

Bezpečnostný projekt

Časť:

Bezpečnostná smernica na ochranu osobných údajov

v pôsobnosti Pamiatkového úradu Slovenskej republiky

(aktualizácia k 26.9.2011)

Zhrnutie :

Bezpečnostná smernica na ochranu osobných údajov bola vypracovaná v zmysle § 16, ods. (3) a (6) zákona č. 428/2002 Z.z. o ochrane osobných údajov v znení zákona č. 602/2003 Z.z., zákona č. 576/2004 Z.z. a zákona č. 90/2005 Z.z.

PhDr. Katarína KOSOVÁ
Generálna riaditeľka
Pamiatkového úradu SR

Autor:	Ing. Roman LESKOVSKÝ Entry Net, s.r.o. Technický riaditeľ	podpis :		dátum :
Na vedomie:	RNDr. Euboslav ŠKOVIERA Poverená zodpovedná osoba za PÚ SR	podpis :	_____	dátum :
	Oprávnené osoby		Záznam o poučení oprávnených osôb bude uložený u zodpovednej osoby	

© Entry Net, s. r. o.

Bezpečnostná smernica je autorským dielom spracovateľského kolektívu Entry Net, s.r.o. Bratislava. 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 (napr. § 15 až 18 zákona č. 618/2003 Z.z. o autorskom práve a právach súvisiacich s autorským právom „Autorský zákon“ v znení neskorších predpisov).

Obsah

Výklad základných pojmov a používané skratky	4
1. Dôvod vypracovania Bezpečnostnej smernice	6
2. Dislokácia, zriadenie, pôsobnosť a organizačná štruktúra	8
2.1 Dislokácia	8
2.2 Zriadenie	8
2.3 Pôsobnosť	8
2.4 Organizačná štruktúra.....	9
3. Účel a podmienky spracúvania osobných údajov	10
3.1 Prevádzkovateľ	10
3.2 Zmluvní Sprostredkovatelia	11
3.2.1 Ministerstvo kultúry Slovenskej republiky	11
3.2.2 Ďalšie spoločnosti.....	11
3.3 Prevádzkované informačné systémy	12
3.3.1 IS Personalistika, mzdy a účtovníctvo.....	12
3.3.2 IS Ústredný zoznam pamiatkového fondu	12
3.3.3 IS Archív Pamiatkového úradu SR.....	13
3.3.4 Knižničný informačný systém.....	13
3.3.5 Ostatné agendy	13
3.4 Evidencia informačných systémov.....	14
3.5 Účel spracúvania osobných údajov	15
3.5.1 Účel spracúvania osobných údajov v IS PMÚ.....	15
3.5.2 Účel spracúvania osobných údajov v IS ÚZPF.....	15
3.5.3 Účel spracúvania osobných údajov v IS ARCHÍV	15
3.5.4 Účel spracúvania osobných údajov v KIS	15
4. Popis IS, obsah a charakter spracúvaných osobných údajov	16
4.1 IS PMÚ	16
4.1.1 Personálna agenda	16
4.1.2 Mzdová agenda	18
4.1.3 Účtovná agenda	19
4.1.4 Rozsah osobných údajov v IS PAM	20
4.2 Automatizované spracúvanie s využitím CJES	22
4.2.1 Charakteristika softvéru SOFTIP PROFIT	23
4.2.2 Popis aplikačného prostredia CJES	25
4.2.3 Popis databázového prostredia CJES	25
4.2.4 Postup a podmienky prístupu do CJES.....	26
4.2.5 Poverená osoba za CJES.....	26
4.2.6 Určenie oprávnenej osoby CJES	26
4.2.7 Vytvorenie prístupu do CJES.....	27
4.3 IS ÚZPF	28
4.3.1 Automatizované spracúvanie	29
4.3.2 Neautomatizované spracúvanie	29
4.4 IS ARCHÍV	30
4.5 KIS.....	31
4.7.1 Rozsah osobných údajov	31
5. Podmienky spracúvania osobných údajov.....	33
6. Získavanie osobných údajov	35
7. Poskytovanie, sprístupňovanie a zverejňovanie osobných údajov	37
8. Nakladanie s osobnými údajmi po splnení účelu spracúvania.....	39

9. Prístup k osobným údajom	40
10. Sprostredkovateľ	41
11. Dohľad nad ochranou osobných údajov	42
12. Určenie a povinnosti oprávnenej osoby	45
13. Bezpečnosť osobných údajov pri ich spracúvaní	47
14. Práva dotknutých osôb	49
15. Cezhraničný prenos osobných údajov	50
16. Evidencia a registrácia IS	51
17. Bezpečnosť osobných údajov pri ich spracúvaní	52
18. Technická bezpečnosť IS	54
18.1 Technická bezpečnosť neautomatizovaných IS	54
18.1.1 Pravidlá používania NIS	54
18.2 Technická bezpečnosť automatizovaných IS	55
18.2.1 Úlohy, funkcie a zodpovednosti osôb v informačných systémoch	55
18.2.2 Organizácia a zodpovednosť za informačnú bezpečnosť	56
18.2.3 Funkcie v informačnom systéme	57
18.2.4 Správa infraštruktúry IT	58
18.2.5 Správa užívateľov	58
18.2.6 Identifikácia a autentizácia	58
18.2.7 Riadenie prístupu	60
18.2.8 Audít a účtovateľnosť	60
18.2.9 Opakované použitie	61
18.2.10 Manipulácia s médiami	61
18.2.11 Používanie elektronickej pošty	61
18.2.12 Používanie ďalších komunikačných kanálov	62
18.2.13 Používanie Internetu	62
18.2.14 Používanie mobilných počítačov a práca doma	63
18.2.15 Ochrana počítača počas neprítomnosti užívateľa	63
18.2.16 Depozit hesiel	63
18.2.17 Antivírusová ochrana	64
18.2.18 Šifrovanie dát	65
18.2.19 Riešenie bezpečnostných incidentov	65
18.2.20 Archivácia, zálohovanie a obnova	66
19. Spolupráca s Úradom na ochranu osobných údajov SR	67
20. Záverečné a prechodné ustanovenia	68
21. Niektoré zákony upravujúce účel spracúvania osobných údajov	69
Špecifikácia príloh	71
Vyhotovovacia doložka	72

Výklad základných pojmov a používané skratky

Základný pojem	Výklad pojmu	Používaná skratka, poznámka, zdroj
Zákon č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov	Zákon upravuje zásady ochrany osobných údajov fyzických osôb pri ich spracúvaní v informačných systémoch	Zákon http://www.dataprotection.gov.sk
Prevzaté právne akty Európskych spoločenstiev a Európskej únie	Záväzné právne akty, ktoré Slovenská republika prevzala zákonným spôsobom, upravuje sa nimi ochrana osobných údajov pri ich spracúvaní	Napr. Smernica Európskeho parlamentu a Rady 95/46/ES, Dohovor Rady Európy č. 108 http://www.dataprotection.gov.sk
Úrad na ochranu osobných údajov Slovenskej republiky	Orgán štátnej správy s celoslovenskou pôsobnosťou, ktorý vykonáva dozor nad ochranou osobných údajov a nezávisle sa podieľa na ochrane základných práv a slobôd fyzických osôb pri spracúvaní ich osobných údajov	Úrad § 33 až 38 Zákona http://www.dataprotection.gov.sk
Bezpečnostný projekt	Vymedzuje rozsah a spôsob technických, organizačných a personálnych opatrení prijatých na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na informačný systém z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti. V zmysle Zákona obsahuje bezpečnostný zámer, analýzu bezpečnosti informačného systému a bezpečnostnú smernicu	BP § 16 Zákona
Bezpečnostný zámer	Vymedzuje základné bezpečnostné ciele, ktoré je potrebné dosiahnuť na ochranu informačného systému pred ohrozením jeho bezpečnosti	BZ § 16, ods. 4 Zákona
Analýza bezpečnosti informačného systému	Podrobný rozbor stavu bezpečnosti informačného systému, ktorá obsahuje najmä kvalitatívnu analýzu rizík, rozsah a obsah využitia bezpečnostných štandardov ako aj určenie iných metód a prostriedkov ochrany osobných údajov	ABIS § 16, ods. 5 Zákona
Bezpečnostná smernica	Bezpečnostná smernica upresňuje a aplikuje závery z bezpečnostného projektu na konkrétne podmienky prevádzkovaného informačného systému	BS §16, ods. 6 Zákona
Osobné údaje	Údaje týkajúce sa určenej alebo určiteľnej fyzickej osoby, ktorú možno určiť na základe jednej či viacerých charakteristík alebo znakov	OÚ § 3 Zákona
Klasifikované informácie, údaje a informačné aktíva	Informácie a údaje, ktoré prevádzkovateľ informačného systému označil ako interne dôverné, chráni ich, ich strata, vyzradenie alebo neužitie môže spôsobiť vážne materiálne alebo nemateriálne škody (napr. kritické business údaje, bezpečnostné nastavenia informačného systému, režim ochrany popis využitých technických prostriedkov objektivej ochrany, strážne smernice a pravidlá fyzickej ochrany objektu ...)	KI
Spracúvanie osobných údajov	Vykonávanie akýchkoľvek operácií alebo súboru operácií s osobnými údajmi, napr. ich získavanie, zhromažďovanie, zaznamenávanie, usporadúvanie, prepracúvanie, triedenie, prehliadanie, uchovávanie, likvidácia, poskytovanie, sprístupňovanie alebo zverejňovanie	§ 4, ods. 1, písm. a) Zákona
Informačný systém	Akýkoľvek usporiadaný súbor, sústava alebo databáza obsahujúca jeden alebo viac osobných údajov, ktoré sa systematicky spracúvajú na potreby dosiahnutia účelu s použitím	IS § 4, ods. 1, písm. g) Zákona

	automatizovaných, čiastočne automatizovaných alebo iných ako automatizovaných prostriedkov spracúvania. Podľa vyššie uvedeného môže byť informačný systém tvorený dátami spracúvanými automatizovaným spôsobom s využitím aplikačného programového vybavenia alebo informáciami spracúvanými v písomnej forme vo vedených operátoch a registroch.	
Centrálny jednotný ekonomický systém Softip Profit	System založený na technológii klient-server, ktorý tvoria aplikácie zabezpečujúce rýchle a pritom pohodlné riadenie ekonomických, personálnych, mzdových a logistických informácií	<i>CJES</i>
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 audiovíziu.	<i>MK SR</i>
Datacentrum Ministerstva kultúry SR	Centrum výpočtovej techniky MK SR, v ktorom sú prevádzkované centralizované informačné systémy rezortu kultúry	<i>Datacentrum</i>
Organizácia v zriaďovateľskej pôsobnosti MK SR	Organizácia, ktorý v zmysle stanovenej pôsobnosti, s prihliadnutím k osobitným zákonom a v zmysle zriaďovacej listiny vydanéj MK SR realizuje predmet svojej činnosti.	<i>Organizácia MK SR alebo iba Organizácia, v skratke O MK SR</i>
Účel spracúvania	Vopred jednoznačne vymedzený alebo ustanovený zámer spracúvania osobných údajov	<i>§ 4, ods. 1, písm. h) Zákona</i>
Súhlas dotknutej osoby	Akýkoľvek slobodne daný, výslovný a zrozumiteľný prejav vôle, ktorým dotknutá osoba na základe poskytnutých informácií vedome vyjadruje súhlas so spracúvaním svojich osobných údajov	<i>§ 4, ods. 1, písm. i) Zákona</i>
Prevádzkovateľ	Ten kto sám alebo spoločne s inými určuje účel a prostriedky spracúvania osobných údajov	<i>Prevádzkovateľ § 4, ods. 2 Zákona</i>
Sprostredkovateľ	Ten, kto spracúva osobné údaje v mene prevádzkovateľa, na základe podmienok dojednaných v písomnej zmluve alebo v písomnom poverení	<i>Sprostredkovateľ § 4, ods. 3 Zákona</i>
Zodpovedná osoba	Fyzická osoba, ktorá na základe písomného poverenia prevádzkovateľa dozerá na dodržiavanie zákonných ustanovení pri spracúvaní osobných údajov	<i>ZO § 19 Zákona</i>
Oprávnená osoba	Fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovnoprávneho vzťahu, na základe poverenia, zvolenia alebo vymenovania, ktorá môže osobné údaje spracúvať len na základe pokynu prevádzkovateľa, zástupcu prevádzkovateľa alebo sprostredkovateľa (ďalej len „Pracovný pomer“)	<i>OO § 4, ods. 4 Zákona</i>
Dotknutá osoba	Každá fyzická osoba, o ktorej sa spracúvajú osobné údaje.	<i>DO § 4, ods. 5 Zákona</i>
Ochrana práv dotknutej osoby	Zákon upravuje práva dotknutej osoby na informácie o stave a podmienkach spracúvanie jej osobných údajov v informačných systémoch, pričom tieto práva je možné v nevyhnutnej miere obmedziť iba na základe osobitného zákona.	<i>§ 20 a 21 Zákona</i>

1. Dôvod vypracovania Bezpečnostnej smernice

1. Bezpečnostná smernica (ďalej len „Smernica“) bola vypracovaná v zmysle zákona č. 428/2002 Z.z. o ochrane osobných údajov v znení neskorších predpisov ¹ (ďalej len Zákon“).
2. Základným cieľom aplikácie a následnej implementácie Zákona je určiť a implementovať integrované zásady ochrany osobných údajov v podmienkach organizácií v zriaďovateľskej pôsobnosti Ministerstva kultúry SR (ďalej len „Organizácie“).
3. Pri vypracovaní Smernice boli využité závery Bezpečnostného projektu na ochranu osobných údajov Ministerstva kultúry SR (ďalej len „MK SR“) ako zriaďovateľa Organizácií, Bezpečnostnej politiky informačných systémov v rezorte kultúry SR.
4. Pri vypracovaní Smernice boli aplikované zákonným spôsobom prevzaté normy a štandardy na hodnotenie a riadenie bezpečnosti v automatizovaných IS a ostatná aplikovateľná legislatíva Slovenskej republiky, platná v čase vypracovania a vydania tejto Smernice. ² Podrobný zoznam aplikovateľnej legislatívy je uvedený v čl. 21 tejto Smernice.
5. Smernicami sa aplikujú závery vyplývajúce z analýz bezpečnosti IS, ktoré boli vykonané v jednotlivých miestach ich prevádzkovania u Organizácií.
6. Dôvodom aktualizácie Bezpečnostnej smernice sú vykonané technické, organizačné a personálne zmeny po ukončení implementácie Centrálného jednotného ekonomického systému SOFTIP PROFIT (ďalej len „CJES“), ktorého nasadením do prostredia a pôsobnosti rezortu kultúry došlo k významnej zmene doterajších podmienok a prostriedkov najmä automatizovaného spracúvania osobných údajov Prevádzkovateľom, jeho zmluvnými sprostredkovateľmi, bez zmeny stanoveného účelu ich spracúvania.
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 oprávnených 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.

¹ § 16, ods. 3 a 6 Zákona.

² napr. ISO/IEC 17799:2005; ISO/IEC 27000 v znení ISO/IEC 27001 Information technology - Security techniques – Information security management systems – Requirements, ISO/IEC 27002 Information technology - Security techniques – Code of practice for information security management a ISO/IEC 20006 IT Security techniques: Requirements for bodies providing audit and certification of Information Security Managements Systems (ISMS), Zákon NR SR č. 275/2006 o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení Výnosu Ministerstva financií SR z 8. septembra 2008 č. MF/013261/2008-132 o štandardoch pre informačné systémy verejnej správy a jeho vykonávacej vyhlášky, Prevádzkový poriadok WAN VPN MK SR a Prevádzkový poriadok CJES v znení ich neskorších zmien a dodatkov.

8. Smernica je výsledkom:

- a.) Bezpečnostnej politiky informačných systémov v rezorte kultúry SR s požiadavkou jej operatívnej aplikácie do podmienok Organizácií, upravených podmienok bezpečnostnej správy a administrácie automatizovaných informačných systémov,
- b.) vykonanej rizikovej analýzy v prevádzkovaných IS Organizácie 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 Bezpečnostného projektu na ochranu osobných údajov Organizácie. Jej súčasťou sú aplikačné prílohy, šablóny a vzory písomností, ktorých podrobný zoznam je uvedený v čl. 22 tejto Smernice.

2. Dislokácia, zriadenie, pôsobnosť a organizačná štruktúra

2.1 Dislokácia

Informačné systémy, sú prevádzkované v pracovných priestoroch PÚ SR so sídlom na adrese Cesta na Červený most č. 6, 814 06 Bratislava.

2.2 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, v súlade so zákonom č. 49/2002 Z. z. o ochrane pamiatkového fondu v znení neskorších predpisov, formou Rozhodnutia MK SR o vydaní zriaďovacej listiny PÚ SR zo dňa 1. apríla 2002 vydaného pod č. MK:572/2002-1.

2.3 Pôsobnosť

Prevádzkovateľ je v zmysle zriaďovacej listiny štátna rozpočtová organizácia svojimi príjmami a výdavkami zapojená na štátny rozpočet. Hospodári samostatne podľa schváleného rozpočtu, vo svojom mene nadobúda práva a zaväzuje sa.

Zriaďovateľom PÚ SR je Ministerstvo kultúry Slovenskej republiky, ktoré garantuje a kontroluje jeho činnosť a v prípade zistenia nedostatkov prijíma potrebné opatrenia.

PÚ SR je orgánom štátnej správy na ochranu pamiatkového fondu.

Riadi a kontroluje výkon štátnej správy na úseku ochrany pamiatkového fondu uskutočňovaný krajskými pamiatkovými úradmi, ktoré ju vykonávajú vo svojom územnom obvode, ktorým je územný obvod kraja.

Rozhoduje v prvom stupni v správnom konaní vo veciach zverených mu zákonom na úseku ochrany pamiatkového fondu.

Pamiatkový úrad vykonáva v druhom stupni štátnu správu na úseku ochrany pamiatkového fondu vo veciach, o ktorých v prvom stupni rozhodujú Krajské pamiatkové úrady (ďalej len „KPÚ“).

Rieši a koordinuje odborné a výskumné úlohy rozpracúva teóriu a metodológiu ochrany pamiatkového fondu.

V rámci svojho poslania realizuje najmä tieto činnosti:

- plní funkciu správcu príslušnej časti štátneho informačného systému,
- vedie osobitný archív v oblasti ochrany pamiatkového fondu,
- vedie Ústredný zoznam pamiatkového fondu,
- zabezpečuje rozvoj teórie a metodológie reštaurovania, buduje študijné, vývojové a analyticko-technologické pracovisko a laboratóriá,
- zabezpečuje výskumné a reštaurátorské práce ako účelovú pomoc štátu na ohrozených kultúrnych pamiatkach,
- vykonáva a koordinuje dokumentačnú, vzdelávaciu, výchovnú, edičnú a propagačnú činnosť,
- poskytuje odbornú a metodickú pomoc KPÚ,
- spolupracuje s občianskymi združeniami a nadáciami zriadenými na záchranu, využívanie a prezentáciu pamiatkového fondu, podieľa sa na medzinárodných projektoch ochrany a obnovy kultúrnych pamiatok a pamiatkový území a spolupracuje s medzinárodnými organizáciami a partnerskými inštitúciami v zahraničí.

Štatutárnym orgánom PÚ SR je generálny riaditeľ, ktorého po prerokovaní s Pamiatkou radou vymenúva a odvoláva minister kultúry Slovenskej republiky.

Generálny riaditeľ riadi činnosť PÚ SR v súlade so zriaďovacou listinou a zodpovedá za ňu ministrovi kultúry Slovenskej republiky.

Generálny riaditeľ ustanovuje svojich zástupcov z vedúcich zamestnancov, ktorých priamo riadi.

Organizačnú štruktúru, náplň činnosti jednotlivých pracovísk a vzájomné vzťahy medzi nimi upravuje organizačný poriadok PÚ SR, ktorý vydáva generálny riaditeľ.

2.4 Organizačná štruktúra

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

3. Účel a podmienky spracúvania osobných údajov

3.1 Prevádzkovateľ

Prevádzkovateľom v zmysle Zákona a zriaďovacej listiny je Pamiatkový úrad Slovenskej republiky.

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.

3.2 Zmluvní Sprostredkovatelia

3.2.1 Ministerstvo kultúry Slovenskej republiky

Ministerstvo kultúry Slovenskej republiky (ďalej len „MK SR“ alebo „Ministerstvo“) so sídlom na adrese Nám. SNP č. 13, 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,
- zabezpečenia bezpečnej a spoľahlivej prevádzky softvéru potrebného na činnosť CJES,
- koncepčné a metodické riadenie rozvoja a prevádzky CJES,
- pravidelné prehodnocovanie stavu CJES, 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. 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.

Zákonom požadovanú zmluvu alebo písomné poverenie sprostredkovateľa na spracúvanie osobných údajov v mene prevádzkovateľa nahrádza prevádzkový poriadok WAN VPN MK SR v znení jeho neskorších dodatkov, ktorý bol vydaný v súlade s Organizačným poriadkom MK SR.

3.2.2 Ďalšie spoločnosti

Prevádzkovateľ 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 spoločnosti Tempest a.s., SWAN, a.s. a pod., ktoré spravidla vystupujú iba ako technologický sprostredkovateľ.

