka trvá. Údaje s krátkodobou hodnotou by mali byť mazané v priebehu dní.

Ak sú záznamy uložené offline, je potrebné zabezpečiť obmedzenú dostupnosť k daným údajom. V prípade uchovávanía musí organizácia zabezpečiť práva dotknutých osôb. Pri mazaní údajov zo živých databáz taktiež musí vymazať všetky zálohy daných údajov. Ak dochádza k vymazaniu osobných údajov, tak výmaz osobných údajov musí byť skutočný, t.j. nezostanú žiadne kópie informácií v systémoch Prevádzkovateľa.

17.5.22 Obnova

Obnovou rozumieme obnovenie celého alebo vybraného dátového priestoru a prostredia po bezpečnostnom incidente alebo po inej strate dát z bezpečnostnej zálohy.

Obnova je riešená prostredníctvom obnovy z vytvorených záloh.

17.5.22.1 Test obnovy informačného systému

U nosných informačných systémov a u informačných systémov verejnej správy je nevyhnutné v určených intervaloch vykonávať test obnovy informačného systému aby bola zabezpečená jeho obnova v prípade skutočného výpadku.

17.5.23 Ochrana proti výpadkom napájania

Je zabezpečené ukladanie spracúvaných dát v určenom časovom limite na hardvér, zálohovanie dát v zmysle platnej smernice a náhradné zdroje napájania.

Servery a aktívne sieťové prvky musia byť zabezpečené proti strate dát pri výpadku elektrickej energie záložným zdrojom. Všetky informačné systémy, v ktorých sa spracúvajú osobné údaje sú umiestnené na serveroch.

17.5.24 Zodpovednosť používateľov

Všetci užívatelia sú povinní dodržiavať pravidlá informačnej bezpečnosti, a to hlavne:

- každý užívateľ prevezme výpočtovú techniku na základe preberacieho protokolu, resp. dodatku k preberaciemu protokolu,
- dodržiavanie pravidiel pri výbere, používaní a ochrane hesla a iných zariadení na vykonanie autentizácie,
- meniť svoje heslá často a pravidelne. Týmto sa zvyšuje istota voči neoprávnenému použitiu účtu užívateľa. Zvyčajne je zmena hesla preddefinovaná správcou systému, ale je povinnosťou užívateľa meniť heslo aj vtedy, keď ho k tomu automaticky systém nenúti,
- zmeniť heslo okamžite po podozrení z neoprávneného použitia účtu. Odporúča sa o tejto skutočnosti informovať správcu systému, nakoľko z histórie prístupu k účtu užívateľa je možno posúdiť, kto neoprávnene účet používa, resp. vykonal neautorizované pokusy o prihlásenie sa k účtu,
- zmeniť heslo okamžite po zistení, že heslo je známe inej osobe, alebo osobám,
- nenechávať osobné počítače prihlásené do systému, alebo siete bez dozoru oprávneného užívateľa,
- neumožniť prácu iným pracovníkom pod svojim užívateľským menom,
- udržiavať pracovné miesto upratané, nenechávať dokumenty alebo médiá obsahujúce osobné údaje voľne na pracovnom stole počas neprítomnosti,

