POSÚDENIE VPLYVU
NA OCHRANU OSOBNÝCH ÚDAJOV
PODĽA ZÁKONA 18/2018 Z. Z.

Obsah

1. **Základné pojmy**

2. **Systematický opis plánovaných spracovateľských operácii a účely spracúvania, vrátane prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ;**

3. **Posúdenie nutnosti a primeranosti spracovateľských operácii vo vzťahu k účelu;**

4. **Posúdenie rizika pre práva a slobody dotknutých osôb, ktoré vyplýva zo samotnej podstaty zamýšľaného spracúvania osobných údajov;**

5. **Opatrenia na riešenie rizík vrátane záruk, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany osobných údajov a na preukázanie súladu s týmto nariadením;**

6. **Zohľadnenie práv a oprávnených záujmov dotknutých osôb a ďalších osôb, ktorých sa zamýšľané spracúvanie týka.**

Význam skratiek používaných v dokumente:
OÚ *Osobné údaje*
IS *Informačný systém*
ID *Identifikačné údaje; Identifikátor*
AIS *Automatizovaný informačný systém*
DIS *Dokumentárny informačný systém*
BP *Bezpečnostný projekt*
TP *Technické prostriedky používané na spracúvanie osobných údajov*
IT *Informačné technológie*
VT *Výpočtová technika*
PC *Osobný počítač*
OS *Operačný softvér*
HW *Hardware*
SW *Software*
LAN *Lokálna počítačová sieť*
ASW *Aplikačný SW /funkčný programový celok pre manipuláciu s údajmi/*
AV *Antivírový software*
BOZP *Bezpečnosť a ochrana zdravia pri práci*
PO *Požiarna ochrana*
CO *Civilná ochrana*
EPS *Elektrická požiarna signalizácia*
HaZZ *Hasičský a záchranný zbor*
SHZ *Stabilné hasiace zariadenie*
GDPR *General Data Protection Regulation*

1. ZÁKLADNÉ POJMY

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,

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**,**

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,

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 o jej zdravotnom stave,

spracúvaním osobných údajov je spracovateľská operácia alebo súbor spracovateľských operácií s osobnými údajmi alebo so 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,

obmedzením spracúvania osobných údajov je označenie uchovávaných osobných údajov s cieľom obmedziť ich spracúvanie v budúcnosti,

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,

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 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,

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,

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,

dotknutou osobou je každá fyzická osoba, ktorej osobné údaje sa spracúvajú,

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 takýto predpis alebo táto zmluva ustanovuje účel a prostriedky spracúvania osobných údajov,

sprostredkovateľom 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,

zodpovednou osobou je osoba určená prevádzkovateľom alebo sprostredkovateľom, ktorá plní úlohy podľa zákona,

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 zák. 18/2018 Z.z.,

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,

skupinou podnikov je ovládajúci podnik a ním ovládané podniky,

hlavnou prevádzkarňou je

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 prevádzkareň 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,

vnútropodnikovými pravidlami sú postupy ochrany osobných údajov, ktoré dodržiava prevádzkovateľ alebo sprostredkovateľ so sídlom, miestom podnikania, organizačnou zložkou, prevádzkarňou alebo trvalým pobytom na území Slovenskej republiky na účely prenosu osobných údajov prevádzkovateľovi alebo sprostredkovateľovi v tretej krajine,

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

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,

členským štátom je štát, ktorý je členským štátom Európskej únie alebo zmluvnou stranou Dohody o Európskom hospodárskom priestore,

treťou krajinou je krajina, ktorá nie je členským štátom,

zamestnancom úradu je zamestnanec v pracovnom pomere alebo v obdobnom pracovnom vzťahu podľa osobitného predpisu alebo štátny zamestnanec, ktorý vykonáva štátnu službu v štátnozamestnaneckom pomere podľa osobitného predpisu

2. SYSTEMATICKÝ OPIS PLÁNOVANÝCH SPRACOVATEĽSKÝCH OPERÁCII A ÚČELY SPRACÚVANIA, VRÁTANE PRÍPADNÉHO OPRÁVNENÉHO ZÁUJMU, KTORÝ SLEDUJE PREVÁDZKOVATEĽ

Profil prevádzkovateľa: ***Evolution14 s.r.o., Karpatské námestie 10A, 831 06 Bratislava, IČO: 51788772*** *je spoločnosť, ktorá sa zaoberá :*
- Maloobchodný predaj odevov

1/ Informačný systém: IS Mzdy a personalistika

Zoznam osobných údajov spracúvaných v informačných systémoch mzdy a personalistika

Aj osobitné kategórie osobných údajov a to hlavne z dôvodu evidencie rodných čísel.

