ZMLUVA O POSKYTOVANÍ KOMPLEXNÝCH SLUŽIEB
v oblasti ochrany osobných údajov č. IS00718

Uzavretá medzi poskytovateľom a objednávateľom :

1. Poskytovateľ:	**ISIT Slovakia, s.r.o.**
	Klincová 37
	821 08 Bratislava
V zastúpení:	Lenka Václavová, konateľ spoločnosti
IČO:	44 783 990
DIČ :	2022839104
IČ DPH :	SK2022839104

Obchodný register: Okresný súd Bratislava 1, oddiel Sro, vložka číslo 58669/B
Bankové spojenie: ČSOB a.s., Číslo účtu. SK59 7500 0000 0040 2403 0210
e-mail : audit@datasoftconsulting.sk
zodpovedná osoba : Roman Václav , LL.M., tel : 0910 905154
(ďalej ako „poskytovateľ")

2. Objednávateľ:	**Oblastná organizácia cestovného ruchu Trenčianske Teplice**
	M. R. Štefánika 4
	914 51 Trenčianske Teplice
v zastúpení:	PhDr. Štefan Škultéty, predseda predstavenstva
IČO:	42274885
DIČ:	2023747209
Bankové spojenie:	Slovenská sporiteľňa, a.s.
Číslo účtu:	SK64 0900 0000 0051 2366 2138
e-mail.:	silvia.havelkova@teplice.sk

(ďalej ako „objednávateľ")

uzatvárajú v súlade súst. § 269 a nasl. zák. č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov (ďalej len „Obchodný zákonník") zmluvu o poskytovaní služieb (ďalej len „zmluva") v nasledovnom znení:

Článok I.
Predmet zmluvy

1 Predmetom zmluvy je záväzok poskytovateľa poskytovať užívateľovi počas trvania tejto zmluvy služby podľa podmienok tejto zmluvy a záväzok užívateľa uhradiť poskytovateľovi za plnenie jeho činností dohodnutú odmenu podľa podmienok
tejto zmluvy.

2. Poskytovateľ sa zaväzuje pre objednávateľa v rámci predmetu zmluvy poskytovať:
a) zabezpečenie súladu s ochranou osobných údajov podľa platnej legislatívy v čase trvania zmluvy, vrátane metodických pokynov a vyhlášok dozorného úradu
b) vytvorenie bezpečnostnej dokumentácie k ochrane citlivých aktív a osobných údajov
c) výkon dohľadu nad ochranou osobných údajov formou zodpovednej osoby s nahlásením na dozorný úrad v rozsahu §44-46 zákona č. 18/2018 Z.z.. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

e) školenie pre oprávnené osoby objednávateľa v rozsahu min. 1x ročne

Článok II.
Práva a povinnosti zmluvných strán

1. Objednávateľ sa zaväzuje poskytovať súčinnosť poskytovateľovi a to predovšetkým poskytnutím všetkých relevantných informácií a to pri výkone auditu, výkone funkcie zodpovednej osoby a podporných činnostiach ktoré dodáva poskytovateľ, pričom tento zodpovedá za spracovane informácií, ktoré boli poskytnuté, identifikované a verifikované objednávateľom.

2. Objednávateľ určí oprávnenú osobu, ktorá bude komunikovať so zodpovednou osobou:

   Meno oprávnenej osoby : Silvia Havelková

   telefónne číslo : 0905 573 213

   mail : silvia.havelkova@teplice.sk

3. Cieľom naplnenia tejto zmluvy je efektívne a odborné plnenie predmetu zmluvy. Objednávateľ zodpovedá za správnosť, pravdivosť a úplnosť informácií poskytnutých poskytovateľovi. Objednávateľ poskytne poskytovateľovi svoju súčinnosť v rozsahu potrebnom pre splnenie povinností poskytovateľa vyplývajúcich zo zmluvy.

4. Poskytovateľ je povinný plniť svoje povinnosti vyplývajúce z tejto zmluvy s odbornou starostlivosťou, riadne a včas, a to v súlade s pokynmi objednávateľa.

5. Neoddeliteľnú súčasť tejto zmluvy tvorí príloha č. 1 Popis základných bezpečnostných opatrení prevádzkovateľa.

Článok III.
Odmena poskytovateľa a platobné podmienky

1. Odmena za služby poskytnuté v zmysle článku I. tejto zmluvy sa na základe dohody zmluvných strán určuje v celkovej výške **960,- Eur** bez DPH (slovom:.. deväťstošesťdesiat.. Eur bez DPH).

Odmena v dohodnutej celkovej výške bude rozdelená do **12 mesačných splátok** , teda v sume**,- 80,- Eur + dph / mesiac**, pričom objednávateľ platí za službu mesiac vopred a to počnúc od mesiaca .... **MÁJ 2018** ..... do mesiaca ...**APRÍL 2019** .... vrátane.

2. Podkladom na úhradu odmeny podľa tohto článku je uzatvorená Zmluva o poskytovaní komplexných služieb so splátkovým kalendárom, kde budú jasne definované mesačné splátky, základ dane, DPH, suma spolu, variabilný symbol, dátum splatnosti. Splátkový kalendár je neoddeliteľnou súčasťou tejto zmluvy.

3.V prípade omeškania objednávateľa s úhradou odmeny podľa tohto článku je poskytovateľ oprávnený účtovať objednávateľovi penále z omeškania vo výške 0,02% za každý deň omeškania.

Článok IV.
Trvanie zmluvy

1. Zmluva sa uzatvára na dobu určitú v trvaní 12 mesiacov odo dňa podpísania zmluvy s možnosťou ďalšieho predĺženie.
2. Túto zmluvu môže každá zo zmluvných strán vypovedať s 3 mesačnou výpovednou lehotou, ktorá začína plynúť od prvého dňa kalendárneho mesiaca nasledujúceho po mesiaci, v ktorom bola výpoveď doručená druhej zmluvnej strane.

3. V prípade predčasného vypovedania tejto zmluvy musia zmluvné strany splniť svoje záväzky, vrátane úhrady cieľovej sumy.

Článok V.
Komunikácia

1. Zmluvné strany sa dohodli, že všetky informácie a právne úkony podľa tejto zmluvy si budú doručovať niektorou z nasledovných foriem:
a) e-mailom na adresy uvedené v záhlaví,
b) doporučenou poštou s doručenkou alebo kuriérom na adresu uvedenú v záhlaví,
c) osobne oproti písomnému potvrdeniu.

Článok VI.
Spoločné a záverečné ustanovenia

1. Ani jedna zmluvná strana nie je oprávnená bez predchádzajúceho písomného súhlasu druhej zmluvnej strany postúpiť práva a povinnosti vyplývajúce z tejto zmluvy na akúkoľvek tretiu právnickú alebo fyzickú osobu

2. Zmluvné strany sa dohodli, že akékoľvek budúce spory vyplývajúce z tejto zmluvy budú prednostne riešené rokovaniami zúčastnených strán za účelom dohody.

3. Táto zmluva sa uzatvára písomne a je možno ju meniť a dopĺňať len po vzájomnej dohode zmluvných strán, výlučne vo forme písomného dodatku k tejto zmluve.

4. Zmluva sa vyhotovuje v 2 (dvoch) vyhotoveniach, z ktorých každá zmluvná strana obdrží po jednom vyhotovení.

V Trenčianskych Tepliciach, dňa 17.05.2018

Oblastná organizácia cestovného ruchu
Trenčianske Teplice
M.R. Štefánika 4
914 51 Trenčianske Teplice
IČO: 42274885

.....
objednávateľ

ISIT Slovakia s.r.o.
Klincová 37, 821 08 Bratislava
IČO: 44783990
IČ DPH: SK202[illegible]

.....
poskytovateľ

SPLÁTKOVÝ KALENDÁR

Faktúra k Zmluve o poskytovaní komplexných služieb

VS : IS00718

1. Poskytovateľ: **ISIT Slovakia, s.r.o.**
Klincová 37
821 08 Bratislava
V zastúpení: Lenka Václavová, konateľ spoločnosti
IČO: 44 783 990
DIČ : 2022839104
IČ DPH : SK2022839104
Obchodný register: Okresný súd Bratislava 1, oddiel Sro, vložka číslo 58669/B
Bankové spojenie: ČSOB a.s., Číslo účtu. SK59 7500 0000 0040 2403 0210
e-mail : audit@datasoftconsulting.sk