- zakazuje sa kopírovanie dát obsahujúcich osobné údaje do iných IS, alebo ich ukladanie na médiá, vyhotovovanie tlačенých dokumentov, pokiaľ to nevyžadujú zavedené a schválené pracovné postupy,
- zakazuje sa vykonávať zásahy do technickej infraštruktúry, pripájať neautorizované zariadenia ako modemy, prenosné počítače, osobné organizéry, záznamníky a iné,
- každý užívateľ je povinný dodržiavať základné zásady antivírovej ochrany, zásady bezpečného používania Internetu a elektronickej pošty,
- práca na PC, ktorá by mohla viesť k narušeniu ochrany osobných údajov pri ich spracúvaní je zakázaná v prítomnosti neoprávnenej osoby,
- po ukončení práce na PC zabezpečí užívateľ svoje pracovisko v súlade so zavedeným prevádzkovým poriadkom,
- v prípade vyzradenia, zneužitia, poškodenia, zničenia, straty alebo pri odcudzení osobných údajov, alebo podozrenia z pokusu o vyššie uvedené je užívateľ povinný oboznámiť s touto skutočnosťou zodpovednú osobu poverenú výkonom dohľadu nad ochranou osobných údajov.
- rešpektovať príkazy a pokyny IT Administrátora,
- manipulovať so zariadeniami tak, aby nedošlo k ich poškodeniu, v súlade s používateľskými príručkami,
- narábať s nosičmi informácií podľa platných smerníc,
- viesť záznamy podľa prevádzkovej dokumentácie,
- nedovoliť manipuláciu s PC a tlačiarňou nepovolaným osobám,
- informovať o poruchách na zariadení IT Administrátora,
- nepoužívať iný softvér ako je špecifikované v dokumentácii k PC, je zakázané používať neautorizovaný softvér,
- nepoužívať iný hardvér ako je špecifikovaný v dokumentácii k PC,
- neodpájať tlačiareň, ani inak s ňou manipulovať nepovoleným postupom,
- všetky neštandardné situácie, ktoré by mohli viesť k bezpečnostnému incidentu, alebo naznačujú, že k nemu došlo, okamžite hlásiť IT Administrátorovi – zariadenie nevypínať, ale počkať na príkaz príslušného nadriadeného a spracovať Záznam o bezpečnostnom incidente,
- Práca na PC, ktorá by mohla viesť k narušeniu ochrany osobných údajov je zakázaná v prítomnosti neoprávnenej osoby.

17.5.25 Bezpečnostné riziká v automatizovaných informačných systémoch

Spôsob a politika správy techniky a programového vybavenia, v ktorých sa ukladajú a spracovávajú osobné údaje dotknutých osôb, sú vedené na veľmi dobrej úrovni. Počas vykonanej Analýzy bolo zistené, že osoby zodpovedné za správu informačných technológií disponujú veľmi dobrou odbornosťou a majú nadštandardné znalosti o technológiách, za ktoré zodpovedajú. Nižšie uvedené riziká predstavujú súhrn eventuálnych možností, ktoré môžu mať negatívny dopad na bezpečnosť automatizovaných informačných systémov.

Závažné riziká:

- neexistuje schválený a zavedený dokument celkovej bezpečnostnej politiky,
- nedochádza ku pravidelnej nezávislej revízii informačnej bezpečnosti v organizácii,
- nie sú identifikované možné príčiny prerušenia činností organizácie, ich pravdepodobnosti ani závažnosť dopadov a možných následkov na informačnú bezpečnosť

Ďalšie riziká:

- únik osobných údajov v dôsledku neoprávneného používania systémových technických

prostriedkov,

- únik osobných údajov ako následok neoprávneného použitia neevidovaných nosičov dát,
- únik osobných údajov v dôsledku svojvoľného porušovania stanovených postupov a procedúr pri práci s automatizovanými IS,
- únik osobných údajov ako dôsledok nekomplexného výkonu funkcie administrátora a bezpečnostného správcu informačných systémov,
- únik osobných údajov ako dôsledok nezabezpečenej komunikácie elektronickej pošty, alebo siete,
- únik osobných údajov ako dôsledok nepresne vymedzených, spravovaných a konkretizovaných prístupových oprávnení užívateľov informačných systémov.

Opatrenia využité k minimalizácii vyhodnotených bezpečnostných rizík budú ďalej konkretizované Bezpečnostnými smernicami na ochranu osobných údajov.