- meno, priezvisko a titul, národnosť, štátna príslušnosť, dátum a miesto narodenia, rodné číslo,
- kontakty /telefón, e-mail a pod.../, kontaktné adresy,
- informácie o poistení a čísla bankových účtov, číslo OP alebo pasu, číslo VP
- informácie o vykonanej práci a mzde, vzdelanie, rodinný stav, fotografia
- vojak - nevojak
- zdravotný stav, zmenená pracovná schopnosť
- zdravotná poisťovňa,
- materská dovolenka, dôchodok, jeho výška
- platové náležitosti,

- údaje týkajúce sa zrážok zo mzdy,
- príjem zamestnanca za každý rok,
- priebeh predchádzajúcich zamestnaní, pracovné zaradenie (funkcia, kategória), pracovná prax
- jazykové znalosti.
- lekárske potvrdenie

O rodinných príslušníkoch zamestnancov sa spracovávajú údaje:

- meno, priezvisko, rodné priezvisko manžela/ky
- dátum narodenia rodné číslo manžela/ky
- mená, priezviská, dátumy narodení, rodné čísla detí
- bankové údaje, číslo osobného účtu
- telefón, e-mail a pod.../, kontaktné adresy, rodné číslo, informácie o príjme (pre potreby soc. dávok)

Tieto údaje prevádzkovateľ spracováva v aplikačnom softvéri a v dokumentoch za účelom:

- vedenia personálnej a mzdovej agendy zamestnancov
- uchádzači o zamestnanie

Zoznam osobných údajov pre aplikačný softvér:

- meno, priezvisko a titul, číslo občianskeho preukazu, rodné číslo,
- fotografia (so súhlasom zamestnanca so zverejnením na web portáloch),
- kontakty /telefón, e-mail a pod.../, kontaktné adresy, informácie o vykonanej práci a mzde,
- číslo bankového účtu zamestnanca
- informácie o poistení, číslo OP alebo pasu, číslo VP

Popis funkcii subsystému BOZP, PO – Bezpečnosť a ochrana zdravia pri práci zamestnancov a požiarna ochrana spoločnosti.

Hlavným poslaním IS BOZP, PO bezpečnosť a ochrana zdravia pri práci a požiarna ochrana je spracúvanie osobných údajov fyzických osôb vyplývajúcich z plnenia úloh pre prevádzkovateľa IS spojených s komplexným zabezpečením BOZP, PO – bezpečnosti a ochrany zdravia pri práci zamestnancov, požiarnej ochrany a s tým súvisiace úkony. Vedie evidenciu a registráciu pracovných úrazov, ako aj evidenciu z vykonaných kontrol dodržiavania predpisov BOZP a PO, školení a pod..

Prevádzkovateľ v IS spracúva nasledovné osobné údaje:

- meno, priezvisko, titul
- rodné meno, predošlé meno
- adresa, bydlisko

- dátum narodenia, miesto narodenia
- rodné číslo
- pracovné zaradenie, funkcia
- lekárska správa, zdravotnícky posudok
- doplňujúce identifikačné údaje (napr.: pracovný úraz a pod.)

Okruh dotknutých osôb: Zamestnanci spoločnosti v stálom pracovnom pomere alebo inom obdobnom pracovnoprávnom vzťahu v súlade so zákonníkom práce a súvisiacimi predpismi.

Technológia spracúvania osobných údajov: Automatizovaná a dokumentárna.

Okruh užívateľov, ktorým sa osobné údaje sprístupňujú: Dotknuté osoby

Okruh užívateľov, ktorým sa osobné údaje poskytujú: Zdravotné poisťovne, Sociálna poisťovňa, súdy, orgány činné v trestnom konaní.

Osobné údaje sa nezverejňujú, osobné údaje nie sú predmetom cezhraničného toku, sprostredkovateľ nespracúva osobné údaje v mene prevádzkovateľa.

2/ Informačný systém: IS Účtovnícka agenda

Tento informačný systém predstavuje ekonomickú časť informačného systému. Jeho účelom je spracúvanie osobných údajov pri plnení úloh vyplývajúcich pre spoločnosť s komplexným zabezpečením finančného hospodárenia vrátane správy majetku a vykonávania koordinácie finančnej agendy, technicko-administratívne riadenie hospodárenia s prostriedkami, vedenia účtovnej evidencie majetku, navrhovania finančnej koncepcie v súlade s príslušnými zákonmi a všeobecne záväznými právnymi predpismi a zákonom č. 502/2001 Z. z. o finančnej kontrole a vnútornom audite a o zmene a doplnení niektorých zákonov, plnenie úloh spojených s komplexným zabezpečením investičnej akcie a s tým súvisiace úkony.

Zoznam osobných údajov spracúvaných v informačných systémoch účtovnícka agenda

Aj osobitné kategórie osobných údajov a to hlavne z dôvodu evidencie rodných čísel.

- meno, priezvisko a titul, národnosť, štátna príslušnosť, dátum a miesto narodenia, rodné číslo,
- kontakty /telefón, e-mail a pod.../, kontaktné adresy,
- informácie o poistení a čísla bankových účtov,

Tieto údaje prevádzkovateľ spracúva v dokumentoch za účelom:

- vedenia účtovníctva
- vedenie fakturácie

Zoznam osobných údajov pre aplikačný softvér:

- meno, priezvisko a titul, číslo občianskeho preukazu, obchodné meno, ak sa jedná o PO alebo FO - podnikateľa,
- číslo bankového účtu, kontakty /telefón, e-mail a pod.../, kontaktné adresy

Okruh dotknutých osôb: Zamestnanci, zmluvní a obchodní partneri, externé fyzické osoby, a pod.