2. Objednávateľ: **Oblastná organizácia cestovného ruchu Trenčianske Teplice**
M. R. Štefánika 4
914 51 Trenčianske Teplice
v zastúpení: PhDr. Štefan Škultéty, predseda predstavenstva
IČO: 42274885
DIČ: 2023747209
Bankové spojenie: Slovenská sporiteľňa, a.s.
Číslo účtu: SK64 0900 0000 0051 2366 2138
e-mail.: silvia.havelkova@teplice.sk

Odmena za služby poskytnuté v zmysle článku I. tejto zmluvy

Por.č.	Dátum splatnosti	Základ dane	20% DPH	Suma spolu
1.	31.05.2018	80,- Eur	16,- Eur	96,- Eur
2.	30.06.2018	80,- Eur	16,- Eur	96,- Eur
3.	31.07.2018	80,- Eur	16,- Eur	96,- Eur
4.	31.08.2018	80,- Eur	16,- Eur	96,- Eur
5.	30.09.2018	80,- Eur	16,- Eur	96,- Eur
6.	31.10.2018	80,- Eur	16,- Eur	96,- Eur
7.	30.11.2018	80,- Eur	16,- Eur	96,- Eur
8.	31.12.2018	80,- Eur	16,- Eur	96,- Eur
9.	31.01.2019	80,- Eur	16,- Eur	96,- Eur
10.	28.02.2019	80,- Eur	16,- Eur	96,- Eur
11.	31.03.2019	80,- Eur	16,- Eur	96,- Eur
12.	30.04.2019	80,- Eur	16,- Eur	96,- Eur

Tento doklad slúži zároveň ako podklad k uplatneniu si DPH.

Oblastná organizácia cestovného ruchu
Trenčianske Teplice
M.R. Štefánika 4
914 51 Trenčianske Teplice
IČO: 42274885

ISIT Slovak
Klincová 37, 821
IČO: 447(
IČ DPH: SK2(

.....
objednávateľ

.....
poskytovateľ

Popis základných bezpečnostných opatrení prevádzkovateľa

Pri spracúvaní osobných údajov podľa ustanovení zákona č. 18/2018 Z. z. o ochrane osobných údajov.

Ako príloha č. 1 k Zmluve o poskytnutí služieb v oblasti ochrany osobných údajov

Prevádzkovateľ :

.....

Zodpovedná osoba :

Roman VÁCLAV, [illegible]
Tel.: 0910 905
roman@vacla

.....

O b s a h

I. Úvod 3
II. Rozsah pôsobnosti 3
III. Predmet 3
IV. Použité skratky 4
V. Vymedzenie niektorých pojmov 5
VI. Popis základných bezpečnostných opatrení a spôsob ich uplatňovania v podmienkach prevádzkovateľa 9
Technické opatrenia 9
Ochrana pred neoprávneným prístupom 9
Riadenie prístupu OO 9
Ochrana proti škodlivému kódu 10
Sieťová bezpečnosť 10
Zálohovanie 11
Likvidácia OÚ a dátových nosičov 11
Aktualizácia operačného systému a programového aplikačného vybavenia 12
Pseudonymizácia OÚ 12
Organizačné opatrenia – personálne opatrenia ZODPOVEDNÁ OSOBA 13
Riadenie prístupu OO k OÚ 15
Organizácia spracúvania OÚ 15
Likvidácia OÚ 23
Bezpečnostné incidenty 23

I. Úvod

Účelom dokumentu „Popis základných bezpečnostných opatrení" (ďalej len „ dokument") je popísať a aplikovať základné bezpečnostné opatrenia pri spracúvaní osobných údajov u prevádzkovateľa , kde je výkonom dohľadu nad ochranou osobných údajov zodpovednou osobou **Roman Václav, LL.M.** a je neoddeliteľnou prílohou zmluvy o poskytovaní služieb medzi zodpovednou osobou a prevádzkovateľom.

Popis opatrení , ktoré je povinný implementovať prevádzkovateľ , sú povinní rešpektovať všetci zamestnanci prevádzkovateľa – oprávnené osoby, ktorí spracúvajú osobné údaje fyzických osôb. V prípade nerešpektovaní týchto základných opatrení hrozí vznik bezpečnostných incidentov pri spracúvaní osobných údajov, za ktoré nesie zodpovednosť v zmysle zákonníka práce a interných predpisov zamestnávateľa tá konkrétna oprávnená osoba, ktorá incident spôsobila a v zmysle zákona na ochranu OÚ prevádzkovateľ.

Tento dokument bol spracovaný v súlade so zákonom č. 18/2018 Z. z. o ochrane osobných údajov a obsahuje len základné bezpečnostné opatrenia, ďalšie budú rozpracované v samostatnej bezpečnostnej dokumentácii.

II. Rozsah pôsobnosti

Dokument sa vzťahuje na všetky informačné systémy (agendy) prevádzkované u prevádzkovateľa, kde oprávnené osoby prevádzkovateľa za konkrétne stanoveným účelom spracúvajú osobné údaje fyzických osôb – dotknutých osôb a platí pre všetky spôsoby spracúvania, teda vrátane spracovateľských operácií získavania, uchovávania, poskytovania, sprístupňovania tretím stranám, kde môže najčastejšie dochádzať k narušeniu dôvernosti, dostupnosti a integrity osobných údajov.

III. Predmet

Predmetom tohto dokumentu je:

1. Popis základných technických, organizačných a personálnych opatrení pri spracúvaní osobných údajov a ich využitie v konkrétnych podmienkach.

2. rozsah oprávnení a popis povolených činností jednotlivých oprávnených osôb, spôsob ich identifikácie a autentizácie pri prístupe k informačnému systému.

IV. Použité skratky

AIS - Automatizovaný informačný systém

DO - Dotknutá osoba

EZS - Elektronický zabezpečovací systém

FO - Fyzická osoba

HW - Hardvérové technické vybavenie

BI - Bezpečnostný incident

IS - Informačný systém

OO - Oprávnená osoba

OOÚ - Ochrana osobných údajov

OS – Operačný systém

ŠO - Špeciálne okruhy (ŠO)

OÚ - Osobný údaj

PV - Priestory určené pre styk s verejnosťou, zásobovaním a odberateľmi

PZ - Priestory určené pre prácu zamestnancov

SW - Softvérové vybavenie

VPN - Virtual Private Network – virtuálna privátna sieť

ZEP - Zaručený elektronický podpis

Zákon č. 18/2018 Z. z. – zákon č. 18/2018 Z. z. o ochrane osobných údajov.

V. Vymedzenie niektorých pojmov

Osobné údaje sú:

údaje, týkajúce sa identifikovanej fyzickej osoby alebo identifikovateľnej fyzickej osoby, ktorú možno identifikovať priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora, iného identifikátora, ako je napríklad meno, priezvisko, identifikačné číslo, lokalizačné údaje,1) alebo online identifikátor, alebo na základe jednej alebo viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú identitu, fyziologickú identitu, genetickú identitu, psychickú identitu, mentálnu identitu, ekonomickú identitu, kultúrnu identitu alebo sociálnu identitu.

Súhlas so spracúvaním osobných údajov je:

akýkoľvek vážny a slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby vo forme vyhlásenia alebo jednoznačného potvrdzujúceho úkonu, ktorým dotknutá osoba vyjadruje súhlas so spracúvaním svojich osobných údajov

Spracúvanie osobných údajov je:

spracovateľská operácia alebo súbor spracovateľských operácií s osobnými údajmi alebo so súbormi osobných údajov, najmä získavanie, zaznamenávanie, usporadúvanie, štrukturovanie, uchovávanie, zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie, bez ohľadu na to, či sa vykonáva automatizovanými prostriedkami alebo neautomatizovanými prostriedkami.

Poskytovanie osobných údajov je:

odovzdávanie osobných údajov na spracúvanie inému prevádzkovateľovi alebo inému zástupcovi prevádzkovateľa, alebo jeho sprostredkovateľovi.

Sprístupňovanie osobných údajov je:

oznámenie osobných údajov alebo umožnenie prístupu k nim inej právnickej osobe, alebo fyzickej osobe s výnimkou dotknutej osoby, alebo oprávnenej osoby, ktorá ich nebude spracúvať ako prevádzkovateľ, zástupca prevádzkovateľa, alebo sprostredkovateľ.

Zverejňovanie osobných údajov je:

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 v operáte, ich umiestnením na úradnej tabuli, alebo na inom verejne prístupnom mieste.

Likvidácia osobných údajov je:

zrušenie osobných údajov rozložením, vymazaním alebo fyzickým zničením hmotných nosičov tak, aby sa z nich osobné údaje nedali reprodukovať.