18. Spôsob, forma a periodicita výkonu kontrolných činností

18.1 Druhy kontrolných mechanizmov

- a. priebežné kontrolné činnosti, vykonávané:
 - poverenými osobami:
 - kontrola zabezpečenia písomného súhlasu so spracúvaním osobných údajov od dotknutých osôb na začiatku spracúvania agendy,
 - kontrola dodržiavania politiky čistého stola, t.j. uloženie dokumentov s obsahom osobných údajov do určených uzamykateľných úschovných objektov,
 - kontrola, či sú vypnuté elektrické spotrebiče a ďalšie zariadenia, ktoré by mohli spôsobiť poškodenie alebo zničenie kancelárskych priestorov kde sú spracúvané osobné údaje,
 - kontrola úplnosti spracúvaných osobných údajov a kontrola úplnosti a správnosti spracovania osobných údajov,
 - zodpovednou osobou:
 - kontrola dodržiavania zmluvných ustanovení pri výkone činností zamestnancov dodávateľa informačného systému (napr. pri nasadení legislatívnych aktualizácií a zlepšení systému),
 - kontrola uzatvorenia dohody o mlčanlivosti pri výkone činností v systéme,
 - kontrola dodržiavania procesu pridelovania prístupových práv a kontrola úrovne prístupových práv oprávnených osôb v systéme,
 - správcami IT infraštruktúry:
 - kontrola vykonaných záznamov (logov) operačného systému a ostatného SW na pracovných staniciach oprávnených osôb,
 - kontrola dodržiavania informačnej bezpečnosti,
- b. periodické kontroly, vykonávané:
 - zodpovednou osobou:
 - kontrola dodržiavania ustanovení smernice vykonávaná minimálne 2x ročne,
 - kontrola súladu spracúvania osobných údajov s ustanoveniami legislatívy SR vykonávaná minimálne raz ročne,
 - kontrola pridelených prístupov oprávnených osôb do systému,
 - správcami IT infraštruktúry:
 - kontrola úspešnosti aktualizácie pracovných staníc (aplikácie záplat operačných systémov a nainštalovaného aplikačného programového vybavenia),
- c. náhodné kontroly, vykonávané:
 - zodpovednou osobou:
 - kontrola dodržiavania požiadavky dohľadu pri výkone servisných a/alebo iných činností – vykonávaná v prípade upratovania priestorov spracúvania osobných údajov,
 - kontrola dodržiavania požiadavky na likvidáciu poškodených, neúplných a ďalej nepotrebných osobných údajov, ako aj nevyžiadaných dokumentov žiadateľov o zamestnanie na skartovacích zariadeniach,
 - správcami IT infraštruktúry:
 - kontrola dodržiavania zákazu neautorizovanej zmeny HW a SW konfigurácie,
- d. následné kontroly, vykonávané spravidla zodpovednou osobou za účelom overenia stavu odstránenia nedostatkov zistených pri výkone niektorej z predchádzajúcich typov kontrol.

18.2 Kontrolný záznam

O vykonaní kontroly v oblasti osobných údajov je vedený písomný záznam minimálne v nasledujúcom rozsahu:

- dátum kontroly,
- predmet kontroly, t.j. kontrolovaná oblasť resp. ciele kontroly,
- kto kontrolu vykonal,
- zistený stav,
- vyjadrenie kontrolovaného,
- úlohy na odstránenie zistených nedostatkov,
- záznam o odstránení zistených nedostatkov.

19. Postupy pri haváriách, poruchách a iných mimoriadnych situáciách

19.1 Preventívne opatrenia

Za účelom minimalizácie rizika výskytu a potenciálnych dopadov pri výskyte havárií, porúch a iných mimoriadnych udalostí sú v spoločnosti zavedené nasledujúce preventívne opatrenia:

- na bezpečné uchovávanie osobných údajov v papierovej forme sú určené uzamykateľné úschovné objekty (napr. registračky, skrine alebo trezory), kde sú po ukončení práce a pri opustení pracoviska uchovávané spracúvané osobné údaje,
- pri opustení pracoviska je oprávnená osoba povinná vykonať kontrolu, či sú vypnuté elektrické a ďalšie zariadenia, ktoré by mohli spôsobiť poškodenie alebo zničenie priestorov spoločnosti, ako aj v nich uchovávaných osobných údajov,
- oprávnené osoby sú pri opustení pracoviska povinné zatvoriť a uzamknúť úschovný objekt a pri odchode bezpečne uzatvoriť pracovisko,
- výkon servisných zásahov a zmien v hardvérovej a softvérovej konfigurácii technických prostriedkov (pracovných staníc a komponentov zostavy, ako napr. lokálna tlačiareň) sú vykonávané len autorizovaným odborným personálom; pričom neautorizované zmeny hardvéru a softvéru (napr. inštalácia SW, pripájanie externých zariadení) sú zakázané,
- na zabezpečenie dostupnosti osobných údajov v elektronickej forme pre prípad obnovy je vykonávané ich zálohovanie.