Technológia spracúvania osobných údajov: Automatizovaná a dokumentárna.

Okruh užívateľov, ktorým sa osobné údaje sprístupňujú: Určení zamestnanci

Evolution14 s.r.o., Karpatské námestie 10A, 831 06 Bratislava, IČO: 51788772

Okruh užívateľov, ktorým sa osobné údaje poskytujú: Zdravotné poisťovne, Sociálna poisťovňa, súdy, orgány činné v trestnom konaní.

Osobné údaje sa nezverejňujú, osobné údaje nie sú predmetom cezhraničného toku, sprostredkovateľ nespracúva osobné údaje v mene prevádzkovateľa.

3/ Informačný systém: IS Klienti

Zoznam osobných údajov spracúvaných v informačných systémoch evidencie klientov

Aj osobitné kategórie osobných údajov a to hlavne z dôvodu evidencie klientov

- meno, priezvisko a titul, obchodné meno, / PO alebo FO – podnikateľ /,
- adresa klienta
- kontakty /telefón, e-mail a pod.../, kontaktné adresy

Tieto údaje prevádzkovateľ spracováva v aplikačnom softvéri a v dokumentoch za účelom:

- vedenia klientskej databázy
- zákaznícky servis

4/ Informačný systém: IS E-shop

Zoznam osobných údajov spracúvaných v informačných systémoch E-shop

Zoznam osobných údajov pre aplikačný softvér a dokumentáciu:

- meno, priezvisko a titul, obchodné meno, / PO alebo FO – podnikateľ /,
- kontakty /telefón, e-mail a pod.../, kontaktné adresy, miesto dodania tovaru

Tieto údaje prevádzkovateľ spracováva v aplikačnom softvéri a v dokumentoch za účelom:

- objednávky

- fakturácie

5/ Informačný systém: IS Kamerový systém

Kamerový systém je určený na získavanie osobných údajov monitorovaním alebo iným zaznamenávaním na nosič informácií. Vykonáva sa iba vtedy, ak sú splnené podmienky zákona a na dobu nevyhnutnú pre spracúvanie získaných osobných údajov.

Osobné údaje kamerový systém zaznamenáva – statickým alebo dynamickým videozáznamom fyzickej osoby, ktorý je možné využívať ako všeobecne použiteľný identifikátor dotknutej osoby, ktorý sa nachádza v monitorovanom priestore. Priestor prístupný verejnosti sa monitoruje len na účely ochrany verejného poriadku a bezpečnosti, odhaľovania kriminality, narušenia bezpečnosti štátu, ochrany majetku alebo zdravia. Tento priestor je zreteľne označený ako monitorovaný. Vyhotovený záznam sa používa len na účely trestného konania alebo konania o priestupkoch.

Obsluhu bezpečnostného kamerového systému, zaznamenávanie a ďalšiu manipuláciu s osobnými údajmi vykonáva iba určená oprávnená osoba prevádzkovateľa. Ak záznam vyhotovený kamerovým systémom nie je využitý na účely trestného konania alebo konania o priestupkoch, **likviduje sa najneskôr v lehote 15 dní odo dňa nasledujúceho po dni, v ktorom bol záznam vyhotovený**.

6/ Informačný systém: IS Registratúra

V IS registratúry osobné údaje bez osobitných kategórií. Jedná sa hlavne o evidenciu prijatej a odoslanej korešpondencie.

Používané osobné údaje :

- meno, priezvisko a titul, obchodné meno, / PO alebo FO – podnikateľ /,
- kontakty /telefón, e-mail a pod.../, kontaktné adresy

3. POSÚDENIE NUTNOSTI A PRIMERANOSTI SPRACOVATEĽSKÝCH OPERÁCII VO VZŤAHU K ÚČELU

Prevádzkovateľ implementuje primerané technické a organizačné opatrenia, aby zabezpečil, že štandardne jeho systémy budú spracúvať len osobné údaje, ktoré sú nevyhnutne potrebné (a žiadne iné) pre každý konkrétny účel spracúvania. Rovnako tieto systémy ***musia zabezpečiť, že sa údaje nebudú spracúvať neobmedzene, ale len na nevyhnutnú dobu***. Rovnako musia takéto opatrenia ***zabezpečiť, aby osobné údaje neboli štandardne prístupné neobmedzenému počtu zamestnancov prevádzkovateľa, ale len zamestnancom, ktorí nevyhnutne potrebujú prístup k týmto osobným údajom.***

4. POSÚDENIE RIZIKA PRE PRÁVA A SLOBODY DOTKNUTÝCH OSÔB, KTORÉ VYPLÝVA ZO SAMOTNEJ PODSTATY ZAMÝŠĽANÉHO SPRACÚVANIA OSOBNÝCH ÚDAJOV