Obmedzenie spracúvania osobných údajov je:

označenie uchovávaných osobných údajov s cieľom obmedziť ich spracúvanie v budúcnosti.

Informačný systém je:
akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom základe alebo geografickom základe

***Účel spracúvania osobných údajov* je:**
vopred jednoznačne vymedzený alebo ustanovený zámer spracúvania osobných údajov, ktorý sa viaže na určitú činnosť.

Cezhraničný tok osobných údajov je:
prenos osobných údajov mimo územia Slovenskej republiky subjektom so sídlom alebo s trvalým pobytom v cudzine, alebo ich výmena s týmito subjektmi.

Adresa je:
súbor údajov o pobyte fyzickej osoby, do ktorého patria názov ulice, orientačné, prípadne súpisné číslo domu, názov obce, prípadne názov časti obce, poštové smerovacie číslo, názov okresu, názov štátu.

***Všeobecne použiteľný identifikátor* je:**
trvalý identifikačný osobný údaj dotknutej osoby, ktorý zabezpečuje jej jednoznačnosť v informačných systémoch (rodné číslo).

Genetické údaje sú:
údaje týkajúce sa zdedených genetických charakteristických znakov fyzickej osoby alebo nadobudnutých genetických charakteristických znakov fyzickej osoby, ktoré poskytujú jedinečné informácie o fyziológii alebo zdraví tejto fyzickej osoby a ktoré vyplývajú najmä z analýzy biologickej vzorky danej fyzickej osoby.

Biometrické údaje sú:
osobné údaje, ktoré sú výsledkom osobitného technického spracúvania osobných údajov týkajúcich sa fyzických charakteristických znakov fyzickej osoby, fyziologických charakteristických znakov fyzickej osoby alebo behaviorálnych charakteristických znakov fyzickej osoby a ktoré umožňujú jedinečnú identifikáciu alebo potvrdzujú jedinečnú identifikáciu tejto fyzickej osoby, ako najmä vyobrazenie tváre alebo daktyloskopické údaje.

Údaje týkajúce sa zdravia sú:
osobné údaje týkajúce sa fyzického zdravia alebo duševného zdravia fyzickej osoby vrátane údajov o poskytovaní zdravotnej starostlivosti alebo služieb súvisiacich s poskytovaním zdravotnej starostlivosti, ktorými sa odhaľujú informácie o jej zdravotnom stave.

Profilovanie je:
akákoľvek forma automatizovaného spracúvania osobných údajov spočívajúceho v použití osobných údajov na vyhodnotenie určitých osobných znakov alebo charakteristík týkajúcich sa fyzickej osoby, najmä na analýzu alebo predvídanie znakov alebo charakteristík dotknutej osoby súvisiacich s jej výkonnosťou v práci, majetkovými

pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom

Pseudonymizácia je:
spracúvanie osobných údajov spôsobom, že ich nie je možné priradiť ku konkrétnej dotknutej osobe bez použitia dodatočných informácií, ak sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na ne technické a organizačné opatrenia na zabezpečenie toho, aby osobné údaje nebolo možné priradiť identifikovanej fyzickej osobe alebo identifikovateľnej fyzickej osobe

Logom je:
záznam o priebehu činnosti používateľa v automatizovanom informačnom systéme

Šifrovaním je:
transformácia osobných údajov spôsobom, ktorým opätovné spracúvanie je možné len po zadaní zvoleného parametra, ako je kľúč alebo heslo

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

Prevádzkovateľ je:
každý, kto sám alebo spoločne s inými vymedzí účel a prostriedky spracúvania osobných údajov a spracúva osobné údaje vo vlastnom mene; prevádzkovateľ alebo konkrétne požiadavky na jeho určenie môžu byť ustanovené v osobitnom predpise alebo medzinárodnej zmluve, ktorou je Slovenská republika viazaná, ak takýto predpis alebo táto zmluva ustanovuje účel a prostriedky spracúvania osobných údajov.

Sprostredkovateľ je:
každý, kto spracúva osobné údaje v mene prevádzkovateľa.

Príjemcom je:
každý, komu sa osobné údaje poskytnú bez ohľadu na to, či je treťou stranou; za príjemcu sa nepovažuje orgán verejnej moci, ktorý spracúva osobné údaje na základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, v súlade s pravidlami ochrany osobných údajov vzťahujúcimi sa na daný účel spracúvania osobných údajov

Treťou stranou je:
každý, kto nie je dotknutou osobou, prevádzkovateľ, sprostredkovateľ alebo inou fyzickou osobou, ktorá na základe poverenia prevádzkovateľa alebo sprostredkovateľa spracúva osobné údaje,

Oprávnená osoba 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, ktorá môže osobné údaje spracúvať len na základe pokynu prevádzkovateľa, zástupcu prevádzkovateľa, alebo sprostredkovateľa, ak tento zákon, alebo osobitný zákon neustanovuje inak.

Porušením ochrany osobných údajov je:
porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene alebo k neoprávnenému poskytnutiu prenášaných, uchovávaných osobných údajov alebo inak spracúvaných osobných údajov, alebo k neoprávnenému prístupu k nim,

Dotknutá osoba je:
každá fyzická osoba, o ktorej sa spracúvajú osobné údaje.

Zodpovednou osobou je:
osoba určená prevádzkovateľom alebo sprostredkovateľom, ktorá plní úlohy podľa zákona č. 18/2018 Z.z. o ochrane osobných údajov.

Zástupcom je:
fyzická osoba alebo právnická osoba so sídlom, miestom podnikania, organizačnou zložkou, prevádzkarňou alebo trvalým pobytom v členskom štáte, ktorú prevádzkovateľ alebo sprostredkovateľ písomne poveril podľa § 35

Autenticita je:
vlastnosť zaisťujúca, že identita subjektu alebo zdroja je taká, za ktorú sa prehlasuje. Autenticita je aplikovaná na entity, ako sú užívatelia, procesy, systémy a informácie.

***Dôvernosť* je:**
vlastnosť, že aktíva nie sú prístupné neautorizovaným jednotlivcom, entitám alebo procesom.

Integrita je:
vlastnosť, že aktíva nebudú pozmenené, poškodené, narušené neautorizovaným spôsobom.

Dostupnosť je:
vlastnosť zaisťujúca autorizovaným užívateľom prístup k informáciám a aktívam vtedy, keď to potrebujú.

Bezpečnostný incident je:
Udalosť, ktorá spôsobila narušenie dôvernosti, dostupnosti alebo integrity spracúvaných osobných údajov.

Kódexom správania je:
súbor pravidiel ochrany osobných údajov dotknutej osoby, ktorý sa prevádzkovateľ alebo sprostredkovateľ zaviazal dodržiavať

VI. Popis základných bezpečnostných opatrení a spôsob ich uplatňovania v podmienkach prevádzkovateľa

Technické opatrenia

- Vstupy do budovy a vnútorných priestorov prevádzkovateľa musia byť riadené režimovými opatreniami tak, aby sa zamedzilo neautorizovanému prístupu iných ako oprávnených osôb v priestoroch, kde dochádza k akejkoľvek forme spracúvania osobných údajov fyzických osôb s výnimkou priestorov, kde dotknuté osoby vstupujú za účelom spracúvania svojich osobných údajov

- ISOU (agendy) musia byť umiestnené v chránených priestoroch - oddelených miestnostiach s primeraným rozsahom technických opatrení, s vylúčením pohybu iných ako oprávnených osôb a ochránené pred nepriaznivými vplyvmi okolia. V prípade ak je dotknutá osoba osobne prítomná pri spracúvaní svojich osobných údajov oprávnenou osobou, jej pohyb v takýchto priestoroch musí byť riadený spôsobom, aby nezískala prístup k osobným údajom iných dotknutých osôb (diskrétna zóna, politika čistého stola a obrazovky atď)

Bezpečné uloženie fyzických nosičov OÚ

– Na uchovávanie papierovej evidencie obsahujúcej osobné údaje z IS, v ktorých sa spracúvajú aj OÚ z kategórie zvlášť citlivých OÚ (RČ, zdravotný stav...) je nevyhnutné vyhradiť uzamykateľné skrine. Prístup ku skriniam musí byť riadený a manipulácia s kľúčmi zdokumentovaná v kľúčovom poriadku. Kľúče od skriniek musia mať len OO poverené spracúvaním OÚ príslušného IS.