19.2 Havárie a poruchy

V prípade havárie alebo poruchy pracovnej stanice používateľa je v závislosti od jej rozsahu vykonaný servisný zásah, pričom chybný komponent je nahradený a systém je reінštalovaný, resp. je zabezpečená náhradná pracovná stanica.

V prípade havárie alebo poruchy niektorého z kľúčových komponentov IT infraštruktúry (napr. databázový server) je v závislosti od jej rozsahu vykonaný odborný servisný zásah, pričom chybný komponent je nahradený a systém reінštalovaný prípadne je zabezpečený náhradný technický prostriedok s následnou obnovou osobných údajov z vykonaných záloh, pričom tieto aktivity sú vykonávané v rámci plnenia servisných alebo iných zmluvných vzťahov medzi spoločnosťou a dodávateľom služieb.

V prípade výskytu havárie infraštruktúry budovy (napr. prerušenie vodovodu alebo ústredného kúrenia s následným zatopením priestorov) v závislosti od jej rozsahu zabezpečí zodpovedná osoba a/alebo oprávnené osoby prítomné na pracovisku prenesenie osobných údajov z postihnutých priestorov mimo dosah havárie, pričom musí byť zabezpečená ich primeraná ochrana (napr. formou dohľadu poverenou osobou).

V prípade havárie väčšieho rozsahu a výskytu mimoriadnej situácie (napr. požiaru budovy) zodpovedná osoba, prípadne iná určená osoba, alebo oprávnené osoby prítomné na pracovisku v závislosti od rozsahu udalosti a v prípade, že nie sú ohrozené ľudské životy, zabezpečia prenesenie spracúvaných osobných údajov z postihnutých priestorov mimo dosah havárie, pričom musí byť zaistená ich primeraná ochrana. Tiež je potrebné zabezpečiť ochranu osobných údajov v prípade zásahu a výkone záchranných prác.

Pre prípad úplného zničenia serverovne sú záložné dáta uložené aj mimo priestorov serverovne.

19.3 Bezpečnostné incidenty

Bezpečnostný incident – akékoľvek konanie, situácia alebo udalosť, ktorými došlo alebo ktoré smerujú k poškodeniu, zničeniu, strate, zmene, neoprávnenému prístupu a sprístupneniu, poskytnutiu alebo zverejneniu, alebo akémukoľvek inému neprípustnému spôsobu spracúvania osobných údajov alebo sú spôsobilé narušiť bezpečnosť alebo funkčnosť IS.

Zamestnanci, ktorí zistia bezpečnostný incident alebo bezpečnostný nedostatok okamžite toto oznámia zodpovednej osobe. V prípade závažného bezpečnostného incidentu okamžite kontaktujú zodpovedného, ktorý informuje správcu IS.

Po oznámení sa spracuje Záznam o bezpečnostnom incidente v IS podľa vzoru v prílohe Bezpečnostných smerníc. Vyhodnotenie vykoná bezpečnostný správca alebo poverená zodpovedná osoba na základe údajov z vyplneného formulára prípadne poskytnutých doplňujúcich informácií. Bezpečnostný správca eviduje všetky bezpečnostné incidenty a zodpovedá za ich doriešenie.

19.3.1 Klasifikácia bezpečnostných incidentov a použitých riešení

- Bezpečnostný incident nízkej úrovne – má len lokálny (priestorovo aj časovo) dopad napríklad: neuzamknutie chráneného priestoru, prítomnosť neoprávnenej osoby v chránenom priestore,
- Bezpečnostný incident strednej úrovne
 - Má dopad, ktorý Prevádzkovateľ ešte dokáže ošetriť z vlastných zdrojov,
 - Má už dopad na okolie Prevádzkovateľa
 - Právne dôsledky (porušenie zákona, možná žaloba poškodených)
- Bezpečnostný incident vysokej úrovne
 - Spôsobíť vážnu ujmu aj okoliu
 - Právne dôsledky
 - Poškodenie dobrého mena nielen Prevádzkovateľa, ale aj SR