Prevádzkovateľ si uvedomuje dôležitosť ochrany informácií, ktoré sú dôležité pre činnosť organizácie a napĺňanie podnikateľského zámeru, je rozhodnutá chrániť si svoje dobré meno a kvalitu poskytovaných služieb. Z tohto dôvodu prijala Bezpečnostnú politiku IT, ktorá popisuje spôsob zaistenia celkovej bezpečnosti IS. Ďalej sa zaväzuje splniť všetky požiadavky legislatívy platnej v Slovenskej republike, zmluvné požiadavky finančné a organizačné podmienky potrebné na realizáciu bezpečnostných opatrení, vzdelávať a školiť všetkých zamestnancov s cieľom zvyšovať povedomie o bezpečnosti.
Po uplatnení zásad a opatrení uvedených v dokumentácii zostanú nekryté nasledovné riziká:

- odcudzenie alebo zničenie osobných údajov pri násilnom preniknutí cudzích osôb do priestorov prevádzkovateľa,
- zničenie, alebo poškodenie písomností a počítačov vplyvom poruchy sieťových rozvodov,
- zničenie objektu prevádzkovateľa a v ňom uložených AIS a DIS požiarom, záplavou alebo inou živelnou pohromou.

5. OPATRENIA NA RIEŠENIE RIZÍK VRÁTANE (PRÁVNYCH) ZÁRUK, BEZPEČNOSTNÝCH OPATRENÍ A MECHANIZMOV NA ZABEZPEČENIE OCHRANY OSOBNÝCH ÚDAJOV A NA PREUKÁZANIE SÚLADU S TÝMTO NARIADENÍM

Technické opatrenia

Osobné údaje je potrebné ukladať do tzv. zabezpečených priestorov prevádzkovateľa a chrániť ich pred prístupom neoprávnených osôb. Všetky priestory prevádzkovateľa je potrebné zabezpečiť pred neoprávneným vstupom použitím vhodných zábranných prostriedkov (bezpečnostné mreže a pod.), ako aj ochrannými mechanizmami (alarmy, zámky a pod.).
Monitory v jednotlivých kanceláriách umiestniť tak, aby sa so spracúvanými osobnými údajmi nemohla oboznámiť neoprávnená osoba pri vstupe do miestnosti. Ak sa inak nedá, tak používať privátne filtre na obmedzenie výhľadu nepovolaným osobám.

Tie aktíva, ktorých činnosť si nevyžaduje častú prítomnosť prevádzkovateľa uzamknúť a v pravidelných intervaloch kontrolovať.

Z hľadiska požiarnej bezpečnosti je plnenie zákona o ochrane pred požiarmi
– prevádzka je vybavená hasiacou technikou.

Ochrana pred neoprávneným prístupom

Zabezpečenie šifrovania údajov, aby sa správa webhostingu nedostal k prístupovým údajom. Zabezpečiť, pokiaľ je možné, aby pri pripojený externého konzultanta spoločnosti cez vzdialený prístup sa nemohol oboznámiť so žiadnymi osobnými údajmi – uzavrieť dokument obsahujúci osobné údaje.

Riadenie prístupu oprávnených osôb

Cieľom tohto typu opatrení je umožniť prístup do informačných systémov len autorizovaným používateľom a oprávneným osobám.
Zriadenie prístupu vykonáva konateľ spoločnosti, pričom dbá na dodržiavanie požiadavky, že prístup by mal mať používateľ len do tých častí informačného systému, ktoré nevyhnutne potrebuje.

Udelenie prístupových práv vykonáva konateľ spoločnosti, pričom:
- každý používateľ má jedinečné ID, aby bola zabezpečená zodpovednosť, resp. preukázateľnosť vykonaných činností v rámci informačného systému.

Používateľské ID je potrebné pravidelné kontrolovať, minimálne v intervale jedenkrát za 6 mesiacov.

Ochrana proti škodlivému kódu a sieťová bezpečnosť

Prijaté opatrenia proti škodlivému kódu prevádzkovateľ implementuje na úrovni:
- detekcie škodlivého kódu
- opravného softvéru a riadenia zmien, ako súčasť bezpečnostných opatrení pre riadenie zmien
- primeranom prístupe pracovníkov k informačným systémom.

V podmienkach prevádzkovateľa je zakázané používanie neautorizovaného softvéru. Tento môže byť obstarávaný len z dôveryhodných zdrojov a to tak, aby nedošlo k porušeniu autorských práv. Všetky pracovné stanice musia byť opatrené antivírusovým detekčným softvérom, ako aj nápravným softvérom a to pre potreby automatickej: kontroly všetkých súborov a médií (archívne, záložné a pod.), kontroly elektronickej pošty a kontroly webovej stránky prevádzkovateľa.

Súbory s definíciami škodlivého kódu a skenovacie procesy antivírusového softvéru musia byť pravidelne aktualizované, minimálne však v intervale jedenkrát za deň.
Pre potreby filtrovania prenosu a blokovania neautorizovaného prístupu k aktívam prevádzkovateľa je potrebné, aby pracovné stanice boli zabezpečené firewallom.

