

Bezpečnostný projekt o ochrane osobných údajov

OBSAH

- I. Účel a cieľ*
- II. Rozsah platnosti*
- III. Definícia pojmov*
- IV. Bezpečnostné opatrenia a ich využitie*
- V. Rozsah oprávnení a popis povolených činností oprávnených osôb*
 - V.1.a. Postup práce pri spracovaní personálnej a mzdovej agendy*
 - V.1.b. Postup práce pri spracovaní evidencie dotknutých osôb*
 - V.2 Spôsob identifikácie a autentizácie*
 - V.3 Povinnosti používateľov automatizovaného informačného systému*
- VI. Rozsah zodpovednosti*
 - VI.1 Zodpovednosť oprávnených osôb*
 - VI.2 Zodpovednosť zodpovednej osoby*
- VII. Kontrolná činnosť*
- VIII. Havarijné postupy*

I. ÚČEL A CIEĽ

Smernica stanovuje pravidlá pre spracúvanie osobných údajov. Cieľom je zabezpečiť ochranu osobných údajov pri manuálnom a automatizovanom spracúvaní.

II. ROZSAH PLATNOSTI

Smernica platí pre všetkých zamestnancov spoločnosti. Zväzne stanovuje povinnosti pre všetky oprávnené osoby, ktoré spracúvajú osobné údaje a zodpovedné osoby, ktoré dozerajú na dodržiavanie zákonných ustanovení pri spracúvaní osobných údajov. Porušenie smernice sa považuje za závažné porušenie pracovnej disciplíny.

III. DEFINÍCIA POJMOV

Osobné údaje – údaje týkajúce sa určenej alebo určiteľnej fyzickej osoby, pričom takouto 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.

Spracúvanie osobných údajov – vykonávanie akýchkoľvek operácií alebo súboru operácií s osobnými údajmi, napr. ich získavanie, zhromažďovanie, zaznamenávanie, usporadúvanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, premiestňovanie, využívanie, uchovávanie, likvidácia, ich prenos, poskytovanie, sprístupňovanie alebo zverejňovanie.

Prevádzkovateľ – Z&Z PARKETY, s.r.o., Južná trieda 121,040 01 Košice

Oprávnená osoba – každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovného pomeru

Zodpovedná osoba – osoba poverená výkonom dohľadu, ktorú prevádzkovateľ informačného systému písomne poveril dozeráť na dodržiavanie zákonných ustanovení pri spracúvaní osobných údajov.

Dotknutá osoba – každá fyzická osoba, o ktorej sa spracúvajú osobné údaje, zamestnanci uchádzači o zamestnanie, zákazníci

Informačný systém – akýkoľvek usporiadaný súbor, sústava alebo databáza obsahujúca jeden alebo viac osobných údajov, ktoré sú systematicky spracúvané na potreby dosiahnutia účelu podľa osobitných kritérií a podmienok s použitím automatizovaných, čiastočne automatizovaných alebo iných ako automatizovaných prostriedkov spracúvania bez ohľadu nato, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe, napr. kartotéka, zoznam, register, operát, záznam alebo sústava obsahujúca spisy, doklady, zmluvy, potvrdenia, posudky, hodnotenia, testy.

Automatizovaný informačný systém – (ďalej len „AIS“) súhrn technických prostriedkov výpočtovej techniky, programové a aplikačné vybavenie, údajová základňa, pamäťové médiá s údajmi, inštaláčne médiá, dokumentácia súvisiaca s technickým a programovým vybavením určeným na automatizované spracovanie údajov.

Používateľský účet – slúži na identifikáciu používateľa v automatizovanom informačnom systéme, umožňuje správne priradenie pridelených používateľských práv prihlásenému používateľovi, tvorí ho názov účtu a heslo.

Oprávnený používateľ – zamestnanec, ktorému bol zriadený používateľský účet a pridelené príslušné prístupové práva umožňujúce mu plnenie pracovných povinností.

Pracovné dokumenty – všetky súbory, ktoré používatelia automatizovaného informačného systému vytvorili alebo prevzali pre potreby spoločnosti.

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

Bezpečnostné opatrenie – vykonávaná prax, pracovný postup alebo zariadenie, ktoré znižujú riziko.