19.3.2 Odstraňovanie následkov bezpečnostných incidentov

- Odstránenie menej závažného následku bezpečnostného incidentu vo vzťahu k IS Prevádzkovateľ rieši personálnymi alebo technickými opatreniami a ich prehodením či zmenou.
- Odstránenie závažného následku bezpečnostného incidentu Prevádzkovateľ rieši oznámením príslušným orgánom podozrenie z naplnenia niektorej zo skutkových podstát trestného činu alebo priestupku vo vzťahu k zneužitia osobných údajov.
- Odstraňovaniu následkov bezpečnostných incidentov predchádza aktívna preventívna činnosť prevádzkovateľa zameraná na úplné odstránenie alebo aspoň minimalizáciu príčin vzniku bezpečnostných incidentov.

V prípade havarijného stavu, ohrozenia a pod. prechádza činnosť IS do výnimočného režimu. V tomto režime sú jednotlivé funkcie používateľov obmedzené. Úlohou informačného systému je zabezpečiť ochranu osobných údajov. Činnosť informačného systému v tomto režime zabezpečuje správca siete (plní aj funkciu bezpečnostného manažéra pre IT).

Jeho činnosť je nasledovná:

- zabezpečiť znemožnenie prístupu všetkých používateľov k prostriedkom IS,
- v prípade narušenia je zodpovedný za núdzovú prevádzku,
- v prípade zničeného systému je zodpovedný za obnovenie najnovšej zálohy,
- zabezpečiť odstránenie príčiny havárie alebo ohrozenia,
- po ukončení havarijného stavu povolí prístup k prostriedkom.

20. Spolupráca s Úradom na ochranu osobných údajov SR

1. Úrad na ochranu osobných údajov SR predstavuje nezávislý dozorný orgán, ktorého postavenie je upravené v nariadení GDPR (články 51 až 59), ako aj v zákone č. 18/2018 Z. z. o ochrane osobných údajov (§ 80 až § 84). Úrad môže u Prevádzkovateľa vykonávať kontrolu spracúvania osobných údajov u Prevádzkovateľa.³⁵ Priebeh kontrolnej činnosti je stanovený Zákonom.³⁶
2. Pri výkone kontroly súčinnosť s kontrolným orgánom zabezpečuje štatutárny zástupca v súčinnosti so zodpovednou osobou, ak boli splnené podmienky na jej poverenie v zmysle Zákona.
3. Osoby uvedené v predchádzajúcom bode majú byť oboznámené s protokolom o vykonaní kontroly a túto skutočnosť potvrdia podpisom protokolu.
4. O prebiehajúcej kontrole, o predmete kontroly a o kontrolných zisteniach musí byť informovaný štatutárny zástupca Prevádzkovateľa.
5. Účastníkom konania za Prevádzkovateľa je štatutárny zástupca Prevádzkovateľa alebo ním písomne poverená osoba.
6. Počas výkonu kontroly alebo počas konania Úradu voči Prevádzkovateľovi poskytujú zamestnanci Prevádzkovateľa Úradu a ním povereným kontrolným osobám potrebnú súčinnosť, najmä vstup do priestorov, prístup k materiálom, údajom a prístup do prevádzkovaných IS.
7. Zodpovedná osoba za Prevádzkovateľa (ak bola poverená) vedie evidenciu všetkej korešpondencie Prevádzkovateľa s Úradom (prípadne iná poverená osoba generálnym riaditeľom Prevádzkovateľa).

20.1 Postavenie Úradu na ochranu osobných údajov

Úrad na ochranu osobných údajov Slovenskej republiky je orgánom štátnej správy s celoslovenskou pôsobnosťou, ktorý sa podieľa na ochrane základných práv fyzických osôb pri spracúvaní osobných údajov a ktorý vykonáva dozor nad ochranou osobných údajov. sídlom Úradu je Bratislava. Úrad pri výkone svojej pôsobnosti postupuje nezávisle a riadi sa ústavou, ústavnými zákonmi, zákonmi, ostatnými všeobecne záväznými právnymi predpismi a medzinárodnými zmluvami, ktorými je Slovenská republika viazaná.