Zálohovanie

Zálohovanie databáz počítačového systému je proces, pri ktorom sa vytvorí kópia všetkých databázových súborov programu alebo jej najdôležitejšej časti, nevyhnutná na obnovu funkčnosti všetkých databáz v prípade jeho havárie, poruchy alebo krádeže počítača.
Na vytvorenie zálohových súborov sa najčastejšie používajú štandardné komprimačné algoritmy akými sú napr. ZIP, RAR.

Periodicita zálohovania:
1. Denné zálohovanie (prevádzkové) - vykonávanie denných záloh na ten istý pevný disk počíta na ktorom je umiestnený program a to každý deň po ukončení práce v aplikačnom programe prostredníctvom funkcie aplikačného programu.
2. Týždenné/ Mesačné zálohovanie (archivačné) – vykonávanie záloh na externé médium - server. Zálohy slúžiace na archiváciu dát, vytvárajú sa v pravidelnom intervale. Zálohovanie na externé médiá je bezpečnejší spôsob, ktorý eliminuje riziká technickej alebo inej poruchy pevného disku. Na druhej strane je ale vyššie riziko narušenia údajov, nakoľko sa údaje nachádzajú na viacerých médiách.

Likvidácia osobných údajov

Oprávnená osoba je oprávnené spracúvať osobné údaje iba počas doby nevyhnutej pre dosiahnutie daného účelu. Po skončení účelu spracúvania je potrebné zabezpečiť likvidáciu dokladov obsahujúcich osobné údaje vedené v písomnej forme na papieri, pokiaľ osobitný zákon neustanovuje inak !

! Prevádzkovateľ je povinný osobné údaje zlikvidovať, keď sa naplní účel spracúvania !

Spôsoby likvidácie osobných údajov:
1. papierová podoba: fyzicky zničiť v škartačnom stroji, pokiaľ likvidujeme len časť údajov – textu na papierovom nosiči, je nutné tento údaj začierniť spôsobom, aby nebolo možné odhaliť jeho obsah
2. elektronická podoba: trvalé vymazanie zo servera, pevného disku, prekrytie osobných údajov prázdnymi znakmi, alebo iným textom.

Aktualizácia OS a programového aplikačného vybavenia

Je zabezpečená pravidelná aktualizácia OS a aplikačných programov, antivírusového systému z prostredia internetu.
Pravidelná aktualizácia umožňuje užívateľovi využívať najnovšie verzie softvérových aplikácií a antivírusovú ochranu. Používateľ je upozornený na automatickú aktualizáciu a možnosť jej nainštalovania reštartovaním systému ihneď alebo pri jeho vypnutí.

Organizačné opatrenia - Personálne opatrenia

Cieľom personálnych opatrení na zaistenie ochrany osobných údajov je zredukovať riziko ľudského zlyhania pri ochrane osobných údajov, najmä takých prejavov, ako odcudzenie, strata, po škodenie, zmena, rozširovanie, neoprávnené zverejňovanie osobných údajov alebo ich poskytovanie neoprávneným osobám.

Medzi základné opatrenia patria najmä:
a) Nakladať s osobnými údaje smú len oprávnené osoby konkrétneho pracoviska. Spracovávanie údajov musí byť v súlade so zákonom ochrane osobných údajov v znení neskorších predpisov.
b) Zabezpečiť, aby prístup k osobným údajom v IS mali iba oprávnené osoby, a prevádzkovateľ.
c) Používanie technických prostriedkov pre spracúvanie osobných informácii je povolené iba osobám oprávneným oboznamovať sa s osobnými informáciami. Zamestnanci, ktorý majú pridelené technické prostriedky, sú zodpovední za ich správny chod a musia dodržiavať všetky zásady práce s nimi.
d) Každá oprávnená osoba je povinná zachovávať mlčanlivosť o osobných údajoch, ktoré spracúvajú. Povinnosť mlčanlivosti trvá aj po ukončení spracovania. Povinnosť mlčanlivosti nemajú, ak je to podľa osobitného zákona nevyhnutné na plnenie úloh orgánov činných v trestnom konaní. Povinnosť mlčanlivosti platí aj pre iné fyzické osoby, ktoré v rámci svojej činnosti prídu do styku s osobnými údajmi. Povinnosť mlčanlivosti trvá aj po zániku funkcie oprávnenej osoby alebo po skončení jej pracovného pomeru alebo obdobného pracovného vzťahu. Povinnosť mlčanlivosti platí aj pre iné fyzické osoby, ktoré v rámci svojej činnosti prídu do styku s osobnými údajmi – IT technik. Povinnosť mlčanlivosti trvá aj po zániku funkcie oprávnenej osoby alebo po skončení jej pracovného pomeru alebo obdobného pracovného vzťahu.

Pri narušení informačnej bezpečnosti v oblasti informačného systému a miestnej siete činnosti koordinuje konateľ/ poverený informatik . Pri narušení informačnej bezpečnosti v oblasti dokumentov, telefónnych a mobilných sietí koordinuje činnosti poverený pracovník.

