Mesto Gabčíkovo

Mestský úrad Gabčíkovo, 930 05 Gabčíkovo, Hlavná č. 1039/21
IČO: 0030539100

Bezpečnostná politika na zabezpečenie ochrany osobných údajov

Smernica
na technické a organizačné opatrenia
na zabezpečenie ochrany osobných údajov

V Gabčíkove, dňa 25.5.2018

PhDr. Iván Fenes LL.M, MBA
primátor mesta

Smernica je spracovaná na základe Nariadenia Európskeho parlamentu a Rady č. 2016/679 (ďalej „GDPR") a zákona č. 18/2018 Z. z. o ochrane osobných údajov a ďalších štandardov a predpisov

Identifikácia informačných systémov (IS), v ktorých sa spracovávajú osobné údaje:

- IS správa registratúry
- IS hospodárska mobilizácia
- IS prístup k informáciám
- IS protispoločenská činnosť
- IS správne konanie
- IS súdne spory
- IS zverejňovanie zmlúv a objednávok
- IS účtovné doklady
- IS pedagogická dokumentácia
- IS školská jedáleň
- IS opatrovateľská činnosť, zdravotná dokumentácia
- IS mzdy a personalistika
- IS evidencia obyvateľstva
- IS dane a poplatky
- IS prevádzkovanie cintorína
- IS evidencia SHR
- IS matrika
- IS sociálna agenda
- IS overovanie podpisov
- IS pomoc v hmotnej núdzi
- IS stavebný úrad
- IS kataster
- IS kamerový systém
- IS propagácia
- IS záznam o činnostiach spracovania volieb
- IS zásady používania súborov COOKIES

OBSAH SMERNICE

Použité označenia:

BOZP	bezpečnosť a ochrana zdravia pri práci
CD	prenosný disk
DVD	prenosný disk
FaOB	fyzická a objektová bezpečnosť
HDD	pevný disk
HW	hardvér
CHP	chránený priestor
IS	informačný systém
LAN	lokálna počítačová sieť
MZP	mechanické zábranné prostriedky
PC	počítač (aj prenosné)
SW	Software (programy)
TP	technický prostriedok
TZP	technické zabezpečovacie prostriedky
WAN	počítačová sieť (internet)

Mesto Gabčíkovo so sídlom: Mestský úrad Gabčíkovo, Hlavná č. 1039/21, 930 05, IČO: 0030539100 (ďalej „prevádzkovateľ"), na zabezpečenie postupu spracovania osobných údajov dotknutých osôb na základe § 19 a § 20 Zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „zákon“) a čl. 13 a 14 Nariadenia Európskeho parlamentu a rady (ďalej „GDPR") 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (ďalej len „nariadenie“) a ďalších predpisov, s ohľadom na povahu, rozsah, a účel spracúvania osobných údajov a na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva fyzickej osoby ustanovuje túto smernicu.

ZÁKLADNÉ USTANOVENIA

Účel a určenie smernice

1. Účelom smernice je ustanovenie technických a organizačných opatrení na zabezpečenie ochrany osobných údajov u prevádzkovateľa podľa § 29, 30, 31, 32, 39, 42, 78 ods. 11 zákona.
2. Pre zabezpečenie ochrany osobných údajov prevádzkovateľ sa schváli túto smernicu a nesledujúce interné smernice (ďalej „interné smernice"):
- Bezpečnostná analýza rizík pri spracovaní ochrany osobných údajov podľa § 32 ods. 2, 39 ods. 2 zákona - informačné technológie.
- Bezpečnostná politika podľa zákona, vyhlášky Národného bezpečnostného úradu č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti v znení neskorších predpisov, vyhláška Národného bezpečnostného úradu č. 339/2004 Z. z. o bezpečnosti technických prostriedkov - informačné technológie.
- Spracovateľské činnosti prevádzkovateľa.
- Smernica o vyšetrovaní bezpečnostných incidentov.
- Smernica o rozsahu oprávnení a povolených činností.
- Smernica na poskytovanie informácií, záznamy spracovateľských činnostiach a práva dotknutých osôb pri spracovaní osobných údajov.

3. Táto smernica a interné smernice sú určené pre prevádzkovateľa a oprávnené osoby prevádzkovateľa, ktorým bol vydaný pokyn alebo poverenie na spracovávanie osobných údajov na základe rozsahu a povolených činnosti, a ktoré sú povinné ju držiavať.
4. Smernica sa primerane týka aj neoprávnených osôb, ktoré v prípade ak sa aj náhodne oboznámia s osobnými údajmi. V takomto prípade sú povinné rovnako zachovávať zachovať mlčanlivosť a pravidlá ochrany osobných údajov.

Vymedzenie niektorých pojmov

1. Na účely tejto smernice sa rozumie:
a) **súhlasom dotknutej osoby** 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,
b) **genetickými údajmi** sú osobné 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,
c) **biometrickými údajmi** 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,

d) **údajmi týkajúcimi 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 ojej zdravotnom stave,
e) **spracúvanie osobných údajov** znamená spracovateľská operácia alebo súbor spracovateľských operácií s osobnými údajmi alebo súbormi osobných údajov, najmä získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, 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,
f) **obmedzením spracúvania osobných údajov** je označenie uchovávaných osobných údajov s cieľom obmedziť ich spracúvanie v budúcnosti,
g) **oprávnená osoba** je osoba, ktorej podľa tejto smernice bol vydaný pokyn alebo bola poverená spracúvaním osobných údajov, a ktorá je povinná dodržiavať príslušné technické a organizačné opatrenia uložené touto a iným internými smernicami prevádzkovateľa.
h) **neoprávnená osoba** je osoba, ktorá nebola poverená k spracovaniu osobných údajov. Za neoprávnenú osobu podľa tejto smernice sa považuje aj oprávnená osoba, ktorá nemá určený prístup k osobným údajom, podľa osobitnej smernice, s ktorými sa náhodne alebo zámerne oboznámila.
i) **profilovaním** 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,
j) **pseudonymizáciou** 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 osoby alebo identifikovateľnej fyzickej osobe,
k) **logom** je záznam o priebehu činnosti používateľa v automatizovanom informačnom systéme,
l) **šifrovaním** je transformácia osobných údajov spôsobom, ktorým opätovné spracúvanie je možné len po zadaní zvoleného parametra ako je kľúč alebo heslo,
m) **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,
n) **informačným systémom** 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,
o) **porušením ochrany osobných údajov** je porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene alebo neoprávnenému poskytnutiu prenášaných, uchovávaných osobných údajov alebo inak spracúvaných osobných údajov, alebo k neoprávnenému prístupu k nim,
p) **dotknutou osobou** je každá fyzická osoba, ktorej osobné údaje sa spracúvajú,
q) **prevádzkovateľom** 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 tento predpis alebo táto zmluva ustanovuje účel a prostriedky spracúvania osobných,
r) **sprostredkovateľom** je každý, kto spracúva osobné údaje v mene prevádzkovateľa,
s) **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,
t) **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,
u) **zodpovednou osobou** je osoba určená prevádzkovateľom alebo sprostredkovateľom, ktorá plní úlohy podľa tohto zákona,
v) **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 § 34 zákona,
w) **podnikom** je fyzická osoba - podnikateľ alebo právnická osoba vykonávajúca hospodársku činnosť bez ohľadu na jej právnu formu, vrátane združení fyzických osôb alebo združení právnických osôb, ktoré pravidelne vykonávajú hospodársku činnosť,
x) **skupinou podnikov** je ovládajúci, ktorý podniká ním ovládané podniky,
y) **hlavnou prevádzkarňou sú:**
1. miesto centrálnej správy prevádzkovateľa v Európskej únii, ak ide o prevádzkovateľa s prevádzkarňami vo viac než jednom členskom štáte, okrem prípadu, keď sa rozhodnutia o účeloch a prostriedkoch spracúvania osobných údajov prijímajú v inej prevádzkarni prevádzkovateľa v Európskej únii a táto iná prevádzka má právomoc presadiť vykonanie takýchto rozhodnutí, pričom v takom prípade sa za hlavnú prevádzkareň považuje prevádzkareň, ktorá takéto rozhodnutia prijala,
2. miesto centrálnej správy sprostredkovateľa v Európskej únii, ak ide o sprostredkovateľa s prevádzkarňami vo viac než jednom členskom štáte alebo ak sprostredkovateľ nemá centrálnu správu v Európskej únii, prevádzkareň sprostredkovateľa v Európskej únii, v ktorej sa v kontexte činností prevádzkarne sprostredkovateľa uskutočňujú hlavné spracovateľské činnosti, a to v rozsahu, v akom sa na sprostredkovateľa vzťahujú osobitné povinnosti podľa tohto zákona,
z) **medzinárodnou organizáciou** je organizácia a jej podriadené subjekty, ktoré sa riadia medzinárodným právom verejným, alebo akýkoľvek iný subjekt, ktorý bol zriadený dohodou medzi dvoma alebo viacerými krajinami alebo na základe takejto dohody,
aa) **členským štátom** je štát, ktorý je členským štátom Európskej únie alebo zmluvnou stranou Dohody o Európskom hospodárskom priestore,
ab) **treťou krajinou** je krajina, ktorá nie je členským štátom EU.