Podrobné informácie o úlohách, pôsobnosti a postavení Úradu sú dostupné na adrese www.dataprotection.gov.sk

³⁵ § 90 Zákona.

³⁶ § 90 – § 98 Zákona.

21. Záverečné a prechodné ustanovenia

1. Táto Smernica je internou normou, záväznou pre všetkých zamestnancov Prevádzkovateľa, ktorí sa v rámci pracovného zaradenia zoznamujú s osobnými údajmi spracúvanými v IS, na túto prácu boli náležite určení, boli poučení o právach a povinnostiach ustanovených Zákonom a zodpovednosti za ich porušenie.
2. Smernica je v nevyhnutom rozsahu záväzná pre zmluvných dodávateľov a tretie strany.
3. Smernica nadobúda platnosť jej schválením štatutárnym zástupcom Prevádzkovateľa a rozdeľuje sa podľa osobitného rozdeľovníka.
4. Smernica nadobúda účinnosť dňom nasledujúcim po dni ukončenia implementácie Bezpečnostného projektu na ochranu osobných údajov.
5. Kontrolu dodržiavania ustanovení Smernice vykonáva poverená zodpovedná osoba za Prevádzkovateľa a poverené osoby za jednotlivé interné organizačné zložky Prevádzkovateľa (ako boli poverené).
6. Gestorom riadenia zmien a aktualizácie Smernice je zodpovedná osoba za Prevádzkovateľa, ktorá navrhované zmeny ustanovení Smernice predkladá k ich odsúhlaseniu a schváleniu štatutárnemu zástupcovi Prevádzkovateľa.
7. Porušenie ustanovení tejto Smernice je považované za porušenie pracovnej disciplíny a budú z neho vyvodené sankcie v súlade so Zákonníkom práce a Pracovným poriadkom Prevádzkovateľa.
8. Výnimky z povinností vyplývajúcich z tejto Smernice môže udeľovať štatutárny zástupca Prevádzkovateľa alebo ním písomne poverená osoba. Výnimka musí byť v súlade so Zákonom, udelená písomne a musí byť daná na vedomie poverenej zodpovednej osobe za Prevádzkovateľa.

22. Niektoré zákony upravujúce účel a podmienky spracúvania osobných údajov

Predpis	Názov
{Z 40/1964}	Občiansky zákonník
{Z 71/1967}	o správnom konaní (správny poriadok)
{Z 85/1990}	o petičnom práve
{Z 2/1991}	o kolektívnom vyjednávaní
{Z 308/1991}	o slobode náboženskej viery a postavení cirkví a náboženských spoločností
{Z 513/1991}	Obchodný zákonník
{Z 460/1992}	Ústava Slovenskej republiky
{Z 152/1994}	o sociálnom fonde a o zmene a doplnení zákona č. 286/1992 Zb. o daniach z príjmov v znení neskorších predpisov
{Z 270/1995}	o štátnom jazyku Slovenskej republiky
{Z 10/1996}	o kontrole v štátnej správe
{Z 212/1997}	o povinných výtlačkoch periodických publikácií, neperiodických publikácií a rozmnoženín audiovizuálnych diel
{Z 211/2000}	o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií)
{Z 302/2001}	o samospráve vyšších územných celkov (zákon o samosprávnych krajoch)
{Z 311/2001}	Zákonník práce
{Z 416/2001}	o prechode niektorých pôsobností z orgánov štátnej správy na obce a na vyššie územné celky
{Z 540/2001}	o štátnej štatistike
{Z 575/2001}	o organizácii činnosti vlády a organizácii ústrednej štátnej správy
{Z 49/2002}	o ochrane pamiatkového fondu
{Z 215/2002}	o elektronickom podpise a o zmene a doplnení niektorých zákonov
{Z 227/2002}	o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu
{Z 283/2002}	o cestovných náhradách
{Z 291/2002}	o Štátnej pokladnici a o zmene a doplnení niektorých zákonov
{Z 395/2002}	o archívoch a registratúrach a o doplnení niektorých zákonov
{Z 431/2002}	o účtovníctve
{Z 444/2002}	o dizajnoch
{Z 461/2003}	o sociálnom poistení
{Z 462/2003}	o náhrade príjmu pri dočasnej pracovnej neschopnosti zamestnanca a o zmene a doplnení niektorých zákonov
{Z 552/2003}	o výkone práce vo verejnom záujme
{Z 553/2003}	o odmeňovaní niektorých zamestnancov pri výkone práce vo verejnom záujme a o zmene a doplnení niektorých zákonov
{Z 595/2003}	o dani z príjmov
{Z 601/2003}	o životnom minime a o zmene a doplnení niektorých zákonov
{Z 5/2004}	o službách zamestnanosti a o zmene a doplnení niektorých zákonov
{Z 215/2004}	o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov
{Z 357/2004}	o ochrane verejného záujmu pri výkone funkcií verejných funkcionárov
{Z 365/2004}	o rovnakom zaobchádzaní v niektorých oblastiach a o ochrane pred diskrimináciou a o zmene a doplnení niektorých zákonov (antidiskriminačný zákon)
{Z 523/2004}	o rozpočtových pravidlách verejnej správy a o zmene a doplnení niektorých