Riadenie prístupu oprávnených osôb k IS

Ochrana počítača pred nepovolaným prístupom stanovením pravidiel pre IS prevádzkovateľa pomocou vstupných hesiel do LAN / WIFI siete, PC systému ako aj aplikačných programov.

Používať najmä:

- heslo pre prihlásenie sa do operačného systému počítača
- zabezpečenie pomocou kľúča počítača
- heslo pri vstupe do aplikačného programu
- do budúcnosti riešiť prístup k PC niektorými z moderných hardvérových prostriedkov (čipové karty, hardvérový kľúč)
- iné heslá pre rôzne úrovne vstupu do informačného systému, ktoré sa pravidelne menia.

Cieľom tohto typu opatrení je umožniť prístup do sieťových zdrojov a informačných systémov prevádzkovateľa len autorizovaným používateľom a oprávneným osobám.

Vstupné a prihlasovacie heslá

Oprávnená osoba je povinná počítač, na ktorom spracúva osobné údaje, zabezpečiť heslom v súlade s ustanoveniami príslušnej bezpečnostnej dokumentácie, to znamená heslo sa musí mať min. 6 znakov a musí sa skladať z kombinácií písmen a čísiel, malých a veľkých písmen resp. špeciálnych znakov (+,*,@, &,#...).

Organizácia spracúvania osobných údajov

Manipulácia s papierovou dokumentáciou
Osobné údaje sú v informačnom systéme spracúvané aj neautomatizovaným spôsobom v písomnej podobe na papieri uložené v papierových zakladacích obaloch. Tieto dokumenty oprávnená osoba ukladá do uzamykateľných kontajnerov, alebo do iných uzamykateľných zariadení a v uzamykateľnej miestnosti. Dokumenty obsahujúce osobné údaje musia byť v čase neprítomnosti oprávnenej osoby neprístupné, a to buď uzamknutím miestnosti alebo skrine do ktorých sú osobné údaje vkladané. V žiadnom prípade nesmú doklady obsahujúce osobné údaje byť počas neprítomnosti oprávnenej osoby prístupné komukoľvek, kto vojde do miestnosti v ktorom sa spracúvajú osobné údaje. Oprávnená osoba je povinná dvere, kde sú umiestnené PC a informačné systémy obsahujúce osobné údaje, pri svojom odchode z pracoviska, ak sa na pracovisku nenachádza už žiadna oprávnená osoba, uzamknúť a zavrieť okná.

Prenášanie písomností obsahujúcich osobné údaje

a) Písomnosti s osobnými údajmi v podobe objednávok, faktúr, potvrdení o platbe je možné prenášať mimo pracoviska výhradne v zalepenej obálke alebo uzavretom obale, s otvorom prelepeným lepiacou páskou a priečne opečiatkovaným pečiatkou prevádzky a podpisom oprávnenej osoby.
b) Takto pripravené písomnosti prenáša len na túto činnosť poverený personál prevádzkovateľa.
c) Písomnosti obsahujúce osobné údaje sa v prípade potreby zasielania, posielajú výhradne len doporučenou poštovou zásielkou prvou triedou alebo kuriérom.
d) V prípade, že prevádzkovateľ dostane zásielku obsahujúce osobné údaje v poškodenom obale, preverí dôvod poškodenia u doručujúcej osoby a odsúhlasí obsah zásielky s odosielateľom.

Rozmnožovanie písomností obsahujúcich osobné údaje

a) Rozmnožovaním sa rozumie opakovaná tlač dokumentov z automatizovaného systému, vyhotovovanie fotokópií, odpisov a výpisov písomností s citlivými osobnými údajmi.
b) Rozmnožovať písomnosti môže zodpovedná osoba alebo ňou poverená osoba, ktorá je oprávnená na prácu s osobnými údajmi v IS. Táto osoba je povinná tlačiť a kopírovať dokumenty tak, aby sa s nimi neoprávnená osoba nemohla oboznámiť – výstup z tlačiarne nesmie oprávnená osoba nechať voľne položený v zásobníku tlačiarne. Akýkoľvek výstup z tlačiarne, ktorý nie je a nebude predmetom ďalšieho spracúvania musí oprávnená osoba zlikvidovať skartovaním.