POPIS TECHNICKÝCH, ORGANIZAČNÝCH A PERSONÁLNYCH OPATRENÍ A SPÔSOB ICH UPLATŇOVANIA V KONKRÉTNYCH PODMIENKACH

1. Prevádzkovateľ vymedzuje v súlade so zákonom účel, prostriedky spracúvania osobných údajov a informačné systémy. Prevádzkovateľ je prevádzkovateľom nasledujúcich informačných systémov, podľa zákona:

- IS správa registratúry
- IS hospodárska mobilizácia
- IS prístup k informáciám
- IS protispoločenská činnosť
- IS správne konanie
- IS súdne spory
- IS zverejňovanie zmlúv a objednávok
- IS účtovné doklady
- IS pedagogická dokumentácia
- IS školská jedáleň
- IS opatrovateľská činnosť, zdravotná dokumentácia

- IS mzdy a personalistika
- IS evidencia obyvateľstva
- IS dane a poplatky
- IS prevádzkovanie cintorína
- IS evidencia SHR
- IS matrika
- IS sociálna agenda
- IS overovanie podpisov
- IS pomoc v hmotnej núdzi
- IS stavebný úrad
- IS kataster
- IS kamerový systém
- IS propagácia
- IS záznam o činnostiach spracovania volieb
- IS zásady používania súborov COOKIES.

2. Každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi, v informačných systémoch prevádzkovateľa, v rámci svojho pracovného pomeru alebo na základe iného zmluvného vzťahu (ďalej „oprávnená osoba") resp. poverenia, musí byť pred prvým spracovávaním poučená v rozsahu tejto smernice..
3. Zabezpečenie poučenia zabezpečuje zodpovedná osoba a poučená oprávnená osoba podpíše pokyn, rovnako ako osoba ktorá vykonala poučenie. Poučenie sa vykonáva pred prvým spracovávaním osobných údajov. Zodpovedná osoba ustanoví rozsah oprávnení a povolených činností, prístup do chráneného priestoru a IS, v ktorom sa spracúvajú osobné údaje. Bezpečnostný správca následne nastaví príslušné prístupy k schváleným IS a CHP.
4. V prípade zrušenia pracovného pomeru, poverenia alebo iného zmluvného vzťahu oprávnenej osoby, zodpovedná osoba neodkladne informuje bezpečnostného správcu a správcu objektu o tejto skutočnosti, ktorý okamžite zablokujú prístup do IS a chráneného priestoru a vykonajú ďalšie opatrenia podľa rozsahu oprávnení a povolených činností.
5. Dotknutou osobou je každá fyzická osoba, o ktorej sa spracúvajú osobné údaje v jednotlivých IS.

Vymedzenie účelu spracúvania osobných údajov

1. Prevádzkovateľ spracúva osobné údaje dotknutých osôb za účelom a prostriedkami určenými v súlade so zákonmi a osobitnými predpismi.
2. Je neprípustné získavať a spracovávať osobné údaje v inom rozsahu a za iným účelom, než je stanovené v tejto smernici a iných interných predpisov prevádzkovateľa.
3. Oprávnené osoby spracovávajú osobné údaje v rozsahu a podľa oprávnení a povolených operácií, ustanovených v smernici - Rozsah oprávnení a povolených činností.
4. Účel, právny základ a rozsah spracovania osobných údajov v jednotlivých informačných systémoch je uvedený v Zozname osobných údajov.
5. Prevádzkovateľ spracúva osobné údaje samostatne ako prevádzkovateľ (sprostredkovateľ). Typické procesy spracúvania osobných údajov u prevádzkovateľa sú identifikované v tabuľke č.2.

Tabuľka č. 2.

Proces	**Kto vykonáva (komu sa poskytuje, sprístupňuje, poskytuje)**	**Poznámka**
Spracúvanie osobných údajov	Oprávnené osoby	Získavanie, zhromažďovanie, zaznamenávanie, usporadúvanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, premiestňovanie, využívanie, uchovávanie, likvidáciu, prenos, poskytovanie alebo sprístupňovanie
Likvidácia osobných údajov	**Oprávnené osoby, správca IT (ďalej len bezpečnostný správca)** Bežný proces spracúvania vykonávaný oprávnenými osobami na základe bezpečnostnej smernice po splnení účelu spracúvania Vykonávajú: oprávnené osoby	Vykonáva sa na zariadení pre likvidáciu nosičov informácií podľa lehoty uloženia dokumentov, záznamov, pamäťových médií, ktoré obsahujú osobné údaje

Tabuľka č. 3

Proces	**Kto vykonáva (komu sa poskytuje, sprístupňuje)**	**Poznámka**
Zverejňovanie osobných údajov	Zverejňujú sa osobné údaje na nástenkách, časopise prevádzkovateľa, web stránky prevádzkovateľa, kniha, intranet, facebook, nástenky na základe súhlasu dotknutých osôb v rozsahu: meno, priezvisko, pracovné zaradenie, fotografia. - Zverejňujú sa osobné údaje podľa § 78 ods. 3 zákona	Zverejňovanie osobných údajov dotknutých osôb - zamestnancov prevádzkovateľa v rozsahu titul, meno, priezvisko, pracovné zaradenie, odborný útvar, miesto výkonu práce, telefónne číslo, faxové číslo, emailová adresa a identifikačné údaje zamestnávateľa