3.3 Prevádzkované informačné systémy

Prevádzkovateľ systematicky spracúva osobné údaje prostredníctvom v nasledovných informačných systémoch:

3.3.1 IS Personalistika, mzdy a účtovníctvo

IS Personalistika, mzdy a účtovníctvo (ďalej len „IS PMÚ“) integruje spracúvanie osobných údajov v nasledovných agendách:

- Personálna agenda,
- Mzdová agenda,
- Účtovná agenda,

Uvedenými agendami sa realizuje Personálna agenda, Mzdová agenda, Sociálne a zdravotné poistenie, a činnosti spojené s pracovnoprávnymi vzťahmi, spracúvanie účtovnej agendy a styk so Štátnou pokladnicou. Uvedeným IS sa zabezpečuje fakturácia a vystavovanie účtovných dokladov, obeh účtovných dokladov, úhrada účtovných dokladov, evidencia a archivácia účtovných dokladov a pod.

3.3.2 IS Ústredný zoznam pamiatkového fondu

Informačný systém Ústredný zoznam pamiatkového fondu (ďalej len „IS ÚZPF“), ktorým sa zabezpečuje pôsobnosť Prevádzkovateľa podľa osobitného zákona (zákon č. 49/2002 Z.z. o ochrane pamiatkového fondu), t.j. na činnosti súvisiace s výkonom štátnej správy a štátneho dozoru na úseku ochrany pamiatkového fondu (národných kultúrnych pamiatok hnutel'ných a nehnuteľných, pamiatkových rezervácií a pamiatkových zón), evidencia zákonom požadovaných údajov o predmetoch pamiatkového fondu a vlastníkoch predmetov pamiatkového fondu.

IS ÚZPF taktiež obsahuje a striktno vymedzeným spôsobom vedie osobitnú evidenciu pamiatkového fondu, týkajúcu sa vlastníkov národných kultúrnych pamiatok, umiestnenia hnutel'ných národných kultúrnych pamiatok a archeologických nálezísk, ktoré podľa Zoznamu utajovaných skutočností v pôsobnosti Ministerstva kultúry SR číslo MK – 3156/2007-10/10476 zo dňa 28.6.2007 spadajú do pôsobnosti zákona č. 215/2004 Z.z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov. Tieto nespádajú do oblasti ochrany osobných údajov.

3.3.3 IS Archív Pamiatkového úradu SR

Informačný systém Archív Pamiatkového úradu (ďalej len „IS ARCHÍV“), ktorým sa realizuje pôsobnosť Prevádzkovateľa podľa osobitného zákona (zákon č. 49/2002 Z.z. o ochrane pamiatkového fondu), tj na činnosti súvisiace s vedením archívu osobitného významu v oblasti ochrany pamiatkového fondu. Archív Pamiatkového úradu Slovenskej republiky je verejným špecializovaným archívom pre oblasť ochrany pamiatkového fondu na Slovensku. Organizačne podlieha Ministerstvu kultúry SR, štátny odborný dozor vykonáva Ministerstvo vnútra SR.

Bol zriadený rozhodnutím Odboru archívniectva a spisovej služby MV SR z 22. mája 1992 ako archív osobitného významu s názvom Archív Slovenského ústavu pamiatkovej starostlivosti. S účinnosťou od 1. apríla 2002 bol premenovaný na Archív Pamiatkového úradu SR. Jeho archívne dokumenty sú súčasťou archívneho kultúrneho dedičstva Slovenskej republiky.

Pôsobnosť a kompetencie Prevádzkovateľa pri vedení IS ARCHÍV sa ďalej upravujú zákonom č.395/2002 Z.z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov a zákona č. 242/2007 Z.z. ktorým sa mení a dopĺňa vyhláška Ministerstva vnútra Slovenskej republiky č. 628/2002 Z.z., ktorou sa vykonávajú niektoré ustanovenia zákona o archívoch a registratúrach a o doplnení niektorých zákonov v znení vyhlášky č. 251/2005 Z.z.

3.3.4 Knižničný informačný systém

Knižničný informačný systém (ďalej len „KIS“) zahŕňa samotnú knižnicu Pamiatkového úradu SR a k nej pridružený automatizovaný systém na správu knižničného fondu a správu používateľov a bádateľov. Knižnica je odbornou knižnicou, ktorej fondy zodpovedajú kultúrnemu, vedeckému, spoločenskému a štátno-správnemu poslaniu Pamiatkového úradu SR a jeho právnych predchodcov. Od svojho vzniku v roku 1919 sa zameriava na literatúru o ochrane pamiatok, pričom si všíma všetky príbuzné disciplíny – históriu, dejiny umenia, architektúru, archeológiu, archívniectvo a pomocné vedy historické, etnológiu, reštaurovanie atď. V jej fondoch sa nachádza aj právnická literatúra, zbierky zákonov, slovníková a encyklopedická literatúra. Najväčšie zastúpenie má literatúra slovenskej proveniencie, ale veľmi početný je aj fond cudzojazyčnej literatúry, najmä českej, maďarskej, poľskej, nemeckej, anglickej a francúzskej.

Rozdelenie knižničných fondov:

- fond všeobecnej odbornej literatúry – 20 000 ks
- fond reštaurátorskej literatúry – 2 000 ks
- fond encyklopedickej a slovníkovej literatúry – 2 000 ks
- fond periodík – 7 000 ks (kompletné ročníky odborných slovenských a zahraničných časopisov)
- fond kníh veľkých formátov – 1 000 ks

3.3.5 Ostatné agendy

Analyzované boli aj ďalšie oblasti v ktorých by mohlo dochádzať k spracúvaniu osobných údajov v pôsobnosti Zákona 428/2002 Z.z., ale buď sa nejedná o informačný systém v pôsobnosti Zákona, alebo na uvedené spracúvanie osobných údajov, či evidenciu IS je udelená výnimka (napr.: Kniha návštev). Napriek tomu aj u týchto činností sa postupuje v súlade so Zákonom a sú dodržiavané všetky ustanovenia týkajúce sa spracúvania osobných údajov.

3.4 Evidencia informačných systémov

V zmysle príslušných stanovení Zákona týkajúcich sa registrácie a evidencie IS (§§ 24 až 32) sa povinnosť registrácie na IS uvedené v bode 3.3. nevzťahuje z nasledovných dôvodov:

- a) IS podlieha dohľadu zodpovednej osoby, ktorú poveril Prevádzkovateľ a ktorá vykonáva dohľad nad ochranou osobných údajov podľa Zákona, alebo
- b) IS obsahuje údaje fyzických osôb spracúvané na účely plnenia predzmluvných vzťahov, alebo
- c) uplatňovania práv a povinností vyplývajúcich pre prevádzkovateľa z existujúceho alebo ukončeného pracovnoprávneho vzťahu, štátnozamestnaneckého pomeru s týmito osobami, vrátane osobných údajov ich blízkych osôb, alebo
- d) obsahujú osobné údaje potrebné na uplatňovanie práv alebo plnenie povinností vyplývajúcich z osobitného zákona alebo sú spracúvané na základe osobitného zákona.

S prihliadnutím k ustanoveniu § 29 Zákona je Prevádzkovateľ o IS, ktoré nepodliehajú registrácii, povinný viesť evidenciu v zmysle, rozsahu a za podmienok určených Zákonom a to najneskôr odo dňa začatia spracúvania osobných údajov v IS. Evidencia prevádzkovaných informačných systémov bola zavedená, jej prípadná aktualizácia bude vykonaná v priebehu implementácie vypracovaného bezpečnostného projektu.

3.5 Účel spracúvania osobných údajov

Účel spracúvania osobných údajov v jednotlivých IS Prevádzkovateľa je nasledovný :

3.5.1 Účel spracúvania osobných údajov v IS PMÚ

Účel spracúvania osobných údajov v IS PMÚ je vymedzený osobitnými zákonmi uvedenými v čl. 21 tejto Smernice. V medziach stanoveného účelu sú vedené a priebežne aktualizované agendy uvedené v čl. 3.3., bod 3.3.1. tejto Smernice nasledovne:

- vedenie komplexnej personálnej a mzdovej agendy, podkladov na realizáciu miezd a úhradu mimo mzdových prostriedkov (napr. cestovných náhrad),
- realizácia finančných operácií, platieb a vedenie účtovníctva, ktoré súvisí s predmetom pôsobnosti Prevádzkovateľa,
- realizácia zmluvných vzťahov s fyzickými osobami, ktoré nie sú v zamestnaneckom pomere s Prevádzkovateľom, ale vykonávajú zmluvné činnosti, vytvárajú dielo, alebo za finančnú odmenu poskytujú Prevádzkovateľovi služby.

Účelom spracúvania osobných údajov je vedenie komplexnej personálnej a mzdovej agendy a podkladov na realizáciu miezd pre dotknuté osoby, ktoré sú, alebo môžu byť s prevádzkovateľom v pracovnoprávnom vzťahu, štátnozamestnaneckom pomere, služobnom pomere, členskom vzťahu, na základe poverenia, zvolenia alebo vymenovania alebo v rámci výkonu verejnej funkcie (ďalej len „Zamestnanec“), pracovníkov na dohodu, žiadateľov o zamestnanie a osôb pri realizácii výberových konaní (dochádza k spracúvaniu osobných údajov a podriadených zložiek (KPÚ a Oblastné reštaurátorské úrady). Uvedený účel spracúvania osobných údajov je vymedzený osobitnými zákonmi, ktorý je ďalej konkretizovaný v jednotlivých popisoch činností IS.

3.5.2 Účel spracúvania osobných údajov v IS ÚZPF

Účelom spracúvania osobných údajov v IS ÚZPF je evidencia údajov o vlastníkoch nehnuteľných a hnutel'ných národných kultúrnych pamiatok.

3.5.3 Účel spracúvania osobných údajov v IS ARCHÍV

Účelom spracúvania údajov v IS ARCHÍV je vedenie, aktualizácia, poskytovanie, sprístupňovanie a zverejňovanie údajov z IS ARCHÍV, pričom samotný IS ARCHÍV neobsahuje osobné údaje dotknutých osôb.

K spracúvaniu osobných údajov dochádza výhradne pri vedení, ukladaní a archivácii Bádateľských listov, ktoré sú zákonnou podmienkou prístupu k archívnym fondom vedeným v pôsobnosti PÚ SR.

3.5.4 Účel spracúvania osobných údajov v KIS

Účelom spracúvania osobných údajov v KIS je evidencia čitateľov a bádateľov pre potreby ich dosiahnuteľnosti a evidencii finančných prostriedkov a výpožičných listov v súlade so zákonom č. 183/2000 Z.z. o knižniciach. Uvedený účel spracúvania osobných údajov je vymedzený osobitnými zákonmi, ktorý je ďalej konkretizovaný v jednotlivých popisoch činností IS.

4. Popis IS, obsah a charakter spracúvaných osobných údajov

Táto kapitola sa zaoberá popisom základných vlastností IS uvedených v čl. 3.1., obsahom, charakterom, podmienkami, prostriedkami a subjektmi spracúvania osobných údajov.

4.1 IS PMÚ

Automatizované spracúvanie osobných údajov v personálnej 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. 4.2.

Aplikácia a jej moduly sú popísané v dodanej dokumentácii k aplikačnému programovému vybaveniu s dôrazom na modul, ktorý pri spracúvaní osobných údajov určene oprávnené osoby využívajú.

4.1.1 Personálna agenda

Personálna agenda je v automatizovanej aj neautomatizovanej forme spracovávaná v pôsobnosti osobného úradu, ktorý je rozdelený na oddelenie pre štátnu službu a oddelenie pre verejnú službu. Každý zamestnanec uvedených oddelení má pri spracúvaní osobných údajov postavenie oprávnenej osoby.

Zabezpečenie činností je IS je podporované využitím kancelárskeho balíka MS Office, ktorým sa zabezpečuje vyhotovenie, tlač a archivácia požadovaných dokumentov súvisiacich s uzatvorením, priebehom, ukončením a dokumentáciou pracovného pomeru (pracovná zmluva, platový dekrét, osobný dotazník, prehlásenie o poistení v zdravotnej poisťovni, súhlas dotknutej osoby na spracúvanie jej osobných údajov, ak sa v zmysle Zákona požaduje a pod..)

Ochrana osobných údajov vedených v personálnej agende sa prioritne zabezpečuje riadeným prístupom do priestorov ich spracúvania, riadeným prístupom k PC na ktorých sú osobné údaje spracúvané.

V neautomatizovanej (písomnej) forme je personálna agenda vedená formou osobných spisov a agend:

- a) zamestnancov v štátnozamestnaneckom pomere,
- b) zamestnancov pri výkone práce vo verejnom záujme,
- c) zamestnancov v zamestnaneckom pomere,
- d) agendy pracovnoprávných vzťahov založených dohodou o vykonaní práce,
- e) agendy pracovnoprávných vzťahov založených dohodou o brigádnickej práci študentov,
- f) agendy evidencie uchádzačov o zamestnanie a realizácie výberových konaní,
- g) agendy súvisiacej s realizáciou konkurzov.

Osobné spisy zamestnancov podľa bodu a), b) a c) tohto článku vedie Prevádzkovateľ v rozsahu a spôsobom požadovanom osobitnými zákonmi, ktoré stanovujú účel, podmienky, prostriedky a subjekty spracúvania osobných údajov - bližšie viď čl. 21 tejto Smernice.

Z uvedeného dôvodu sa písomný súhlas dotknutej osoby na získavanie jej osobných údajov a údajov blízkych osôb nepožaduje.

Písomný súhlas dotknutej osoby je Prevádzkovateľ povinný získať v prípade, ak sú osobné údaje získavané kopírovaním, skenovaním alebo iným zaznamenávaním úradných dokladov na nosič informácií (občianskych preukazov a cestovných pasov) čo pri vykonaní Analýzy bolo zistené a Prevádzkovateľ z uvedených dôvodov získava súhlas dotknutých osôb, avšak nebol zistený účel získavania uvedených kópií - pravdepodobne slúžia výhradne na uľahčenie práce a prenos osobných údajov medzi oddeleniami, čím vzniká bezpečnostné riziko, preto Prevádzkovateľovi odporúčame uvedené kópie nevykonávať a stávajúce z osobných spisov zlikvidovať, nakoľko nie sú potrebné na splnenie účelu spracúvania osobných údajov. Oprávnené osoby boli poučené, že v prípadoch, kedy je potrebné kopírovať úradné dokumenty je potrebné získať od dotknutej osoby dodatočný súhlas priamo na takýto účel

Nakoľko všetky spracúvané osobné údaje v tejto agende sú vyžadované osobitnými zákonmi a nie je potrebné získavať súhlas na spracúvanie osobných údajov je Prevádzkovateľ povinný v súlade s §10 Zákona informovať dotknutú osobu o účele a podmienkach spracúvania osobných údajov. Z dôvodu jednoznačnosti takejto informácie bude v rámci implementácie BP vypracované tlačivo „Informácia DO o účele a podmienkach spracúvania osobných údajov“, ktorú dotknutá osoba podpíše pri nástupe do zamestnania.

Evidencia uchádzačov o zamestnanie je vedená v rozsahu potrebnom na plánovanie a rozvoj ľudských zdrojov v pôsobnosti Prevádzkovateľa. Po dobu trvania účelu na spracúvanie osobných údajov (výber uchádzačov na uvoľnené alebo novovytvorené pracovné pozície) sa písomný súhlas na spracúvanie osobných údajov nepožaduje, nakoľko sa v zmysle Zákona jedná o opatrenia na zavedenie predzmluvných vzťahov a opatrení na žiadosť dotknutej osoby.

Uvedená agenda je vybavovaná spravidla do 30 dní od doručenia a v prípade, že dotknutá osoba nie je pozvaná na osobný pohovor sú jej všetky zaslané údaje vrátené spolu s oznámením o tom, že pre dotknutú osobu nie je voľné pracovné miesto.

Osobitnou kategóriou osobných údajov spracúvaných v pôsobnosti Personálneho oddelenie sú údaje z registra trestov. Pre verejnú službu je osobitným zákonom podmienkou preukázania bezúhonnosti predloženie Výpisu z registra trestov. V evidencii sa však nachádzajú aj Odpisy z registra trestov, ktorých predloženie bolo do roku 2008 podmienkou zo zákona a je teda nutné ich držať v evidencii.

Odpismi z registra trestov preukazujú (preukazovali) 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.

U Prevádzkovateľa sa s uvedenými dokumentmi môže oboznamovať len generálny riaditeľ a určené oprávnené osoby. Súčasťou spracúvaných osobných údajov sú aj majetkové priznania niektorých dotknutých osôb (všetci štátni zamestnanci a vedúci zamestnanci pri výkone práce vo verejnom záujme sú zo zákona o štátnej službe a zákona o výkone práce vo verejnom záujme povinní podávať majetkové priznania). Zamestnanci PÚ SR, ktorým vyplýva zo zákona povinnosť podávať majetkové priznania, odovzdávajú vyplnené majetkové priznania určenému zamestnancovi osobného úradu v zalepenej obálke.

Oprávnená osoba z osobného úradu vo všetkých prípadoch zamestnaneckého vzťahu vykoná prihlásenie poisťenca do sociálnej poisťovne a príslušnej zdravotnej poisťovne, čo prebieha formou predpísaných tlačív prostredníctvom doporučenej zásielky alebo zabezpečenou elektronickou komunikáciou.

Podľa aplikovaných interných postupov môže predložiť návrh na uzatvorenie dohody obsahujúci požadované osobné údaje ktorýkoľvek organizačný útvar Prevádzkovateľa.

Všetky dokumenty a materiály zamestnancov v štátnozamestnaneckom pomere a v pracovnoprávnom vzťahu obsahujúce osobné údaje týkajúce sa personálnej agendy sú vkladané

do osobných spisov zamestnanca, ktoré sú uložené v uzamykateľných skriniach (príručná registratúra) v priestoroch osobného úradu.

Majetkové priznania štátnych zamestnancov a vedúcich zamestnancov pri výkone práce vo verejnom záujme sú uchovávané v zalepenej obálke v uzamykateľnej skrini v priestoroch osobného úradu. Prístup k údajom nachádzajúcim sa v majetkových priznaniach má len vedúci služobného úradu.

Prístup k osobným údajom personálnej agendy je riadený. Prístup k agende majú len určení zamestnanci osobného úradu. Čiastočný prístup majú aj nadriadení zamestnanci, ktorí majú možnosť nahliadnutia do osobných spisov priamo v kancelárii zamestnancov osobného úradu v rámci svojich podriadených. V etape analýzy neboli uvedené oprávnené osoby určené a niektoré ani poučené. Určenie oprávnených osôb a ich poučenie bude vykonané v rámci implementácie Bezpečnostného projektu. Bezpečnostné riziko je zanedbateľné, pretože všetky osoby s prístupom k osobným údajom boli poučené o mlčanlivosti podľa iných predpisov ({Z552/2003} alebo {Z312/2001}).

Po skončení účelu spracúvania sú osobné spisy zamestnancov uchovávané v príručnej registratúre osobného úradu a následne po uzavretí spisu sú presunuté do registratúrneho strediska v súlade s registratúrnym plánom.

4.1.2 Mzdová agenda

Mzdová agenda je v automatizovanej aj neautomatizovanej forme spracovávaná v pôsobnosti oddelenie mzdovej účtárne.

Ochrana osobných údajov vedených v mzdovej agende sa prioritne zabezpečuje riadeným prístupom do priestoru ich spracúvania a diferencovaným zabezpečeným prístupom k aplikácii.

Poverené oprávnené osoby pri spracúvaní osobných údajov taktiež postupujú podľa osobitných zákonov, ktoré sú uvedené v čl. čl. 21. tejto Smernice.

Neautomatizované spracúvanie je realizované formou mzdových listov, ktoré obsahujú písomnosti a tlačivá požadované osobitnými zákonmi.

Osobné údaje zamestnancov potrebné na spracovanie mzdovej agendy sú uchovávané na ekonomicko-prevádzkovom úseku na oddelení mzdovej účtárne. Uchovávané sú v písomnej forme (mzdové listy a ďalšie) v uzamykateľných skriniach (príručná registratúra) v samostatnej kancelárii.

Oprávnené osoby pri spracúvaní mzdovej agendy automatizovaným ako aj neautomatizovaným spôsobom vykonávajú:

- a) výpočet miezd,
- b) výpočet poisteného,
- c) vystavovanie a tlač účtovných dokladov,
- d) obeh účtovných dokladov,
- e) evidencia a archivácia 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.

Vlastnú realizáciu finančných úhrad mzdových prostriedkov vykonáva na základe vystavených účtovných dokladov referent personalistiky a miezd, ktorý je taktiež určený pre styk so Štátnou pokladnicou.

Pri spracúvaní Mzdovej agendy sú členom odborových organizácií zo mzdy strhávané príspevky. Za odvádzanie príspevkov zodpovedá oddelenie mzdovej učtárne. Zamestnanci dávajú písomný súhlas so strhnutím príspevku odborovej organizácii. V uvedenom prípade však skorej odporúčame žiadosť dotknutej osoby o takéto strhávanie, kedy nie sú potrebné k vykonaniu žiadne ďalšie úkony, pretože tak Prevádzkovateľ bude konať na žiadosť dotknutej osoby. V prípade, že si vyžaduje súhlas stavia sa do pozície Sprostredkovateľa pre odborovú organizáciu a v tomto prípade by musela byť medzi PÚ SR a odborovou organizáciou uzavretá písomná zmluva, alebo písomné poverenie.