Úlohy a povinnosti prevádzkovateľa pri práci s automatizovaným IS

a) Oprávnená osoba využíva k spracúvaniu osobných údajov len tie aktíva, ktoré boli prevádzkovateľom schválené. Je neprípustné k spracúvaniu používať súkromné notebooky, mobily bez toho, aby určený pracovník prevádzkovateľa – konateľ alebo poverený pracovník IT takéto použitie schválil.
b) Priebežne počas práce s IS sleduje jeho činnosť a prípadné nekorektné správanie konzultuje s nadriadeným, prípadne s pracovníkom IT alebo konateľom.
c) Oprávnená osoba je povinná v prípade podozrenia výskytu technickej poruchy na elektronických technických zariadeniach, ktorá by mohla mať za následok narušenie bezpečnosti osobných údajov, neodkladne informovať svojho zodpovedného pracovníka IT alebo konateľa.
d) Oprávnená osoba pri práci s PC nesmie ignorovať tzv. varovné správy alebo príznaky chýb, či inú nesprávnu alebo neobvyklú činnosť PC, ale takúto „odchýlku“ bezodkladne nahlásiť osobe, ktorá je zodpovedná za údržbu a servis počítačov, v ktorých sa nachádzajú osobné údaje t.j. pracovníkovi IT.
e) Pri spracúvaní osobných údajov prostredníctvom PC, je oprávnená osoba povinná zabezpečiť, aby obrazovky monitora nesprístupňovali osobné údaje dotknutých osôb iným fyzickým osobám (napr. komukoľvek kto vojde do miestnosti, kde sa spracúvajú osobné údaje).
f) Oprávnená osoba sa musí vyvarovať konaniu, ktoré by malo za následok infikovanie počítača škodlivými kódmi, sťahovaniu spoločensky neprípustného obsahu a inštalácii softvéru, ak tento nebol vopred prevádzkovateľom schválený.
g) Oprávnená osoba je povinná používať technické prostriedky tak, aby sa neumožnilo zdieľanie dát chránených autorskými právami ako aj osobných údajov iným používateľom siete internet.
h) Oprávnená osoba nesmie použiť aktíva prevádzkovateľa na akýkoľvek neoprávnený útok, pokus o útok alebo prienik do iných informačných systémov a obdobnej prevádzkovateľom neschválenej alebo protiprávnej činnosť.
i) Oprávnená osoba smie používať technické prostriedky prevádzkovateľa na súkromné účely len s jeho súhlasom. Pomocný obslužný personál nesmie mať prístup k informačnému systému. V neprítomnosti oprávnených osôb musí byť priestor s IS uzamknutý a prístup do počítača musí byť chránený heslom.
j) Oprávnená osoba je povinná dbať na to, aby svojim chovaním nespôsobila inú, nemateriálnu ujmu, poškodenie dobrého mena a povesti prevádzkovateľa.
k) Zdržiavanie sa osôb vrátane oprávnených, v priestoroch, kde sa nachádzajú informačné systémy obsahujúce osobné údaje, po pracovnej dobe je možné iba so súhlasom štatutárneho orgánu prevádzkovateľa / konateľa.

Zásady pre používanie prenosných počítačov

a) V prípade práce s prenosným počítačom súbory s osobnými údajmi, dôvernými informáciami ukladať len v nevyhnutných prípadoch. Používateľ zodpovedá za fyzickú ochranu prenosného zariadenia proti krádeži, zneužitiu, poškodeniu.
b) Je zakázané pracovať s dôvernými informáciami a osobnými údajmi na verejne prístupných

miestach. (kaviarne, čakárne a pod.)
c) Súbory s osobnými údajmi a dôvernými informáciami uložené na fyzickom médiu počas presunu musia byť uložené v šifrovanej forme, šifrovanej pomocou špecializovaného softvéru použitím dostatočne silného kryptografického algoritmu, alebo spustiteľné len špeciálnou aplikáciou.
d) V prípade, ak oprávnená osoba pracuje s osobnými údajmi prevádzkovateľa v domácom prostredí nesmie za týmto účelom využívať súkromné e - mailové schránky na voľne dostupných e - mailových serveroch, ale výlučne pracovné e - mailové schránky. Taktiež musí prijať také opatrenia, aby osobné údaje spracúvané v domácom prostredí neboli neoprávnené sprístupnené, poskytnuté, zverejnené resp. aby nedošlo k akýmkoľvek neprípustným formám spracúvania, kedy by sa s osobnými údajmi mohli oboznámiť neoprávnené osoby.

Zásady pri práci s elektronickou poštou

a) Je zakázané prostredníctvom emailu, telefonických hovorov, prípadne iných komunikačných prostriedkov šíriť dôverné informácie prevádzkovateľa IS.
b) Pri odosielaní osobných údajov prostredníctvom elektronickej pošty oprávnená osoba vždy dôsledne preverí správnosť e - mailovej adresy. Oprávnená osoba je povinná používať antivírusovú ochranu prichádzajúcej a odchádzajúcej pošty a nikdy ju nevypínať.
c) Pri odosielaní elektronickej pošty oprávnená osoba využíva zabezpečenie. Oprávnená osoba nereagujte na správy typu: „pošlite tento e - mail všetkým svojim známym“. Je to porušenie internetovej etiky, obťažuje to ostatných používateľov a zahlcuje to komunikačné linky.
d) Je zakázané posielanie a otváranie príloh - pripojených súborov v elektronickej pošte, ktoré môžu nejakým spôsobom ohroziť alebo poškodiť prevádzku informačného systému, trvale alebo dočasne znížiť jeho výkonnosť alebo ohroziť jeho bezpečnosť.

