Smernica

Ochrana osobných údajov

Názov organizácie: Slovenský rýchlokorčuliarsky zväz

Sídlo: Za Hornádom 15/1, 052 01 Spišská Nová Ves

Dátum spracovania: 1.5.2017

**Účel a cieľ**

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

**Rozsah platnosti**

Smernica stanovuje povinnosti pre všetkých zamestnancov organizácie Správa telovýchovných zariadení, ktorí spracúvajú osobné údaje. Porušenie smernice sa považuje za závažné porušenie pracovnej disciplíny.

**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, šírenie, zaznamenávanie, usporadúvanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, premiestňovanie, využívanie, uchovávanie, blokovanie, likvidácia, ich prenos, poskytovanie, sprístupňovanie alebo zverejňovanie.

Prevádzkovateľ – 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 ustanovené podmienky. Prevádzkovateľom je Slovenský rýchlokorčuliarsky zväz.

Sprostredkovateľ – každý, kto spracúva osobné údaje v mene prevádzkovateľa, v rozsahu a za podmienok dojednaných s prevádzkovateľom v písomnej zmluve.

Oprávnená osoba – každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovnoprávneho vzťahu s organizáciou Správa telovýchovných zariadení a ktorá spracúva osobné údaje v rozsahu a spôsobom určenom v poučení v zmysle zákona o ochrane osobných údajov.

Dotknuté osoby – každá fyzická osoba, o ktorej sa spracúvajú osobné údaje.

Informačný systém osobných údajov – je 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 tohto zákona rozumie aj súbor osobných údajov, ktoré sú spracúvané alebo pripravené na spracúvanie čiastočne automatizovanými alebo inými ako automatizovanými prostriedkami spracúvania.

Automatizované prostriedky spracúvania – (ďalej len „APS“) súhrn technických prostriedkov výpočtovej techniky, operačné systémy a aplikačné vybavenie, údajová základňa, pamäťové médiá s údajmi, inštalačné médiá, dokumentácia súvisiaca s technickým a programovým vybavením určeným na automatizované spracovanie údajov.

Užívateľský účet – slúži na identifikáciu užívateľa automatizovanými prostriedkami spracúvania, umožňuje správne priradenie pridelených užívateľských práv prihlásenému užívateľovi, tvorí ho názov účtu a heslo.

Oprávnený užívateľ – zamestnanec pracovnom vzťahu s organizáciou Slovenský rýchlokorčuliarsky zväz, ktorému bol zriadený užívateľský účet a pridelené príslušné prístupové práva umožňujúce mu plnenie pracovných povinností.

Pracovné dokumenty – všetky súbory, ktoré používatelia automatizovaných prostriedkov spracúvania vytvorili alebo prevzali pre potreby organizácie Slovenský rýchlokorčuliarsky zväz.

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

Bezpečnostný incident – neočakávaná alebo nežiadúca udalosť, ktorá môže ohroziť bezpečnosť osobných údajov.

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

Stav núdze – udalosť, ktorej pretrvávanie alebo opakovanie by mohlo spôsobiť ohrozenie záujmov organizácie Slovenský rýchlokorčuliarsky zväz.

**Bezpečnostné opatrenia**

Všetci zamestnanci spoločnosti sú povinní dodržiavať bezpečnostné opatrenia, ktoré sú realizované na ochranu objektov, majetku osôb a osobných údajov. Medzi základné realizované bezpečnostné opatrenia patria:

**Technické opatrenia**

|  |  |
| --- | --- |
| **Opatrenie** | **Spôsob využitia** |
| **Ochrana priestorov** | |
| nainštalovaný kamerový systém | obmedzenie a riadenie prístupu osôb |
| nainštalovaný elektronický zabezpečovací systém |
| oddelenie priestorov na spracúvanie osobných údajov - samostatná kancelária |
| písomné dokumenty uložené v uzamykateľných skriniach |
| rozmiestnenie nábytku a počítačov vylučuje odpozeranie osobných údajov z  monitora, prípadne z písomných dokumentov zo stola | ochrana pred náhodným sprístupnením údajov |
| zariadenia na likvidáciu písomných dokumentov | spoľahlivá likvidácia osobných údajov |
| nainštalované hlásiče požiaru a hasiace prístroje | ochrana pred živelnou katastrofou |
| **Automatizované prostriedky spracúvania** | |
| prihlásenie do počítačov vyžaduje meno a heslo používateľa | uplatňovaná povinnosť identifikácie a autentizácie pri prístupe k  informačnému systému, riadenie prístupu k aktívam |
| aplikácie používané na spracúvanie osobných údajov pre spustenie vyžadujú meno a heslo používateľa |
| inštalované opravné programové balíčky pre operačné systémy i aplikácie | zvyšovanie bezpečnosti programového vybavenia |
| ochrana proti škodlivým programom - antivírová ochrana | ochrana proti počítačovým vírusom, pred poškodením údajov, prípadne pred sprístupnením údajov |
| zriadené bezpečné pripojenie na internet – firewall (kontrola, obmedzenie a zamedzenie prepojenia informačných systémov s internetom) | ochrana pred prienikom do počítačovej siete |
| používané záložné napájacie zdroje pre dôležité počítače (sekretariát, recepcia hotelov) | ochrana pre chybami, ktoré môžu nastať pri výpadku el. energie |