	zákonov
{Z 578/2004}	o poskytovateľoch zdravotnej starostlivosti, zdravotníckych pracovníkoch, stavovských organizáciách v zdravotníctve a o zmene a doplnení niektorých zákonov
{Z 580/2004}	o zdravotnom poistení a o zmene a doplnení zákona č. 95/2002 Z. z. o poisťovníctve a o zmene a doplnení niektorých zákonov
{Z 583/2004}	o rozpočtových pravidlách územnej samosprávy a o zmene a doplnení niektorých zákonov
{Z 650/2004}	o doplnkovom dôchodkovom sporení a o zmene a doplnení niektorých zákonov
{Z 36/2005}	o rodine a o zmene a doplnení niektorých zákonov
{Z 82/2005}	o nelegálnej práci a nelegálnom zamestnávaní a o zmene a doplnení niektorých zákonov
{Z 300/2005}	Trestný zákon
{Z 301/2005}	Trestný poriadok
{Z 473/2005}	o poskytovaní služieb v oblasti súkromnej bezpečnosti a o zmene a doplnení niektorých zákonov (zákon o súkromnej bezpečnosti)
{Z 124/2006}	o bezpečnosti a ochrane zdravia pri práci a o zmene a doplnení niektorých zákonov
{Z 125/2006}	o inšpekcii práce a o zmene a doplnení zákona č. 82/2005 Z. z. o nelegálnej práci a nelegálnom zamestnávaní a o zmene a doplnení niektorých zákonov
{Z 126/2006}	o verejnom zdravotníctve a o zmene a doplnení niektorých zákonov
{Z 275/2006}	o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov
{Z 250/2007}	o ochrane spotrebiteľa a o zmene zákona Slovenskej národnej rady č. 372/1990 Zb. o priestupkoch v znení neskorších predpisov
{Z 330/2007}	o registri trestov a o zmene a doplnení niektorých zákonov
{Z 355/2007}	o ochrane, podpore a rozvoji verejného zdravia a o zmene a doplnení niektorých zákonov
{Z 663/2007}	o minimálnej mzde
{Z 167/2008}	o periodickej tlači a agentúrnom spravodajstve a o zmene a doplnení niektorých zákonov (tlačový zákon)
{Z 448/2008}	o sociálnych službách a o zmene a doplnení zákona č. 455/1991 Zb. o živnostenskom podnikaní (živnostenský zákon) v znení neskorších predpisov
{Z 522/2008}	o vyznamenaní Slovenskej republiky
{Z 539/2008}	o podpore regionálneho rozvoja
{Z 206/2009}	o múzeách a o galériách a o ochrane predmetov kultúrnej hodnoty a o zmene zákona Slovenskej národnej rady č. 372/1990 Zb. o priestupkoch v znení neskorších predpisov
{Z 400/2009}	o štátnej službe a o zmene a doplnení niektorých zákonov
{Z 563/2009}	o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov
{Z 9/2010}	o sťažnostiach
{Z 324/2011}	o poštových službách
{Z 351/2011}	o elektronických komunikáciách
{Z 56/2012}	o cestnej doprave
{Z 102/2014}	o ochrane spotrebiteľa pri predaji tovaru alebo poskytovaní služieb na základe zmluvy uzavretej na diaľku alebo zmluvy uzavretej mimo prevádzkových priestorov predávajúceho a o zmene a doplnení niektorých zákonov
{Z 103/2014}	o divadelnej činnosti a hudobnej činnosti a o zmene a doplnení niektorých zákonov