- zobrazovacie jednotky (monitory) musia byť umiestnené tak, aby nebolo možné náhodné odpozeranie OÚ.
- každá miestnosť, kde dochádza k fyzickej likvidácii písomných dokumentov musí byť vybavená zariadeniami na likvidáciu listín – skartovačka.

Ochrana pred neoprávneným prístupom

- Ochrana obsahu dátových nosičov – musí byť zabezpečená ochrana dátových nosičov ich bezpečnou manipuláciou a evidenciou.
- Pravidlá prístupu tretích strán k IS musia byť definované v zmluvách o poskytnutí externých služieb (sprostredkovateľské zmluvy)
- **Pri prenose údajov mimo organizáciu sa vyžaduje šifrovanie dát** prostriedkami aplikácií alebo vhodným voľne šíriteľným šifrovacím programom.

Riadenie prístupu OO

- Identifikácia, autentizácia a autorizácia OO v IS – musí byť zabezpečená jednoznačná identifikácia OO pomocou užívateľského profilu zriadeného správcom siete.

- Zaznamenávanie vstupov jednotlivých OO do IS – musí byť zabezpečené pomocou reportov v jednotlivých aplikáciách
- Prístup k automatizovaným prostriedkom spracúvania osobných údajov je realizovaný pomocou PC a iných zariadení. Dáta môžu byť umiestnené centrálne na databázových serveroch v príslušných serverovniach. Autorizácia užívateľov je trojstupňová:
    - Autorizácia operačným systémom zariadenia, z ktorého sa pristupuje k aplikácii. (jej vykonávanie sa zabezpečuje menom a heslom,
    - Overovanie identity sa vykonáva nastavením príslušnej domény v danej LAN, do ktorej sa pristupuje. Pre heslo je nastavená príslušná politika zahŕňajúca požiadavku na dĺžku hesla, zloženie hesla, pravidelnú zmenu hesla, a pamätanie si určitého počtu predchádzajúcich hesiel).
    - Autorizácia samotnou aplikáciou. (Vykonáva sa menom a heslom užívateľa. Ak to aplikácia umožňuje, je potrebné nastaviť politiku pre heslá, ako v bode a.).

Ochrana proti škodlivému kódu

- Detekcia prítomnosti škodlivého kódu v prichádzajúcej elektronickej pošte a v iných súboroch prijímaných z verejne prístupnej počítačovej siete alebo z dátových nosičov – musí byť zabezpečená pomocou nainštalovaného, správne konfigurovaného, aktualizovaného a pravidelne monitorovaného antivírového programu
- Ochrana pred nevyžiadanou elektronickou poštou – musí byť zabezpečená v nastaveniach prichádzajúcej pošty.
- Používanie legálneho a prevádzkovateľom schváleného softvéru – prevádzkovateľ môže používať len legálny softvér, ktorý je inštalovaný správcom IS.
- Pravidlá sťahovania súborov z verejne prístupnej počítačovej siete – Oprávnená osoba využíva služby Internetu (povolené je využívanie iba verejných služieb WWW - world wide web a FTP - file transfer protocol) za účelom plnenia pracovných úloh, pričom dodržiava bezpečnostné opatrenia prijaté prevádzkovateľom za účelom zabezpečenia ochrany osobných údajov, nepoužíva verejné komunikačné systémy na rýchly prenos správ (ICQ, AOL, IRC a pod.),

Sieťová bezpečnosť

- Kontrola, obmedzenie alebo zamedzenie prepojenia IS, v ktorom sú spracúvané OÚ s verejne prístupnou počítačovou sieťou – musí byť zabezpečené konfiguráciou siete a nastavením bezpečnostnej politiky.
- Ochrana vonkajšieho a vnútorného prostredia prostredníctvom nástroja sieťovej bezpečnosti je zabezpečená pomocou firewall.
- Sieťovú bezpečnosť zabezpečiť tak, aby sa minimalizovala možnosť neoprávneného prístupu. Systém ochrany pred útokom z internetu je potrebné zdokumentovať v dokumentácii IT. Táto časť dokumentácie podlieha určitému stupňu utajenia. Dokumentácia musí obsahovať pridelenie zodpovednosti za správu, udržiavanie a kontrolu funkčnosti nastavených bezpečnostných prvkov. Systém ochrany musí zabezpečiť minimálne nasledovné:

- šifrovanie komunikácie v prípade, ak sa prenos dát realizuje aj prostredím verejnej dátovej siete (napr. Internet).
- oddelenie lokálnej siete od Internetu prostredníctvom firewallu.
- blokovanie nepotrebných komunikačných portov.
- autorizáciu externých HW zariadení pristupujúcich do lokálnej siete.
-

- **Servery a aktívne prvky siete:** musia byť umiestnené tak, aby sa zabránilo príležitosti na neautorizovaný fyzický prístup. Znamená to, že sú umiestňované v zónach s najvyšším stupňom autorizácie, podľa platnej bezpečnostnej politiky Názov prevádzkovateľa.

- **Kabeláž sieťovej infraštruktúry:** musí byť zabezpečená proti neoprávnenému prístupu vhodnými ochrannými prvkami. Primárne musí byť kabeláž vedená v priestoroch, ktoré nie sú prístupné verejnosti.

Zálohovanie

- Test funkcionality dátového nosiča zálohy – sa vykonáva po jeho vytvorení
- Vytváranie záloh s vopred zvolenou periodicitou – zálohy sa musia vytvárať v určenej periodicite na hardvérový prostriedok, zabezpečené virtuálne riešenie alebo na zálohovací server. Musí sa vytvoriť aj duplicitný systém zálohovania na externý DVD disk, ktorý musí byť ukladaný v protipožiarnej skrini v archíve.
- Test obnovy IS zo zálohy vykonávať podľa potreby.
- Bezpečné fyzické ukladanie záloh – zálohy sa musia ukladať v uzamykateľnej skrini.
- Pokiaľ prevádzkovateľ používa server/servery, tieto musia byť vybavené zálohovaním a archiváciou dát.

Zálohovanie dodávky elektrickej energie: Servery a dôležité zariadenia prevádzkovateľa (routery, komunikačné prvky...) sú vybavené záložnými zdrojmi napájania.

Za implementáciu tohto opatrenia zodpovedá odbor informatiky, resp. poverený PC technik/informatik.

Likvidácia OÚ a dátových nosičov

- Bezpečné vymazanie OÚ z dátových nosičov, fyzicky zničiť CD, DVD ich prelomením.
- Zariadenie na likvidáciu dátových nosičov OÚ – vždy použiť skartovačku alebo zlikvidovať listinné dokumenty spálením.

Aktualizácia operačného systému a programového aplikačného vybavenia

- Operačné systémy a aplikačný softvér sa aktualizujú vždy pri uvoľnení novej verzie externým správcom IT technológií. Dbať na dodržiavanie zmluvných podmienok s externým dodávateľom.
- Operačný systém musí zabezpečovať nasledovné

  - Nesmie dovoliť užívateľovi meniť nastavenia operačného systému.
  - Nesmie dovoliť užívateľovi použiť možnosť zapamätania hesla.
  - Nesmie dovoliť užívateľovi ukladanie dát na lokálne zariadenia (pevné disky, USB...), len na tie, ktoré schváli prevádzkovateľ.
  - Nesmie umožniť užívateľovi výber tlače na tlačiarne, ktoré by sa nenachádzali v miestnosti, z ktorej sa realizuje pripojenie.
  - Musí zabezpečiť automatické odpájanie užívateľov pri nečinnosti užívateľov trvajúcej dlhšie ako 30minút.
  - Musí zabezpečiť automatické spustenie šetriaceho režimu pri reaktivite užívateľa trvajúcej dlhšie ako 5min. Prechod zo šetriaceho do aktívneho režimu musí vyžadovať zadanie hesla užívateľa.
  -

Pseudonymizácia OÚ

Zabezpečiť pseudonymizáciu spracúvaných osobných údajov spôsobom, že ich nie je možné priradiť ku konkrétnej dotknutej osobe bez použitia dodatočných informácií, ak sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na informácie technické a organizačné opatrenia na zabezpečenie toho, aby osobné údaje nebolo možné priradiť identifikovanej fyzickej osobe alebo identifikovateľnej fyzickej osobe

Organizačné opatrenia – personálne opatrenia ZODPOVEDNÁ OSOBA

Poverenie osoby zodpovednej za výkon ochrany OÚ u prevádzkovateľa: Štatutárny orgán prevádzkovateľa písomne poverí výkonom dohľadu nad OOÚ zodpovednú osobu. Toto poverenie je poverením zodpovednej osoby v zmysle zákona č. 18/2018 Z. z. Takto poverená Zodpovedná osoba vystupuje voči Úradu na ochranu osobných údajov ako zodpovedná osoba.

Zodpovedná osoba :

Roman Václav LL.M., tel : 0910 905154, mail : roman@vaclav.sr

Nahlásenie poverenej zodpovednej osoby na úrad: Poverená osoba bude prevádzkovateľom nahlásená na Úrad na ochranu osobných údajov písomne.

Zmena zodpovednej osoby: Poverená zodpovedná osoba môže byť nahradená inou osobou v súlade s ustanoveniami zákona na ochranu osobných údajov a uzatvorenou zmluvou s externou zodpovednou osobou. Ak vyprší lehota zmluvy a zodpovednej osobe skončí výkon funkcie zodpovednej osoby alebo sa prevádzkovateľ rozhodne poveriť inú zodpovednú osobu, preukázateľne upozorní na tieto skutočnosti dozorný orgán a zároveň ich dá na vedomie zodpovednej osobe, ktorej poverenie končí.

Zodpovednosť za ochranu OÚ: Zodpovednosť za ochranu OÚ musí byť zahrnutá do pracovných náplní zamestnancov. Za realizáciu zodpovedá personálny odbor.

Dohody o uchovávaní dôvernosti: Zamestnanci prichádzajúci do styku s OÚ, musia podpisovať dohody o uchovávaní dôvernosti, ako súčasť pracovných zmlúv. Dohoda musí byť podpísaná pred prvým spracúvaním OÚ. Za uzatváranie dohôd zodpovedá personálny odbor.

Školenia a vzdelávanie: Všetci zamestnanci, a kde je to relevantné aj užívatelia z tretích strán musia prechádzať pravidelnými školeniami o prostriedkoch, procesoch a procedúrach používaných u prevádzkovateľa. Školenia musia byť realizované pred prvým začatím práce a taktiež musia byť vykonávané preškolenia z príslušných postupov v pravidelných intervaloch. Za zabezpečenie školení zodpovedá personálny odbor.

Poučenie oprávnených osôb: Odporúča sa pravidlo poučiť všetky osoby, ktoré majú alebo môžu mať prístup k IS tak, aby nedochádzalo k chybám pri spracúvaní OÚ. O poučení sa vykonáva písomný záznam, ktorý je treba uchovať, ako doklad o vykonaní poučenia. Záznam musí podpísať osoba, ktorá poučenie vykonala aj osoba, ktorá bola poučená.

Vzdelávanie administrátorov a užívateľov: Administrátori systémov a užívatelia prevádzkovateľa absolvujú minimálne raz ročne vhodné školenia (v súvislosti s používaním a bezpečnosťou AIS). Školenia musia slúžiť aj na budovanie povedomia o informačnej bezpečnosti a ochrane OÚ.

Rozsah zodpovednosti oprávnených osôb - OO

1. OO je každý zamestnanec, ktorý prichádza do styku s OÚ v rámci svojho pracovného zaradenia, a ktorý môže OÚ spracúvať len na základe pokynu prevádzkovateľa. OO majú nasledovné zodpovednosti, oprávnenia a povinnosti, platné pre všetky OO :
   a) uplatňovať a dodržiavať základné organizačné a technické opatrenia popisované týmto dokumentom na zabezpečenie OOÚ spracúvaných v IS prevádzkovateľa pred odcudzením, stratou, poškodením, neoprávneným prístupom, zmenou a rozširovaním;
   b) zachovávať mlčanlivosť o OÚ, s ktorými príde do styku. Informácie o OÚ nesmie využiť ani pre osobnú potrebu a bez súhlasu prevádzkovateľa IS ich nesmie zverejniť a nikomu poskytnúť ani sprístupniť. Povinnosť mlčanlivosti trvá aj po zániku tejto funkcie alebo po skončení štátnozamestnaneckého pomeru, alebo obdobného pracovného vzťahu. Povinnosť mlčanlivosti neplatí, ak je to nevyhnutné na plnenie úloh orgánov činných v trestnom konaní a vo vzťahu k Úradu na ochranu osobných údajov pri plnení jeho úloh;
   c) spracúvať OÚ len v rozsahu a za podmienok dojednaných s prevádzkovateľom v písomnej zmluve alebo v písomnom poverení;
   d) od DO vyžadovať len také OÚ, ktoré sú nevyhnutné na dosiahnutie účelu spracúvania. K takýmto OÚ môže priradiť ďalšie OÚ DO, ktoré bezprostredne súvisia s daným účelom spracúvania, len ak na ne DO upozorní a táto s tým písomne súhlasí. Zároveň treba mať na pamäti §8 zákona o minimalizácii rozsahu spracúvaných osobných údajov;
   e) od DO získať písomný súhlas so spracúvaním OÚ, ak sa jedná o spracúvanie OÚ na základe súhlasu a tento súhlas archivovať v súlade s registratúrnym poriadkom a plánom. Súhlas obsahuje najmä údaj o tom, kto súhlas poskytol, komu sa tento súhlas dáva, na aký účel, zoznam OÚ, dobu platnosti súhlasu a podmienky jeho odvolania;
   f) v priestoroch prístupných verejnosti zabezpečiť diskrétnosť spracúvania OÚ, teda nepripustiť, aby sa k OÚ DO dostali nepovolané osoby;
   g) získavať OÚ nevyhnutné na dosiahnutie účelu spracúvania kopírovaním, skenovaním alebo iným zaznamenávaním úradných dokladov na nosič informácií možno len vtedy, ak **s tým DO písomne súhlasí alebo ak to umožňuje osobitný zákon;**
   h) zabezpečovať správnosť a aktuálnosť OÚ;
   i) informovať prevádzkovateľa o nutnosti likvidácie OÚ, pokiaľ takáto povinnosť vyplynie z registratúrneho poriadku a plánu, alebo z ustanovení zákona č. 18/2018
   j) na likvidáciu papierových dokumentov s OÚ použiť vhodné skratkovacie zariadenie;
   k) príslušné OO sú v mene prevádzkovateľa oprávnené získavať potrebné OÚ od okruhu DO vymedzených v evidenčnom liste jednotlivých IS;
   l) OO sú oprávnené vstupovať do IS obsahujúcich OÚ, ktoré sú spracúvané v písomnej alebo elektronickej podobe a spracúvať ich výlučne v rámci plnenia si svojich pracovných povinností.

2. Porušenie povinností popísaných v odseku 1 sa považuje za porušenie pracovnej disciplíny.

Riadenie prístupu OO k OÚ

Heslá sú bežným prostriedkom overenia užívateľskej identity pre prístup do IS alebo službe. Užívatelia sú preto povinní používať heslo pri prihlasovaní sa do operačného systému, siete a aplikácie spracúvajúcej OÚ.

Heslá nesmú byť uložené na počítačovom systéme v nechránenej podobe. Heslá je treba udržovať v dôvernosti.

Organizácia spracúvania OÚ

Pravidlá spracúvania OÚ v chránenom priestore

1. OO sa povoľuje používať výlučne softvér, ku ktorému má prevádzkovateľ platnú licenciu. Používať neautorizovaný softvér sa zakazuje.

2. Na jednotlivých pracoviskách dodržiavať politiku tzv. čistého stola a obrazovky – papierové a počítačové médiá s OÚ nie je povolené nechávať bez dozoru voľne položené na pracovisku. PC nesmú zostať bez dozoru prihlásené do systému; pri opustení pracoviska je potrebné systém uzamknúť, aby sa zabránilo neautorizovanému prístupu do počítačov. Papierové a počítačové médiá s OÚ sa musia ukladať do vhodných uzamykateľných skríň, a to najmä v mimopracovnom čase.

3. Je dovolené kopírovanie a tlač len takých dokumentov, ktoré sú potrebné k výkonu pracovnej činnosti. Tlačiť alebo kopírovať iné písomnosti sa zakazuje.

4. K zabráneniu odcudzenia a šírenia OÚ je zakázané ponechávať kopírované alebo vytlačené dokumenty obsahujúce OÚ bez dozoru v kopírke, alebo tlačiarňach. Po skopírovaní alebo vytlačení dokumentu obsahujúceho OÚ je zamestnanec, ktorý kopírovanie, alebo tlač vykonal, povinný skopírované, alebo vytlačené dokumenty ihneď z kopírky, alebo tlačiarne odobrať.

5. Vytlačené dokumenty, ktoré obsahujú OÚ a nie sú už potrebné, alebo boli vytlačené omylom je osoba, ktorá ich vytlačila, povinná okamžite skartovať. V žiadnom prípade sa nesmú použiť na ďalšiu tlač alebo ako pracovný papier, ani ako papier určený do zberu. Do zberu môžu ísť len skartované dokumenty.

6. Zakazuje sa poskytovanie OÚ o inej osobe prostredníctvom telefónu, okrem poskytovania údajov orgánom činným v trestnom konaní (túto problematiku rieši samostatný dokument), faxu a nechránenej emailovej komunikácie.
7. Heslá sú bežným prostriedkom overenia užívateľskej identity pre prístup do IS alebo službe. Užívatelia sú preto povinní používať heslo pri prihlasovaní sa do operačného systému, siete a aplikácie spracúvajúcej OÚ.

Riadenie komunikácie a prevádzky

1. **Akceptácia nových prostriedkov spracúvania OÚ:** Musia byť stanovené akceptačné kritéria pre nové IS, aktualizácie existujúcich systémov prípadne pre nové verzie a pred samotnou akceptáciou musia byť vykonané vhodné testy a zálohovanie systému (za predpokladu, že to dané systémy umožňujú). Za realizáciu zodpovedá odbor IT.

2. **Likvidácia zariadení:** Likvidácia nefunkčných, poškodených alebo vyraďovaných zariadení, na ktorých sa nachádzajú spracúvané OÚ sa musí vykonávať bezpečným spôsobom tak, aby nemohlo dôjsť k strate dôvernosti OÚ nachádzajúcich sa na príslušnom zariadení. Pri likvidácii zariadení sa musí brať na zreteľ najmä: likvidácia pevných diskov, USB, Flash, CD, DVD, magnetických pások, diskiet.... Za bezpečnú likvidáciu zariadení zodpovedá odbor IT.

Zásady jednotného poskytovania informácií DO:

Poskytovanie informácií DO:

Na základe zákona č. 18/2018 Z. z. je Názov prevádzkovateľa povinná poskytovať DO informácie o stave spracúvania jej OÚ . Právo na poskytnutie informácie DO vzniká na základe písomnej žiadosti. Názov prevádzkovateľa ako prevádzkovateľ IS v zmysle zákona č. 18/2018 Z. z. má podľa tohto zákona povinnosť zabezpečiť primeranú úroveň ochrany OÚ prijatím vhodných technických, personálnych a organizačných opatrení. Z tejto požiadavky vyplývajú určité obmedzenia v použití informačných kanálov, ktorými sa vykonáva komunikácia medzi DO a Názov prevádzkovateľa. Na druhej strane je potrebné snažiť sa maximálne vyjsť v ústrety DO pri poskytovaní informácií., za dodržania všetkých požadovaných bezpečnostných opatrení.
Existujúce komunikačné kanály pre poskytovanie informácií DO:

- telefonická komunikácia.
- elektronická komunikácia emailom.
- komunikácia prostredníctvom faxu.
- písomná komunikácia slovenskou poštou.
- osobná komunikácia.

Pri použití ktoréhokoľvek z vyššie uvedených komunikačných kanálov, je potrebné zabezpečiť nasledovné:

1. presnú identifikáciu žiadateľa. Jeho autenticitu. Preukázateľné zabezpečenie skutočnosti, že žiadosť o poskytnutie informácií je skutočne od DO alebo osoby, ktorá je oprávnená žiadať v mene DO o poskytnutie informácií.
2. nepopierateľnosť odoslania žiadosti, preukázateľné zabezpečenie nemožnosti poprieť skutočnosť, že žiadosť o poskytnutie informácií bola odoslaná DO.

3. zabezpečenie dôvernosti a integrity odosielaných informácií počas ich prenosu k DO.
4. preukázateľné zabezpečenie toho, že informácie boli DO komunikačným kanálom doručené.

Žiadosť o poskytnutie informácií DO:

Na základe zákona č.18/2018 Z. z. má DO právo vyžadovať poskytnutie informácií len na základe písomnej žiadosti. Žiadosť musí obsahovať presnú identifikáciu DO a autorizáciu žiadosti vlastnoručným podpisom.
Názov prevádzkovateľa umožňuje aj iné formy žiadosti o poskytnutie informácií než je písomná forma. Postup pre akceptáciu žiadosti poskytnutej v inej forme ako písomnej a zabezpečenie požiadaviek na bezpečnosť podľa článku 4 tejto BS, je popísaný v nasledujúcich článkoch pri jednotlivých druhoch komunikácie.

Využívanie telefonickej komunikácie na poskytovanie informácií DO:

Prijatie žiadosti.
Pri telefonickej komunikácii je veľmi ťažké zabezpečiť autenticitu DO, ktorá telefonicky žiada o poskytnutie informácie. A to aj napriek tomu, ak osoba na druhej strane linky môže poznať všetky dôležité identifikátory DO.
Z tohto dôvodu nemôže byť na odpoveď použitý telefonicky komunikačný kanál, ale len písomná forma odpovede.
Zamestnanec prijímajúci žiadosť zaeviduje a upozorní DO , že odpoveď dostane iným komunikačným kanálom (slovenská pošta, elektronická pošta) na adresu, ktorú má daná DO zadanú ako komunikačnú. Bezpečnostné opatrenia , ktoré je potrebné dodržať, sú popísané v nasledujúcich článkoch príkazu.

Odosielanie informácií.
DO, ktorej OÚ Názov prevádzkovateľa spracúva je možné poskytovať telefonicky len všeobecné informácie, napr. také, ktoré sú verejne publikované na webovej stránke Názov prevádzkovateľa. Telefonicky je možné poskytovať rady DO. Na tieto úkony nie je potrebná identifikácia klienta (DO).

Využívanie elektronickej komunikácie na poskytovanie informácií DO:

Prijatie žiadosti.
Pri elektronicky zaslanej žiadosti o poskytnutie informácií DO sa riadi pravidlami uvedenými pre telefonickú komunikáciu. Žiadosť možno akceptovať, no odpoveď musí byť zaslaná buď emailom so zabezpečením bezpečnostných požiadaviek alebo v písomnej forme slovenskou poštou na komunikačné adresy DO.

Odosielanie informácií.
DO, ktorej OÚ spracúva Názov prevádzkovateľa je možné poskytovať nezabezpečenou elektronickou poštou len všeobecné informácie, napr. také, ktoré sú verejne publikované na webovej stránke Názov prevádzkovateľa.

Odoslať informácie obsahujúce OÚ DO elektronickou poštou je možné len v prípade, ak využíva ZEP a prevádzkovateľ vlastní jeho verejný kľúč, ktorým môže zašifrovať odosielané informácie, alebo sa použije s DO dohodnutá bezpečná forma šifrovania odosielaných informácií . Informácie sa odosielajú na emailovú adresu, ktorú má DO uvedenú ako komunikačnú. Je zakázané odosielať odpoveď na adresu, z ktorej prišla žiadosť, v prípade že sa nezhoduje s adresou uvedenou ako komunikačná adresa. Heslo alebo dešifrovací kľúč musí byť DO doručený inou cestou , než akou išli odosielané informácie

Využívanie komunikácie prostredníctvom faxu na poskytovanie informácií DO:

Prijatie žiadosti.
Pri faxom zaslanej žiadosti o poskytnutie informácií DO sa riadi pravidlami uvedenými pre telefonickú komunikáciu. Žiadosť možno akceptovať, no odpoveď musí byť zaslaná buď emailom so zabezpečením bezpečnostných požiadaviek, alebo v písomnej forme slovenskou poštou na komunikačné adresy jednotlivých DO.
Odosielanie informácií.
DO, ktorej OÚ spracúva Názov prevádzkovateľa je možné poskytovať nezabezpečenou faxovou komunikáciou len všeobecné informácie, napr. také, ktoré sú verejne publikované na webovej stránke Názov prevádzkovateľa.
Odoslať informácie faxom, ktoré obsahujú OÚ DO je zakázané.

Využívanie písomnej komunikácie (Slovenská pošta) na poskytovanie informácií DO:

Prijatie žiadosti.
Písomnú žiadosť, pokiaľ spĺňa požadované náležitosti na identifikáciu, je možné akceptovať v plnom rozsahu. Informácie je možné odoslať len na komunikačnú adresu DO.

Odosielanie informácií.

Odoslať informácie obsahujúce OÚ DO slovenskou poštou je možné len v prípade, ak je pošta odoslaná do vlastných rúk. Adresa, na ktorú sa informácie odosielajú, musí byť zhodná s adresou uvedenou ako komunikačná adresa.