Stav núdze – udalosť, ktorej pretrvávanie alebo opakovanie by mohlo spôsobiť ohrozenie záujmov prevádzkovateľa.

IV. BEZPEČNOSTNÉ OPATRENIA A ICH VYUŽITIE

Medzi základné realizované bezpečnostné opatrenia patria:

- 1 · ochrana areálu a kontrola vstupu osôb,*
- 2 · povinná identifikácia a autentizácia pri prístupe k AIS,*
- 3 · zálohovanie a antivírová ochrana,*
- 4 · zamykanie miestností.*

Bezpečnostné opatrenia slúžia na obmedzenie a riadenie fyzického prístupu osôb, na riadenie logického prístupu k osobným údajom v elektronickej forme, na zabezpečenie dôvernosti a dostupnosti chránených osobných údajov.

Všetci zamestnanci organizácie sú povinní:

- 1 · dodržiavať bezpečnostné opatrenia, ktoré sú realizované na ochranu objektov, majetku osôb a osobných údajov,*
- 2 · dodržiavať interné smernice a predpisy,*
- 3 · v prípade úniku alebo podozrenia z úniku informácií z informačného systému, oznámiť túto skutočnosť zodpovednej osobe.*

V. ROZSAH OPRÁVNENÍ A POPIS POVOLENÝCH ČINNOSTÍ OPRÁVNENÝCH OSÔB

Medzi oprávnené osoby patria:

- 1 · ekonómka,*
- 2 · riaditeľ.*

Všetky osoby, ktorých pracovnou náplňou je spracúvanie osobných údajov – oprávnené osoby – musia byť poučené o povinnostiach vyplývajúcich zo zákona č. 428/2002 Z. z. o ochrane osobných údajov. O poučení sa vedie písomný záznam.

Osobné údaje je možné spracúvať pre potreby organizácie len na základe platných zákonov, právnych predpisov a interných dokumentov.

Spracúvajú sa len typy osobných údajov, ktoré je nevyhnutné spracúvať.

Likvidáciu osobných údajov môže oprávnená osoba vykonať len na základe súhlasu zodpovednej osoby.

Pri dočasnom opustení pracoviska sú všetci zamestnanci povinní odhlasovať sa z programov na spracovanie osobných údajov, prípadne používať šetrič obrazovky s nastaveným heslom, odkladať a uzamykať písomné dokumenty, ktoré obsahujú osobné údaje.

V.1. Postup práce pri spracovaní personálnej a mzdovej agendy

Ekonomka je oprávnená zisťovať osobné údaje o zamestnancoch a ich rodinných príslušníkoch, spracúvať ich manuálne a v elektronickej forme, prehliadať, usporadúvať a využívať ich na tvorbu dokumentov nevyhnutných pre personálnu a mzdovú agendu; opravovať, meniť, uchovávať a archivovať dokumenty, ktoré obsahujú osobné údaje.

Kópie úradných dokladov je možné vytvárať len na základe písomného súhlasu dotknutej osoby.

Súhlas musí obsahovať údaj o tom, kto súhlas poskytol, komu sa súhlas dáva, na aký účel, zoznam alebo rozsah osobných údajov, dobu platnosti súhlasu a podmienky jeho odvolania.

V prípade žiadostí o prijatie do zamestnania, ktoré sú doručené poštou, je potrebné písomne oznámiť žiadateľovi termín do kedy bude jeho žiadosť evidovaná a následne zlikvidovaná. Zároveň je potrebné ho požiadať, aby do tohto termínu zasielal prípadné zmeny osobných údajov.

Ak je žiadosť bezpredmetná, žiadateľ nie je vhodný, je potrebné písomne oznámiť žiadateľovi okamžitú likvidáciu žiadosti a jeho osobných údajov. Úradné doklady a kópie úradných dokladov, ktoré obsahujú osobné údaje, je potrebné vrátiť odosielateľovi.

Poskytovať a sprístupňovať osobné údaje o inej osobe cez telefón je zakázané. Oprávnené osoby môžu telefonicky potvrdiť, že dotyčná osoba je zamestnaná v organizácii, bez poskytovania ďalších osobných údajov.

Preberať potvrdenia o práceneschopnosti môže iba poučená osoba.