{Z 214/2014}	o správe, prevádzke a používaní informačného systému Centrálny elektronický priečinok pri dovoze, vývoze a tranzite tovaru a o doplnení zákona č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente)
{Z 284/2014}	o Fonde na podporu umenia a o zmene a doplnení zákona č. 434/2010 Z. z. o poskytovaní dotácií v pôsobnosti Ministerstva kultúry Slovenskej republiky v znení zákona č. 79/2013 Z. z.
{Z 307/2014}	o niektorých opatreniach súvisiacich s oznamovaním protispoločenskej činnosti a o zmene a doplnení niektorých zákonov
{VMF55/2014}	Výnos Ministerstva financií Slovenskej republiky o štandardoch pre informačné systémy verejnej správy
{Z 39/2015}	o poisťovníctve a o zmene a doplnení niektorých zákonov
{Z 40/2015}	o audiovizii a o zmene a doplnení niektorých zákonov
{Z 126/2015}	o knižniciach a o zmene a doplnení zákona č. 206/2009 Z. z. o múzeách a o galériách a o ochrane predmetov kultúrnej hodnoty a o zmene zákona Slovenskej národnej rady č. 372/1990 Zb. o priestupkoch v znení neskorších predpisov v znení zákona č. 38/2014 Z. z.
{Z 160/2015}	Civilný sporový poriadok
{Z 161/2015}	Civilný mimosporový poriadok
{Z 162/2015}	Správny súdny poriadok
{Z 185/2015}	Autorský zákon
{Z 189/2015}	o kultúrno-osvetovej činnosti
{Z 343/2015}	o verejnom obstarávaní a o zmene a doplnení niektorých zákonov
{Z 357/2015}	o finančnej kontrole a audite a o zmene a doplnení niektorých zákonov
{Z 91/2016}	o trestnej zodpovednosti právnických osôb a o zmene a doplnení niektorých zákonov
{Z 18/2018}	o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
	a ďalšie. Kvôli prehľadnosti môže byť uvádzaný skrátený názov predpisu, v skutočnosti celý správny názov môže obsahovať aj: a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a pod. Nie všetky uvedené zákony sa musia dotýkať činností Prevádzkovateľa, ale boli konfrontované v rámci analýzy ochrany osobných údajov.

23. Špecifikácia príloh

Príloha č. 1	Vzor záznamu o spracovateľských činnostiach
Príloha č. 2a	Písomné poverenie zodpovednej osoby
Príloha č. 2b	Odvolanie poverenia zodpovednej osoby
Príloha č. 3	Určenie oprávnených osôb
Príloha č. 4	Poverenie oprávnenej osoby k spracúvaniu osobných údajov
Príloha č. 5	Informácia dotknutej osobe o spracúvaní osobných údajov
Príloha č. 6	Súhlas dotknutej osoby
Príloha č. 7	Evidenčný list záznamového média
Príloha č. 8	Evidenčný list technických prostriedkov
Príloha č. 9	Záznam o vykonanej kontrole v IS
Príloha č. 10	Záznam o bezpečnostnom incidente v IS
Príloha č. 11a	Písomná zmluva so sprostredkovateľom – vzor
Príloha č. 11b	Dotazník pre sprostredkovateľa – vzor
Príloha č. 12	Prihláška na kurz

24. Vyhotovovacia doložka

Bezpečnostná smernica bola vyhotovená v dvoch výtlačkoch s textovými a grafickými prílohami, ktoré boli pridelené nasledovne:

Výtlačok č. 1 – generálna riaditeľka Prevádzkovateľa

Výtlačok č. 2 – elektronický výtlačok Entry Net, s.r.o. (pre spis)