4.1.3 Účtovná agenda

Účtovná agenda je v automatizovanej aj neautomatizovanej forme spracúvaná v pôsobnosti referentov Ekonomicko-prevádzkového úseku Prevádzkovateľa, ktorí pri spracúvaní osobných údajov majú postavenie oprávnenej osoby.

V rámci neautomatizovaného spracúvania údajov v účtovnej agende sú oprávneným osobám Ekonomicko-prevádzkového úseku za účelom automatizovaného zaúčtovania (vedenia účtovníctva) poskytované v písomnej forme požadované podklady, vrátane osobných údajov dotknutých osôb v rozsahu potrebnom na zaúčtovanie dohôd a zmlúv s fyzickými osobami..

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

Oprávnené osoby Prevádzkovateľa pri spracúvaní osobných údajov postupujú podľa osobitných zákonov, zavedených interných predpisov a určených procedúr (napr.: Registratúrny poriadok a registratúrny plán, Zásady obehu účtovných a iných dokladov a pod.).

4.1.4 Rozsah osobných údajov v IS PAM

V automatizovanom aj neautomatizovanom IS PAM sú spracúvané nasledovné infotypy osobných údajov dotknutých osôb v nasledovnom maximálnom rozsahu:

- priezvisko
- meno
- titul
- adresa trvalého pobytu, prípadne prechodného pobytu
- dátum narodenia
- miesto narodenia
- rodné číslo
- osobné číslo
- pohlavie
- rodinný stav
- rodinní príslušníci
- počet detí
- štátna príslušnosť
- absolvované školy a vzdelanie
- výnimky zo vzdelania
- doby v zamestnaní
- dátum uzatvorenia pracovného pomeru
- dôvod vzniku pracovného pomeru
- spôsob získania zamestnanca
- skúšobná doba
- dátum skončenia pracovného pomeru (PP)
- dôvod skončenia PP
- spôsob skončenia PP
- pracovná kategória
- druh pracovného pomeru
- pracovné zaradenie
- organizačný útvar
- fond pracovnej doby
- mzdové náležitosti
- dovolenka
- porušenie pracovnej disciplíny
- nárok na starobný dôchodok
- zmenená pracovná schopnosť
- služobné hodnotenie
- školenia a kurzy
- číslo telefónu
- predchádzajúci zamestnávateľia
- doba základnej vojenskej služby
- údaje o priznaní invalidného, čiastočne invalidného dôchodku
- údaje o zmenenej pracovnej schopnosti
- zdravotná poisťovňa zamestnanca
- meno a priezvisko manželky/manžela , druha / družky
- rodné číslo manželky/manžela, druha / družky – dátum narodenia, rodné meno
- meno a priezvisko dieťaťa
- rodné číslo dieťaťa
- názov a adresa školy, ktorú dieťa nad 16 rokov navštevuje
- údaje o dôchodkovom poistení zamestnanca
- údaje o zákonných zrážkach zamestnanca (výživné)

- údaje o sporení, pôžičkách a zrážkach na poistenie zamestnanca
- údaje o osobnom účte zamestnanca
- údaje o dočasnej práceneschopnosti zamestnanca, materských dávkach a o ošetrovaní chorého člena rodiny
- výška príspevkov pre odborovú organizáciu
- daňové vyhlásenie k dani z príjmu,
- daňový bonus,
- vyhlásenie zamestnanca na uplatnenie zníženia sadzby poistného na starobné poistenie,
- doklad o návšteve školy (16-25 r.),
- doklad o stupni invalidity.
- číslo zmluvy o DDS (rodné číslo)
- názov zamestnávateľa
- adresa sídla zamestnávateľa a PSČ
- dátum prvého príspevku DDS
- číslo sociálneho poistenia
- rodné priezvisko
- posledné priezvisko
- titul za menom
- číslo OP
- e-mailová adresa
- adresa prechodného pobytu
- dohodnutá doba trvania PP
- miesto výkonu práce
- vzdelanie požadované
- podobizeň nie je ukladaná, ale jediný exemplár je nalepený na preukaz zamestnanca a ten je odovzdaný DO, po skončení pracovného pomeru je podobizeň vrátená.

4.2 Automatizované spracúvanie s využitím CJES

Pre zabezpečenie automatizovaných činností v 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 MKSR 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 (viď príloha č.1 uvedenej zmluvy - Špecifikácia technickej podpory)

Podpora prevádzky bude poskytovaná formou prevádzkových zásahov a preventívnych zásahov.

Údržba APV SOFTIP PROFIT (bod 2.1.3) 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. (príloha 1.16.4.)

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.

4.2.1 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 platov, sociálnu starostlivosť o zamestnancov až po ďalšie vzdelávanie zamestnancov. Sekciu tvoria aplikácie: Personalistika, Mzdy a Dochádzka.

4.2.1.1 Základné vlastnosti programového balíka SOFTIP PROFIT

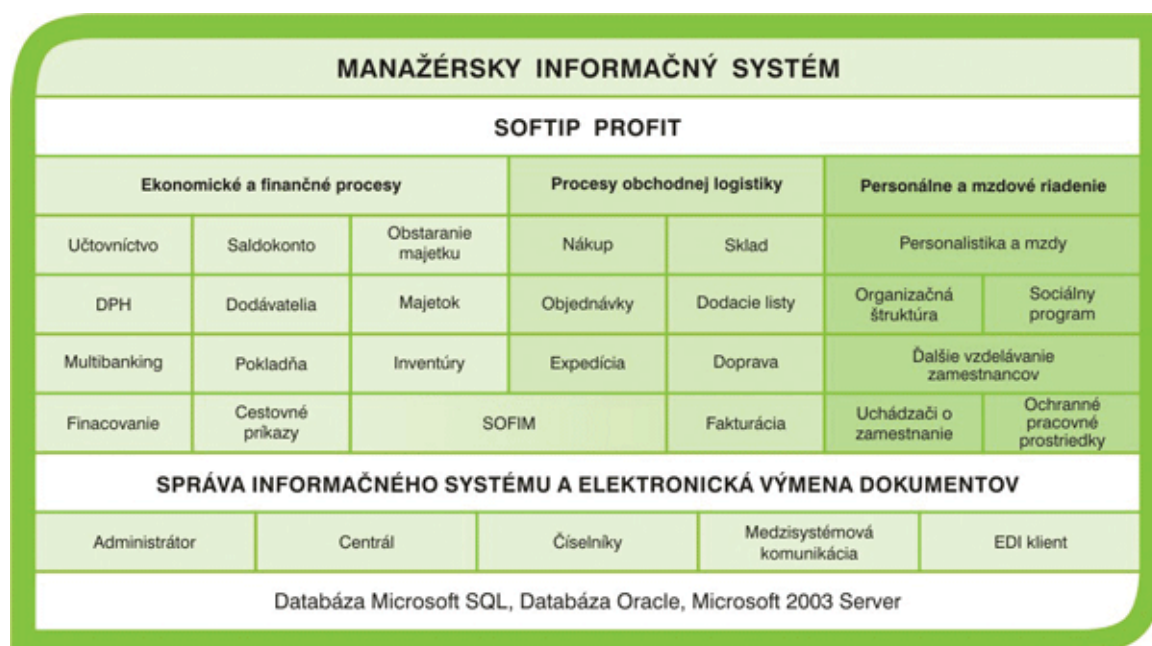
- Je založený na technológii klient/server a pracuje v prostredí MS Windows.
- Pracuje s databázou MS SQL.
- Prepojenie na kancelárske systémy Microsoft Office, údaje z modulov Softip Profit sú exportovateľné do aplikácií Microsoft Word a Microsoft Excel. Programy kancelárskeho systému Microsoft Office 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.
- Spoľahlivosť – využíva transakčné vlastnosti databázového servera s možnosťou zálohovania a obnovy až do posledne potvrdenej transakcie.

4.2.1.2 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, pridelovať 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,
- doplňujúca 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:



4.2.2 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.

4.2.3 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 clustery. Je použitá technológia Microsoft cluster. Nad Microsoft clusterom je nainštalovaný SQL cluster.

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

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

Na servery 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.

4.2.4 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.

4.2.5 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)

4.2.6 Určenie oprávnenej osoby CJES

Spracúvať osobné údaje môže podľa Zákona výlučne 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 pokynu 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 oprávnenej osoby je vykonané prostredníctvom ZO, záznam o poučení (podpísaný Oprávnenou osobou) je uložený v dokumentácii Bezpečnostného projektu, alebo v osobnom spise.

4.2.7 Vytvorenie prístupu do CJES

Pre vytvorenie konta a vygenerovanie prístupových oprávnení je postup nasledovný:

4.2.7.1 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.

4.2.7.2 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.

4.2.7.3 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.

4.3 IS ÚZPF

IS Ústredný zoznam pamiatkového fondu je v automatizovanej aj neautomatizovanej forme spracovávaný v pôsobnosti Odboru štátneho informačného systému a využívaný na vedenie a aktualizáciu nasledovných registrov:

- register hnutelných kultúrnych pamiatok,
- register nehnuteľných kultúrnych pamiatok,
- register pamiatkových rezervácií,
- register pamiatkových zón.

Evidencia pamiatkového fondu sa člení podľa ďalších kritérií napr.:

- územné rozdelenie (kraje, okresy, mesta, obce a katastre),
- druhové členenie (architektúra, zvlášť ľudová architektúra, archeológia, historická zeleň, technické pamiatky, pamiatky historické a výtvarné pamiatky),
- členenie podľa typu (kostoly, meštianske domy, kaštiele, hrady a pod.).

Okrem prehľadov podľa územného, druhového a typového rozdelenia sú v IS ÚZPF vedené nasledovné kategórie klasifikovaných údajov:

- údaje stavebno-technického stavu pamiatok,
- údaje o vlastníctve a vlastníkoch kultúrnych pamiatok,
- údaje o náraste alebo úbytku kultúrnych pamiatok pamiatkového fondu.

Osobné údaje fyzických osôb (dotknutých osôb podľa Zákona) odvodených od vlastníctva hnutelných alebo nehnuteľných kultúrnych pamiatok, ktoré sú podľa Zákona sa spracúva výhradne za účelom zabezpečenia písomného alebo iného kontaktu na vlastníkov pri výkone štátnej správy na úseku ochrany pamiatkového fondu. Osobné vlastníkov sú v IS ÚZPF spracúvané v nasledovnom maximálnom rozsahu:

- meno,
- priezvisko,
- titul,
- adresa.

Pokiaľ Prevádzkovateľ pri výkone štátnej správy na úseku ochrany pamiatkového fondu alebo činnostiach spadajúcich do jeho pôsobnosti zverejňuje osobné údaje vlastníkov kultúrnych pamiatok (napr. v katalógu pamiatok), zverejnenie vykonáva výhradne vo vyššie uvedenom maximálnom rozsahu a po predchádzajúcom písomnom súhlase dotknutej osoby, ktorej osobné údaje budú v súvislosti s vlastníctvom kultúrnej pamiatky zverejnené.

To neplatí, ak osobné údaje vlastníkov, ich vlastníckych vzťahov ku kultúrnym pamiatkam a umiestnenie hnutelných kultúrnych pamiatok je predmetom ochrany utajovaných skutočností podľa osobitného zákona, tak, ako ich v zozname utajovaných skutočností vydalo Ministerstvo kultúry Slovenskej republiky.

4.3.1 Automatizované spracúvanie

Automatizované spracúvanie osobných údajov v IS ÚZPF sa vykonáva s využitím aplikácie Ochrana pamiatkového fondu (ďalej len „AIS OP“, ktorú zhotovila a Prevádzkovateľovi dodala spoločnosť TEMPEST, a.s. Bratislava. Prevádzkovateľom AIS OP je PÚ SR, odborným garantom AIS OP je Odbor štátneho informačného systému, ktorý prostredníctvom zamestnanca zodpovedného za prevádzku, administráciu a správu AIS OP zodpovedá za:

- dodržiavanie licenčných podmienok na základe zmluvy s dodávateľom aplikácie AIS OP,
- navštevovanie požadovaných údajov do databázy programu AIS OP,
- bezpečnosť a ochranu údajov v AIS OP,
- zálohovanie údajov v databáze AIS OP,
- pridelovanie prístupových oprávnení do AIS OP a vedenie ich evidencie (pridelovanie prístupových oprávnení zabezpečuje podľa požiadavky štatutárneho zástupcu PÚ SR),
- spolupracuje so zamestnancom zodpovedným za GIS pri presune dát z AIS OP do GIS,
- inštaláciu software, ktorú oznamuje koordinátorovi správy siete,
- požiadavky na softwarové a hardwarové vybavenie, ktoré predkladá koordinátorovi správy siete,
- správu e-mailovej schránky uzkp@pamiatky.gov.sk.

Ochrana osobných údajov pri ich automatizovanom spracúvaní v IS ÚZPF sa prioritne zabezpečuje riadeným prístupom do miesta spracúvania osobných údajov a klasifikovaných informácií, riadeným diferencovaným prístupom do aplikácie, jej bezpečnostnou správou a striktným oddelením od vonkajšej počítačovej siete.

4.3.2 Neautomatizované spracúvanie

Neautomatizované spracúvanie osobných údajov sa realizuje v rozsahu vymedzenom osobitným zákonom o ochrane pamiatkového fondu t.j. pri príjme, evidencii, triedení, ukladaní, poskytovaní, odosielaní, ukladaní, likvidácii a archivácii písomností súvisiacich s výkonom štátnej správy a štátneho dozoru na úseku ochrany pamiatkového fondu. Uvedené činnosti sa vykonávajú v zmysle zavedeného Registratúrneho poriadku a registratúrneho plánu.

Ochrana osobných údajov pri ich neautomatizovanom spracúvaní v IS ÚZPF sa prioritne zabezpečuje riadeným prístupom do miesta spracúvania osobných údajov, dôsledným dodržiavaním záväzných pravidiel administratívnej bezpečnosti, registratúry a archivácie písomností.

4.4 IS ARCHÍV

Aktuálne úlohy, poslanie a pôsobnosť IS ARCHÍV určuje zákon č.395/2002 Z.z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov a zákona č. 242/2007 Z.z. ktorým sa mení a dopĺňa vyhláška Ministerstva vnútra Slovenskej republiky č. 628/2002 Z.z., ktorou sa vykonávajú niektoré ustanovenia zákona o archívoch a registratúrach a o doplnení niektorých zákonov v znení vyhlášky č. 251/2005 Z.z.

Poslaním archívu je starostlivosť o archívne dokumenty (ich zhromažďovanie, preberanie od pôvodcov, ich bezpečné uschovanie, ochrana a evidencia), ich odborné a vedecké spracovávanie a využívanie, ako aj sprístupňovanie na vedecké a iné účely.

Archív v rámci svojej pôsobnosti plní okrem iných aj tieto úlohy:

- riadi a usmerňuje budovanie archívnych a knižničných fondov na Pamiatkovom úrade a krajských pamiatkových úradoch,
- sprístupňuje archívne a knižničné fondy bádateľom k štúdiu pre vedecké, úradné a súkromné účely,
- dopĺňa a kompletizuje pramennú základňu pre dejiny ochrany pamiatkového fondu na Slovensku,
- vykonáva archívne výskumy,
- buduje centrálnu databanku údajov o archívnych fondoch z iných príbuzných organizácií a inštitúcií s tematikou ochrany pamiatkového fondu na Slovensku,
- spracováva bibliografiu ochrany pamiatkového fondu,
- vykonáva fotodokumentáciu kultúrnych pamiatok a fotolaboratórne práce,
- pravidelne vydáva Informátor archívu.

Medzi odbornú archívnu starostlivosť archívu patria archívne dokumenty písomné, obrazové, zvukové alebo iné záznamy s jedinečnou historickou informačnou hodnotou, ktoré vznikli ako výsledok činnosti:

- právnych predchodcov PÚ SR, Pamiatkového úradu SR v Bratislave a KPÚ
- iných organizácií a subjektov, ktoré spracovávajú dokumentáciu ku pamiatkam a pamiatkovému fondu,
- významných osobností pracujúcich na úseku dejín, teórie, výskumu a projektovania v oblasti pamiatkovej starostlivosti.

IS ARCHÍV vo vedených archívnych fondoch neobsahuje osobné údaje fyzických osôb, tieto vznikajú výhradne pri vedení a ukladaní Bádateľských listov, ako zákonnej podmienky prístupu k archívnym fondom.

Bádateľský list sa vyplňa ručne, okrem účelu prístupu k archívnym dokumentom a ich zoznamu obsahuje nasledovné osobné údaje dotknutej osoby (bádateľa):

- meno,
- priezvisko,
- dátum a miesto narodenia,
- rodné číslo (tento údaj sa v podmienkach PÚ SR ne získava),
- adresa trvalého pobytu,
- telefón, fax, e-mail,
- adresa prechodného pobytu.

Vyššie uvedené údaje sú spracúvané výhradne neautomatizovaným písomným spôsobom.

Ochrana osobných údajov pri ich neautomatizovanom spracúvaní v IS ARCHÍV sa prioritne zabezpečuje riadeným prístupom do miesta spracúvania osobných údajov, dôsledným dodržiavaním záväzných pravidiel administratívnej bezpečnosti, registratúry a archivácie písomností.

4.5 KIS

Knižničný informačný systém je spracovaný na základe zákona č. 183/2000 Z.z. o knižniciach. V uvedenom IS sú osobné údaje spracúvané za účelom evidencie čitateľov a bádateľov 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 IS Knižnica je získanie predchádzajúceho písomného súhlasu dotknutej osoby na spracúvanie jej osobných údajov, ktorý je integrovaný do „Prihlášky za používateľa“ a spĺňa požiadavky Zákona. Podpísaním prihlášky používateľa sa čitateľ ďalej 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 – Prevádzkovateľ sa zaväzuje použiť poskytnuté osobné údaje len pre svoju vnútornú potrebu.

Súhlas dotknutej osoby sa získava formou písomnej prihlášky používateľa, ktorý obsahuje náležitosti požadované Zákomom a aplikuje záväzné stanovisko Úradu na ochranu osobných údajov SR č. 1/2010 z 10. mája 2010 vo veci spracúvania osobných údajov dotknutých osôb – čitateľov resp. používateľov a ich zákonných zástupcov subjektmi tvoriacimi knižničný systém na účely poskytnutia knižnično-informačných služieb.

4.7.1 Rozsah osobných údajov

Na základe záväzného stanoviska č. 1/2010 Úradu na ochranu osobných údajov SR zo dňa 10. mája 2010 vydané podľa § 38 ods. 1 písm. c) zákona č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov:

Pri prihlasovaní maloletej osoby do 15 rokov za čitateľa, resp. používateľa sú knižnice oprávnené získavať a následne spracúvať jej osobné údaje v rozsahu:

- meno,
- priezvisko,
- adresa trvalého pobytu,
- adresa prechodného pobytu,
- dátum narodenia,
- miesto narodenia
- vzdelanie (ZŠ, SŠ).

Zároveň sú oprávnené získavať a následne spracúvať aj osobné údaje zákonného zástupcu maloletej osoby do 15 rokov v rozsahu:

- titul,
- meno,
- priezvisko,
- dátum narodenia,
- miesto narodenia,
- adresa trvalého pobytu,
- adresa prechodného pobytu,
- číslo občianskeho preukazu,
- doba platnosti občianskeho preukazu.

Pri prihlasovaní dotknutej osoby za čitateľa, resp. používateľa, ktorej bol vydaný občiansky preukaz podľa zákona č. 224/2006 Z. z. sú knižnice oprávnené získavať a následne spracúvať osobné údaje dotknutej osoby – čitateľa, resp. používateľa v rozsahu:

- titul,
- meno,

- priezvisko,
- dátum narodenia,
- miesto narodenia,
- adresa trvalého pobytu,
- adresa prechodného pobytu,
- číslo občianskeho preukazu,
- doba platnosti občianskeho preukazu.
- vzdelanie (ZŠ, SŠ, VŠ),
- status osoby (študent, dôchodca, iné).

Získavanie a ďalšie spracúvanie osobných údajov knižnicami nad rámec uvedeného rozsahu osobných údajov na účel poskytnutia knižnično-informačných služieb v automatizovanej, inej ako automatizovanej a čiastočne automatizovanej forme, svojím rozsahom, obsahom a spôsobom spracúvania a využívania nezodpovedá účelu ich spracúvania.

5. Podmienky spracúvania osobných údajov

1. Účel a prostriedky spracúvania osobných údajov stanovuje Organizácia pre tie IS, ktorých je Prevádzkovateľom.
2. Účelom spracúvania osobných údajov je vopred jednoznačne vymedzený zámer spracúvania osobných údajov, ktorý sa viaže na určitú činnosť³.
3. Spôsob spracúvania a využívania osobných údajov Organizáciou musí vždy zodpovedať stanovenému účelu ich spracúvania a musí byť v súlade so zákonmi.
4. 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,⁴
 - 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 údajov⁵ s uvedením povolených činností pri spracúvaní osobných údajov,
 - i.) spôsob získavania osobných údajov,
 - j.) spôsob nakladania s údajmi po splnení účelu ich spracúvania,
 - k.) doba archivácie osobných údajov po splnení 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,⁶
 - o.) tretie krajiny do ktorých je uskutočňovaný cezhraničný prenos osobných údajov a právny základ cezhraničného toku.
5. Vyplnenie a aktualizáciu údajov uvedených v predchádzajúcom bode do formulára podľa prílohy č. 1 tejto Smernice (Formulár evidencie údajov o informačnom systéme) zabezpečuje zodpovedná osoba za Organizáciu, ktorá na základe poverenia štatutárneho zástupcu Organizácie vykonáva dohľad nad ochranou osobných údajov pri ich spracúvaní v Organizácii.
6. Navrhované podmienky spracúvania osobných údajov uvedené v bode č. 4 tohto článku Smernice posúdi pred začatím ich spracúvania poverená zodpovedná osoba z pohľadu zaistenie ich súladu so Zákonom. V odôvodnených alebo komplikovaných prípadoch

³ §4 ods. 1, písm. h) Zákona.