Bezpečnostné incidenty

Zaznamenávanie údajov je potrebné pre prijatie vhodných priebežných opatrení, ako aj následnej analýzy priebehu bezpečnostného incidentu s cieľom zamedzenia opätovnému výskytu. Ak je to nutné zodpovedný pracovník prevádzkovateľa implementuje opatrenia pre zamedzenie ďalších dôsledkov incidentu, ako aj možnosti jeho opakovania. Následne treba nahlásiť incident ak unikli osobné údaje **najneskôr do 72 hodín úradu na ochranu osobných údajov.** Kontrolnú činnosť zabezpečuje konateľ spoločnosti alebo ním určený pracovník.

6. ZOHĽADNENIE PRÁV A OPRÁVNENÝCH ZÁUJMOV DOTKNUTÝCH OSÔB A ĎALŠÍCH OSÔB, KTORÝCH SA ZAMÝŠĽANÉ SPRACÚVANIE TÝKA.

Základným bezpečnostným zámerom tohto dokumentu je ochrana osobných údajov všetkých dotknutých osôb – zamestnancov prevádzkovateľa (aj potenciálnych), ktorí poskytli svoje osobné údaje pre účel vytvorenia pracovno-právneho vzťahu. Pod túto skutočnosť ďalej spadá ochrana osobných údajov externých spolupracovníkov, s ktorými prevádzkovateľ môže dôjsť do styku v rámci jeho predmetov podnikania. Rovnako tak budú chránené osobné údaje dotknutých osôb, klientov – zákazníkov prevádzkovateľa. Ďalej môžu byť dotknutými osobami v zmysle tohto bezpečnostného zámeru aj všetky osoby, ktorým je umožnený vstup do priestorov prevádzkovateľa.

Prevádzkovateľ zabezpečuje dotknutým osobám nasledovné:

- pred začatím spracúvania jednoznačne a konkrétne vymedzí účel spracúvania,

- povinnosť oznámenia incidentu dotknutej osobe v závažných prípadoch,
- právo na prenosnosť údajov dotknutých osôb,
- právo na výmaz dotknutej osoby (ak sú dáta protizákonne spracúvané),
- možnosť odvolať súhlas dotknutej osoby kedykoľvek,
- na rozdielne účely získavať osobné údaje osobitne,
- osobné údaje získané na rôzne účely nezdružovať,
- spracúvať len správne, úplné a aktualizované osobné údaje,
- nesprávne a neúplné osobné údaje blokovať, opraviť alebo doplniť,
- nesprávne údaje, ktoré nie je možné opraviť alebo doplniť zlikvidovať,
- zabezpečiť, aby osobné údaje boli spracúvané vo forme umožňujúcej identifikáciu dotknutých osôb počas doby nie dlhšej, ako je nevyhnutné na dosiahnutie účelu spracúvania,
- zlikvidovať osobné údaje, ktorých účel spracúvania sa skončil,
- spracúvať osobné údaje v súlade s dobrými mravmi,
- nevynucovať súhlas dotknutej osoby hrozbou odmietnutia zmluvného vzťahu, dodania služieb alebo tovaru,
- vo všeobecne zrozumiteľnej forme poskytnúť informácie o stave spracúvania osobných údajov v rozsahu: názov, sídlo alebo trvalý pobyt, právnu formu a identifikačné číslo prevádzkovateľa; meno a priezvisko štatutárneho orgánu prevádzkovateľa; identifikačné označenie informačného systému; účel spracúvania, zoznam osobných údajov a okruh dotknutých osôb; okruh príjemcov, ktorým sú alebo budú údaje sprístupnené, tretie strany, ktorým osobné údaje sú alebo budú poskytnuté; tretie krajiny, do ktorých sa uskutočňuje prenos osobných údajov; právny základ informačného systému; formu zverejnenia, ak sa zverejnenie osobných údajov vykonáva; všeobecnú charakteristiku opatrení za zabezpečenia ochrany osobných údajov a dátum začatia a dobu spracúvania,
- vo všeobecne zrozumiteľnej forme presné informácie o zdroji, z ktorého boli osobné údaje získané,
- vo všeobecne zrozumiteľnej forme odpis osobných údajov,
- opraviť nesprávne, neúplné alebo neaktuálne osobné údaje,
- likvidovať osobné údaje po splnení účelu spracúvania; vrátiť úradné doklady, ak boli predmetom spracúvania,
- likvidáciu osobných údajov, ak došlo k porušeniu zákona.
- bezodkladné písomné oznámenie dotknutej osobe a Úradu na ochranu osobných údajov SR, že na základe písomnej žiadosti oprávnenej osoby, ktorej práva boli obmedzené, boli jej nesprávne, neúplné alebo neaktuálne osobné údaje opravené,
- prípadne zlikvidované; ak boli predmetom spracúvania úradné doklady obsahujúce osobné údaje, že jej boli vrátené,

- realizáciu technických, personálnych a organizačných opatrení a dohliada na ich aplikáciu v praxi,
- dohľad pri výbere sprostredkovateľa a prípravu písomnej zmluvy alebo poverenia pre sprostredkovateľa; preveruje dodržiavanie dohodnutých podmienok,
- dohľad nad cezhraničným tokom osobných údajov.

Vypracoval: Peter Jurák

Schválil: