METROPOLA TRADE s.r.o.

POSÚDENIE VPLYVU NA OCHRANU OSOBNÝCH ÚDAJOV DPIA

Data Protection Impact Assessment podľa GDPR v súlade so Zákonom č. 18/2018 Z.z. - o ochrane osobných údajov a o zmene a doplnení niektorých zákonov a nariadením Európskej Únie upravujúce ochranu osobných údajov a Rady EÚ č. 2016/679

Vypracoval: Ing. Lenka PAPÍKOVÁ /externý konzultant 0948 310 013/

ÚVODNÉ PREHLÁSENIE

Spoločnosť METROPOLA TRADE s.r.o. ako autorizovaný partner NTN-SNR, v zastúpení konateľky a majiteľky. čestne prehlasuje:

1 . Organizácia má menej ako 250 zamestnancov a spracovanie osobných údajov nie je jej hlavnou činnosťou, neexistuje u nej riziko pre dotknutie sa práv a slobody osôb a organizácia nespracúva citlivé údaje za účelom poskytnutia tretím stranám

2. METROPOLA TRADE s.r.o. zavádza technické, organizačné a procesné opatrenia na za účelom preukázania súladu s princípmi GDPR a to najmä:

- implementácia zámernej a nevyhnutnej ochrany dát
- vypracovanie smernice DPIA, čiže posúdenie vplyvu jednotlivých činností spracovania na ochranu osobných údajov
- vymenovanie poverenej a zodpovednej osoby pre ochranu osobných údajov

MENO OSOBY POVERENEJ PRE OCHRANU OSOBNÝCH ÚDAJOV (DATA PROTECTION OFFICER):

Osoba je zodpovedná za správu OÚ a implementáciu GDPR do praxe: **Peter Molčányi**

3. METROPOLA TRADE prehlasuje, že dáta ako zdravotný stav, sexuálna orientácia, religiózne zaradenie, členstvo a sympatie alebo nesympatie k politickým stranám a hnutiam, súkromné maily, kontá na sociálnych sieťach a pod. nevyžaduje, nespracováva a neuchováv

Pri ochrane osobných údajov, ktoré podliehajú ochrane v zmysle GDPR, postupuje v zmysle usmernení a príslušných zákonov. Táto príručka – usmernenie, okrem iného aj popisuje jednotlivé dáta a ich stupeň a spôsob ochrany.

V Košiciach dňa 1.1.2018 Bc. Marcela Blašková

OBSAH

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
GDPR	General Data Protection Regulation

1. ZÁKLADNÉ POJMY

Osobnými údajmi sú údaje týkajúce sa určenej alebo určiteľnej fyzickej osoby, pričom takou osobou je osoba, ktorú možno určiť priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora alebo na základe jednej či viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú, fyziologickú, psychickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu.

Dotknutou osobou každá fyzická osoba, ktorej sa osobné údaje týkajú,

Prevádzkovateľom každý, kto sám alebo spoločne s inými vymedzí účel spracúvania osobných údajov, určí podmienky ich spracúvania a spracúva osobné údaje vo vlastnom mene; ak účel, prípadne aj podmienky spracúvania osobných údajov ustanovuje zákon, priamo vykonateľný právne záväzný akt Európskej únie alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, prevádzkovateľom je ten, kto je na plnenie účelu spracúvania za prevádzkovateľa ustanovený alebo kto spĺňa zákonom, priamo vykonateľným právne záväzným aktom Európskej únie alebo medzinárodnou zmluvou, ktorou je Slovenská republika viazaná, ustanovené podmienky,

Zástupcom prevádzkovateľa každý, kto na území Slovenskej republiky zastupuje prevádzkovateľa so sídlom, organizačnou zložkou, prevádzkarňou alebo trvalým pobytom v tretej krajine,

Sprostredkovateľom každý, kto spracúva osobné údaje v mene prevádzkovateľa, v rozsahu a za podmienok dojednaných s prevádzkovateľom v písomnej zmluve a v súlade so zákonom,