⁴ spracúvanie sa vykonáva na základe predchádzajúceho písomného súhlasu dotknutej osoby alebo je vykonávané na základe osobitného zákona, ktorý stanovuje účel, podmienky, prostriedky subjekty ich spracúvania (v takom prípade je potrebné uviesť odkaz na konkrétne ustanovenie zákona, ktoré spracúvanie osobných údajov ukladá).

⁵ do tejto kategórie spadajú napr. zamestnanci, ktorí k osobným údajom pristupujú v rámci ich pracovného zaradenia a stanovených pracovných povinností.

⁶ 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.

posúdenia súladu podmienok spracúvania osobných údajov so Zákonom spolupracuje poverená zodpovedná osoba za Organizáciu s poverenou zodpovednou osobou za MK SR.

7. V prípade kladného posúdenia podľa predchádzajúceho bodu a zabezpečenia zákonných podmienok pri spracúvaní osobných údajov povolí spracúvanie osobných údajov štatutárny zástupca Organizácie na základe predloženého a schváleného Formulára evidencie informačného systému.
8. Ak v priebehu spracúvania osobných údajov príde k zmene niektorej zo skutočností uvedených v bode 4 tohto článku Smernice, posúdenie uvedené v bode 5. – 7. sa zopakuje.
9. Účel spracúvania osobných údajov v Organizácii musí byť v súlade s jej pôsobnosťou určenou zriaďovacou listinou, organizačným poriadkom alebo štatútom Organizácie. Spracúvanie osobných údajov za iným účelom sa zakazuje.
10. Bez predchádzajúceho schválenia a ďalších obmedzení je možné spracúvať osobné údaje, ktoré boli získané náhodne, bez predchádzajúceho určenia účelu a prostriedkov spracúvania, bez zámeru ich ďalšieho spracúvania v usporiadanom systéme podľa osobitných kritérií a nie sú ďalej systematicky spracúvané.⁷ Organizácia takéto údaje nezverejní ani neposkytne ďalším subjektom.
11. Spracúvanie osobných údajov iným spôsobom, ako stanovuje táto Smernica sa zakazuje.

⁷ §2a písm. b) Zákona.

6. Získavanie osobných údajov

1. Získavanie osobných údajov je vykonávanie akýchkoľvek operácií, ktoré vedú k nadobudnutiu osobných údajov o dotknutej osobe na ich spracúvanie v IS Organizácie.
2. Dotknutá osoba musí byť pred poskytnutím svojich osobných údajov vopred oboznámená s podmienkami ich spracúvania v IS a to v rozsahu stanovenom Zákonom.⁸ Takéto oboznámenie nie je potrebné, ak s ohľadom na všetky okolnosti vie Organizácia na žiadosť Úradu kedykoľvek preukázať, že v čase získavania osobných údajov boli všetky potrebné informácie dotknutej osobe už známe.
3. Pri získaných osobných údajoch musí byť uvedený zdroj od ktorého boli získané, s výnimkou tých údajov, pre ktoré je ich zdroj evidentný aj bez jeho explicitného uvedenia.⁹
4. V prípade, ak Organizácia získa osobné údaje z iného zdroja ako od samotnej dotknutej osoby, musí byť pred ich vložením do IS rozhodnuté o spôsobe oboznámenia dotknutej osoby s podrobnosťami ich spracúvania v súlade so Zákonom.¹⁰
5. Pri získavaní osobných údajov je možné vytvárať kópie úradných dokladov iba ak to osobitný zákon výslovne umožňuje bez súhlasu dotknutej osoby alebo s písomným súhlasom dotknutej osoby. Takýto súhlas si nemožno od dotknutej osoby vynucovať ani jeho získanie ináč podmieňovať.
6. Do IS možno poskytnúť len pravdivé osobné údaje. Za nepravdivosť osobných údajov zodpovedá ten, kto ich do informačného systému poskytol. Organizácia považuje poskytnutý osobný údaj za pravdivý, kým sa nepreukáže opak.
7. Opravu nepravdivých, nesprávnych alebo neaktuálnych osobných údajov oznámi Organizácia do 30 dní od jej vykonania dotknutej osobe a každému, komu ich poskytol. Od oznámenia možno upustiť, ak sa tým neporušia práva dotknutej osoby.
8. Pri získavaní osobných údajov musí byť vždy zachovaná ich diskretnosť.
9. Ustanovenia bodu 2. až 8 tohto článku Smernice sa nepoužijú pri spracúvaní osobných údajov k nasledovným účelom:
 - a.) spracúvanie osobných údajov dotknutej osoby je nevyhnutné na účely tvorby umeleckých alebo literárnych diel, pre potreby informovania verejnosti masovokomunikačnými prostriedkami a ak osobné údaje spracúva prevádzkovateľ, ktorému to vyplýva z predmetu jeho činnosti; to neplatí, ak spracúvaním osobných údajov na takýto účel prevádzkovateľ porušuje právo dotknutej osoby na ochranu jej osobnosti a súkromia alebo takéto spracúvanie bez súhlasu dotknutej osoby vylučuje osobitný zákon alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná¹¹,
 - b.) spracúvanie osobných údajov je nevyhnutné na plnenie zmluvy, v ktorej vystupuje dotknutá osoba ako jedna zo zmluvných strán, na zavedenie predzmluvných vzťahov alebo opatrení vykonávaných na žiadosť dotknutej osoby,¹²
 - c.) pre potreby poštového styku a evidencie údajov v rozsahu titul, meno, priezvisko a adresa dotknutej osoby bez možnosti priradiť k nim ďalšie jej osobné údaje,¹³

⁸ §10, ods. 1 Zákona.

⁹ Môže ísť napríklad o osobné údaje, ktoré sú určenou oprávnenou osobou získavané priamo od dotknutej osoby.

¹⁰ §10, ods. 2 Zákona s prihliadnutím na výnimky uvedené v §10 ods. 3 Zákona.

¹¹ § 7, ods. 4, písm. a) Zákona.

¹² §7, ods. 4, písm. b) Zákona.

¹³ §7, ods. 4, písm. d) Zákona.

- d.) ak predmetom spracúvania sú už zverejnené osobné údaje; v týchto prípadoch je potrebné osobné údaje náležite označiť,
 - e.) na účely identifikácie fyzickej osoby pri jej jednorazovom vstupe do priestorov Organizácie v rozsahu titul, meno, priezvisko a číslo občianskeho preukazu, alebo iného dokladu totožnosti,¹⁴
 - f.) na účely verejného poriadku a bezpečnosti monitorovaním pomocou videozáznamu alebo audiozáznamu priestoru prístupného verejnosti, ktorý je zreteľne označený ako monitorovaný,¹⁵
 - g.) na činnosti uvedené v predchádzajúcom bode nie je potrebný súhlas dotknutej osoby, ak takto získané osobné údaje (vyhotovený záznam) budú Organizáciou využité výhradne k stanovenému účelu, ktorým je trestné konanie alebo konanie o priestupkoch; ak osobitný zákon neustanovuje inak.
10. Pokiaľ získavanie a následné spracúvanie osobných údajov nie je vykonávané podľa osobitných zákonov, ktoré stanovujú účel a podmienky ich spracúvania alebo pri ich získavaní nie je možné uplatniť výnimky stanovené Zákonom¹⁶, musí byť vždy pred ich zaradením do IS získaný predchádzajúci písomný súhlas dotknutej osoby podľa vzoru uvedeného v prílohe č. 8 tejto Smernice.
11. Získavanie osobných údajov dotknutých osôb iným, ako vyššie uvedeným spôsobom sa zakazuje.

¹⁴ §10, ods. 4 Zákona.

¹⁵ §10, ods. 7 Zákona,

¹⁶ § 7 a 9 Zákona.

7. Poskytovanie, sprístupňovanie a zverejňovanie osobných údajov

1. Na účely tejto Smernice sa **poskytovaním**¹⁷ osobných údajov rozumie odovzdávanie osobných údajov na spracúvanie inej právnickej osobe, fyzickej osobe, prípadne subjektu v cudzine s výnimkou dotknutej osoby, vlastného prevádzkovateľa, sprostredkovateľa alebo oprávnenej osoby.
2. **Sprístupňovaním**¹⁸ osobných údajov sa rozumie oznámenie osobných údajov alebo umožnenie prístupu k nim inej právnickej osobe, fyzickej osobe, prípadne subjektu v cudzine s výnimkou dotknutej osoby, vlastného prevádzkovateľa, sprostredkovateľa alebo oprávnenej osoby.
3. **Zverejňovaním**¹⁹ osobných údajov sa rozumie publikovanie, uverejnenie alebo vystavenie osobných údajov na verejnosti prostredníctvom masovokomunikačných prostriedkov, verejne prístupných počítačových sietí, verejným vykonaním alebo vystavením diela, verejným vyhlásením, uvedením vo verejnom zozname, v registri alebo operáte, ich umiestnením na úradnej tabuli alebo na inom verejne prístupnom mieste.
4. Organizácia umožní sprístupnenie, poskytnutie alebo zverejnenie osobných údajov iba za podmienok a v rozsahu stanovenom Zákonom alebo osobitnými zákonmi, ktoré stanovujú účel, podmienky, prostriedky a subjekty spracúvania osobných údajov.
5. Zákonnosť sprístupnenia, poskytnutia alebo zverejnenia osobných údajov musí byť preskúmaná ešte v čase pred ich vykonaním.
6. Ten, kto sprístupnenie alebo poskytnutie osobných údajov od Organizácie požaduje, je povinný vopred doložiť odkazom na konkrétne ustanovenia Zákona 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 Organizáciu.²⁰
7. Pri každom zverejnení osobných údajov Organizácia spolu s údajmi uvedie odkaz na konkrétne ustanovenie zákona, ktoré toto zverejnenie umožňuje alebo ukladá, vrátane účelu, spôsobu, doby, miesta, obsahu a rozsahu zverejnenia osobných údajov.
8. 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 Organizáciou a treťou stranou (napr. subdodávateľ, technický alebo upratovací servis, havarijné zásahy a pod.).
9. Oprávnenie prístupu do miesta spracúvania osobných údajov pre zamestnancov tretích strán, ktoré neboli určené ako oprávnené osoby podľa predchádzajúceho bodu posúdi zodpovedná osoba za Organizáciu, ktorá taktiež vykoná ich poučenie o zásadách ochrany osobných údajov.²¹
10. V prípade, ak dôvodom prístupu do miesta spracúvania osobných údajov je aj sprístupnenie osobných údajov podľa bodu 8 tohto článku Smernice, musí tretia strana (subdodávateľ) spĺňať rovnaké požiadavky ako sprostredkovateľ, určené v článku 8, bod 2 – 5 tejto Smernice. V zmluve uzatvorenej medzi Organizáciou a treťou stranou musí byť tretej strane

¹⁷ § 4, ods. 1, písm. b) Zákona.

¹⁸ § 4, ods. 1, písm. c) Zákona.

¹⁹ § 4, ods. 1, písm. d) Zákona.

²⁰ bližšie viď. článok 9 tejto Smernice.

²¹ viď príloha č. 7 tejto Smernice

stanovená povinnosť poučiť svojich zamestnancov, ktorí budú prichádzať do styku s osobnými údajmi spracúvanými v súlade s §17 Zákona a článkom 10 tejto Smernice.

8. Nakladanie s osobnými údajmi po splnení účelu spracúvania

1. Po splnení účelu spracúvania sú osobné údaje archivované a neskôr vyradované podľa platných predpisov Organizácie.²²
2. 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 Zákonom.
3. Likvidáciu osobných údajov oznámi Organizácia do 30 dní od jej vykonania dotknutej osobe a každému, komu ich poskytol. Od oznámenia možno upustiť, ak sa tým neporušia práva dotknutej osoby.

²² Registratúrny poriadok a Registratúrny plán Organizácie.

9. Prístup k osobným údajom

1. Prístup zamestnancov Organizácie 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 Organizácie takéto spracúvanie zabezpečuje.
4. Prístup k osobným údajom majú iba určení zamestnanci organizačných zložiek Organizácie, ktoré spracúvanie osobných údajov za daným účelom zabezpečujú.
5. Podmienkou určenia oprávnenej 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 Organizácie schvaľuje štatutárny zástupca Organizácie 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 Organizácie. Poverená zodpovedná osoba za Organizáciu vedie agendu žiadostí o prístup k osobným údajom, zoznam oprávnených osôb s prístupom k osobným údajom a na základe predložených požiadaviek vykonáva jeho aktualizáciu podľa vzoru uvedeného v prílohe č. 4 tejto Smernice.
7. Interné zložky Organizácie vykonávajú spracúvanie osobných údajov v zmysle, rozsahu a za podmienok stanovených zákonmi, zriaďovacou listinou, organizačným poriadkom alebo štatútom Organizácie.
8. Prístup k spracúvaným osobným údajom nad vymedzený rámec sa zakazuje.

10. Sprostredkovateľ

1. Sprostredkovateľom²³ je orgán verejnej moci, fyzická alebo právnická osoba ktorá spracúva osobné údaje v mene Organizácie, ako Prevádzkovateľa IS.
2. Sprostredkovateľ je povinný spracúvať osobné údaje len v rozsahu a za podmienok dojednaných s Organizáciou v písomnej zmluve alebo v písomnom poverení.²⁴
3. Zmluva alebo poverenie musia byť uzavreté pred začiatkom spracúvania osobných údajov Sprostredkovateľom a musí obsahovať najmä:
 - a.) identifikačné údaje Prevádzkovateľa (Organizácie) a sprostredkovateľa²⁵,
 - b.) účel spracúvania osobných údajov,
 - c.) zoznam alebo rozsah spracúvaných osobných údajov,
 - d.) okruh dotknutých osôb,
 - e.) povolené operácie s osobnými údajmi,
 - f.) zákaz vykonávania iných ako povolených činností s osobnými údajmi,
 - g.) zákaz ďalšieho sprístupňovania, poskytovania a zverejňovania osobných údajov bez predchádzajúceho písomného súhlasu Organizácie,
 - h.) záväzok mlčanlivosti o sprístupnených alebo poskytnutých osobných údajoch, ktorý ostáva v platnosti aj po skončení spracúvania osobných údajov alebo po ukončení zmluvného vzťahu s Organizáciou²⁶. Mlčanlivosť je záväzná aj pre všetkých zamestnancov sprostredkovateľa, ktorí boli určení na oboznamovanie sa s osobnými údajmi v IS Organizácie,
 - i.) poučenie o právach a povinnostiach ustanovených Sprostredkovateľovi Zákonom a o zodpovednosti za ich porušenie,
 - j.) dobu platnosti zmluvného vzťahu, povinnosť likvidácie spracúvaných osobných údajov alebo ich vrátenia Organizácii po jeho skončení.
4. Sprostredkovateľ musí poskytovať záruky bezpečnosti pri spracúvaní osobných údajov, najmä v oblasti technickej, organizačnej a personálnej bezpečnosti. Organizácia pred uzavretím zmluvy alebo poverenia so sprostredkovateľom primeraným spôsobom zhodnotí dostatočnosť a mieru naplnenia týchto záruk, za týmto účelom môže požadovať od sprostredkovateľa súčinnosť.
5. Sprostredkovateľ musí spĺňať ďalšie legislatívne požiadavky kladené na spracúvanie osobných údajov, vyplývajúce najmä zo Zákona.

²³ §4, ods. 3 a § 5, ods. 2 až 4 Zákona.

²⁴ vzor písomnej zmluvy o spracúvaní osobných údajov sprostredkovateľom v mene prevádzkovateľa je uvedený v prílohe č. 13 tejto Smernice.

²⁵ v minimálnom rozsahu meno, priezvisko, dátum narodenia a adresu trvalého pobytu - ak ide o fyzickú osobu obchodné meno, identifikačné číslo a sídlo alebo miesto podnikania - ak ide o právnickú osobu alebo fyzickú osobu – podnikateľa.

²⁶ §18, ods. 1 Zákona.

11. Dohľad nad ochranou osobných údajov

1. Organizácia zabezpečuje výkon dohľadu nad ochranou osobných údajov v rozsahu a za podmienok určených Zákonom.²⁷
2. Písomné poverenie zodpovednej osoby alebo viacerých zodpovedných osôb vykonáva štatutárny zástupca Organizácie, pritom postupuje podľa Zákona²⁸ (napr. zodpovedná osoba za Organizáciu, zodpovedná osoba za internú organizačnú zložku Organizácie, zodpovedná osoba za prevádzkovaný IS, zodpovedná osoba za prevádzku informačno-komunikačných technológií, zodpovedná osoba za procedúru alebo operáciu pri spracúvaní osobných údajov a pod., podľa podmienok, obsahu a rozsahu spracúvaných osobných údajov u Organizácie).
3. Vzor písomného poverenia zodpovednej osoby je uvedený v prílohe č.3 tejto Smernice. Zakladá sa do osobného spisu zamestnanca, jeho kópia sa zakladá do dokumentácie Bezpečnostného projektu na ochranu osobných údajov Organizácie.
4. Organizácia písomne informuje Úrad o poverení jednej zodpovednej osoby za Organizáciu, formou a spôsobom požadovanými Zákonom²⁹, a to do 30 dní odo dňa jej poverenia alebo po zmene zodpovednej osoby, ktorá bola skôr nahlásená Úradu. Vzor oznámenia prevádzkovateľa o poverení osoby zodpovednej za dohľad nad ochranou osobných údajov je uvedený v prílohe č. 2 tejto Smernice.
5. Každá zodpovedná osoba poverená výkonom dohľadu nad ochranou osobných údajov musí byť bezúhonná³⁰, musí mať spôsobilosť na právne úkony v plnom rozsahu a musí byť odborne vyškolená v rozsahu stanovenom Zákonom.³¹ V prípade, že zamestnanec navrhnutý do pozície zodpovednej osoby takéto školenie neabsolvoval, zabezpečí jeho vyškolenie Organizácia. Doklad o absolvovanom školení, alebo jeho kópia je súčasťou osobného spisu zamestnanca, kópia osvedčenia o vyškolení zodpovednej osoby sa taktiež zakladá do Bezpečnostného projektu na ochranu osobných údajov Organizácie.
6. Zodpovedná osoba poverená za Organizáciu v rámci dohľadu nad ochranou osobných údajov vykonáva najmä nasledovné činnosti:
 - a.) vedie a aktualizuje prehľad o platnej legislatíve v oblasti ochrany osobných údajov Organizácie,³²
 - b.) realizuje technické, organizačné a personálne opatrenia a dohliada na ich aplikáciu v podmienkach Organizácie,
 - c.) navrhuje a zabezpečuje aktualizáciu dokumentácie Bezpečnostného projektu na ochranu osobných údajov Organizácie v prípade vzniku legislatívnych zmien alebo v súvislosti s plánovanou obsahovou zmenou pri spracúvaní osobných údajov,³³ ktorými sú technické, organizačné a personálne podmienky spracúvania osobných údajov,

²⁷ §19 Zákona.

²⁸ § 19, ods. 2 Zákona

²⁹ §19, ods. 5 a 6 Zákona.

³⁰ §35 ods. 4 Zákona. „Za bezúhonného občana sa na účely Zákona považuje občan, ktorý nebol právoplatne odsúdený za úmyselný trestný čin alebo za trestný čin, za ktorý mu bol uložený nepodmienečný trest odňatia slobody. Bezúhonnosť sa preukazuje výpisom z registra trestov, ktorý nie je starší ako tri mesiace v čase poverenia“.

³¹ §19, ods. 3 a 12 Zákona.

³² §19, ods. 4 Zákona.

³³ §19, ods. 7, písm. f) Zákona.