Povinnosti, zodpovednosť a právomoci pri spracovávaní osobných údajov			
P.č.	**Oprávnená osoba**	**Povinnosti pri spracovaní osobných údajov**	**Právomoci pri spracovaní osobných údajov**
1	Poučená oprávnená osoba	Zachovávanie mlčanlivosti podľa zákona, dodržiavanie bezpečnostných smerníc	Spracovanie osobných údajov podľa povolenia, oboznamovanie sa s príslušnými osobnými údajmi podľa schválených prístupových práv
2	Bezpečnostný správca (privilegovaná oprávnená osoba)	Zachovávanie mlčanlivosti podľa zákona, dodržiavanie bezpečnostných smerníc	Zabezpečenie ochrany IS, bezpečnostný manažment IS, nastavovanie prístupových práv k adresárom, identifikácie resp. autentizácie privilegovaných oprávnených osôb a oprávnených osôb, archivácia osobných dát, vykonávanie a kontrola bezpečnostných opatrení v automatizovanom IS, prijímania opatrení na zamedzenie vzniku bezpečnostných incidentov, prijímanie opatrení na obnovu činnosti IS v prípade vzniku bezpečnostných incidentov, vyšetrovanie bezpečnostných incidentov podľa bezpečnostných smerníc
3	Štatutárny orgán	Zachovávanie mlčanlivosti podľa zákona, dodržiavanie interných bezpečnostných smerníc týkajúcich sa ochrany osobných údajov	Schvaľovanie prístupových práv do IS, príslušných adresárov, riadenie vyšetrovania bezpečnostných incidentov a prijímania opatrení na zamedzenie vzniku bezpečnostných incidentov, kontrolná činnosť pri ochrane osobných údajov, schvaľovanie bezpečnostnej dokumentácie (smerníc), kontrol na zabezpečenie ochrany osobných údajov, poverovanie bezpečnostného správcu, vyvodzovanie dôsledkov v súlade so zákonníkom práce pri riešení bezpečnostných incidentov
4	Zodpovedná osoba		Poskytuje informácie a poradenstvo prevádzkovateľovi a zamestnancom, ktorí vykonávajú spracúvanie osobných údajov, o ich povinnostiach podľa tohto zákona, osobitných predpisov alebo medzinárodných zmlúv, ktorými je Slovenská republika viazaná, týkajúcich sa ochrany osobných údajov. Monitoruje súlad s týmto zákonom, osobitnými predpismi alebo medzinárodnými zmluvami, ktorými je Slovenská republika viazaná, týkajúcimi sa ochrany osobných údajov a s pravidlami prevádzkovateľa súvisiacimi s ochranou osobných údajov vrátane rozdelenia povinností, zvyšovania povedomia a odbornej prípravy osôb, ktoré sú zapojené do spracovateľských operácií a súvisiacich auditov ochrany osobných údajov. Poskytuje na požiadanie poradenstvo, ak ide o posúdenie vplyvu na ochranu osobných údajov a monitorovanie jeho vykonávania podľa § 42 zákona.

			Spolupracuje s úradom pri plnení svojich úloh. Plní úlohy kontaktného miesta pre úrad v súvislosti s otázkami týkajúcimi na spracúvania osobných údajov vrátane predchádzajúcej konzultácie podľa § 43 zákona, podľa potreby aj konzultácie v iných veciach. Plní ďalšie povinnosti pri ochrane osobných údajov uložených internými smernicami prevádzkovateľa. Zachováva mlčanlivosť podľa zákona, dodržiava bezpečnostné smernice, výkon dohľadu nad ochranou osobných údajov podľa zákona. Posudzuje, či spracúvaním nevzniká nebezpečenstvo narušenia práv a slobôd dotknutých osôb. Zodpovedná osoba, pokiaľ nie je štatutárnym orgánom určené inak, zabezpečuje vykonávanie kontrolnej činnosti a vedenie dokumentácie podľa tejto smernice a interných predpisov prevádzkovateľa.

Tabuľka č. 4

Prostriedky a spôsob spracúvania osobných údajov

1. Osobné údaje je možné spracúvať len oprávnenými osobami a to len osobné údaje správne, úplné a podľa potreby aktualizované vo vzťahu k účelu spracúvania. Osobné údaje je možné spracúvať len v priestoroch určených na tento účel (ďalej „chránené priestory" - „CHP") a v IS, ktoré sú umiestnené v CHP a zabezpečené na tento účel.
2. Informácie podľa § 19, 21 zákona musia byť poskytnuté dotknutej osobe pri ich získavaní. Dostupnosť zabezpečuje príslušná oprávnená osoba alebo zodpovedná osoba.
3. Dotknutá oprávnená osoba bez zbytočného odkladu zlikviduje tie osobné údaje, ktorých účel spracúvania sa skončil. Nevykonáva sa likvidácia tých údajov, ktoré je potrebné archivovať v súlade so zákonom č. 395/2002 Z. z. o archívoch a registratúrach v znení neskorších predpisov a registratúrnym plánom a smernicou - lehoty uloženia dokumentov, záznamov, pamäťových médií, ktoré obsahujú s osobné údaje.
4. Likvidácia sa vykonáva spôsobom, ktorý zabezpečí ich bezpečnú skartáciu tak, aby ani náhodným spôsobom nedošlo k zneužitiu, úniku, prezradeniu alebo k inému spôsobu straty dôvernosti. Za bezpečnú likvidáciu sa považuje likvidácia písomností alebo pamäťových nosičov na zariadení pre fyzickú likvidáciu nosičov informácií alebo ich spálením, prípadne likvidácia iným bezpečným spôsobom. Za likvidáciu dátových nosičov informácií (napr. CD, DVD, USB, HDD) zodpovedá bezpečnostný správca.
5. Likvidácia príslušných osobných údajov sa vykonáva príslušnou oprávnenou osobou, bez zbytočného odkladu, po skončení účelu spracovávania.

Organizačné (režimové) opatrenia

1. Osobné údaje, ktoré majú charakter písomnosti, hmotného nosiča informácií sa v pracovnej i v mimopracovnej dobe ukladajú do úschovných objektov, určených na tento účel, umiestnených v príslušnom CHP. Za ukladanie týchto osobných údajov zodpovedá príslušná oprávnená osoba.

2. Osobné údaje je možné poskytovať len príslušným oprávneným osobám spôsobom, ktorým nemožno narušiť dôvernosť osobných údajov, pričom je zakázané poskytovať osobné údaje telefonicky alebo e-mailom bez šifrovania alebo anonymizácie údajov.
3. Šifrovanie sa vykonáva prostredníctvom šifrovacieho režimu nastaveného v rámci poštovej aplikácie alebo prostredníctvom špeciálneho programu, podľa návodu od výrobcu.
4. Všetky návštevy vstupujúce do CHP sú prijímané a sprevádzané priamo navštívenou oprávnenou osobou.
5. Oprávnená osoba zabezpečí, že návšteva alebo stránka sa ani náhodne neoboznámi s osobnými údajmi iných dotknutých osôb. Za týmto účelom sa vybavujú dotknuté osoby (stránky) jednotlivo pri dodržaní diskrétnej zóny.
6. Oprávnená osoba je povinná po skončení práce alebo pracovnej doby, t. j. pred odchodom z CHP vypnúť elektrické spotrebiče, presvedčiť sa o uzatvorení okien, uzatvorení prívodu vody, uložiť dokumenty s osobnými údajmi do určeného priestoru alebo úschovného objektu v CHP, ktorý sa po skončení pracovnej doby uzamkne, vypnúť technický prostriedok informačného systému. Posledná odchádzajúca oprávnená osoba (po kontrole priestorov) uzamyká priestory CHP a objektu.
7. Kopírovanie úradných dokumentov (ďalej „kópie") s osobnými údajmi môže vykonávať len príslušná oprávnená osoba na základe súhlasu dotknutej osoby a spracúvajú sa len po dobu potrebnú na splnenie účelu spracúvania (Neodkladne ako sú údaje vložené do príslušného automatizovaného informačného systému sa kópie zlikvidujú).
8. Ak dokumenty s osobnými údajmi prenáša osoba, ktorá nie je oprávnenou osobou, musia byť tieto zabezpečené tak, aby táto osoba nemala prístup k obsahu osobných údajov. V tomto prípade musí dať súhlas na takéto prenášanie zodpovedná osoba, ktorá vyhodnotí riziko ohrozenia osobných údajov a vydá pokyny na zabezpečenie ochrany prenášaných osobných údajov.
9. Zasielanie osobných údajov dotknutým osobám sa vykonáva poštou v zalepenej obálke alebo prostredníctvom technického prostriedku, po predošlom zašifrovaní alebo anonymizácii súborov obsahujúcich osobné údaje.
10. Odovzdávanie osobných údajov iným osobám v rámci priestupkového alebo trestného konania (napríklad Policajný zbor, prokuratúra, súdy) je možné len s povolením štatutárneho orgánu, na základe písomnej žiadosti príslušného orgánu a v súlade s príslušným osobitným zákonom (napríklad §76a zákona o policajnom zbore). Štatutárnym orgánom určená oprávnená osoba odovzdá príslušné osobné údaje príslušnému orgánu, len na základe záznamu o odovzdaní. Záznam o odovzdaní sa archivuje po dobu troch rokov u zodpovednej osoby.

Organizačné opatrenia pre kamerový systém

1. Záznamy je možné spracúvať len oprávnenými osobami, výhradne v priestoroch určených na tento účel (ďalej „chránené priestory" - „CHP") a v záznamovom zariadení, ktoré je umiestnené v príslušnom chránenom priestore.
2. Záznamy, ktoré majú charakter písomnosti, hmotného nosiča informácií sa v pracovnej i v mimopracovnej dobe ukladajú do úschovných objektov, určených na tento účel, umiestnených v príslušnom CHP.
3. Záznamy z kamerového systému je možné poskytovať len príslušným oprávneným osobám (kontrolným orgánom napríklad na základe § 15 ods. 7 zákona alebo §76a zákona o policajnom zbore) spôsobom, ktorým nemožno narušiť dôvernosť záznamov, pričom je zakázané poskytovať záznamy internetom bez šifrovania.
4. Oprávnená osoba zabezpečí, aby neoprávnené osoby (napríklad návštevy) sa ani náhodne neoboznámili so zobrazovanými záznamami. Za týmto účelom sa neoprávnené osoby, ktoré vstúpili do chráneného priestoru tak, aby, sa nemohli oboznámiť so záznamom z kamerového systému. Za týmto účelom oprávnená osoba zabezpečí otočenie (vypnutie) obrazovky záznamového zariadenia tak, aby neoprávnená osoba nemala možnosť sledovať záznamy zo zobrazovacieho zariadenia.

5. Kamerové systémy alebo ich jednotlivé časti, či už po častiach alebo v celku, sa môžu prenášať, premiestňovať alebo inštalovať len so súhlasom primátora.
6. Ak záznamy prenáša osoba, ktorá nie je oprávnenou osobou, musia byť tieto zabezpečené tak, aby táto osoba nemala prístup k obsahu záznamov nosiča informácií
7. Zasielanie záznamov (nosičov informácií) oprávneným osobám sa vykonáva poštou v zalepenej obálke „Doporučene" alebo prostredníctvom technického prostriedku, po predošlom zašifrovaní súborov obsahujúcich záznamy z kamerového systému.
8. Odovzdávanie záznamov v rámci priestupkového alebo trestného konania (napríklad Policajný zbor, prokuratúra, súdy) je možné len s povolením prevádzkovateľa, na základe písomnej žiadosti príslušného orgánu a v súlade s príslušným osobitným zákonom (napríklad §76a zákona o policajnom zbore). Príslušná oprávnená osoba odovzdá príslušné záznamy na nosiči informácií príslušnému orgánu, len na základe záznamu o odovzdaní (príloha č. 2). Záznam o odovzdaní sa archivuje po dobu troch rokov.
9. Dokumenty alebo pamäťové média so záznamami možno vypožičať na nevyhnutne potrebný čas, a to len oprávnenej osobe, ktorá má povolený prístup k príslušným záznamom alebo odovzdať oprávneným osobám na základe osobitného zákona podľa záznamu o vypožičaní (odovzdaní).
10. Rozmiestnenie (nastavenie) jednotlivých kamier kamerového systému sa vykonáva tak, aby zabezpečovali výhradne monitorovanie priestorov na určené účely (príloha č. 1). Priestory kde sú rozmiestnené kamery musia byť na vstupe do týchto priestorov zreteľne označené („Priestor je monitorovaný kamerovým systémom"). Kamery nesmú monitorovať priestory, kde oprávnene očakáva súkromie (napr. súkromné priestory, prezliekame, umyvárne, WC a pod.), Kamery nesmú sledovať, čo sa deje vo vnútri susedných, priľahlých budov. Označenie monitorovaných priestorov mesta sa vykonáva podľa Metodického usmernenia Úradu na ochranu osobných údajov.

Pravidlá vstupu osôb a vjazdu dopravných prostriedkov do objektu alebo chráneného priestoru a podmienky výstupu osôb z objektu alebo chráneného priestoru

1. Na vstup/výstup do/z objektu je určený len hlavný vstup. Zamestnanci prevádzkovateľa vstupujú do objektu počas pracovnej doby aj mimo nej podľa potreby pre plnenie pracovných úloh. Vstup je realizovaný pomocou prideleného kľúča hlavným vstupom, čiže kontrola vstupu do objektu je zabezpečená prostredníctvom prideleného kľúča. Mimo pracovnej doby zamestnanci môžu vstúpiť do objektu len so súhlasom štatutárneho orgánu. Návštevy vstupujú do objektu so súhlasom zamestnanca prevádzkovateľa (navštívenej osoby), ktorý si ich na vstupe do objektu prevezme. Návštevy po splnení účelu pobytu v objekte vyprevadí z objektu navštívená osoba. Návštevy mimo pracovnej doby môžu do objektu vstupovať iba so súhlasom štatutárneho orgánu.
2. Oprávnené osoby vstupujú do CHP v pracovnom čase, ako i mimo neho podľa potreby. Oprávnená osoba vstupuje do CHP pomocou prideleného kľúča. Pred vstupom do CHP táto osoba vizuálne skontroluje stav neporušenia MZP a TZP v CHP a zabezpečenia osobných údajov (napr. či nedošlo ku kradmému vniknutiu do trezoru). Po vstupe do CHP uzavrie za sebou dvere a vykonáva v ňom potrebné činnosti. Pri krátkodobom opustení CHP oprávnená osoba dvere CHP uzamkne. Po skončení činnosti CHP je oprávnená osoba po výstupe z CHP povinná skontrolovať zabezpečenie OÚ, vypnutie elektrických zariadení a technického prostriedku a uzamknúť dvere do CHP a objektu. Vstup do chráneného priestoru v pracovnej dobe aj v mimo pracovnej doby je inej osobe v závislosti od plnenia jej činnosti v CHP (napr. upratovanie, oprava MZP/ TZP v CHP) možný len po predchádzajúcom súhlase príslušného vedúceho, všetky osoby vstupujúce do CHP vstupujú len v sprievode oprávnených osôb. Pri vstupe návštev do CHP táto oprávnená osoba príjme opatrenia, aby nedošlo k neoprávnenej manipulácii s IS, napr. uschovanie osobných údajov, písomností do úschovného objektu a vykoná všetky opatrenia, aby sa táto osoba nemohla oboznámiť s osobnými údajmi. Oprávnená osoba, zdržujúca sa v CHP, zodpovedá za uzatvorenie dverí do CHP po vstupe a výstupe z/do CHP. Dlhšie otvorenie dverí do CHP je možné len z dôvodov hodných zvláštneho zreteľa. V tomto prípade oprávnená osoba zabezpečí uschovanie osobných údajov do úschovného objektu a zabezpečí, aby nedošlo k neoprávnenej manipulácii s osobnými údajmi.

3. Za pracovnú dobu je považovaná pracovná doba určená v pracovnom poriadku prevádzkovateľa. Doba mimo túto dobu je považovaná za mimopracovnú dobu.
4. V objekte je používanie mobilných telefónov neobmedzené. V CHP nie je dovolené bez povolenia štatutárneho orgánu používanie mobilných telefónov, videokamier, fotoaparátov alebo iných komunikačných alebo audiovizuálnych záznamových zariadení. Pri použití týchto prostriedkov oprávnená osoba musí zabezpečiť, aby nedošlo k neoprávnenej manipulácii s osobnými údajmi.
5. S osobné údaje sa môže spracovávať výlučne v príslušnom CHP. Pri spracúvaní osobných údajov môžu byť prítomné iba oprávnené osoby. Spracovanie a ukladanie osobných údajov sa vykonáva len v CHP. Oprávnené osoby využívajú za účelom spracovania a manipulácie s osobnými údajmi len miestnosť CHP, ktorá je na tento účel vybavená a zabezpečená. Po ukončení práce s osobnými údajmi sa musia tieto ukladať v úschovnom objekte v CHP a musia sa vypnúť technické prostriedky.

Pravidlá spôsobu kontroly objektu alebo chráneného priestoru po opustení pracoviska zamestnancami, ktoré zabezpečia, že nedôjde k neoprávnenej manipulácii s osobnými údajmi

1. Oprávnená osoba je povinná po skončení práce v CHP a pred odchodom z CHP vypnúť elektrické spotrebiče, uložiť osobné údaje do úschovného objektu a vypnúť technické prostriedky. Odchádzajúca oprávnená osoba (po vizuálnej kontrole priestorov s cieľom ubezpečiť sa, že nedôjde k neoprávnenej manipulácií s osobnými údajmi), uzamyká objekt, vypína technický prostriedok a uzamyká CHP. Ostatní zamestnanci sú po odchode z pracoviska rovnako povinní skontrolovať uzavretie okien pracoviska, vypnutie príslušných elektrických spotrebičov, uzamknutie pracoviska. Posledná osoba odchádzajúca z pracoviska je povinná skontrolovať, či v objekte neostala žiadna iná osoba, vykoná kontrolu vypnutia elektrických spotrebičov, vody, uzamkne pridelenú kanceláriu alebo priestory, vizuálne skontroluje uzatvorenie dverí do CHP a uzamyká vstup do objektu. V prípade zistených nedostatkov kontaktuje štatutárny orgán a riadi sa jeho pokynmi.

Pravidlá určujúce podmienky používania, prideľovania, označovania, úschovy a evidencie originálov a kópií bezpečnostných kľúčov, identifikačných kariet a uzamykateľných systémov

1. Štatutárnym orgánom poverená osoba vedie evidenciu o mieste uloženia všetkých bezpečnostných kľúčov spolu s evidenciou čísla zámku alebo bezpečnostného úschovného objektu, ku ktorému patria, v knihe evidencie kľúčov. Kniha evidencie kľúčov sa ukladá u príslušného zamestnanca.
2. Kópie bezpečnostných kľúčov od CHP a úschovného objektu sú uložené v zalepenej obálke, v objekte v uzamykateľné skrinke. Na obálke je uvedené, kto kľúč môže vybrať a použiť. Tieto kľúče možno použiť v prípadoch uvedených v krízovom pláne. O použití tohto kľúča je informovaný príslušný zamestnanec a o ich použití sa vykoná záznam do Knihy evidencie kľúčov.
3. Bezpečnostné kľúče od objektu sa vydávajú zamestnancom na základe povolenia štatutárneho orgánu a na základe podpisu v knihe evidencie kľúčov. Kópie bezpečnostných kľúčov od objektu sú uložené v zalepenej obálke u štatutárneho orgánu. Na obálke je uvedené, kto kľúč môže vybrať a použiť.
4. Kľúče od iných priestorov sú vydávané zamestnancom na základe povolenia štatutárneho orgánu.
5. Dodatočné kópie bezpečnostných kľúčov môžu byť vyhotovené iba na základe písomného súhlasu štatutárneho orgánu, o čom sa uvedie záznam v knihe evidencie kľúčov.
6. V prípade havarijnej situácie u podnikateľa (napr. požiar, výpadok elektrickej energie, zaplavenie, výpadok kúrenia a pod.) sú za týmto účelom v kancelárii príslušného zamestnanca uložené kľúče od vchodov do priestorov objektu, v ktorých sa nachádzajú hlavné uzávery vody,

plynu, elektrických a slaboprúdových rozvodov. O každom použití týchto kľúčov musí byť informovaný štatutárny orgán.
7. V prípade straty, poškodenia bezpečnostného kľúča rozhodne štatutárny orgán o prijatí príslušných opatrení.

Určujúce podmienky manipulácie s mechanickými zábrannými prostriedkami a podmienky ich používania - Úschovné objekty

1. Úschovný objekt sa používa na ukladanie osobných údajov.
2. Na prístup k osobným údajom uloženým v úschovnom objekte oprávnená osoba používa pridelený kľúč. Úschovný objekt sa otvára na nevyhnutne potrebnú dobu, na vybratie alebo vloženie osobných údajov.
3. Úschovný objekt je možné používať len v súlade s návodom od výrobcu.
4. Za správne používanie úschovného objektu, v súlade s návodom od výrobcu, zodpovedá oprávnená osoba. Kontrolu správneho používania úschovného objektu vykonáva poverená osoba.
5. Úschovný objekt sa po skončení pracovného času uzamkne a skontroluje poslednou odchádzajúcou oprávnenou osobou.

Vstupné dvere do CHP

1. Vstupné dvere do CHP sa otvárajú len na dobu nevyhnutne potrebnú na vstup a výstup osôb alebo na prinesenie alebo vynesenie materiálu.
2. Otváranie dverí do CHP je možné iba oprávnenou osobou, ktorá má na tento účel pridelený kľúč.
3. V prípade potreby otvorenia dverí do CHP na dlhšiu dobu (napr. z dôvodu prenášania materiálu a pod.) zabezpečí oprávnená osoba, aby nedošlo k neoprávnenej manipulácií s US (napríklad pred odpozorovaním).
3. Dvere do CHP je možno používať len v súlade s návodom od výrobcu.
4. Po skončení práce v CHP je odchádzajúca oprávnená osoba povinná dvere uzamknúť.

PRAVIDLÁ NA VÝKON FYZICKEJ OCHRANY

1. Účelom fyzickej ochrany (vlastný zamestnanci počas pracovnej doby) objektu je:
• zabezpečiť kontrolu prístupu do objektu a chráneného priestoru tak, že do objektu (chráneného priestoru) budú vpustené len osoby, ktoré majú príslušné oprávnenie, resp. sú uvedené v zozname oprávnených osôb,
• zabezpečiť kontrolu dodržiavania zásad pre pohyb (donášanie/vynášanie) materiálu a iných aktív do/z objektu,
• zabezpečiť ochranu proti páchaniu majetkovej kriminality,
• zabezpečiť ochranu objektu (chráneného priestoru) proti preniknutiu nepovolaných osôb,
• s využitím MZP a TZP včas reagovať na bezpečnostný incident a vykonať zásah proti narušiteľovi alebo privolať pomoc (PZ).

ROZSAH OPRÁVNENÍ A POPIS POVOLENÝCH ČINNOSTÍ A SPÔSOB ICH IDENTIFIKÁCIE A AUTENTIZÁCIE PRI PRÍSTUPE K INFORMAČNÉMU SYSTÉMU

Zoznam, povinnosti a oprávnenia osôb pri používaní technických a systémových prostriedkov, bezpečnostný správca

1. V IS môžu pracovať a spracovávať osobné údaje len oprávnené osoby, ktoré majú pridelené a schválené prístupové práva a povolené činnosti pri spracovaní osobných údajov, sú poučené, majú podpísané poučenie - Záznam o pučení do príslušného IS.
2. Bezpečnostný správca v otázkach ochrany osobných údajov zabezpečuje bezpečnosť automatizovaných informačných systémov. Funkciou bezpečnostného správcu (ďalej len „bezpečnostný správca) je osoba poverená štatutárnym orgánom (príloha č. l).
3. Bezpečnostný správca je zodpovedný za bezpečnosť IS a priamo vykonáva správu bezpečnosti IS tým, že:
a) zodpovedá za vývoj, zavedenie, údržbu bezpečnostných funkcií systému
a bezpečnostné nastavenia operačného systému, používateľských softvérových prostriedkov,
b) riadi a kontroluje používateľské účty pre registráciu nových používateľov do informačného systému a prideľovanie prístupových práv používateľom v súlade s ich schváleným oprávnením a potrebami pre výkon činnosti,
c) spravuje autentizačné funkcie a autorizačné funkcie systémových prostriedkov,
d) vykonáva koordináciu riadenia zmien konfigurácie systému a technických prostriedkov,
e) vyhodnocuje kontrolné záznamy o činnosti technických prostriedkov a používateľov,
f) koordinuje opatrenia pri bezpečnostných incidentoch a ich vyšetrovanie, vypracováva správy o bezpečnostných incidentoch (neoprávnených manipuláciách a pod.),
g) plánuje a vykonáva fyzickú kontrolu technických prostriedkov,
h) kontroluje bezpečné uloženie informácií na elektronických nosičoch informácií,
i) kontroluje vykonávanie údržby technických prostriedkov,
j) vykonáva správu šifrovacích kľúčov u technických prostriedkov tam, kde boli inštalované šifrovacie prostriedky na ochranu osobných údajov,
k) organizuje obnovu funkčnosti informačného systému po havárii alebo poruche technických prostriedkov,
l) inštaluje a konfiguruje potrebné systémové, programové a používateľské prostriedky, bezpečnostné nastavenia operačného systému v súlade s touto smernicou,
m) vykonáva údržbu a aktualizáciu bezpečnostných a antivírusových prostriedkov,
n) vykonáva správu automatizovaných zálohovacích systémov a zálohovanie dát,
o) vykonáva a zodpovedá za zálohovanie systémových prostriedkov,
p) na účel spätnej identifikácie osoby, miesta a času a zabezpečí zaznamenanie každého vstupu oprávnenej osoby do informačného systému,
q) vykonáva protiopatrenia pri zistení narušenia alebo pokuse o narušenie bezpečnosti informačného systému,
r) vykonáva kontrolu kontrolných záznamov o činnosti technických prostriedkov a používateľov, o udalostiach z hľadiska porušenia bezpečnosti pri prevádzkovaní technického prostriedku informuje štatutárny orgán,
s) spracúva a vedie záznam o používateľskom účte oprávnenej osoby, o hlásení bezpečnostných incidentov a zázname o servisnej činnosti v IS,
t) podieľa sa na vyšetrovaní bezpečnostných incidentov.
Oprávnená osoba - používateľ používa jemu pridelené technické prostriedky informačného systému na spracovanie osobných údajov len v rozsahu svojich pracovných povinností. V otázkach bezpečnosti informačného systému sa riadi ustanoveniami týchto smerníc a pokynmi bezpečnostného správcu. Má oprávnenia na:
- spúšťanie aplikačného programového vybavenia, vytváranie, modifikovanie a ukladanie dát prostredníctvom aplikačného programového vybavenia v rozsahu, ktorý poskytuje aplikačné

programové vybavenie prideleného technického prostriedku v rámci príslušného informačného systému,
4. Používateľ nemá oprávnenia na:
- prácu na iných ako pridelených technických prostriedkoch informačného systému,
- inštaláciu a konfiguráciu systémových prostriedkov a ich služieb,
- inštaláciu aplikačného programového vybavenia na technické prostriedky,
- inštaláciu a konfiguráciu tlačiarní,
- zasielanie dokumentov a správ obsahujúcich osobné údaje elektronickou poštou alebo faxom (okrem šifrovaním, anonymizovaním dát alebo heslom zabezpečených dát),
- pristupovanie k aplikáciám a dátam, na ktoré nie je oprávnený a pokúšať sa obísť bezpečnostné mechanizmy operačného systému a IS,
- premiestňovanie IS z CHP, vykonávanie zmeny konfigurácie alebo pripájanie technického prostriedku k verejným alebo iným sieťam,
- menenie konfigurácie Software.
5. Používateľ je povinný:
- bez meškania hlásiť všetky bezpečnostné incidenty bezpečnostnému správcovi,
- chrániť prístupové heslá pred zneužitím,
- používať len autorizovaný softvér.

Opis identifikácie a autorizácie používateľov

l. Rozsah úkonov, ktoré môže oprávnená osoba vykonávať s osobnými údajmi určuje bezpečnostný správca a sú zakódované prostredníctvom identifikátora používateľa a k nemu priradených prístupových práv a oprávnení v priamej väzbe na technický prostriedok.

ROZSAH ZODPOVENOSTI OPRÁVNENÝCH OSÔB

Povinnosť zachovať mlčanlivosť

1. Všetky oprávnené osoby sú povinné zachovávať mlčanlivosť o osobných údajoch, ktoré spracúvajú. Povinnosť mlčanlivosti trvá aj po ukončení pracovného pomeru.
2. Povinnosť mlčanlivosti platí aj pre iné fyzické osoby, ktoré sa v rámci svojej činnosti (napr. údržba a servis IS), aj náhodou oboznámia s osobnými údajmi.
3. Povinnosť mlčanlivosti trvá aj po zániku funkcie oprávnenej osoby alebo po ukončení jej pracovného alebo iného zmluvného vzťahu.
4. Povinnosť mlčanlivosti neplatí, ak je to nevyhnuté na plnenie úloh súdov, orgánov činných v trestnom konaní a Úradu na ochranu osobných údajov.

Zálohovanie

1. Údaje z databázových systémov, užívateľské súbory a iné dôležité dáta sa zálohujú minimálne l x za deň. Za zálohovanie je zodpovedný bezpečnostný správca.
2. Týždenné úplné zálohy (l x za 7 dní - piatok) ako ak inkrementálne (rozdielové) zálohy (l x za deň – pondelok až piatok) sa vykonávajú na pevné disky (HDD) zálohovacieho servera (BACKUP SERVER) a uchovávajú sa ako archívne. Režim prepisovania záložných súborov je stanovený tak, aby existovalo vždy 5 úplných záloh (história 5 týždňov) a tomu zodpovedajúci počet rozdielových záloh (24 záloh) Za vykonávanie archivácie dát a uloženie a funkčnosť zálohovacieho servera zodpovedá bezpečnostný správca alebo oprávnené osoby poverené bezpečnostným správcom.
3. Zálohovací server sa nachádza na inom mieste ako je miestnosť prevádzkových serverov.

Zodpovednosť za bezpečnosť osobných údajov

1. Prevádzkovateľ a oprávnené osoby sú povinné zabezpečiť bezpečnosť osobných údajov, chrániť ich pred náhodným ako aj nezákonným poškodením, náhodnou stratou, zmenou, nedovoleným prístupom a sprístupnením, ako aj pred akýmkoľvek inými neprípustnými formami spracúvania v rozpore s touto smernicou, vyhláškou a zákonom.
2. Zodpovedná osoba:
a) poskytuje informácie a poradenstvo zamestnancom, ktorí vykonávajú spracúvanie osobných údajov, o ich povinnostiach podľa tohto zákona, osobitných predpisov alebo medzinárodných zmlúv, ktorými je Slovenská republika viazaná, týkajúcich sa ochrany osobných údajov,
b) monitoruje súlad s týmto zákonom, osobitnými predpismi alebo medzinárodnými zmluvami, ktorými je Slovenská republika viazaná, týkajúcimi sa ochrany osobných údajov a s pravidlami prevádzkovateľa súvisiacimi s ochranou osobných údajov vrátane rozdelenia povinností, zvyšovania povedomia a odbornej prípravy osôb, ktoré sú zapojené do spracovateľských operácií a súvisiacich auditov ochrany osobných údajov,
c) poskytuje na požiadanie poradenstvo, ak ide o posúdenie vplyvu na ochranu osobných údajov a monitorovanie jeho vykonávania podľa § 42 zákona,
d) spolupracuje s úradom pri plnení svojich úloh,
e) plní úlohy kontaktného miesta pre úrad v súvislosti s otázkami týkajúcimi sa spracúvania osobných údajov vrátane predchádzajúcej konzultácie podľa § 43 zákona podľa potreby aj konzultácie v iných veciach.
f) Iné úlohy uložené touto smernicou alebo internými smernicami.
3. Zodpovedná osoba pri výkone svojich úloh náležite zohľadňuje riziko spojené so spracovateľskými operáciami, pričom berie do úvahy povahu, rozsah, kontext a účel spracúvania osobných údajov.
4. Zodpovedná osoba na základe písomnej žiadosti dotknutej osoby informuje túto osobu o stave spracúvania jej osobných údajov, prípadne iných informácií v súlade s § 19 zákona.
5. Zodpovedná osoba spoločne s bezpečnostným správcom vykonávajú vyšetrovanie bezpečnostných incidentov, spracovávajú zápis o vyšetrení bezpečnostného incidentu a navrhujú opatrenia na zabezpečenie ochrany osobných údajov.
6. Zodpovedná osoba, pokiaľ nie je štatutárnym orgánom určené inak, zabezpečuje vykonávanie kontrolnej činnosti a vedenie dokumentácie podľa tejto smernice a interných predpisov.

SPÔSOB, FORMA A PERIODICITA VÝKONU KONTROLNÝCH ČINNOSTÍ ZAMERANÝCH NA DODRŽIAVANIE BEZPEČNOSTI INFORMAČNÉHO SYSTÉMU

Spôsob, forma a periodicita kontrolných činností zameraných na dodržiavanie bezpečnosti informačného systému

1. Za výkon kontrolnej a servisnej činnosti o ochrane osobných údajov pri používaní IS zodpovedá štatutárny orgán, alebo štatutárnym orgánom poverená oprávnená osoba (bezpečnostný správca, zodpovedná osoba, iná určená osoba). Pri zistení bezpečnostného incidentu bezpečnostný správca alebo osoba, ktorá ho zistí je povinná hlásiť tento vedeniu prevádzkovateľa. Osoba poverená vykoná kontrolu a spracuje záznam o kontrolnej činnosti.

Spôsob, forma a periodicita kontrolných činností zameraných na dodržiavanie bezpečnosti informačného systému

1. Za výkon kontrolnej a servisnej činnosti o ochrane osobných údajov pri používaní IS zodpovedá štatutárny orgán, alebo štatutárnym orgánom poverená oprávnená osoba (bezpečnostný správca, zodpovedná osoba, iná určená osoba). Pri zistení bezpečnostného incidentu bezpečnostný správca

je povinný hlásiť tento vedeniu prevádzkovateľa. Osoba poverená vykonať kontrolu spracuje záznam o kontrolnej činnosti.
2. V prípade bezpečnostného incidentu štatutárnym orgánom poverená osoba spolu s bezpečnostným správcom zabezpečí vyšetrenie bezpečnostného incidentu a následne na základe záverov z vyšetrovania navrhne mu príslušné opatrenia a sankcie v súlade s vnútornými smernicami. Osoba poverená vyšetriť bezpečnostný incident spracuje záznam o vyšetrení bezpečnostného incidentu (príloha č. 3).
3. Kontrolná činnosť sa vykonáva nasledovne:

P.č.	**Kontrolovaná skutočnosť**	**Predmet kontroly**	**Periodicita výkonu kontrolných činností**	**Forma kontroly**
1	**Identifikácia zmien/ aktuálnosti stavu zabezpečenia**	Identifikácia zmien u prevádzkovateľa od poslednej kontroly, ktorá má vplyv na ochranu osobných údajov, najmä zmeny vo fyzickom a objektovom zabezpečení, personálne a organizačné zmeny, zmeny v IT zabezpečení, zmeny v rámci informačných systémov	*Vykonáva sa periodicky najmenej lx za rok v zmysle platnej servisnej zmluvy*	*Vykonáva sa kontrolnou činnosťou zodpovednej, alebo určenej osoby*

P.č.	Kontrolovaná skutočnosť	Predmet kontroly	Periodicita výkonu kontrolných činností	Forma kontroly
1	Kontrola aktuálnosti zdokumentovaných bezpečnostných opatrení a plnenia zákonných povinností prevádzkovateľom	Posúdenie aktuálnosti používanej dokumentácie k ochrane osobných údajov, a splnenia náležitostí podľa zákona a nariadenia, nasledovne: - Dokumentácia k ochrane osobných údajov -Poverenie zástupcu prevádzkovateľa, resp. sprostredkovateľa - Poverenie zodpovednej osoby - Záznamy o spracovateľských činnostiach (ako prevádzkovateľ a sprostredkovateľ) - Súhlasy dotknutých osôb -Zabezpečenie informovanosti dotknutých osôb - Posúdenie vplyvu na ochranu osobných údajov -Školenia osôb poverených spracúvaním osobných údajov -Preverenie s p rostred kováte ľo v -Zmluvy so sprostredkovateľmi -Prenos osobných údajov do tretích krajín, resp. medzinárodných organizácií -Poverenie mlčanlivosťou -Oznamovanie porušení ochrany osobných údajov	Vykonáva sa periodicky najmenej 1 x za rok v zmysle platnej servisnej zmluvy	Vykonáva sa kontrolnou činnosťou zodpovednej, alebo určenej osoby. Zabezpečenie práv dotknutých osôb.

P.č.	Kontrolovaná skutočnosť	Predmet kontroly	Periodicita výkonu kontrolných činností	Forma kontroly
3	Kontrola dodržiavania prijatých bezpečnostných opatrení	Prevádzkovateľ zabezpečuje kontrolu dodržiavania prijatých bezpečnostných opatrení sám, alebo prostredníctvom ním určených osôb, najmä: - Kontrola dodržiavania prijatých IT opatrení bezpečnostným správcom, alebo prevádzkovateľom - Kontrola zabezpečenia FO a OB prevádzkovateľom alebo ním určenými osobami -Kontrola dodržiavania kľúčového režimu prevádzkovateľom alebo ním určenými osobami Kontrola dodržiavania organizačných opatrení oprávnenými osobami - zabezpečuje zodpovedná/určená osoba prostredníctvom vzdelávania	Vykonáva sa periodicky najmenej 1 x za rok v zmysle platnej servisnej zmluvy	Vykonáva sa kontrolnou činnosťou bezpečnostného správcu, prevádzkovateľa, alebo ním určených osôb, zodpovednej osoby, alebo určenej osoby
Iné kontroly	Podľa potreby	Vykonáva sa neperiodický, podľa potreby	Vykonáva sa kontrolnou činnosťou bezpečnostného správcu, prevádzkovateľa, alebo ním určených osôb, zodpovednej osoby, alebo určenej osoby	

Tabuľka č. 5

Preventívne opatrenia

1. Preventívne opatrenia v oblasti ochrany osobných údajov vykonáva štatutárnym orgánom poverená oprávnená osoba periodicky, prípadne neohlásené s cieľom zistiť stav ochrany osobných údajov.
2. Vykonávanie školení a poučení oprávnených osôb zabezpečí zodpovedná osoba u každej oprávnenej osoby pred začiatkom spracúvania osobných údajov a po každom bezpečnostnom incidente. O vykonanom školení vedie zodpovedná osoba záznam.
3. Preventívne opatrenia v oblasti bezpečnosti IS vykonáva bezpečnostný správca pravidelnou kontrolou IS antivírusovými programami (podľa odporučenia dodávateľa antivírusového programu), prípadne inými prostriedkami a kontrolou konfigurácie technického prostriedku, nastavení operačného systému a správnej činnosti technického prostriedku.

Záverečné ustanovenia

1. Výnimky z bezpečnostných opatrení môže dočasne udeliť štatutárny orgán, pričom je povinný pred udelením výnimky vyhodnotiť riziko, pre práva fyzických osôb. Na základe vyhodnotenia rizika je povinný ustanoviť náhradné bezpečnostné opatrenia. Ak pre práva fyzických osôb by bolo vyhodnotené riziko vysoké, výnimka nesmie byť udelená.
2. Revízia a prípadná novelizácia bezpečnostnej dokumentácie a smerníc týkajúcich sa ochrany osobných údajov sa zabezpečuje l x za 2 roky prípadne, ak je to potrebné, po novelizácii zákona (zabezpečuje zodpovedná osoba).
3. Smernica je záväzná pre všetky oprávnené osoby prevádzkovateľa.
4. Zmeny a doplnky smernice musia mať písomnú formu.
5. Oboznámenie oprávnených osôb so smernicou a o povinnosti ju dodržiavať zabezpečí zodpovedná osoba.
6. Smernica nadobúda účinnosť dňom podpísania.

Súvisiace predpisy

1. Zákon o ochrane osobných údajov v znení neskorších zákonov
2. ISO/IEC 27002 - Informačné technológie.

Prílohy:
Príloha č. 1 - Poverenie bezpečnostného správcu.
Príloha č. 2 - Potvrdenie o odovzdaní osobných údajov.
Príloha č. 3 - Protokol o vyšetrení bezpečnostných incidentov.
Dokumentácia podľa § 3 písm. d) a e) vyhlášky Úradu na ochranu osobných údajov o rozsahu dokumentácií a bezpečnostných opatrení - Záznamy o kontrolnej činnosti a o zistených bezpečnostných incidentoch.

Účinnosť od: 25.05.2018
Plánovaná revízia: 25.05.2020
Záväznosť pre: Všetky oprávnené osoby.

Upozornenie!

V Gabčíkove, dňa 25.05.2018

PhDr. Iván Fenes LL.M, MBA
primátor mesta

Príloha č. 1

Poverenie bezpečnostného správcu

V súlade s technickými a režimovými opatreniami a bezpečnostnou politikou

poverujem

Meno, priezvisko, titul, dátum narodenia: .....

plnením funkcie Bezpečnostný správca, v súlade s Bezpečnostnou smernicou, pri ochrane osobných údajov u prevádzkovateľa:

Mesto Gabčíkovo
Mestský úrad Gabčíkovo, Hlavná č. 1039/21, 930 05
IČO: 0030539100

V Gabčíkove, dňa: 25.5.2018

PhDr. Iván Fenes LL.M, MBA, primátor mesta
Podpis štatutárneho orgánu

Potvrdzujem, že prijímam toto poverenie, a že som bol poučený o svojich povinnostiach pri zabezpečovaní ochrany osobných údajov.

V Gabčíkove, dňa: 25.5.2018

.....
Podpis bezpečnostného správcu

Príloha č.2

Záznam o poskytovaní osobných údajov na spracúvanie inému spracovateľovi

Odovzdávajúci:.....

Preberajúci:.....
(Meno, priezvisko, organizácia, číslo občianskeho preukazu)

Identifikácia odovzdávaných osobných údajov : .....
.....
.....
.....

Dôvod odovzdania osobných údajov (napr. trestné konanie, priestupkové konanie, iný dôvod):
.....
.....
.....

Preberajúci prebratím osobných údajov preberá zodpovednosť za ochranu osobných údajov v súlade so zákonom č. 18/2018 Z. z. o ochrane osobných údajov.

V Gabčíkove, dňa:.....

Odovzdávajúci..... podpis.....

Preberajúci ..... podpis.....

Príloha č.: **3**

Značka: .....

PROTOKOL
zo šetrenia bezpečnostného incidentu (BI) alebo mimoriadnej udalosti (MU)

Miesto.....

Dátum.....**Čas**.....

Text:.....
.....
.....
.....
.....
.....
na základe čoho a koho, akého rozhodnutia bolo vykonané šetrenie BI, MU v akom časovom rozpätí bolo vykonané vyšetrovanie BI, MU - čo bolo predmetom vyšetrovania BI, MU popis skutočností a okolností zistených a preukázaných vyšetrovaním BI, MU ktoré opatrenia boli zrealizované v priebehu vyšetrovania.

Záver:.....
.....
.....
.....
.....
.....
- zhodnotenie, či bol alebo nebol spáchaný BI, MU ktoré interné a iné legislatívne normy boli porušené, a v ktorých ustanoveniach (prip. citovať), v prípade podozrenia zo spáchania trestného činu (TČ) uviesť, o ktorý TČ v zmysle TZ sa môže jednať, klasifikáciu TČ a okolnosti, ktoré nasvedčujú podozreniu (príp,, citovať), ktoré konkrétne aktíva boli ohrozené, vymedzenie okolností, ktoré umožnili spáchanie daného BI, MU (TČ) a určenie zodpovednosti za zistený stav vyčíslenie ekonomických dopadov (keď je možné).

Návrh opatrení:.....
.....
.....
.....
.....
- vymedzenie opatrení, ktoré navrhuje vyšetrovateľ na zamedzenie opakovania sa podobných BI vymedzenie opatrení, ktoré navrhuje vyšetrovateľ na zjednanie nápravy (v prípade zistenia nedostatkov v interných normách, plnenia ustanovení interných a legislatívnych noriem a pod.)

Schvaľuje:..... podpis .....

Spracoval: ..... podpis .....

Číslo		Čísla vymenených strán	Zmenu povolil		Zmenu vykonal
Dátum	Meno	Podpis	Dátum	Meno	Podpis

Záznam o vykonanom oboznámení			
Oboznámená osoba	Dátum	Podpis	Poznámka