V.2 Spôsob identifikácie a autentizácie

Všetky oprávnené osoby sú povinné pri prístupe k informačnému systému prihlásiť sa menom a heslom.

Heslo musí obsahovať minimálne 6 znakov. Kombinácia znakov tvoriacich heslo nesmie byť jednoducho dešifrovateľná, nie je dovolené používať prihlasovacie meno do siete, mená a priezviská používateľov, ich rodinných príslušníkov, dátumy narodení a pod.



Odporúčaná je kombinácia veľkých a malých písmen spolu s číslicami a špeciálnymi znakmi ,,%, /, #, @, &, \$, (, ..., bez použitia diakritických znamienok. Heslá je potrebné pravidelne meniť každých 45 - 60 dní, po uplynutí doby platnosti sa heslá nesmú opakovať.

Za utajenie hesla zodpovedá používateľ. Heslá nesmú byť voľne dostupné, napr. vedľa počítača, pod klávesnicou, na stole a pod.

Používateľ je zodpovedný za neoprávnené sprístupnenie svojho hesla inej osobe, následne i za jeho zneužitie a spôsobené škody.

V.3 Povinnosti používateľov automatizovaného informačného systému

Automatizovaný informačný systém je určený na výkon prác súvisiacich s činnosťou organizácie a môže byť používaný len na tento účel. AIS nesmie byť používaný na súkromné, alebo iné účely, ktoré nesúvisia s činnosťou organizácie.

Základnými prostriedkami AIS, ktoré je možné používať pre plnenie stanovených pracovných povinností sú:

- 1 · počítač, ktorý, ktorý smie oprávnený používateľ používať,*
- 2 · nainštalované programové vybavenie,*
- 3 · sieťové služby dátových serverov,*
- 4 · výpočtová kapacita počítačových systémov pri používaní firemných sieťových aplikácií.*

Používateľ nesmie sám inštalovať akékoľvek programy, nesmie používať a šíriť nelegálne programové vybavenie, nesmie kopírovať a distribuovať nainštalované programy a operačné systémy, ich časti, súvisiacu dokumentáciu a manuály.

Všetky zmeny v konfigurácii počítača a ostatného technického vybavenia môžu byť vykonávané len administrátorom AIS.

Používateľ sa nesmie žiadnymi prostriedkami pokúšať získať prístupové práva, alebo privilegovaný stav, ktorý mu nebol nastavený administrátorom AIS. Pokiaľ používateľ v dôsledku chyby programových alebo technických prostriedkov získa privilegovaný stav, ktorý mu nebol udelený, alebo

Z&Z PARKETY, s.r.o., Južná trieda 121, 040 01 Košice,

Tel.: +421 55-677 09 67, mobil: +421 (0) 918 909 812

E-mail: info@zzparkety.sk, www.ParkettWorld

IČO: 31 683 380, IČ DPH: SK2020485665, vložka č. 4036/V, Okresný súd Košice I

Banka: VÚB, a. s., pob. Košice - č. účtu: 2086581553/0200

prístupové práva, ktoré mu neboli pridelené a nastavené, je povinný túto skutočnosť bezprostredne oznámiť zodpovednej osobe a administrátorovi AIS. Používateľ nesmie vykonávať takú činnosť, ktorá by ostatným používateľom bránila v riadnom používaní AIS.

Používateľ je povinný rešpektovať štruktúru adresárov na svojom počítači i na sieti, udržiavať poriadok v adresároch, rušiť nepotrebné súbory v týchto adresároch, nevytvárať prázdne adresáre, chaotické kópie a pod.

VI. ROZSAH ZODPOVEDNOSTI

VI.1 Zodpovednosť oprávnených osôb

Všetky oprávnené osoby sú povinné zachovávať mlčanlivosť o osobných údajoch, s ktorými prídu do styku, nesmú ich využívať pre vlastnú potrebu, nesmú ich zverejňovať ani nikomu prístupniť.

Povinnosť mlčanlivosti trvá i po skončení pracovného pomeru.

VI.2 Zodpovednosť zodpovednej osoby

Dohľadom nad dodržiavaním zákonných ustanovení pri spracúvaní osobných údajov musí byť písomne poverená zodpovedná osoba, ktorá bola odborne vyškolená. Rozsah odborného školenia zodpovedá najmä obsahu zákona o ochrane osobných údajov a medzinárodných zmlúv o ochrane osobných údajov. Absolvent odborného školenia obdrží písomné potvrdenie o absolvovaní.

Zodpovedná osoba posúdi pred začatím spracúvania osobných údajov, či ich spracúvaním nevzniká nebezpečenstvo narušenia práv a slobôd dotknutých osôb.

Zistenie narušenia práv a slobôd dotknutých osôb pred začatím spracúvania alebo porušenia zákonných ustanovení v priebehu spracúvania osobných údajov zodpovedná osoba bezodkladne písomne oznámi prevádzkovateľovi. Ak prevádzkovateľ po upozornení bezodkladne nevykoná nápravu, oznámi to zodpovedná osoba Úradu na ochranu osobných údajov SR.

Zodpovedná osoba zabezpečuje:

- potrebnú súčinnosť s Úradom na ochranu osobných údajov SR,*
- dohľad nad plnením základných povinností prevádzkovateľa*
- pred začatím spracúvania jednoznačne a konkrétne vymedziť účel spracúvania,*
- určiť prostriedky spôsob spracúvania, získavať osobné údaje výlučne na vymedzený účel,*

- zabezpečiť, aby sa spracúvali len také osobné údaje, ktoré svojim rozsahom a obsahom zodpovedajú účelu a sú nevyhnutné na dosiahnutie účelu spracúvania,
- na rozdielne účely získavať osobné údaje osobitne,
- osobné údaje získané na rôzne účely nezdržovať,
- 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,
- poučenie oprávnených osôb podľa § 17,
- do 30 dní vybavovanie žiadostí dotknutých osôb

- 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 a zodpovednej osoby; 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 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,*
 - *do 30 dní vybavovanie námietok dotknutých osôb voči*
 - *spracúvaniu osobných údajov na účely priameho marketingu bez jej súhlasu,*
 - *využívaniu osobných údajov na účely priameho marketingu v poštovom styku,*
 - *poskytovaniu osobných údajov na účely priameho marketingu,*
 - *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,*
 - *prihlásenie informačných systémov na osobitnú registráciu, oznamovanie zmien a odhlásenie; o informačných systémoch, ktoré nepodliehajú registrácii, vedie predpísanú evidenciu.*

Zodpovedná osoba odporúča technické, organizačné a personálne bezpečnostné opatrenia zodpovedajúce spôsobu spracúvania. V spolupráci s oprávnenými osobami navrhuje úpravy programového vybavenia a tlačených formulárov na základe zmien príslušných zákonov a predpisov tak, aby sa spracúvali iba nevyhnutne potrebné typy osobných údajov.

VII. KONTROLNÁ ČINNOSŤ

Zodpovedná osoba vykoná na základe zistenia narušenia práv a slobôd dotknutých osôb, minimálne však jeden krát ročne, kontrolu zameranú na dodržiavanie ochrany osobných údajov v príslušných informačných systémoch.

Zodpovedná osoba vykoná kontrolu:

- 1 · archivovania písomných dokumentov – vhodnosť podmienok na archivovanie,*
- 2 · v spolupráci so administrátorom AIS kontrolu funkčnosti a úplnosti záloh,*
- 3 · interných predpisov – presnosť a jednoznačnosť pracovných postupov pri spracúvaní osobných údajov.*

VIII. HAVARIJNÉ POSTUPY

V prípade zistenia poruchy akéhokoľvek prostriedku AIS je potrebné na túto skutočnosť upozorniť administrátora AIS. Administrátor AIS rozhodne o ďalšom postupe opravy, s ohľadom na zabezpečenie osobných údajov informuje zodpovednú osobu ak technický prostriedok alebo nosič informácií obsahujúce

osobné údaje, bude kvôli vykonaniu servisného zásahu premiestnený mimo areálu organizácie, prípadne ak servisný zásah bude vykonávať externá firma.

Na predchádzanie vzniku požiar je potrebné dodržiavať preventívne protipožiarne opatrenia v súlade s Požiarnym štatútom. V prípade požiaru sa postupuje podľa poplachových a evakuačných smerníc, ktoré sú súčasťou Požiarneho štatútu.

JUDr. Michal Zima

konateľ