Oprávnenou osobou každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovného pomeru, štátnozamestnaneckého pomeru, služobného pomeru, členského vzťahu, na základe poverenia, zvolenia alebo vymenovania, alebo v rámci výkonu verejnej funkcie, a ktorá spracúva osobné údaje v rozsahu a spôsobom určeným v poučení,

Treťou stranou každý, kto nie je dotknutou osobou, prevádzkovateľom poskytujúcim osobné údaje, Jeho zástupcom, sprostredkovateľom alebo oprávnenou osobou,

Príjemcom každý, komu sú osobné údaje poskytnuté alebo sprístupnené, pričom príjemcom môže byť aj tretia strana; prevádzkovateľ, ktorý spracúva osobné údaje a úrad, ktorý plní úlohy ustanovené zákonom, sa nepovažujú za príjemcu.

Spracúvaním osobných údajov vykonávanie operácií alebo súboru operácií s osobnými údajmi, najmä ich získavanie, zhromažďovanie, šírenie, zaznamenávanie, usporadúvanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, premiestňovanie, využívanie, uchovávanie, blokovanie, likvidácia, ich cezhraničný prenos, poskytovanie, sprístupňovanie alebo zverejňovanie; niektorými operáciami s osobnými údajmi sa podľa prvej vety rozumie

Poskytovaním osobných údajov odovzdávanie osobných údajov tretej strane, ktorá ich ďalej spracúva,

Sprístupňovaním osobných údajov oznámenie osobných údajov alebo umožnenie prístupu k nim príjemcovi, ktorý ich ďalej nespracúva,

Zverejňovaním osobných údajov publikovanie, uverejnenie alebo vystavenie osobných údajov na verejnosti prostredníctvom masovokomunikačných prostriedkov, verejne prístupných počítačových sietí, verejným vykonaním alebo vystavením diela, verejným vyhlásením, uvedením vo verejnom zozname, v registri alebo v operáte, ich umiestnením na úradnej tabuli alebo na inom verejne prístupnom mieste,

Cezhraničným prenosom osobných údajov prenos osobných údajov mimo územia Slovenskej republiky a na územie Slovenskej republiky,

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

Blokovaním osobných údajov dočasné alebo trvalé pozastavenie spracúvania osobných údajov, počas ktorého možno vykonávať len tie operácie s osobnými údajmi, ktoré sú nevyhnutné na splnenie povinnosti uloženej zákonom,

Informačným systémom osobných údajov informačný systém, v ktorom sa na vopred vymedzený alebo ustanovený účel systematicky spracúva alebo má spracúvať akýkoľvek usporiadaný súbor osobných údajov prístupných podľa určených kritérií, bez ohľadu na to, či ide o informačný systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe (ďalej len „informačný systém“); informačným systémom sa na účely zákona rozumie aj súbor osobných údajov, ktoré sú spracúvané alebo pripravené na spracúvanie čiastočne automatizovanými alebo inými ako automatizovanými prostriedkami spracúvania,

Účelom spracúvania osobných údajov vopred jednoznačne vymedzený alebo ustanovený zámer spracúvania osobných údajov, ktorý sa viaže na určitú činnosť,

Súhlasom dotknutej osoby akýkoľvek slobodne daný výslovný a zrozumiteľný prejav vôle, ktorým dotknutá osoba na základe poskytnutých informácií vyjadruje súhlas so spracúvaním svojich osobných údajov,

Podmienkami spracúvania osobných údajov prostriedky a spôsob spracúvania osobných údajov, ako aj ďalšie požiadavky, kritériá alebo pokyny súvisiace so spracúvaním osobných údajov alebo vykonanie úkonov, ktoré slúžia na dosiahnutie účelu spracúvania či už pred začatím spracúvania osobných údajov, alebo v priebehu ich spracúvania,

Biometrickým údajom osobný údaj fyzickej osoby označujúci jej biologickú alebo fyziologickú vlastnosť alebo charakteristiku, na základe ktorej je jednoznačne a nezameniteľne určiteľná; biometrickým údajom je najmä odtlačok prsta, odtlačok dlane, analýza DNA,

Všeobecne použiteľným identifikátorom trvalý identifikačný osobný údaj dotknutej osoby, ktorý zabezpečuje jej jednoznačnosť v informačných systémoch,

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

Anonymizovaným údajom osobný údaj upravený do takej podoby, v ktorej ho nemožno priradiť dotknutej osobe, ktorej sa týka,

Priestorom prístupným verejnosti priestor, do ktorého možno voľne vstupovať a v ktorom sa možno voľne zdržiavať bez časového obmedzenia alebo vo vymedzenom čase, pričom iné obmedzenia, ak existujú a sú osobou splnené, nemajú vplyv na vstup a voľný pohyb osoby v tomto priestore, alebo je to priestor, ktorý tak označuje osobitný zákon,

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

Treťou krajinou krajina, ktorá nie je členským štátom Európskej únie alebo zmluvnou stranou Dohody o Európskom hospodárskom priestore,

Verejným záujmom dôležitý záujem štátu realizovaný pri výkone verejnej moci, ktorý prevažuje nad oprávneným záujmom fyzickej osoby alebo viacerých fyzických osôb a bez jeho realizácie by mohli vzniknúť rozsiahle alebo nenahraditeľné škody.

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

Údaje prevádzkovateľa:	METROPOLA TRADE s.r.o. Benádova č.3 , 04001 Košice IČO : 36 701 700 IČ DPH : SK 202 227 9897
Deň zápisu do OR:	24.11.2006
Právna forma:	Spoločnosť s ručením obmedzeným
Hlavný predmet činnosti:	Autorizovaný distribútor NTN -SNR

1/ Osobné údaje zamestnancov v sekcii MZDY A PERSONALISTIKA

Zoznam osobných údajov spracúvaných v informačných systémoch mzdy a personalistika - 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
- 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)

- meno, priezvisko, rodné priezvisko manžela/ky
- dátum narodenia rodné číslo manžela/ky

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,
- 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, 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/ Osobné údaje v INFORMAČNOM PODNIKOVOM SOFTVÉRI - účtovníctvo

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 spoločnosti METROPOLA TRADE s.r.o.
Okruh užívateľov, ktorým sa osobné údaje poskytujú: Zdravotné poisťovne, 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/ Osobné údaje v INFORMAČNOM PODNIKOVOM SOFTVÉRI - klienti

Zoznam osobných údajov spracúvaných v informačných systémoch (aj osobitné kategórie osobných údajov a to hlavne z dôvodu evidencie klientov).

Zoznam osobných údajov pre aplikačný softvér a dokumentáciu:

- meno, priezvisko a titul, obchodné meno, ak sa jedná o PO alebo FO - podnikateľa
- dátum a miesto narodenia,
- kontakty /telefón, e-mail a pod.../, kontaktné adresy,
- informácie o poistení a čísla bankových účtov

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

- vedenia evidencie klientov

4/ Informačný systém: IS Registratúra

V IS Správa registratúry sú aj osobitné kategórie osobných údajov a to hlavne z dôvodu evidencie došlej a odoslanej pošty.

- meno, priezvisko a titul, adresa trvalého bydliska,

- kontakty /telefón, e-mail a pod.../, kontaktné adresy

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

- evidencia došlej a odoslanej pošty

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:

Denné zálohovanie (prevádzkové) – vykonávanie denných záloh na ten istý pevný disk počítača na ktorom je umiestnený program a to každý deň po ukončení práce v aplikačnom programe prostredníctvom funkcie aplikačného programu.

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 zabezpečené 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 zodpovedný 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 koordinuje poverený pracovník oddelenia IT.

Riadenie prístupu oprávnených osôb k IS

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

Používať najmä:

- heslo pre prihlásenie sa do OS 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.

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 priameho nadriadeného alebo zodpovedného pracovníka IT.

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 je povinná 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 nadriadeného, prípadne štatutárneho orgánu prevádzkovateľa.

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 využívaní 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 otvára nie 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,
- 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.