Využívanie osobnej komunikácie na poskytovanie informácií DO:

Prijatie žiadosti.
Pri osobnej návšteve DO a požadovaní poskytnutia informácií, OO vykoná identifikáciu DO vyžadovaním predloženia preukazu totožnosti a porovnaním identifikátorov ako je meno, priezvisko, dátum narodenia a RČ so záznamom v evidencii DO (Napríklad mzdová a personálna agenda, ...). Ak sa identifikátory zhodujú , OO žiadosť akceptuje a poskytne DO požadované informácie.

Odosielanie informácií.
Informácia požadovaná DO pri osobnej návšteve môže byť poskytnutá ústnou formou, alebo na požiadanie DO aj písomnou formou.

Vytváranie záznamov súvisiacich s poskytovaním informácií DO:

OO, ktoré prijímajú a vybavujú žiadosti DO sú povinné vykonávať záznam o prijatí žiadosti a poskytnutí informácií DO. Záznamy sa vedú v elektronickej forme. Záznam obsahuje informáciu o dátume prijatia žiadosti, dátume poskytnutia informácií, komunikačnom kanále, ktorým bola prijatá žiadosť, komunikačnom kanále, ktorým boli OÚ odoslané DO, identifikácia OO, ktorá žiadosť prijala, identifikácia OO, ktorá žiadosť splnila.

Komunikácia s treťou stranou:

V prípade, ak OO zasiela OÚ DO tretej strane (napríklad jedná sa o poskytovanie OÚ) je OO povinná zabezpečiť primeranú úroveň dôvernosti zasielaných OÚ. Musí zabezpečiť ochranu OÚ počas prenosu vhodnou formou šifrovania a musí zabezpečiť dôvernosť OÚ doručením OÚ len OO tretej strany. Za výber vhodnej formy šifrovania zodpovedá odbor IT.

Riadenie prístupu:

1. Od užívateľov sa musí vyžadovať, aby zabezpečili primeranú ochranu nestrážených prostriedkov.

2. Užívatelia musia mať prístup len k prostriedkom, na ktorých používanie boli autorizovaní.

3. K zabráneniu neautorizovaného spustenia PC, na ktorých sa spracúvajú OÚ, musí byť operačný systém nastavený tak, aby jeho spustenie nebolo možné bez zadania prístupového mena a hesla užívateľa (vytvoriť užívateľské konto, prípadne kontá, ak má byť viac užívateľov).

4. K zabráneniu neautorizovaného spustenia aplikácie spracúvajúcej OÚ je treba systém tejto aplikácie nastaviť tak, aby jej spustenie nebolo možné bez zadania prístupového mena a hesla užívateľa (vytvoriť užívateľské konto, prípadne kontá, ak má byť viac užívateľov).

5. V systéme aplikácii spracúvajúcich OÚ je potrebné (ak to aplikácia umožňuje) nastaviť pravidlá pre blokovanie užívateľského konta (po niekoľkonásobnom zadaní chybného hesla); nastaviť možnosť informovania užívateľa pri jeho prihlásení o pokusoch o neoprávnené vniknutie do aplikácie.

6. K zamedzeniu neoprávneného prístupu k aplikáciám musia byť stanovené záväzné pravidlá pre tvorbu silných hesiel, v každom prípade identifikácie a autentizácie užívateľov.

7. Registrácia a deregistrácia užívateľov IS sa u prevádzkovateľa riadi samostatným pracovným postupom. Postup musí zabezpečiť jednoznačnú identifikáciu každého užívateľa (každý užívateľ má jednoznačný a jedinečný identifikátor). Postup musí ďalej zabezpečiť dôvernosť užívateľských hesiel tak , aby si užívatelia nepoznali navzájom heslá. Heslá užívateľov nesmie poznať ani administrátor systému).

8. Zodpovednosť za prezradenie hesla nesú užívatelia.

Všeobecné opatrenia

1. K zabezpečeniu dodržiavania požiarnych predpisov a predpisov BOZP neustále aktualizovať dokumentáciu dodržiavania predpisov PO a BOZP.

2. Pre minimalizovanie možností neoprávneného šírenia dát, neautorizovaného používania softvéru, prípadne inej neoprávnenej manipulácie s dátami treba odstrániť, prípadne softvérovo zablokovať používanie zapisovacích médií (disketové mechaniky, CD RW mechaniky, USB kľúče), ktoré nie sú nutné pre výkon práce .

3. V zmysle zákona č. 395/2002 Z. z. o archívoch a registratúrach v znení neskorších predpisov musí byť vypracovaný registratúrny poriadok a plán. Z neho vyplývajúce úlohy a opatrenia je potrebné zaviesť neodkladne do praxe - najmä zabezpečenie, aby sa IS s OÚ v písomnej podobe zabezpečil proti požiaru a iným degradačným vplyvom (v zmysle vyhlášky č. 628/2002 Z. z.), a aby sa zabránilo neoprávnenému prístupu k IS v podobe dokumentov s OÚ.

4. K zabráneniu neautorizovaného prístupu k zasielaným správam používať šifrovanie komunikácie v prípadoch, keď predmetom komunikácie sú OÚ.

5. Všetky citlivé aplikácie musia vyžadovať autentizáciu užívateľa pri spúšťaní aplikácie.

6. U prevádzkovateľa je zakázané používať fax na prenos OÚ.

7. K odstráneniu, alebo minimalizovaniu rizika odpočúvania, alebo neoprávneného prístupu k dátam, je zakázané poskytovanie a sprístupňovanie OÚ o inej osobe cez telefón.

8. **Zoznam IS (agiend) a účelov spracúvania:** Poverená zodpovedná osoba vedie zoznam jednotlivých IS, v ktorých prevádzkovateľ spracúva OÚ za konkrétnym účelom spracúvania osobných údajov fyzických osôb

9. **Zmluvy so sprostredkovateľmi:** V prípade zmlúv, na základe ktorých sú externe dodávané služby, pričom zamestnanci dodávateľa majú, alebo môžu mať prístup k OÚ spracúvaných prevádzkovateľom, alebo tretia strana je priamo poverená spracúvaním OÚ, je potrebné spracúvať dodatky týchto zmlúv s cieľom upraviť práva a povinnosti v súvislosti s OOÚ. Zmluva musí spĺňať zákonom stanovené náležitosti a musí obsahovať články, v ktorých sa dodávateľ zaväzuje plniť ustanovenia zákona č.18/2018 Z. z., berie na seba povinnosť vykonať poučenie osôb, ktoré môžu prísť pri výkone svojej činnosti do styku s OÚ prevádzkovateľa a berie na seba prípadnú zodpovednosť za porušenie zákona svojimi zamestnancami pri výkone činnosti vyplývajúcich zo zmluvného vzťahu.

10. **Údržba HW a SW:** Musí byť zabezpečené vykonávanie preventívnej údržby hardvéru a softvéru v plánovaných intervaloch, podľa vopred určeného harmonogramu. Plán preventívnej údržby musí byť súčasťou IT dokumentácie a musí obsahovať presné termíny a popis jednotlivých činností a zodpovedností za ich vykonanie (napr. kontrola funkčnosti záložných zdrojov napájania a stavu ich akumulátorov....). Za implementáciu opatrenia zodpovedá sekcia informatiky.

11. **Servis HW a SW:** Na správu a servis hardvéru a softvéru musí byť vybratá vhodná organizácia, s ktorou sa uzavrie písomná zmluva o spolupráci tak, aby bola zabezpečená technická podpora pre všetky systémy prevádzkovateľa v prípade výskytu problémov technického rázu alebo potreby rozšírenia systémov. Pri servise (opravách zariadení) je potrebné zabezpečiť, aby pri výkone servisných činností nemohlo dôjsť k strate informácií z IS obsahujúcich OÚ. Zariadenia, na ktorých sa nachádzajú citlivé OÚ nesmú opustiť priestor prevádzkovateľa. Za dodržiavanie zodpovedá sekcia informatiky.

12. **Získavanie OÚ:** Spôsob a forma získavania OÚ Musí byť zdokumentovaná a popísaná v pracovných manuáloch. Za vypracovanie manuálov zodpovedajú správcovia jednotlivých IS, uvedení v bezpečnostnom projekte, časti popisujúcej IS.

13. **Všeobecné pravidlá pri získavaní OÚ:** Pri získavaní OÚ od DO **je zakázané** získavať OÚ kopírovaním osobných dokladov bez súhlasu DO. Toto je dovolené len s písomným súhlasom DO, alebo ak to dovoľuje, alebo prikazuje osobitný zákon. Ďalej je zakázané získavať od DO OÚ, ktoré nie sú nevyhnutne potrebné k dosiahnutiu účelu spracúvania a teda nie sú vymedzené v dokumentácii príslušného IS(agendy) podľa definovaného účelu spracúvania.. Pred samotným získaním OÚ OO oznámi DO nasledovné náležitosti:

    a. názov a sídlo prevádzkovateľa IS;
    b. názov a sídlo sprostredkovateľa (ak bol poverený spracúvaním OÚ);
    c. zodpovednú osobu;
    d. účel spracúvania OÚ;
    e. zákon, ktorý poskytnutie OÚ vyžaduje, ak nie sú získavané na základe súhlasu DO. Ak sú OÚ spracúvané na základe súhlasu DO treba túto skutočnosť oznámiť DO a požiadať ju o písomný súhlas;
    f. vykoná poučenie DO o jej právach, ktoré sú nasledovné;

DO má právo od prevádzkovateľa požadovať:
- informácie o stave spracúvania jej OÚ v IS,
- presné informácie o zdroji, z ktorého získal jej OÚ na spracúvanie,
- odpis jej OÚ, ktoré spracúva v IS,
- opravu nesprávnych, neúplných alebo neaktuálnych OÚ, ktoré sú predmetom spracúvania,
- likvidáciu jej OÚ, ak bol splnený účel spracúvania; ak sú predmetom spracúvania úradné doklady obsahujúce OÚ, môžete požiadať o ich vrátenie,
- likvidáciu jej OÚ, ktoré sú predmetom spracúvania, ak došlo k porušeniu zákona č. 18/2018 Z. z. o OOÚ, zo strany prevádzkovateľa.

14. **Súhlas DO:** Pre IS, v ktorých sú OÚ spracúvané na základe súhlasu DO, príslušná OO zabezpečí získanie súhlasu od DO. Súhlas DO musí obsahovať nasledovné náležitosti:
    a. kto súhlas dáva;
    b. komu sa súhlas dáva;
    c. na aký účel spracúvania OÚ alebo dokladu je súhlas daný;
    d. na aké OÚ sa súhlas dáva;
    e. na akú dobu je súhlas vydaný;
    f. podmienky odvolania súhlasu;
    g. súhlas musí byť v písomnej forme a osobne podpísaný DO;
    h. v prípade emailu musí byť súhlas podpísaný elektronickým podpisom.

    Vzor súhlasu je obsahom bezpečnostnej dokumentácie

15. **Poskytnutie OÚ je dobrovoľné, súhlas si nemožno vynucovať odmietnutím poskytnutia nejakej služby, iba v prípade, kedy poskytnutie údajov vyžaduje zákon.**

16. V prípade, že do organizácie príde email obsahujúci OÚ a na ich spracúvanie sa vyžaduje súhlas DO, musí byť z počítača spoľahlivým spôsobom zlikvidovaný a odosielateľ musí byť o tom informovaný. Pod spoľahlivým spôsobom sa rozumie taká likvidácia, aby OÚ obsiahnuté v emailoch už nebolo možné zrekonštruovať.

17. V prípade, že príde do organizácie listová zásielka obsahujúca OÚ, na ktorých spracúvanie sa vyžaduje súhlas DO a zásielka nebude obsahovať požadovaný súhlas DO, musí byť obratom od odosielateľa vyžiadaný príslušný súhlas na spracúvanie OÚ obsiahnutých v listovej zásielke. Ak DO v stanovenom termíne príslušný súhlas neposkytne, nebudú jej OÚ spracúvané.

18. Kopírka a fax musia byť v mimopracovnom čase uzamknuté alebo iným vhodným spôsobom chránené pred neautorizovaným prístupom.

Likvidácia OÚ

1. V prípade ukončenia účelu spracúvania OÚ musí byť zabezpečená ich bezodkladná likvidácia bezpečným spôsobom (za predpokladu, že iný zákon neustanovuje iné podmienky). Likvidácia musí byť prevedená na písomných dokumentoch ale aj na všetkých počítačových médiách (pevné disky, DVD, CD, USB kľúče, diskety....). Za účelom dodržiavania likvidácie OÚ musí byť zdokumentovaný proces monitorovania IS za účelom identifikovania OÚ, ktoré treba zlikvidovať. Za bezpečnú likvidáciu zodpovedá „Zodpovedná osoba" a jednotlivé OO.

2. **Oznámenie o likvidácii OÚ:** DO musia byť vhodnou formou oboznámené o likvidácii ich OÚ. Napríklad elektronickou poštou.

3. **Likvidácia dokumentov:** Likvidácia dokumentov obsahujúcich OÚ musí byť prevádzaná výlučne skartovaním. Zakazuje sa odkladať nepotrebné dokumenty obsahujúce OÚ akýmkoľvek spôsobom (zberné suroviny, kôš, opätovné použitie čistej strany na tlač...).

4. **Likvidácia pamäťových médií:** Likvidácia pamäťových médií, na ktorých sa nachádzajú OÚ, musí byť prevádzaná fyzickým zničením nosičov dát.

Bezpečnostné incidenty

Nahlasovanie BI:

Všetci zamestnanci prevádzkovateľa aj tretích strán, majú povinnosť nahlasovať BI, ktoré sa vyskytnú počas ich práce. **BI sa nahlasujú „Zodpovednej osobe".** Zodpovedná osoba je povinná viesť databázu incidentov a zabezpečuje realizáciu mechanizmu poučenia sa z BI. „Zodpovedná osoba" musí zabezpečiť nasledovné:

a. zadefinovať dovolené spôsoby nahlasovania BI,
b. oboznámenie zamestnancov s definíciou, čo to BI je,
c. stanoviť klasifikačnú stupnicu BI a zabezpečiť ich klasifikáciu podľa stanovenej stupnice,
d. vedenie databázy incidentov s informáciami o tom, kto incident nahlásil, popis incidentu, jeho klasifikácia, dátum a čas nahlásenia, kto bude incident riešiť, kedy boli vykonané aké úkony, ako a kedy bol incident vyriešený.
e. spätnú odozvu pre zamestnancov, ktorí BI nahlásili, ako sa problém rieši a prehľadný prístup k jednotlivým informáciám.
f. Nahlásenie BI Úradu a všetkým DO, ktorých sa BI týka do 72 hodín od zistenia BI

Porušenie BS: Porušenie BS zo strany zamestnancov musí byť riešené disciplinárnym procesom. Za realizáciu zodpovedá personálny odbor.

Na záver potvrdenie platnosti základnej zásady ochrany citlivých aktív

S výnimkou povolených činností oprávnených osôb prevádzkovateľa a jeho sprostredkovateľov sú všetky ostatné spracovateľské operácie a činnosti súvisiace so spracúvaním osobných údajov

Z A K Á Z A N É !

Oznámenie prevádzkovateľa o poverení zodpovednej osoby výkonom dohľadu nad ochranou osobných údajov

podľa § 44 ods. 8 zákona č. 18/2018 Z. z.
o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

Identifikačné údaje prevádzkovateľa

Identifikačné číslo organizácie (IČO)
42274885

Názov prevádzkovateľa (obchodné meno)
Oblastná organizácia cestovného ruchu Trenčianske Teplice

PSČ 914 51 **Obec** Trenčianske Teplice

Ulica M. R. Štefánika **číslo** 4

Právna forma
119 Nezisková organizácia

Zodpovedná osoba

Priezvisko VÁCLAV **Meno** Roman

Titul LL.M. **Dátum narodenia** 15.08.1971

Deň, kedy sa fyzická osoba stala zodpovednou osobou
01.04.2017

Číslo potvrdenia o absolvovaní skúšky 056/2016 **Dátum vydania potvrdenia** 02.03.2016

Svojím podpisom potvrdzujem, že poverenie výkonom funkcie zodpovednej osoby prijímam.

Roman VÁC
Tel.: 091(
roman@

.....
Zodpovedná osoba – Roman Václav

Prevádzkovateľ vyhlasuje, že zodpovedná osoba spĺňa predpoklady podľa zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

Oblastná organizácia cestovného ruchu
Trenčianske Teplice
M.R. Štefánika 4
914 51 Trenčianske Teplice
IČO: 42274885

.....
Odtlačok pečiatky prevádzkovateľa

.....
Dátum, meno a podpis štatutárneho orgánu