- d.) zabezpečuje dohľad pri výbere Sprostredkovateľa, prípravu písomnej zmluvy alebo písomného poverenia Sprostredkovateľa a zodpovedá za jeho obsah. Počas trvania zmluvného vzťahu alebo poverenia preveruje dodržiavanie dohodnutých podmienok,³⁴
 - e.) ak sa uskutočňuje cezhraničný tok osobných údajov, vykonáva dohľad nad jeho realizáciou,³⁵
 - f.) zabezpečuje prihlásenie IS na osobitnú registráciu, oznamovanie zmien a odhlásenie IS z osobitnej registrácie. O IS, ktoré registrácii nepodliehajú vedie evidenciu v rozsahu a za podmienok stanovených Zákonom.³⁶
 - g.) vyjadruje sa k navrhovaným zmenám, pracovným postupom a procedúram týkajúcim sa spracúvania osobných údajov v podmienkach Organizácie,
 - h.) metodicky usmerňuje ďalšie zodpovedné osoby za organizačné zložky Organizácie (ak boli poverené) v otázkach výkonu dohľadu nad ochranou osobných údajov,
 - i.) pred vydaním prvého pokynu na realizáciu spracovateľských operácií vykonáva poučenie oprávnených osôb s prístupom k osobným údajom o čom vedie písomný záznam,³⁷ ktorý sa v jednom výtlačku ukladá v osobnom spise zamestnanca a v jednom výtlačku v dokumentácii Bezpečnostného projektu na ochranu osobných údajov Organizácie, podľa vzoru uvedeného v prílohe č. 6 tejto Smernice.
 - j.) eviduje sťažnosti a žiadosti dotknutých osôb, incidenty a problémy súvisiace so spracúvaním osobných údajov Organizáciou,³⁸
 - k.) o zistených skutočnostiach pri výkone dohľadu nad ochranou osobných údajov, o stave spracúvania osobných údajov Organizáciou a prípadných návrhoch písomne informuje štatutárneho zástupcu Organizácie, minimálne 1 krát za kalendárny rok. Bezodkladne informuje štatutárneho zástupcu Organizácie o zistení porušenia Zákona pri spracúvaní osobných údajov. K predmetným činnostiam poverená zodpovedná osoba využíva prílohy č. 11 a 12 tejto Smernice.
 - l.) pred začatím nového spracúvania osobných údajov alebo pri zmene spôsobu ich spracúvania posúdi, či ich spracúvaním nevzniká nebezpečenstvo narušenia práv a slobôd dotknutých osôb,³⁹
 - m.) zabezpečuje výkon práv dotknutých osôb podľa článku 12 tejto Smernice,
 - n.) vedie a sprístupňuje evidenciu o IS, v ktorých Organizácia vykonáva spracúvanie osobných údajov podľa článku 14 tejto Smernice.
7. Zodpovedná osoba za internú organizačnú zložku Organizácie (ak bola poverená) vykonáva v rámci dohľadu nad ochranou osobných údajov najmä nasledovné činnosti:
- a) vedie a aktualizuje prehľad o platnej legislatíve v oblasti ochrany osobných údajov za organizačnú zložku a interných predpisoch Organizácie, ktorými sa v podmienkach organizačnej zložky realizuje alebo zabezpečuje spracúvanie osobných údajov,
 - b) vypracúva podklady evidencie IS, ktoré postupuje poverenej zodpovednej osobe za Organizáciu,
 - c) v rámci organizačnej zložky kontroluje dodržiavanie zákonov vo vzťahu k ochrane osobných údajov a kontroluje dodržiavanie interných predpisov a tejto Smernice zo

³⁴ § 19, ods. 7, písm. g) Zákona.

³⁵ § 19, ods. 7, písm. h) Zákona.

³⁶ § 19, ods. 7, písm. i) Zákona.

³⁷ § 19, ods. 7, písm. d) Zákona.

³⁸ § 19, ods. 7, písm. e) Zákona.

³⁹ § 19, ods. 4 Zákona.

strany oprávnených osôb. V prípade potreby zabezpečuje metodickú pomoc pri spracúvaní osobných údajov,

- d) poverenej zodpovednej osobe za Organizáciu postupuje zistené sťažnosti, incidenty a problémy pri spracúvaní osobných údajov v rámci organizačnej zložky,
- e) o zistených skutočnostiach pri výkone dohľadu nad ochranou osobných údajov v podmienkach organizačnej zložky a prípadných návrhoch písomne informuje poverenú zodpovednú osobu za Organizáciu, minimálne 1 krát za kalendárny rok. Bezodkladne ju informuje o zistení porušenia Zákona pri spracúvaní osobných údajov. K predmetným činnostiam poverená zodpovedná osoba využíva prílohy č. 11 a 12 tejto Smernice.

12. Určenie a povinnosti oprávnenej osoby

1. V zmysle Zákona a na účely tejto Smernice je oprávnenou osobou fyzická osoba, ktorá v rámci svojho pracovného zaradenia u Organizácie prichádza alebo môže prichádzať do styku s osobnými údajmi a na predmetné činnosti bola náležite určená.⁴⁰
2. Písomný zoznam určených oprávnených osôb s prístupom k osobným údajom vedie a aktualizuje poverená zodpovedná osoba za Organizáciu na základe požiadaviek predkladaných vedúcimi interných organizačných zložiek Organizácie. Zoznam je uložený v dokumentácii Bezpečnostného projektu na ochranu osobných údajov Organizácie a vyhotovuje sa podľa vzoru vedeného v prílohe č. 5 tejto Smernice.
3. Písomný zoznam určených oprávnených osôb s prístupom k osobným údajom je platný po jeho chválení štatutárnym zástupcom Organizácie.
4. Každá oprávnená osoba musí byť pred vydaním prvého pokynu na spracúvanie osobných údajov podľa §17 Zákona poučená o zákonných podmienkach ochrany osobných údajov, spôsobe ich aplikácie u Organizácie a zodpovednosti za ich porušenie.
5. Fyzická osoba navrhovaná na oboznamovanie sa s osobnými údajmi v rámci jej pracovného zaradenia u Organizácie absolvuje poučenie oprávnenej osoby prijímanej do Pracovného pomeru spravidla ku dňu vzniku Pracovného pomeru.⁴¹
6. Poučenie oprávnenej osoby vykonáva poverená zodpovedná osoba za Organizáciu alebo poverená zodpovedná osoba za internú organizačnú zložku Organizácie.
7. Absolvovanie poučenia potvrdí oprávnená osoba vlastnoručným podpisom. Evidenciu písomného poučenia oprávnenej osoby zabezpečuje zodpovedná osoba, ktorá poučenie vykonala. Poučenie sa vyhotovuje v dvoch výtlačkoch, z ktorých jeden sa zakladá do osobného spisu s jeden sa prikladá k dokumentácii Bezpečnostného projektu na ochranu osobných údajov Organizácie, ktorú vedie a aktualizuje poverená zodpovedná osoba za Organizáciu.
8. Každá oprávnená osoba a pracovník tretej strany (subdodávateľ) ktorému budú prístupné osobné údaje spracúvané Organizáciou 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.
9. Oprávnená osoba musí byť informovaná o zodpovednej osobe poverenej dohľadom nad ochranou osobných údajov u Organizácie prípadne v príslušnej organizačnej zložke Organizácie.
10. Oprávnená osoba a pracovník tretej strany (subdodávateľ) musí pri práci s osobnými údajmi dodržiavať:
 - a) zákony Slovenskej Republiky, najmä zákony upravujúce činnosti v pôsobnosti Organizácie,
 - b) povinnosť mlčanlivosti o osobných údajoch, a to aj po ukončení Pracovného pomeru alebo zmluvného vzťahu s Organizáciou.

⁴⁰ vzor určenia oprávnených osôb s prístupom k osobným údajom vid' príloha č. 5 tejto Smernice.

⁴¹ vzor poučenia oprávnenej osoby vid' príloha č. 6 tejto Smernice.

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

13. Bezpečnosť osobných údajov pri ich spracúvaní

1. Organizácia zodpovedá za bezpečnosť spracúvaných osobných údajov tým, že ich chráni pred náhodným ako aj nezákonným poškodením a zničením, náhodnou stratou, zmenou, nedovoleným prístupom a sprístupnením ako aj pred akýmikoľvek inými neprípustnými formami spracúvania⁴².
2. Organizácia 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 Organizácie 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 Organizácie a ich vzájomnou kombináciou,⁴³
 - c) vynášanie písomností obsahujúcich osobné údaje mimo priestorov Organizácie podlieha schváleniu vedúceho príslušného organizačnej zložky Organizácie, prípadne stanovisku poverenej zodpovednej osoby za Organizáciu,
 - d) pri prenose písomností v rámci priestorov Organizácie ako aj pri schválenom prenose písomností mimo priestorov Organizácie 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 oprávnenej 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.

⁴² §15 ods. 1 Zákona.

⁴³ 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 protipožiarné 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.

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,
 - 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 Organizácie je považované za zverejnenie osobných údajov.
5. Každý zamestnanec Organizácie 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 Organizáciu.
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 Organizáciu. 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.

14. Práva dotknutých osôb

1. Dotknuté osoby môžu v styku s Organizáciou vyžadovať realizáciu nasledovných práv:
 - a) vyžadovať informácie o stave spracúvania svojich osobných údajov Organizáciou⁴⁴,
 - b) vyžadovať presné informácie o zdroji, z ktorého boli jej osobné údaje získané,
 - c) vyžadovať odpis údajov, ktoré sú o nej Organizáciou spracúvané,
 - d) opravu nesprávnych, neúplných alebo neaktuálnych údajov,
 - e) požadovať vrátenie úradných dokladov obsahujúcich osobné údaje po splnení účelu ich spracúvania,
 - f) likvidáciu jej osobných údajov, ktoré sú predmetom spracúvania, ak došlo k porušeniu Zákona.
2. Právo dotknutej osoby možno obmedziť len podľa bodu 1 písm. d) a e), ak takéto obmedzenie vyplýva z osobitného zákona alebo jeho uplatnením by bola porušená ochrana dotknutej osoby alebo by boli porušené práva a slobody iných osôb.
3. Požiadavky dotknutej osoby na výkon uvedených práv sú realizované bezplatne.
4. Žiadosti dotknutých osôb na realizáciu práv sú podávané písomne. Každá žiadosť musí obsahovať identifikáciu dotknutej osoby (meno a priezvisko), označenie práva ktorého naplnenie je žiadané, poštovú adresu kam bude zaslaná odpoveď a označenie IS, ktorého sa žiadosť týka.
5. Vybavenie žiadostí zabezpečuje zodpovedná osoba poverená za Organizáciu v lehote do 30 dní odo dňa ich prijatia v zmysle §21 Zákona. Dotknutá osoba je písomne informovaná o spôsobe vybavenia svojej žiadosti.
6. Žiadosti na realizáciu práv podľa tohto článku môže podávať dotknutá osoba iba vo svojom mene. Ak dotknutá osoba nemá spôsobilosť na právne úkony v plnom rozsahu, jej práva môže uplatniť zákonný zástupca. Ak dotknutá osoba nežije, jej práva, ktoré mala podľa Zákona môže uplatniť blízka osoba.
7. Organizácia nevydá žiadne rozhodnutie, ktoré by malo pre dotknutú osobu právne účinky alebo významný dosah výlučne na základe úkonov automatizovaného spracúvania jej osobných údajov.
8. Ustanoveniami tejto Smernice nie sú obmedzené ostatné zákonné práva dotknutej osoby podľa §20 Zákona.

⁴⁴ §26, ods. 3 Zákona.

15. Cezhraničný prenos osobných údajov

1. Pre každý účel spracúvania osobných údajov Organizáciou musí byť formálne rozhodnuté, či je vykonávaný ich cezhraničný prenos.
2. Organizácia môže vykonávať prenos osobných údajov iba do krajín, ktoré zabezpečujú primeranú úroveň ochrany osobných údajov.
3. Organizácia nepochybne spracúvaním osobných údajov subjekt v cudzine.
4. Ochrana osobných údajov spracúvaných Organizáciou, prenesených na územie Slovenskej republiky od subjektov so sídlom alebo s trvalým pobytom v cudzine, sa vykonáva v súlade so Zákonom a touto Smernicou.
5. Organizácia zaručí bezpečnosť osobných údajov, ktoré odovzdáva na cezhraničné spracúvania aj pri ich tranzite.

16. Evidencia a registrácia IS

1. Spracúvanie osobných údajov Organizáciou nepodlieha povinnosti registrácie podľa Zákona o ochrane osobných údajov na základe ustanovenia §25 ods. 2, písm. b) Zákona.
2. O všetkých IS, v ktorých sú spracúvané osobné údaje, vedie Organizácia evidenciu podľa ustanovení §29-§30 Zákona a to najneskôr odo dňa začatia spracúvania údajov v týchto IS.
3. Výnimkou z ustanovenia predchádzajúceho bodu sú IS, v ktorých spracúvané osobné údaje, ktoré slúžia výlučne pre potreby poštového styku s dotknutými osobami a evidencie týchto údajov⁴⁵ alebo obsahujú osobné údaje, ktoré sa spracúvajú výlučne na účely identifikácie osôb pri ich jednorazovom vstupe do priestorov prevádzkovateľa.⁴⁶
4. Evidenciu IS vypracúva⁴⁷ a za jej aktualizáciu zodpovedá zodpovedná osoba poverená za Organizáciu na základe podkladov, ktoré vypracovala a predložila poverená zodpovedná osoba za organizačnú zložku Organizácie (ak bola poverená), do kompetencie ktorej patrí dané spracúvanie osobných údajov.
5. Aktuálna evidencia všetkých IS je uložená u zodpovednej osoby poverenej za Organizáciu.
6. Podľa §32 Zákona je evidencia verejná. Údaje z evidencie Organizácia sprístupní bezplatne komukoľvek, kto o to požiada prostredníctvom organizačných zložiek Organizácie určených na styk a poskytovanie údajov verejnosti v zmysle zákona NR SR č.211/2000 Z.z. v znení neskorších predpisov v spolupráci so zodpovednou osobou poverenou za Organizáciu.

⁴⁵ §7 ods. 4 písm. d) Zákona.

⁴⁶ §10 ods. 4 Zákona.

⁴⁷ Podľa vzoru uvedeného v prílohe č.1 tejto Smernice.

17. Bezpečnosť osobných údajov pri ich spracúvaní

1. Organizácia zodpovedá za bezpečnosť spracúvaných osobných údajov tým, že ich chráni pred náhodným ako aj nezákonným poškodením a zničením, náhodnou stratou, zmenou, nedovoleným prístupom a sprístupnením ako aj pred akýmikoľvek inými neprípustnými formami spracúvania 48.
2. Organizácia 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:
 - h) vytváranie, evidencia, ukladanie, obeh, prenos, archivácia, likvidácia prípadne ďalšie činnosti s písomnosťami prebiehajú podľa platného Registratúrneho poriadku a Registratúrneho plánu Organizácie a schválených zásad tvorby a obehu písomností,
 - i) 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 Organizácie a ich vzájomnou kombináciou, 49
 - j) vynášanie písomností obsahujúcich osobné údaje mimo priestorov Organizácie podlieha schváleniu vedúceho príslušného organizačnej zložky Organizácie, prípadne stanovisku poverenej zodpovednej osoby za Organizáciu,
 - k) pri prenose písomností v rámci priestorov Organizácie ako aj pri schválenom prenose písomností mimo priestorov Organizácie je potrebné dbať na primeranú ochranu dôvernosti prenášaných písomností (uzavreté a nepriehľadné transportné obaly),
 - l) prístup k písomnostiam obsahujúcim osobné údaje majú iba na to určení zamestnanci v postavení oprávnenej osoby,
 - m) v prítomnosti neoprávnených osôb sa práca s písomnosťami obsahujúcimi osobné údaje zakazuje,
 - n) vyhotovené písomnosti obsahujúce osobné údaje sú po ich vyradení z evidencií likvidované skartáciou, znemožňujúcou spätnú rekonštrukciu písomností.

⁴⁸ §15 ods. 1 Zákona.

⁴⁹ 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 protipožiarné 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.

4. Základné zásady bezpečnosti pri spracúvaní osobných údajov v elektronickej forme sú nasledovné:
 - j) každý počítač musí byť vybavený aplikáciou na antivírusovú kontrolu, táto aplikácia musí byť pravidelne aktualizovaná,
 - k) pri prístupe k počítaču je vždy vyžadovaná identifikácia a autentifikácia používateľa,
 - l) fyzický prístup k počítaču a jeho vstupno-výstupným zariadeniam má iba určený zamestnanec, výpočtové zariadenia musia byť umiestnené v zamykaných priestoroch,
 - m) používateľské a prístupové heslá musia byť zvolené tak, aby boli ťažko uhádnuteľné, musia byť pravidelne obmieňané a držané v tajnosti,
 - n) prenosné médiá, ktoré obsahujú osobné údaje musia byť chránené pred stratou, poškodením a neoprávneným prístupom,
 - o) v aplikáciách je používané riadenie prístupu, rozsah povoleného prístupu k osobným údajom je iba v miere nevyhnutnej na výkon pracovných činností používateľa,
 - p) spracúvané osobné údaje musia byť pravidelne zálohované, zálohovanie je zabezpečované centrálnou správou alebo lokálnym zálohovaním, podľa podmienok, obsahu a rozsahu spracúvaných osobných údajov,
 - q) používateľ dodržiava stanovené pravidlá práce s počítačom, aplikáciou a počítačovou sieťou,
 - r) voľné vystavenie osobných údajov na WWW stránkach Organizácie je považované za zverejnenie osobných údajov.
5. Každý zamestnanec Organizácie 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 Organizáciu.
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 Organizáciu. 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.

18. Technická bezpečnosť IS

18.1 Technická bezpečnosť neautomatizovaných IS

Technická bezpečnosť neautomatizovaných IS (ďalej len „NIS“) je tvorená systémom manažérsko-technických a logistických opatrení zabezpečujúcich elimináciu a minimalizáciu hrozieb a rizík pôsobiacich na NIS pri spracúvaní osobných údajov.

Technická bezpečnosť NIS 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.

18.1.1 Pravidlá používania NIS

Pri ničení vyradených písomností a ich konceptov musia byť správne používané inštalované zariadenia na ich skartáciu, ktoré dostatočným spôsobom musia zamedziť rekonštrukcii skartovaných písomností.

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 použité 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. 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.

18.2 Technická bezpečnosť automatizovaných IS

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

18.2.1 Úlohy, funkcie a zodpovednosti osôb v informačných systémoch

Používatelia	Takmer každý zamestnanec PÚ SR 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 Odborom informatiky pri tvorbe bezpečnostných postupov a pravidiel.
Správcovia systémov	Zodpovedajú za každodennú, rutinnú implementáciu bezpečnostných pravidiel a štandardov. Spoločne s vedúcimi zamestnancami aktívne navrhujú najúčinnějšíe bezpečnostné riešenia a striktne dodržia 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.
Vrcholový manažment	Rozhoduje o potrebe a obsahu informačných systémov, opráva organizačné štruktúry a jednotlivcov k prístupu do informačných systémov. Rozhoduje o investíciách do bezpečnosti a posudzuje strategické bezpečnostné zámery.

18.2.2 Organizácia a zodpovednosť za informačnú bezpečnosť

V pôsobnosti Prevádzkovateľa je informačná bezpečnosť riadená prostredníctvom generálnej riaditeľky, ktorá určuje primárnu Bezpečnostnú politiku v rámci informačných technológií a stanovuje bezpečnostného manažéra.

Základné informačné pravidlá a zodpovednosť za informačnú bezpečnosť stanovuje „Prevádzkový poriadok počítačovej siete“.

Za implementáciu a riadenie informačných pravidiel zodpovedá správca, ktorý musí v zmysle celkovej bezpečnostnej politiky plniť a určovať funkciu bezpečnostného manažéra, 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 pracovnoprávneho 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.

18.2.3 Funkcie v informačnom systéme

18.2.3.1 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 dodržovanie 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.

Bezpečnostným manažérom je:

RNDr. Škoviera Luboslav

18.2.3.2 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 stanicach
- udržiavanie predpísaného programového vybavenia jednotlivých staníc
- pridávanie (registráciu) sieťových objektov v doméne

Správcom počítačovej siete KPÚ a ORA Levoča je:

JÁŠEK Rudolf

Správcom počítačovej siete uzla je:

Ing. Robert Urban

**V prípade potreby realizuje správu na základe objednávky spoločnosť
TEMPEST a.s.**

18.2.4 Správa infraštruktúry IT

Za správu infraštruktúry IT zodpovedajú určení administrátori, v tomto prípade sa jedná o externých administrátorov.

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.

18.2.5 Správa užívateľov

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

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

Administrátor je povinný uvedené písomné požiadavky evidovať.

18.2.6 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.

18.2.6.1 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 vrcholovému manažérovi.

Všetky heslá sú definované ako citlivé a dôverné informácie.

Zoznam zakázaných činností::

- Neposkytni nikomu heslo cez telefón
- Neposkytni heslo prostredníctvom email-ovej správy
- Neposkytni heslo vedúcemu
- Nehovor o hesle pred niekým iným
- Neposkytuj 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 pocked PC alebo podobných zariadeniach) bez zakódovania, alebo šifrovania.

Ak máte podozrenie, že váš účet, alebo heslo bolo kompromitované oznámte tento incident IT skupine a zmeňte všetky prístupové heslá.

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

Uvedené pravidlá nie sú však centrálné manažované a preto nie sú bezvýhradne dodržiavané.

18.2.6.2 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. Heslo si oprávnený používateľ stanovuje sám, ale systémovým opatrením je donútený používať heslá s požadovanou bezpečnosťou, ktorá je nastavená prostredníctvom Active directory nasledovne:

Všetky heslá užívateľskej úrovne (email, web, desktop, atď. – zavedené v Active directory – Domain controller) musia 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.

18.2.6.3 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.

18.2.6.4 Identifikácia a autentizácia na úrovni aplikácie

Po identifikácii a autentizácii užívateľov do siete je užívateľ povinný sa identifikovať a autentizovať aj do nosných aplikácií Prevádzkovateľa (SOFTIP PROFIT, AIS OP, GIS a WINASU), alebo je vyžadované prihlásenie sa do siete Prevádzkovateľa s už popísanými bezpečnostnými nastaveniami.

18.2.7 Riadenie prístupu

U Prevádzkovateľa je realizované riadenie prístupu k jednotlivým objektom v súlade s bezpečnostnými štandardmi 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.

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

18.2.8 Audit a účtovateľnosť

Zabezpečené štandardnými prostriedkami OS, resp. aplikačného programového vybavenia.

18.2.8.1 Účtovateľnosť a audit na úrovni pracovnej stanice

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

18.2.8.2 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.

18.2.8.3 Účtovateľnosť a audit na úrovni serverov

Účtovateľnosť a audit na úrovni serverov je riešený štandardnými prostriedkami použitého operačného systému, či už Windows, alebo LINUX. 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.

18.2.9 Opakované použitie

Je zabezpečené opakované použitie zdrojov, ako sú operačná pamäť, oblasti diskovej pamäti, monitory 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 sporič obrazovky a autentizované zamykanie klávesnice heslom.

Pre implementáciu sporiča obrazovky a autentizovaného zamykania klávesnice heslom sú použité štandardné prostriedky operačného systému Windows XP na pracovných staniciach. Odporúča sa od všetkých užívateľov povinné používanie sporiča obrazovky so zamykaním heslom.

18.2.10 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.

Diskety a ďalšie elektronické médiá sú označované a manipuluje sa s nimi nasledovne:

- médiá, ktoré obsahujú osobné údaje musia byť označené evidenčným číslom a zaevidované, každé také médium musí byť pridelené konkrétnej oprávnenej osobe, ktorá za manipuláciu s ním a jeho bezpečné uloženie zodpovedá,
- pokiaľ majú byť diskety alebo iné elektronické médiá pre záznam dát distribuované mimo Prevádzkovateľa musí sa použiť vždy nové médium a na sprievodnom spise musí byť vyznačené evidenčné číslo média,
- v prípade odovzdávania médií musí byť súčasťou odovzdania odovzdávací protokol s potvrdením preberajúcej osoby, podateľne alebo doklad o postúpení využitého transportného média iným bezpečným spôsobom (doporučenou poštovou zásielkou, kuriérom a pod.),

18.2.11 Používanie elektronickej pošty

Pre všetkých užívateľov, ktorí majú prístup k používaniu elektronickej pošty platia zásady, ktoré sú popísané v Prevádzkovom poriadku počítačovej siete a tieto ďalšie zásady:

- užívatelia zodpovedajú za používanie pridelených schránok elektronickej pošty,
- schránku iného užívateľa je možné používať výhradne s jeho súhlasom (delegovanie).
- prostredníctvom elektronickej pošty je zakázané prenášať osobné údaje mimo Prevádzkovateľa, ktoré nie sú chránené heslom alebo iným primeraným spôsobom (šifrovanie).
- elektronickú poštu používať obozretne, aby neboli ohrozené prenášané informácie, ak je nutné prenášať citlivé informácie použije sa šifrovanie, scrambling alebo kompresia chránená heslom,
- elektronická pošta je určená k pracovným účelom, používať elektronickú poštu pre mimopracovné aktivity možno iba pri zachovaní stanovených pravidiel,

18.2.12 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 obsluhu faxového prístroja prijímateľa.

Odvzdávanie 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.

18.2.13 Používanie Internetu

Pre všetkých užívateľov, ktorí majú prístup k používaniu Internetu platia tieto zásady:

- pripojenie je možné realizovať len prostredníctvom určeného kanálu,
- je zakázané kopírovať a spúšťať programy a iné potenciálne nebezpečné dáta,
- užívatelia majú zakázané navštevovať stránky s obsahom, ktorý nesúvisí s ich pracovnou činnosťou, hlavne:
 - stránky zábavného charakteru,
 - audio alebo video nahrávky,
 - internetové vysielanie,
 - online rozhovory (chat),
- prostredníctvom Internetu je zakázané šíriť osobné údaje,
- výmena súborov s osobnými údajmi prostredníctvom voľne prístupných adresárov alebo archívov je zakázaná.

18.2.14 Používanie mobilných počítačov a práca doma

Osobné údaje je zakázané spracovávať na mobilných počítačoch alebo iných počítačoch mimo pracovisko.

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

- môžu sa používať iba autorizované mobilné počítače PÚ SR , ktoré sú primeraným spôsobom chránené pred prístupom neoprávnenej osoby,
- užívatelia sú poučení o rizikách používania mobilných počítačov zodpovednou osobou,
- na mobilnom počítači je nainštalovaný aktuálny antivírusový program,
- pravidelne je vykonávané zálohovanie dát uložených na mobilnom počítači.

V prípade ak sa na mobilnom počítači spracovávajú a ukladajú dôverné informácie, musí byť použité šifrovanie dát na disku.

Práca na domácich a iných počítačoch nepatriacich do správy Prevádzkovateľa je zakázaná.

18.2.15 Ochrana počítača počas neprítomnosti užívateľa

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

Predtým, ako užívateľ opustí pracovisko je povinný:

- a) ak odchádza na dlhší čas - vypnúť počítač (pracovnú stanicu), (anglicky shut down),
- b) ak odchádza na kratšiu dobu - odhlásiť sa (anglicky log out), alebo zamknúť stanicu
 - vo Windows XP/Vista - Štart – Odhlásiť- Prepnúť používateľa
(na klávesnici logo Windows a L)
 - vo Windows 7 – je možné použiť všetky spomínané spôsoby

18.2.16 Depozit hesiel

U Prevádzkovateľa existuje depozit správcovských hesiel a to aj napriek tomu, že za správu sieťovej a komunikačnej infraštruktúry zodpovedá externý dodávateľ sú uložené primárne, správovské a root heslá u koordinátora správy siete v uzamykateľnom trezore. Bezpečnostným rizikom je však ich expirácia, kedy nedochádza k ich výmene v súlade s popísanými štandardmi, ale sú nemenné.

Pre deponovania musia platiť nasledovné pravidlá:

Heslá sa deponujú u zodpovedného pracovníka. Deponované heslá musia 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 koordinátor správy siete, ktorý po overení oprávnenosti takej požiadavky zmení heslo požadovaného užívateľa na heslo prvotné. 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. Potom si užívateľ znovu zmení heslo tak, aby nebolo nikomu známe.

18.2.17 Antivírusová ochrana

U Prevádzkovateľa je aplikovaná antivírusová ochrana ako na serveri, tak aj na pracovných staniciach.

V súčasnosti je riešenie postavené na produktoch SYMANTEC s automatickým update, poskytuje pracovným staniciam i serverom WINDOWS pokročilú proaktívnu ochranu pred všetkými typmi škodlivých kódov, identifikuje, hlási, čistí, odstraňuje a bráni známym i neznámym škodlivým kódom i nežiaducim aplikáciám infikovať počítače a servery v sieti.

Pravidelný automatizovaný upgrade vírusovej databázy zabezpečuje dostatočnú ochranu serverov a klientov proti vírusom.

Požiadavky na antivírusový systém:

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

Za inštaláciu, aktualizáciu a aktiváciu antivírusového systému zodpovedá správca.

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 zodpovednú osobu.
- V žiadnom prípade nevykonávajte sami odstraňovanie počítačových vírusov. V prípade zistenia vírusu prostredníctvom antivírusového program, 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 zodpovednú osobu, ktorá rozhodne o ďalšom postupe.

18.2.18 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.

18.2.19 Riešenie bezpečnostných incidentov

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

Po oznámení sa spracuje Záznam o bezpečnostnom incidente v IS podľa vzoru v prílohe Bezpečnostných smerníc. Vyhodnotenie vykoná bezpečnostný manažér alebo poverená zodpovedná osoba na základe údajov z vyplneného formulára prípadne poskytnutých doplnujúcich informácií.

V prípade havarijného stavu, ohrozenia a pod. prechádza činnosť IS do výnimočného režimu. V tomto režime sú jednotlivé funkcie užívateľov obmedzené. Úlohou informačného systému je zabezpečiť ochranu osobných údajov. Činnosť informačného systému v tomto režime zabezpečuje bezpečnostný manažér pre IT.

Jeho činnosť je nasledovná:

- zabezpečí znemožnenie prístupu všetkých používateľov k prostriedkom IS,
- v prípade narušenia je zodpovedný za núdzovú prevádzku,
- v prípade zničenia systému je zodpovedný za obnovenie najnovšej zálohy,
- zabezpečí odstránenie príčiny havárie alebo ohrozenia,
- po ukončení havarijného stavu povolí prístup k prostriedkom.
- k splneniu uvedených cieľov vyžieva zmluvnú outsourcingovú spoločnosť

18.2.20 Archivácia, zálohovanie a obnova

18.2.20.1 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.

Údaje nachádzajúce sa na pracovných staniciach sa nezálohujú. Používatelia majú možnosť uchovávaní svojich údajov v pridelenom domovskom adresári nachádzajúcom sa na súborovom serveri. Údaje na súborovom serveri sú uchovávané na zrkadlenom disku, tieto údaje sa však nezálohujú.

Okrem uvedeného majú používatelia možnosť zažiadať koordinátora správy siete o zazálohovanie údajov nachádzajúcich sa na pracovnej stanici na CD médium. Používatelia sú vedení k uchovávaní údajov na súborovom serveri. Strata týchto údajov môže úradu spôsobiť nedostupnosť uvedených kritických údajov. Preto odporúčame zvážiť potrebu zálohovania údajov na súborovom serveri prostredníctvom zálohovacieho zariadenia.

18.2.20.2 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 zo zrkadlených diskov, prípadne z vytvorených záloh.

19. Spolupráca s Úradom na ochranu osobných údajov SR

1. Úrad môže u Organizácie vykonávať kontrolu spracúvania osobných údajov v IS.⁵⁰ Priebeh kontrolnej činnosti je stanovený Zákonom.⁵¹
2. Pri výkone kontroly súčinnosť s kontrolným orgánom zabezpečuje zodpovedná osoba za Organizáciu v súčinnosti so zodpovednou osobou za organizačnú zložku Organizácie, ktorej sa kontrola týka.
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 Organizácie.
5. Účastníkom konania za Organizáciu v zmysle §44a Zákona je štatutárny zástupca Organizácie alebo ním písomne poverená osoba.
6. Počas výkonu kontroly alebo počas konania Úradu voči Organizácii poskytujú zamestnanci Organizácie 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 Organizáciu vedie evidenciu všetkej korešpondencie Organizácie s Úradom.

⁵⁰ §38, ods. 1, písm. h) Zákona.

⁵¹ §39 - §43 Zákona.

20. Záverečné a prechodné ustanovenia

1. Táto Smernica je internou normou, záväznou pre všetkých zamestnancov Organizácie, 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 Zákomom 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 organizácie 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 Organizáciu a poverené zodpovedné osoby za jednotlivé interné organizačné zložky Organizácie (ako boli poverené).
6. Gestorom riadenia zmien a aktualizácie Smernice je zodpovedná osoba za Organizáciu, ktorá navrhované zmeny ustanovení Smernice predkladá k ich odsúhlaseniu a schváleniu štatutárnemu zástupcovi Organizácie.
7. Porušenie ustanovení tejto Smernice je považované za porušenie pracovnej disciplíny a budú z neho vyvedené sankcie v súlade so Zákonníkom práce a Pracovným poriadkom Organizácie.
8. Výnimky z povinností vyplývajúcich z tejto Smernice môže udeľovať štatutárny zástupca Organizácie alebo ním písomne poverená osoba. Výnimka musí byť v súlade so Zákomom, udelená písomne a musí byť daná na vedomie poverenej zodpovednej osobe za Organizáciu.

21. Niektoré zákony upravujúce účel spracúvania osobných údajov

Číslo predpisu	Názov predpisu
{Z 40/1964}	Občiansky zákonník
{Z 71/1967}	o správnom konaní
{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 v znení Zákona č. 394/2000 Z.z.
{Z 513/1991}	Obchodný zákonník
{Z 460/1992}	Ústava Slovenskej republiky
{Z 511/1992}	o správe daní a poplatkov
{Z 152/1994}	o sociálnom fonde
{Z 10/1996}	o kontrole v štátnej správe
{Z 168/1996}	o cestnej doprave
{Z 212/1997}	o povinných výtlačkoch periodických publikácií, neperiodických publikácií a rozmnoženín audiovizuálnych diel
{Z 183/2000}	o knižniciach ...
{Z 211/2000}	o slobodnom prístupe k informáciám ...
{Z 302/2001}	Zákon o samospráve vyšších územných celkov (zákon o samosprávnych krajoch)
{Z 311/2001}	ZÁKONNÍK PRÁCE
{Z 312/2001}	o štátnej službe ...
{Z 416/2001}	o prechode niektorých pôsobností z orgánov štátnej správy na obce a na vyššie územné celky
{Z 502/2001}	o finančnej kontrole a vnútornom audite ...
{Z 507/2001}	o poštových službách
{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}	Zákon o elektronickom podpise ...
{Z 227/2002}	o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu
{Z 291/2002}	o Štátnej pokladnici ...
{Z 395/2002}	Zákon o archívoch a registratúrach ...
{Z 428/2002}	o ochrane osobných údajov ...
{Z 431/2002}	o účtovníctve
{Z 444/2002}	o dizajnoch
{Z 461/2003}	o sociálnom poistení
{Z 462/2003}	Zákon o náhrade príjmu pri dočasnej pracovnej neschopnosti zamestnanca ...
{Z 523/2003}	o verejnom obstarávaní ...
{Z 552/2003}	o výkone práce vo verejnom záujme
{Z 553/2003}	o odmeňovaní niektorých zamestnancov pri výkone práce vo verejnom záujme

{Z 595/2003}	o dani z príjmov
{Z 601/2003}	o životnom minime ...
{Z 610/2003}	o elektronických komunikáciách
{Z 618/2003}	o autorskom práve a právach súvisiacich s autorským právom (autorský zákon)
{Z 5/2004}	o službách zamestnanosti a o zmene a doplnení niektorých zákonov
{Z 215/2004}	o ochrane utajovaných skutočností ...
{Z 357/2004}	o ochrane verejného záujmu pri výkone funkcií verejných funkcionárov
{Z 523/2004}	o rozpočtových pravidlách verejnej správy ...
{Z 578/2004}	o poskytovateľoch zdravotnej starostlivosti, zdravotníckych pracovníkoch, stavovských organizáciách v zdravotníctve ...
{Z 580/2004}	o zdravotnom poistení ...
{Z 583/2004}	Zákon o rozpočtových pravidlách územnej samosprávy ...
{Z 650/2004}	o doplnkovom dôchodkovom sporení ...
{Z 36/2005}	o rodine ...
{Z 82/2005}	o nelegálnej práci a nelegálnom zamestnávaní ...
{Z 300/2005}	Trestný zákon
{Z 301/2005}	Trestný poriadok
{Z 25/2006}	o verejnom obstarávaní
{Z 124/2006}	o bezpečnosti a ochrane zdravia pri práci ...
{Z 126/2006}	o verejnom zdravotníctve ...
{Z 275/2006}	o informačných systémoch verejnej správy ...
{Z 330/2007}	o registri trestov
{Z 355/2007}	o ochrane, podpore a rozvoji verejného zdravia ...
{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 ...
{Z 522/2008}	o vyznamenaniach Slovenskej republiky
{Z 539/2008}	o podpore regionálneho rozvoja
{VMF013261/2008}	Výnos MF SR z 8. septembra 2008 č. MF/013261/2008-132 o štandardoch pre informačné systémy verejnej správy
{Z 206/2009}	o múzeách a o galériách a o ochrane predmetov kultúrnej hodnoty ...
{Z 9/2010}	o sťažnostiach
	a ďalšie
	Nie všetky uvedené zákony sa musia dotýkať činností Prevádzkovateľa, ale boli konfrontované v rámci analýzy ochrany osobných údajov rezortu MK SR.

Špecifikácia príloh

Príloha č. 1	Formulár evidencie údajov o informačnom systéme - vzor
Príloha č. 2	Oznámenie prevádzkovateľa o poverení osoby zodpovednej za dohľad nad ochranou osobných údajov
Príloha č. 3	Písomné poverenie osoby zodpovednej za dohľad na ochranou osobných údajov
Príloha č. 4	Určenie oprávnených osôb s prístupom k osobným údajom v IS - vzor
Príloha č. 5	Poverenie oprávnenej osoby na získavanie osobných údajov – vzor
Príloha č. 6	Poučenie oprávnenej osoby – vzor
Príloha č. 7	Poučenie fyzickej osoby – vzor
Príloha č. 8a,8b	Súhlas dotknutej osoby na spracúvanie osobných údajov – vzor
Príloha č. 9	Evidenčný list záznamového média - vzor
Príloha č. 10	Evidenčný list technických prostriedkov – vzor
Príloha č. 11	Záznam o vykonanej kontrole v IS – vzor
Príloha č. 12	Záznam o bezpečnostnom incidente v IS – vzor
Príloha č. 13	Písomná zmluva so sprostredkovateľom – vzor

Vyhotovovacia doložka

Bezpečnostná smernica bola vyhotovená v 2 výtlačkoch s textovými a grafickými prílohami, ktoré boli pridelené nasledovne:

Výtlačok č. 1 - Poverená zodpovedná osoba

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

Evidencia údajov o prevádzkovanom informačnom systéme (IS)
podľa § 29 zákona č. 428/2002 Z.z. o ochrane osobných údajov v znení neskorších predpisov

Názov IS	Personalistika, mzdy a účtovníctvo
Identifikácia prevádzkovateľa, adresa sídla alebo trvalého pobytu	
<i>Názov organizácie:</i>	Pamiatkový úrad Slovenskej republiky
<i>Sídlo organizácie:</i>	Cesta na Červený most č. 6, 814 06 Bratislava
<i>Forma organizácie:</i>	rštatná rozpočtová organizácia
<i>Identifikačné číslo organizácie:</i>	317 551 94
Štatutárny orgán prevádzkovateľa	
<i>Generálna riaditeľka</i>	PhDr. Katarína KOSOVÁ
Osoba zodpovedná za výkon dohľadu nad ochranou osobných údajov	
<i>Odbor ŠIS ...</i>	RNDr. Ľuboslav ŠKOVIERA
Účel spracovania osobných údajov	vedenie komplexnej personálnej a mzdovej agendy a podkladov na realizáciu miezd pre dotknuté osoby, ktoré sú s prevádzkovateľom v pracovnoprávnom vzťahu, štátnozamestnaneckom pomere, služobnom pomere, členskom vzťahu, na základe poverenia, zvolenia alebo vymenovania alebo v rámci výkonu verejnej funkcie, pracovníkov na dohodu, žiadateľov o zamestnanie a osôb pri realizácii výberových konaní
Zoznam osobných údajov	Priezvisko, meno, titul, adresa trvalého pobytu, prípadne prechodného pobytu, dátum narodenia, miesto narodenia, rodné číslo, osobné číslo, pohlavie, rodinný stav, rodinní príslušníci, počet detí, štátna príslušnosť, absolvované školy a vzdelanie, výnimky zo vzdelania, doby v zamestnaní, dátum uzatvorenia pracovného pomeru, dôvod vzniku pracovného pomeru, spôsob získania zamestnania, skúšobná doba, dátum skončenia, pracovného pomeru (PP), dôvod skončenia PP, spôsob skončenia PP, pracovná kategória, druh pracovného pomeru, pracovné zaradenie, organizačný útvar, fond pracovnej doby, mzdové náležitosti, dovolenka, porušenie pracovnej disciplíny, nárok na starobný dôchodok, zmenená pracovná schopnosť, služobné hodnotenie, školenia a kurzy, číslo telefónu, predchádzajúci zamestnávateľia, doba základnej vojenskej služby, údaje o priznaní invalidného, čiastočne invalidného dôchodku, údaje o zmenenej pracovnej schopnosti, zdravotná poisťovňa zamestnanca, meno a priezvisko manželky/manžela, druha / družky, rodné číslo manželky/manžela, druha / družky – dátum narodenia, rodné meno, meno a priezvisko dieťaťa, rodné číslo dieťaťa, názov a adresa školy, ktorú dieťa nad 16 rokov navštevuje, údaje o dôchodkovom poistení zamestnanca, údaje o zákonomých zrážkach zamestnanca (výživné), údaje o sporení, pôžičkách a zrážkach na poistenie zamestnanca, údaje o osobnom účte zamestnanca, údaje o dočasnej práceneschopnosti zamestnanca, materských dávkach a o ošetrovaní chorého člena rodiny, daňové vyhlásenie k dani z príjmu, daňový bonus, vyhlásenie zamestnanca na uplatnenie zníženia sadzby poistného na starobné poistenie, doklad o návšteve školy (16-25 r.), doklad o stupni invalidity, číslo sociálneho poistenia, rodné priezvisko, posledné priezvisko, titul za menom, číslo OP, e-mailová adresa, adresa prechodného pobytu, dohodnutá doba trvania PP, miesto výkonu práce, vzdelanie požadované
Okruh dotknutých osôb	zamestnanci, uchádzači o zamestnanie, pracovníci na dohodu (dohoda o vykonaní práce, dohoda o brigádnickej práci študentov, dohoda o pracovnej činnosti) a účastníci konkurzov a výberových konaní
Okruh príjemcov, ak sa predpokladá alebo je zrejmé, že im budú osobné údaje sprístupnené	Kontrolné orgány, Sociálna poisťovňa, Daňový úrad, Úrad práce, zdravotné poisťovne
Tretie strany, ak sa predpokladá alebo je zrejmé, že im budú osobné údaje poskytnuté	OÚ sa neposkytujú tretím stranám

Tretie krajiny , ak sa predpokladá alebo je zrejmé, že sa do týchto krajín uskutoční prenos osobných údajov a právny základ cezhraničného toku	Neuskutočňuje sa
Právny základ informačného systému	Zákon č. 311/2001 Z.z, Zákonník práce v znení neskorších predpisov
	Zákon č. 552/2003 Z. z., o výkone práce vo verejnom záujme v znení neskorších predpisov
	Zákon č. 431/2002 Z. z., o účtovníctve v znení neskorších predpisov
	Zákon č. 461/2003 Z. z., o sociálnom poistení v znení neskorších predpisov
	ďalšie zákony upravujúce povinnosti zamestnávateľa upravujúce odvody, daň z príjmu, sociálne dávky a iné
Forma zverejnenia (ak sa vykonáva)	nevykonáva sa
Forma neautoatizovného spracúvania	Osobné spisy zamestnancov, zoznamy, prehľady, dohody, konkurzné lístky, mzdové listy
Forma autoatizovného spracúvania	Automatizované spracúvanie je vykonávané prostredníctvom Centrálného jednotného ekonomického systému MK SR SOFTIP Profit, ktorý je v správe MK SR a prístupuje sa k nemu v súlade s Bezpečnostným projektom výhradne zabezpečeným pripojením. Staršie automatizované IS slúžia výhradne k archívnym účelom dát.
Všeobecná charakteristika opatrení na zabezpečenie ochrany osobných údajov	Prístup do budovy cez informátora, EZS, spisy sú uložené v uzamykateľnej skrini alebo v trezore, program je nainštalovaný na PC ktoré spĺňajú podmienky Bezpečnostného projektu, interných IT rutín a ku ktorým majú prístup len oprávnené osoby a je vykonávané pravidelné zálohovanie s bezpečným ukladaním zálohy. Po odhlásení zo systému sa v PC už žiadne dáta nenachádzajú.
	Práca v uvedenom IS je zabezpečené podľa nariadení Bezpečnostného projektu na ochranu osobných údajov.
Uchovávanie/likvidácia	Po skončení účelu spracúvania osobných údajov je papierová dokumentácia likvidovaná (skartácia, spaľovňa), alebo v rozsahu vyžadovanom uvedenými osobitnými zákonmi odovzdávaná v súlade so smernicami do Registratúrneho strediska k archivácii v súlade s Registratúrnym poriadkom a plánom.
Dátum začatia spracúvania osobných údajov	1987
Dátum vykonania evidencie alebo jej aktualizácie	30. september 2011

POVERENIE

zodpovednej osoby

výkonom dohľadu nad ochranou osobných údajov

Pamiatkový Úrad Slovenskej republiky (ďalej len „PÚ“) ako prevádzkovateľ informačných systémov, v ktorých sa spracúvajú osobné údaje dotknutých osôb, zastúpený generálnou riaditeľkou PÚ týmto poveruje:

Meno	Ľuboslav
Priezvisko, titul	ŠKOVIERA, RNDr.
Funkcia	Odbor ŠIS

VZOR

(ďalej len „zodpovedná osoba“)

výkonom dohľadu nad dodržiavaním zákonných ustanovení pri spracúvaní osobných údajov v informačných systémoch PÚ. Poverenie sa vydáva na základe § 19 ods. (2), (3) a (12) zákona č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov (ďalej len „Zákon“).

Zodpovedná osoba je pri výkone poverenia povinná postupovať najmä v zmysle § 19 ods. (4) a (7) Zákona, vid' druhá strana tohto poverenia. Oprávnenia a povinnosti poverenej zodpovednej osoby sú podrobne rozpracované v čl. 11 Bezpečnostných smerníc na ochranu osobných údajov.

Zodpovedná osoba má podľa § 19 ods. (12) Zákona spôsobilosť na právne úkony v plnom rozsahu, splnila podmienku bezúhonnosti a pre plnenie úloh má v informačných systémoch postavenie oprávnenej osoby.

Poverenie sa vydáva na dobu trvania predmetného poverenia zodpovednej osoby.

V Bratislave dňa 20. júna 2011

PhDr. Katarína KOSOVÁ
generálna riaditeľka

Potvrdenie o prevzatí poverenia

zodpovedná osoba

§ 19 ods. (2) zákona

Ak zamestnávateľ zamestnáva viac ako 5 osôb, výkonom dohľadu písomne poverí zodpovednú osobu alebo viaceré zodpovedné osoby, ktoré dozerajú na dodržiavanie zákonných ustanovení pri spracúvaní osobných údajov.

§ 19 ods. (3) zákona

Odborné vyškolenie zodpovednej osoby alebo viacerých zodpovedných osôb zabezpečí prevádzkovateľ. Rozsah odborného školenia zodpovedá najmä obsahu tohto zákona a úlohám z neho vyplývajúcim, ako aj obsahu medzinárodných zmlúv o ochrane osobných údajov, ktoré boli vyhlásené spôsob ustanoveným zákonom. Úrad môže od prevádzkovateľa žiadať podanie dôkazu o vykonanom odbornom školení.

§ 19 ods. (4) zákona

Zodpovedná osoba posúdi pred začatím spracúvania osobných údajov v informačnom systéme, či ich spracúvaním nevzniká nebezpečenstvo narušenia práv a slobôd dotknutých osôb. Zistenie narušenia práv a slobôd pred začatím spracúvania alebo porušenia ustanovení v priebehu spracúvania osobných údajov zodpovedná osoba bezodkladne písomne oznámi prevádzkovateľovi; ak prevádzkovateľ po upozornení bezodkladne nezjedná nápravu, oznámi to zodpovedná osoba úradu.

§ 19 ods. (7) zákona

Zodpovedná osoba zabezpečuje:

- a) potrebnú súčinnosť s úradom patriacich do jeho pôsobnosti; na požiadanie je zodpovedná osoba povinná úradu kedykoľvek predložiť svoje písomné poverenie, písomné oznámenie vystavené pre prevádzkovateľa podľa ods. (4), preukázať rozsah získaných vedomostí odborným školením,
- b) povinnosti podľa ods. (4) zákona,
- c) dohľad nad plnením základných povinností prevádzkovateľa podľa § 6 zákona,
- d) poučenie oprávnených osôb podľa § 17,
- e) vybavovanie žiadosti dotknutých osôb podľa § 20 až 22,
- f) realizáciu technických, organizačných a personálnych opatrení a dohliada na ich aplikáciu v praxi; ak je prevádzkovateľ povinný vypracovať bezpečnostný podprojekt v súlade s § 16 alebo dokumentáciu podľa § 15 ods. (2) písm. b), zabezpečuje ich vypracovanie,
- g) dohľad pri výbere sprostredkovateľa podľa § 5 ods. (3) a (4), prípravu písomnej zmluvy alebo písomného poverenia pre sprostredkovateľa v súlade s § 5 ods. (2) a zodpovedá za jeho obsah; počas trvania zmluvného vzťahu alebo poverenia preveruje dodržiavanie dohodnutých podmienok,
- h) dohľad nad cezhraničným tokom osobných údajov,
- i) prihlásenie informačných systémov na osobitnú registráciu a oznamovanie zmien a odhlásenie informačných systémov osobitnej registrácie; o informačných systémoch, ktoré nepodliehajú registrácii vedie evidenciu v rozsahu ustanovenom týmto zákonom podľa § 29 a 30 a zabezpečuje jej sprístupnenie komukoľvek, kto o to požiada v súlade s § 32.

§ 19 ods. (10) zákona

Prevádzkovateľ je povinný umožniť zodpovednej osobe nezávislý výkon dohľadu nad ochranou osobných údajov a prijať jej oprávnené návrhy; upozornenie na nedostatky alebo vyslovenie požiadavky zodpovednou osobou v súvislosti s plnením jej povinností podľa ods. (7) sa nesmie stať podnetom ani dôvodom na konanie zo strany prevádzkovateľa, ktoré by zodpovednej osobe spôsobilo ujmu.

§ 19 ods. (12) zákona

Zodpovednou osobou môže byť len fyzická osoba, ktorá má spôsobilosť na právne úkony v plnom rozsahu a splňa podmienku bezúhonnosti, ktorá sa preukazuje doložením výpisu z registra trestov nie starším ako tri mesiace, ktorý je prevádzkovateľ povinný uchovávať počas doby výkonu funkcie zodpovednej osoby. Zodpovednou osobou nemôže byť fyzická osoba, ktorá je štatutárnym orgánom prevádzkovateľa a fyzická osoba, ktorá je oprávnená konať v mene štatutárneho orgánu prevádzkovateľa.

Určenie oprávnených osôb s prístupom k osobným údajom

Titul	Meno	Priezvisko	Útvar	Funkcia	Rozsah oprávnení pre IS						Získavanie OÚ	Ukončený PP
					PMÚ							
RNDr.	Luboslav	ŠKOVIERA			A						Z	

VZOR

Legenda rozsahu oprávnení

Informačný systém		Zodpovedná osoba			Rozsah oprávnení	
Číslo	Názov IS	Titul	Meno	Priezvisko	Činnosť	Popis rozsahu oprávnení - činností
1	Personalistika, mzdy a účtovníctvo PMÚ	RNDr.	Ľuboslav	ŠKOVIERA	A	úplný prístup
					C	čiasočný prístup v rozsahu pracovnej náplne
					R	výberové konania
					V	vedúci oddelenia, dochádzka
2					A	úplný prístup
					C	čiasočný prístup v rozsahu pracovnej náplne
3					A	úplný prístup
					C	čiasočný prístup v rozsahu pracovnej náplne
4						
5						

Legenda povolených činností:

B - len čítanie

A - čítanie, zápis, zmena

v prípade, že pre daný IS je povolené len čítanie, tak sa za označenie prístupu pridá /B (napr.: VZ/B)

P O V E R E N I E na získavanie osobných údajov

BIBIANA, medzinárodný dom umenia pre deti (ďalej len „BIBIANA“) ako prevádzkovateľ informačných systémov, v ktorých sa spracúvajú osobné údaje dotknutých osôb, zastúpený štatutárnym zástupcom týmto poveruje:

Meno, priezvisko, titul

Pracovné zaradenie

(ďalej len „poverená osoba“)

na činnosti súvisiace so získavaním osobných údajov podľa § 10 zákona č. 428/2002 Z.z. o ochrane osobných údajov v znení neskorších predpisov (ďalej len „Zákon“) od zamestnancov pri výkone práce vo verejnom záujme, v rámci pracovnoprávných vzťahov založených dohodou o vykonaní práce alebo brigádnickej práci študentov a osobných údajov súvisiacich s vedením agendy uchádzačov o zamestnanie a realizácie výberových konaní.

Osobné údaje sú získavané za účelom ich spracúvania v informačnom systéme PMÚ.

Poverená osoba je povinná pri získavaní osobných údajov postupovať v zmysle §§ 6 až 14 Zákona, bližšie vid' druhá strana tlačiva. Povinnosti a kompetencie oprávnenej osoby sú taktiež konkretizované v Bezpečnostnej smernici na ochranu osobných údajov.

Poverenie sa vydáva na dobu určitú, t.j. na dobu trvania uvedeného pracovného zaradenia.

V Bratislave dňa 20. júna 2011

PhDr. Katarína KOSOVÁ
generálna riaditeľka

Potvrdenie o prevzatí poverenia

poverená oprávnená osoba

(1) Prevádzkovateľ, ktorý mieni získať od dotknutej osoby jej osobné údaje, je povinný najneskôr pri ich získaní informovať dotknutú osobu a bez vyzvania jej vopred oznámiť:

- a) názov a sídlo alebo trvalý pobyt prevádzkovateľa; ak za prevádzkovateľa so sídlom alebo s trvalým pobytom v tretej krajine koná na území Slovenskej republiky zástupca prevádzkovateľa, aj jeho názov a sídlo alebo trvalý pobyt,
- b) názov a sídlo alebo trvalý pobyt sprostredkovateľa, ak v mene prevádzkovateľa alebo zástupcu prevádzkovateľa získava osobné údaje sprostredkovateľ; v takomto prípade je povinný včas oznámiť dotknutej osobe informácie podľa tohto odseku sprostredkovateľ,
- c) účel spracúvania osobných údajov a
- d) ďalšie doplňujúce informácie v takom rozsahu, v akom sú s ohľadom na všetky okolnosti spracúvania osobných údajov potrebné pre dotknutú osobu na zaručenie jej práv a právom chránených záujmov, najmä právo byť informovaná o podmienkach spracúvania svojich osobných údajov:
 1. preukázanie totožnosti oprávnenej osoby, ktorá získava osobné údaje alebo preukázanie príslušnosti oprávnenej osoby hodnoverným dokladom k tomu subjektu, v mene ktorého koná; oprávnená osoba je povinná takejto žiadosti dotknutej osoby bez zbytočného odkladu vyhovieť,
 2. poučenie o dobrovoľnosti alebo povinnosti poskytnúť požadované osobné údaje; ak sa dotknutá osoba sama rozhoduje o poskytnutí svojich osobných údajov, prevádzkovateľ oznámi dotknutej osobe, na základe akého právneho podkladu mieni spracúvať jej osobné údaje; ak dotknutej osobe povinnosť poskytnúť osobné údaje vyplýva z osobitného zákona, prevádzkovateľ oznámi dotknutej osobe zákon, ktorý jej túto povinnosť ukladá a upovedomí ju o následkoch odmietnutia poskytnúť osobné údaje,
 3. tretie strany, ak sa predpokladá alebo je zrejmé, že im budú osobné údaje poskytnuté,
 4. okruh príjemcov, ak sa predpokladá alebo je zrejmé, že im budú osobné údaje sprístupnené,
 5. formu zverejnenia, ak majú byť osobné údaje zverejnené,
 6. tretie krajiny, ak sa predpokladá alebo je zrejmé, že sa do týchto krajín uskutoční prenos osobných údajov,
 7. poučenie o existencii práv dotknutej osoby.

(2) Ak osobné údaje o dotknutej osobe nezískal prevádzkovateľ priamo od tejto dotknutej osoby, je povinný bez zbytočného odkladu, najneskôr však v čase pred ich prvým poskytnutím tretej strane, ak sa takéto poskytovanie predpokladalo už pri získavaní osobných údajov, oznámiť dotknutej osobe informácie podľa odseku 1 písm. a) až c) a ďalšie doplňujúce informácie v takom rozsahu, v akom sú s ohľadom na všetky okolnosti spracúvania osobných údajov potrebné pre dotknutú osobu na zaručenie jej práv a právom chránených záujmov, najmä právo byť informovaná o podmienkach spracúvania svojich osobných údajov

- a) poučenie o možnosti rozhodnúť o spracúvaní získaných osobných údajov,
- b) zoznam osobných údajov,
- c) tretie strany, ak sa predpokladá alebo je zrejmé, že im budú osobné údaje poskytnuté,
- d) okruh príjemcov, ak sa predpokladá alebo je zrejmé, že im budú osobné údaje sprístupnené,
- e) formu zverejnenia, ak majú byť osobné údaje zverejnené,
- f) tretie krajiny, ak sa predpokladá alebo je zrejmé, že sa do týchto krajín uskutoční prenos osobných údajov,
- g) poučenie o existencii práv dotknutej osoby.

Z Á Z N A M o poučení oprávnenej osoby

Podpísaný/á

Meno, priezvisko, titul:

Pracovné zaradenie:

(ďalej len „poučená osoba“)

potvrďuje, že bol(a) v zmysle §§ 17 a 18 zákona č. 428/2002 Z.z. o ochrane osobných údajov v znení neskorších predpisov (ďalej len „Zákon“) poučený(á) o právach a povinnostiach ustanovených Zákonom a o zodpovednosti za ich porušenie.

Bol/a som zároveň informovaný/á o:

- povinnosti zachovávať mlčanlivosť o osobných údajoch, s ktorými prídem do styku; tie nesmiem využiť ani pre osobnú potrebu a bez súhlasu prevádzkovateľa ich nesmiem zverejniť a nikomu poskytnúť ani prístupniť,
- tom, že povinnosť mlčanlivosti trvá aj po zmene pracovného zaradenia, skončení pracovného pomeru alebo zmluvného vzťahu,
- rozsahu oprávnení a obsahu spracovateľských operácií pri spracúvaní osobných údajov, vyplývajúcich z môjho pracovného zaradenia,
- o povinnostiach vyplývajúcich z Bezpečnostnej smernice na ochranu osobných údajov

V Bratislave dňa

poučená osoba

.....
Podpis osoby, ktorá poučenie vykonala

Z Á Z N A M o poučení fyzickej alebo právnickej osoby

Meno, priezvisko, titul:

Dátum narodenia:

Zamestnávateľ (*):

Adresa zamestnávateľa(*):

(ďalej len „poučená osoba“)

potvrďuje, že bol(a) v zmysle § 18, ods. 3 zákona č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov oprávneným zástupcom prevádzkovateľa informačného systému Personalistika, mzdy a účtovníctvo, poučený(á) o právach a povinnostiach ustanovených citovaným zákonom a o zodpovednosti za ich porušenie.

Bol/a som zároveň informovaný/á o:

- povinnosti zachovávať mlčanlivosť o osobných údajoch, s ktorými prídem do styku; tie nesmiem využiť ani pre osobnú potrebu a bez súhlasu prevádzkovateľa ich nesmiem zverejniť a nikomu poskytnúť ani sprístupniť,
- tom, že povinnosť mlčanlivosti trvá aj po zmene pracovného zaradenia, skončení pracovného pomeru alebo zmluvného vzťahu,
- rozsahu oprávnení a obsahu spracovateľských operácií pri spracúvaní osobných údajov výhradne na základe svojich aktivít u Prevádzkovateľa,
- o povinnostiach vyplývajúcich z Bezpečnostnej smernice na ochranu osobných údajov.

V tomto odseku sa v odôvodnených prípadoch uvedie dôvod a rozsah oboznamovania sa s osobnými údajmi.

V Bratislave dňa

poučená osoba

.....
Podpis osoby, ktorá poučenie vykonala

* Nehodiace sa prečiarknite.

S Ú H L A S

dotknutej osoby so spracúvaním osobných údajov

Podpísaný/á

Meno, priezvisko, titul

Pracovné zaradenie

(ďalej len „dotknutá osoba“)

potvrďuje, že bol/a v zmysle § 7 zákona č. 428/2002 Z.z. o ochrane osobných údajov v znení neskorších predpisov poučený/á prevádzkovateľom o právach a povinnostiach dotknutej osoby a

s ú h l a s í

s ich spracúvaním v informačnom systéme XXXXXXXXXXXXX v rozsahu podľa Zoznamu č.1* pre prevádzkovateľa XXXXXXXXXXXXX so sídlom Ulica X, 888 88 Mesto.

Osobné údaje sú spracúvané za účelom vedenia personálnej agendy, v rozsahu a za podmienok stanovených osobitnými zákonmi. Osobitné zákony boli prevádzkovateľom aplikované do procedúr a pracovných postupov na ich vykonanie, tieto boli ďalej konkretizované popisom činností v prevádzkovaných informačných systémoch, ktoré sú uvedené v Bezpečnostnej smernici na ochranu osobných údajov.

Osobné údaje k uvedenému účelu sú získavané od zamestnancov v štátnozamestnaneckom pomere, zamestnancov pri výkone práce vo verejnom záujme, v rámci pracovnoprávných vzťahov založených dohodou o vykonaní práce alebo brigádnickej práci študentov a osobných údajov súvisiacich s vedením agendy uchádzačov o zamestnanie a realizácie výberových konaní.

Dotknutá osoba bola informovaná, že prevádzkovateľ poveril spracúvaním osobných údajov zmluvného sprostredkovateľa, uvedeného v Zozname č.2*.

Súhlas na spracúvanie osobných údajov sa dáva na dobu trvania pracovného pomeru. Po ukončení pracovného pomeru zabezpečí prevádzkovateľ likvidáciu osobných údajov alebo ich archiváciu v zmysle osobitných zákonov.

Dotknutá osoba potvrdzuje, že osobné údaje poskytla dobrovoľne, bez nátlaku, že sú pravdivé a súhlasí s ich využitím k vymedzenému účelu.

V Bratislave dňa

.....
podpis dotknutej osoby

* Zoznam č.1 a 2 vid'. druhá strana tohto tlačiva.

Zoznam č.1

- Rodné číslo, priezvisko, meno, titul, dátum a miesto narodenia, adresa trvalého a prechodného pobytu, štátna príslušnosť,
- osobné číslo, pohlavie, rodinný stav, rodinní príslušníci, počet vyživovaných detí,
- absolvované školy a vzdelanie, výnimky zo vzdelania, doby v zamestnaní, dátum uzatvorenia pracovného pomeru, dôvod vzniku pracovného pomeru, spôsob získania zamestnanca, skúšobná doba, dátum skončenia pracovného pomeru (PP), dôvod skončenia PP, spôsob skončenia PP, pracovná kategória, druh pracovného pomeru, pracovné zaradenie, organizačný útvar
- fond pracovnej doby, mzdové náležitosti, dovolenka, porušenie pracovnej disciplíny, nárok na starobný dôchodok, zmenená pracovná schopnosť, služobné hodnotenie, školenia a kurzy
- číslo telefónu
- predchádzajúci zamestnávateľia, doba základnej vojenskej služby, údaje o priznaní invalidného, čiastočne invalidného dôchodku, údaje o zmenenej pracovnej schopnosti, zdravotná poisťovňa zamestnanca
- meno a priezvisko manželky/manžela, druha / družky, rodné číslo manželky/manžela, druha / družky – dátum narodenia, rodné meno, meno a priezvisko dieťaťa, rodné číslo dieťaťa, názov a adresa školy, ktorú dieťa nad 16 rokov navštevuje,
- údaje o dôchodkovom poistení zamestnanca, údaje o zákonných zrážkach zamestnanca (výživné), údaje o sporení, pôžičkách a zrážkach na poistenie zamestnanca, údaje o osobnom účte zamestnanca, údaje o dočasnej práceneschopnosti zamestnanca, materských dávkach a o ošetrovaní chorého člena rodiny
- výška príspevkov pre odborovú organizáciu, daňové vyhlásenie k dani z príjmu, daňový bonus, vyhlásenie zamestnanca na uplatnenie zníženia sadzby poistného na starobné poistenie,
- doklad o návšteve školy (16-25 r.), doklad o stupni invalidity, číslo zmluvy o DDS (rodné číslo), názov zamestnávateľa, adresa sídla zamestnávateľa a PSČ, meno kontaktnej osoby zamestnávateľa pre DDS, výška príspevku DDS (v Sk alebo %), dátum prvého príspevku DDS, číslo sociálneho poistenia, rodné priezvisko, posledné priezvisko, titul za menom, národnosť, číslo OP, e-mailová adresa, dohodnutá doba trvania PP, miesto výkonu práce, vzdelanie požadované

Zoznam č.2

Prevádzkovateľ poveril spoločnosť **ABCD Security, s.r.o.**, ako zmluvného sprostredkovateľa, ktorý osobné údaje získava v jeho mene priamo od dotknutých osôb na účely identifikácie fyzickej osoby pri jej jednorázovom vstupe do priestorov jeho sídla. Pri uvedených činnostiach sprostredkovateľ postupuje v zmysle § 10, ods. 4 zákona NR SR č. 428/2002 Z.z. o ochrane osobných údajov v znení neskorších predpisov (ďalej len „Zákon“), podľa platných ustanovení Prevádzkového poriadku, schválených Smerníc na výkon strážnej služby a Zmluvy uzatvorenej s prevádzkovateľom.

Spoločnosť **ABCD Security, s.r.o.**, v mene prevádzkovateľa vykonáva taktiež kontrolu pri používaní elektronickej čipovej karty na identifikáciu zamestnancov v dochádzkovom a prepúšťacom systéme Time Guard Plus, ktorý pracuje s vyhodnocovacím softvérom Cerberus, ktorý je nainštalovaný vo vchode do služobných priestorov prevádzkovateľa.

Spoločnosť **ABCD Security, s.r.o.**, v mene prevádzkovateľa ďalej obsluhuje a využíva videomonitorovací systém Q-viev na účely zabezpečenia verejného poriadku, bezpečnosti a odhaľovania kriminality v monitorovaných vnútorných a vonkajších priestoroch (okrem možnosti poskytovania vyhotoveného záznamu na účely trestného konania alebo konania o priestupkoch, ktoré zabezpečuje výhradne oprávnená osoba prevádzkovateľa). Poverený sprostredkovateľ pri uvedených činnostiach postupuje v zmysle ustanovení § 9 ods. 7 a § 13 ods. 7 Zákona.

Informácia dotknutej osobe

(vykonaná v zmysle §10, ods. 1 až 3, zákona č. 428/2002 Z.z.)

o účele a podmienkach spracúvania osobných údajov

Podpísaný/á

Meno, priezvisko, titul:

Pracovné zaradenie:

(ďalej len „dotknutá osoba“)

potvrdzuje, že bol/a v zmysle § 10 zákona č. 428/2002 Z.z. o ochrane osobných údajov v znení neskorších predpisov poučený/á prevádzkovateľom o právach a povinnostiach dotknutej osoby uvedených v §20 zákona a o nasledovných podmienkach a účele spracúvania osobných údajov:

- a) **Pamiatkový úrad Slovenskej republiky** so sídlom na adrese Cesta na Červený most č. 6, 814 06 Bratislava (ďalej len „PÚ“) je prevádzkovateľom informačného systému Personalistika, mzdy a účtovníctvo (ďalej len „IS PMÚ“) v ktorom budú Vaše osobné údaje spracúvané v rozsahu zoznamu č.1, ktorý je uvedený na druhej strane tohto tlačiva.
- b) Účelom spracúvania osobných údajov je plánovanie, zabezpečovanie, rozvoj ľudských zdrojov a realizácia miezd, prípadne realizácia zmluvných vzťahov s fyzickými osobami, ktoré vykonávajú činnosť, vytvárajú dielo podľa autorského zákona, alebo za finančnú odmenu poskytujú Prevádzkovateľovi služby v rámci akvizičnej činnosti. Účel spracúvania je stanovený osobitnými zákonmi pre oblasť pracovno-právnych vzťahov, účtovníctvo, dane, sociálne, zdravotné a dôchodkové poistenie.
- c) Pre splnenie uvedeného účelu spracúvania osobných údajov prevádzkovateľ využíva týchto zmluvných sprostredkovateľov:
§ **Ministerstvo kultúry Slovenskej republiky** (ďalej len „MK SR“ alebo „Ministerstvo“) so sídlom na adrese Nám. SNP č. 13, 813 31 Bratislava, ktoré v zmysle zmluvy zabezpečuje realizáciu a správu Centrálného jednotného ekonomického systému MK SR (ďalej len „CJES“) a dátového skladu pre aplikáciu SOFTIP PROFIT.
- d) Ďalšie podmienky spracúvania osobných údajov:
§ Osobné údaje môžu byť spracúvané prostredníctvom automatizovaných, čiastočne automatizovaných, alebo neautomatizovaných prostriedkov spracúvania, pričom sa uplatňujú primerané technické, organizačné a personálne bezpečnostné opatrenia zodpovedajúce spôsobu spracúvania, ktoré sú deklarované Bezpečnostným projektom na ochranu osobných údajov.
§ Osobné údaje spracúvajú len oprávnené osoby, ktoré boli náležitým spôsobom určené a poučené.
- e) Dobrovoľnosť poskytnutia osobných údajov:
§ Poskytnutie uvedených osobných údajov nie je dobrovoľné; je potrebné na splnenie účelu spracúvania osobných údajov, ktorý určili osobitné zákony SR, vzťahujúce sa na zamestnanosť, sociálne a zdravotné poistenie, daňové a iné povinnosti zamestnávateľa. Z uvedeného dôvodu sa písomný súhlas na spracúvanie osobných údajov nezískava. Prevádzkovateľ pristúpil k informovaniu dotknutej osoby o účele a podmienkach spracúvania osobných údajov podľa § 10 Zákona.
- f) Príjemcovia:
§ Osobné údaje môžu byť sprístupnené len príjemcom, ktorý splnili požadované podmienky na bezpečnosť osobných údajov a ktorých výkon priamo súvisí so splnením účelu spracúvania (Zdravotná poisťovňa, Sociálna poisťovňa, Daňový úrad, Úrad práce, Ústredie práce, sociálnych vecí a rodiny)
- g) Zverejňovanie:
§ Osobné údaje nebudú zverejnené.
- h) Tretie krajiny:
§ Osobné údaje nebudú sprístupnené príjemcom v tretej krajine.

V Bratislave dňa

.....
dotknutá osoba

Zoznam č.1

- Rodné číslo, priezvisko, meno, titul, dátum a miesto narodenia, adresa trvalého a prechodného pobytu, štátna príslušnosť,
- osobné číslo, pohlavie, rodinný stav, rodinní príslušníci, počet vyživovaných detí,
- absolvované školy a vzdelanie, výnimky zo vzdelania, doby v zamestnaní, dátum uzatvorenia pracovného pomeru, dôvod vzniku pracovného pomeru, spôsob získania zamestnanca, skúšobná doba, dátum skončenia pracovného pomeru, dôvod a spôsob skončenia pracovného pomeru, pracovná kategória, druh pracovného pomeru, pracovné zaradenie, organizačný útvar
- fond pracovnej doby, mzdové náležitosti, dovolenka, porušenie pracovnej disciplíny, nárok na starobný dôchodok, zmenená pracovná schopnosť, služobné hodnotenie, školenia a kurzy,
- číslo telefónu,
- predchádzajúci zamestnávateľia, údaje o priznaní invalidného alebo čiastočne invalidného dôchodku, údaje o zmenenej pracovnej schopnosti, zdravotná poisťovňa zamestnanca,
- meno a priezvisko manželky/manžela, druha / družky, rodné číslo manželky/manžela, druha / družky – dátum narodenia, rodné meno, meno a priezvisko dieťaťa, rodné číslo dieťaťa, názov a adresa školy, ktorú dieťa navštevuje,
- údaje o dôchodkovom poistení zamestnanca, údaje o zákonných zrážkach zamestnanca (výživné), údaje o sporení, pôžičkách a zrážkach na poistenie zamestnanca, údaje o osobnom účte zamestnanca, údaje o dočasnej práceneschopnosti zamestnanca, materských dávkach a o ošetrovaní choreho člena rodiny,
- daňové vyhlásenie k dani z príjmu, daňový bonus, vyhlásenie zamestnanca na uplatnenie zníženia sadzby poistného na starobné poistenie,
- doklad o návšteve školy (16-25 r.),
- ostatné údaje vyžadované zákonmi SR.

VI Z O R**Evidenčný list technických prostriedkov**

určených na spracúvanie osobných údajov v informačnom systéme Personalistika. mzdy a účtovníctvo

P.č.	Názov technického prostriedku	Typ	Výrobné číslo	Umiestnenie	Oprávnený užívateľ	Pohyb	Poznámka
1.	Kopírovacie zariadenie	Minolta	VQC7GEF458	Kancelária 121	Mgr. Paveleková Anna		
2.	Tlačiareň	HP 1220C	DTR458/Qwi	Kancelária 122	Dvorská Zuzana	v záručnej oprave	Zapožičaná náhradná tlačiareň z depozitu oddelenia informatiky
3.	PS 11	LIBRA	BDT-5-487-II	Kancelária 251	Dvorská Zuzana		
4.	PS 14	DELL	TRA1258-5	Kancelária 256	Mgr. Paveleková Anna		
5.	PS 16	IBM	LziA45DS	Kancelária 259	Ing. Matúš Pavol		
6.	PS 18	COMPAQ	ANK-585-13	Kancelária 260	Kaliský Štefan		
7.	Skartačné zariadenie	DELL	D-BVN-01/02-2365ft4	Kancelária 260	Oddelenie knižničných služieb		

V Bratislave dňa 15. mája 2007

 podpis poverenej zodpovednej osoby
za IS Personalistika, mzdy a účtovníctvo

Z Á Z N A M

o vykonanej kontrole v informačnom systéme _____

A.) Dátum čas a miesto kontroly

1. Dátum kontroly IS
2. Čas kontroly IS
3. Miesto kontroly IS

B.) Údaje o spracovateľovi záznamu

4. Meno, priezvisko
5. Funkcia v organizácii
6. Funkcia v informačnom systéme
7. Meno, funkcia a súhlas kompetentného nadriadeného, ktorý vykonanie kontroly nariadil

C.) Predmet kontroly

8. Personálna bezpečnosť	
9. Administratívna bezpečnosť	
10. Režimové a organizačné opatrenia	
11. Objektová bezpečnosť	
12. Technická bezpečnosť v neautomatizovanom IS	
13. Systémová bezpečnosť v automatizovanom IS	
14. Komunikačné prostriedky	
15. Iná (napríklad zlúčenie viacerých oblastí)	

WZOR

D.) Výsledok kontroly

<p style="text-align: right;">_____</p> <p style="text-align: right;">podpis spracovateľa</p>

E.) Návrh opatření k náprave zistených nedostatkov

osoba zodpovedná za výkon dohľadu

F.) Výsledok a termíny ich realizácie

osoba zodpovedná za výkon dohľadu

G.) Stanovisko štatutárneho zástupcu prevádzkovateľa

Neboli zistené žiadne nedostatky

štatutárny zástupca prevádzkovateľa IS

Z Á Z N A M

o bezpečnostnom incidente v informačnom systéme

A.) Špecifikácia incidentu

1. Dátum a čas vzniku incidentu
2. Dátum a čas zistenia incidentu
3. Dátum a čas vypracovania záznamu

B.) Oblasť vzniku incidentu

4. Administratívna
5. Personálna
6. Režimová a organizačná
7. Objektová
8. Technická
9. Systémové prostriedky
10. Komunikačné prostriedky
11. Iná (napríklad splynutie viacerých oblastí)

C.) Údaje o spracovateľovi záznamu

12. Meno, priezvisko
13. Funkcia v organizácii
14. Funkcia v informačnom systéme
15. Meno a funkcia kompetenčného nadriadeného

D.) Špecifikácia incidentu

16. Popis miesta incidentu
17. Popis obsahu incidentu
18. Popis zaistených dôkazov

E.) Riešenie incidentu:

19. Meno a priezvisko osoby, ktorej bol incident postúpený k vybaveniu
20. Funkcia v organizácii
21. Funkcia v bezpečnostnom systéme

F.) Návrh opatření využitých k náprave incidentu

osoba zodpovědná za výkon dohledu

G.) Výsledek a termíny ich realizácie

osoba zodpovědná za výkon dohledu

H.) Stanovisko štatutárneho zástupcu prevádzkovateľa

štatutárny zástupca prevádzkovateľa IS

Zmluva o spracúvaní osobných údajov

uzavretá na základe § 5 ods. 2 zákona č. 428/2002 Z.z. o ochrane osobných údajov v znení neskorších predpisov (ďalej len „Zmluva“)

Zmluvné strany

XXXXXXXXXXXXXXXXXXXX

So sídlom: XXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXX

Zastúpené: Xxx XXXX

XXXXXXXXXXXXXXXXXXXX

Číslo účtu: XXXXXXXXXXXXXXXX

IČO: XXXXXXXXX

(ďalej len „Prevádzkovateľ“)

a

XXXXXXXXXXXXXXXXXXXX

So sídlom:

Zastúpený:

Číslo účtu:

IČO:

DIČ:

Označenie registra:

(ďalej len „Sprostredkovateľ“)

uzatvárajú túto Zmluvu vo väzbe na zákon č. 428/2002 Z.z. o ochrane osobných údajov v znení neskorších predpisov (ďalej len „Zákon“) nasledovne.

VZOR

Čl. I

1. Sprostredkovateľ na základe Zmluvy o poskytovaní služieb č. XXXXX, uzatvorenej dňa XX.XX.XXXX, vykonáva pre Prevádzkovateľa činnosti v oblasti (XXXXXXXXXXXXXXXXXXXX) a to najmä pri realizácii týchto aktivít:
 - XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX,
 - XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX,
 - XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX,(ďalej len „Služby“).
2. Účelom spracúvania osobných údajov v IS je XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX (napr. identifikácia fyzickej osoby pri jej jednorázovom vstupe do priestorov sídla Prevádzkovateľa a kontrola oprávnenosti použitia elektronickej identifikačnej karty zamestnanca na registráciu v elektronickom dochádzkovom systéme a umožnenie vstupu do sídla Prevádzkovateľa).
3. Touto Zmluvou sa zabezpečuje ochrana nasledovných infotypov osobných údajov spracúvaných Sprostredkovateľom (konkretizovať podľa skutočne spracúvaných údajov):
 - 3.1. priezvisko,
 - 3.2. meno,
 - 3.3. titul,
 - 3.4. adresa trvalého pobytu,
 - 3.5. dátum narodenia,
 - 3.6. číslo občianskeho preukazu alebo cestovného pasu,
4. Dotknutými osobami sa na účely tejto Zmluvy rozumejú (..... fyzické osoby – žiadatelia o jednorázový vstup a zamestnanci Prevádzkovateľa – preukazujúci oprávnenie na registráciu v elektronickom dochádzkovom systéme a na vstup do priestorov sídla Prevádzkovateľa, ktoré sa realizujú elektronickou identifikačnou kartou.....).

Čl. II

Zmluvné strany sa dohodli na týchto zásadách spracúvania osobných údajov:

1. Sprostredkovateľ je oprávnený spracúvať osobné údaje poskytnuté dotknutými osobami v rozsahu a za podmienok ustanovených v platných právnych predpisoch a dojednaných v tejto Zmluve.
2. Sprostredkovateľ je oprávnený spracúvať len tie údaje, ktoré zodpovedajú účelu ich spracúvania.
3. Prevádzkovateľ si vyhradzuje právo rozhodnúť o poskytovaní získaných osobných údajov z informačného systému tretím stranám, ktoré môže byť vykonané iba na základe predchádzajúceho písomného súhlasu vydaného oprávneným zástupcom Prevádzkovateľa.
4. V súvislosti so spracúvaním osobných údajov sa Prevádzkovateľ zaväzuje poskytovať Sprostredkovateľovi správne a aktuálne osobné údaje, čím nie je dotknutá zodpovednosť dotknutých osôb za pravdivosť poskytnutých osobných údajov.
5. Ak sa požaduje poskytnutie (overenie) osobných údajov v súvislosti s prevádzkovaním informačného systému Prevádzkovateľ tieto poskytne Sprostredkovateľovi formou v termíne Zodpovednou osobou za prípravu a odovzdanie osobných údajov dotknutých osôb na strane Prevádzkovateľa je, oprávnenou osobou za prevzatie osobných údajov dotknutých osôb na strane Sprostredkovateľa je.....
6. Za bezpečnosť poskytnutých osobných údajov zodpovedá Sprostredkovateľ tým, že ich chráni pred odcudzením, stratou, poškodením, neoprávneným prístupom, zmenou a rozširovaním. Sprostredkovateľ sa za týmto účelom zaväzuje prijať primerané technické, organizačné a personálne opatrenia zodpovedajúce spôsobu spracovania osobných údajov v informačnom systéme a to formou a za podmienok stanovených Zákomom.

7. Sprostredkovateľ a jeho zamestnanci, ktorí prichádzajú do styku s osobnými údajmi dotknutých osôb sú povinní zachovávať o nich mlčanlivosť, povinnosť mlčanlivosti trvá aj po ukončení spracúvania osobných údajov. Tým nie sú dotknuté ustanovenia osobitných zákonov.
8. Sprostredkovateľ sa zaväzuje preukázateľne poučiť vlastné oprávnené osoby o ich právach a povinnostiach pri ochrane osobných údajov vyplývajúcich z platných právnych predpisov, ako aj o zodpovednosti v prípade ich porušenia.
9. Sprostredkovateľ sa zaväzuje bezodkladne oznámiť Prevádzkovateľovi každý prípad podozrenia úniku, straty, zničenia, zneužitia alebo iného nenáležitého nakladania s osobnými údajmi.
10. Prevádzkovateľ aj Sprostredkovateľ sa zaväzujú rešpektovať právo dotknutej osoby na informácie súvisiace so spracúvaním jej osobných údajov v informačnom systéme, pokiaľ si ho písomne uplatní.
11. Prevádzkovateľ zodpovedá v plnom rozsahu za dodržiavanie Zákona pri získavaní osobných údajov dotknutých osôb vrátane ustanovenia § 10 Zákona. V prípade, že zo Zákona vyplýva povinnosť Prevádzkovateľa získať preukázateľným spôsobom súhlas dotknutých osôb so spracovaním ich osobných údajov (podľa ustanovenia § 7 Zákona), Prevádzkovateľ zodpovedá za zabezpečenie súhlasu dotknutých osôb a ich informovanie o tom, že spracúvanie osobných údajov v mene Prevádzkovateľa vykonáva zmluvný Sprostredkovateľ.
12. Sprostredkovateľ po skončení účelu spracúvania osobných údajov, najneskôr však po ukončení platnosti tejto Zmluvy, bezodkladne odovzdá Prevádzkovateľovi všetky osobné údaje a doklady súvisiace s ich spracúvaním v informačnom systéme, ktoré mu boli poskytnuté Prevádzkovateľom alebo dotknutými osobami. Ak to nie je možné, zabezpečí bezodkladnú likvidáciu osobných údajov. Prevádzkovateľ po skončení účelu spracúvania osobných údajov zabezpečí úschovu a ochranu osobných údajov v súlade s platnou legislatívou.

Čl. III

13. Táto Zmluva nadobúda platnosť a účinnosť dňom jej podpísania oprávnenými zástupcami zmluvných strán a uzatvára sa na dobu neurčitú.
14. Zmluvné strany prehlasujú, že túto Zmluvu uzatvárajú slobodne a vážne, že ich zmluvná voľnosť nie je obmedzená.
15. Zmluvné strany prehlasujú, že táto Zmluva nebola uzavretá za nevýhodných podmienok alebo v tiesni, že si ju riadne prečítali, jej obsahu porozumeli a na znak súhlasu s jej obsahom pripájajú svoje vlastnoručné podpisy.
16. Pokiaľ niektoré z ustanovení tejto Zmluvy je neplatné, alebo sa stane neskôr neplatným, nemá to vplyv na platnosť ostatných ustanovení tejto Zmluvy. V prípade, že niektoré z ustanovení tejto Zmluvy je neplatné, alebo sa stane neskôr neplatným alebo neúčinným, zaväzujú sa zmluvné strany, že ho nahradia ustanovením, ktoré najviac zodpovedá pôvodnej vôli zmluvných strán a účelu podľa tejto Zmluvy.
17. Táto Zmluva môže byť doplnená a zmenená len písomným dodatkom podpísaným oboma zmluvnými stranami.
18. Táto Zmluva je vyhotovená v dvoch rovnopisoch, pričom každá zo zmluvných strán dostane jeden rovnopis.

V Bratislave, dňa

za Prevádzkovateľa

za Sprostredkovateľa