**Organizačné opatrenia**

|  |  |
| --- | --- |
| **Opatrenie** | **Spôsob využitia** |
| **Ochrana priestorov** | |
| vedená evidencia hesiel EZS (u dodávateľa) | obmedzenie a riadenie prístupu osôb |
| **Automatizované prostriedky spracúvania** | |
| pravidelná zmena hesiel | uplatňovaná povinnosť identifikácie a autentizácie, ochrana hesiel |
| odhlasovanie sa z aplikácií i pri dočasnom opustení pracoviska | uplatňovaná povinnosť identifikácie a autentizácie |
| pravidelne vytvorené zálohy | možnosť rýchlej obnovy informačného systému |
| **Interná legislatíva** | |
| vedené evidencie o informačných systémoch | splnenie zákonných požiadaviek |
| spracovaná smernica Ochrana osobných údajov | identifikácia a autentizácia pri prístupe k informačným systémom |
| spracovaný Požiarny štatút | ochrana pred živelnou katastrofou |

**Personálne opatrenia**

|  |  |
| --- | --- |
| **Opatrenie** | **Spôsob využitia** |
| poučené všetky oprávnené osoby podľa zákona o ochrane osobných údajov | splnenie zákonných požiadaviek, zvyšovanie povedomia o bezpečnosti a potrebe dodržiavať bezpečnostné opatrenia |
| poučení všetci zamestnanci o povinnostiach vyplývajúcich z jednotlivých smerníc |

**Rozsah oprávnení a popis povolených činností oprávnených osôb**

Všetky osoby, ktoré spracúvajú osobné údaje – oprávnené osoby – musia byť poučené o povinnostiach vyplývajúcich zo zákona č. 122/2013 Z. z. o ochrane osobných údajov. O poučení sa vedie písomný záznam. Medzi oprávnené osoby patria:

* predseda predstavenstva,
* generálny sekretár,
* účtovník.

Všetci zamestnanci spoločnosti sú povinní dodržiavať bezpečnostné opatrenia, ktoré sú realizované na ochranu objektov, majetku spoločnosti a majetku osôb, ochranu elektronických dát a osobných údajov.

Osobné údaje je možné spracúvať pre potreby spoločnosti len na základe platných zákonov, právnych predpisov a interných dokumentov. Spracúvajú sa len typy osobných údajov, ktoré je nevyhnutné spracúvať.

Osobné spisy musia byť uložené v uzamykateľných skriniach.

Po skončení práce, sú všetci zamestnanci povinní uzamykať miestnosť, kde sú spracúvané osobné údaje, korektne ukončiť všetky programy a vypnúť PC.

Likvidáciu osobných údajov vykonáva generálny sekretár na základe Registratúrneho poriadku.

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 sprístupniť. Povinnosť mlčanlivosti trvá i po skončení pracovného pomeru.

Informačný systém **Personalistika a mzdy** obsahuje osobitnú kategóriu osobných údajov – rodné číslo.

Účtovník a predseda SRZ sú oprávnení spracúvať osobné údaje o zamestnancoch a ich rodinných príslušníkoch - vyživovaných osobách. Údaje spracúvajú manuálne a v elektronickej forme. Osobné údaje získavajú osobným pohovorom a kopírovaním úradných dokladov a dokumentov o vzdelaní (občiansky preukaz, preukaz zdravotnej poisťovne, osvedčenia o odbornej spôsobilosti). Osobné spisy má účtovník uložené u seba v kancelárii v uzatvorenej skrini.

Účtovník je oprávnený v nevyhnutnom rozsahu poskytovať osobné údaje zamestnancov pre potreby vzdelávania, evidencie pracovných úrazov a pracovnej zdravotnej služby externým dodávateľom.

Osobné údaje sa spracúvajú v informačnom systéme na základe zákona č. 311/2001 Z. z. Zákonník práce v znení neskorších predpisov, zákona č.124/2006 Z. z. o bezpečnosti a ochrane zdravia pri práci a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ďalších zákonov.

**Členovia združenia** - obsahuje osobitnú kategóriu osobných údajov – rodné číslo

Osobné údaje členov občianskeho združenia spracúvajú predseda SRZ. Údaje získava z prihlášok, spracúva tieto osobné údaje: meno, priezvisko, titul, dátum a miesto narodenia, rodné číslo, štátna príslušnosť, adresa trvalého pobytu alebo obdobného pobytu, adresa na doručovanie, adresa elektronickej pošty, číslo bankového účtu, druh športu.

Osobné údaje sú v informačnom systéme spracúvané na základe zákona č. 83/1990 Zb. o združovaní občanov a zákona č. 440/2015 Z. z. o športe a o zmene a doplnení niektorých zákonov.

**Účtovné doklady**

Účtovník je oprávnený spracúvať prostredníctvom automatizovaných a neautomatizovaných prostriedkov spracúvania osobné údaje zamestnancov a členov združenia a zamestnancov dodávateľov. Právnym základom spracúvania sú: zákon č. 431/2002 Z. z. o účtovníctve v znení neskorších predpisov, zákon č.222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov, zákon č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov, zákon č. 283/2002 Z. z. o cestovných náhradách v znení neskorších predpisov a zákon č. 152/1994 Z. z. o sociálnom fonde a o zmene a doplnení zákona č. 286/1992 Zb. o daniach s príjmov v znení neskorších predpisov.

Predseda SRZ zverejňuje na základe zákona č. 211/2010 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov predpísané údaje.

**Evidencia pošty**

Generálny sekretár spracúva osobné údaje odosielateľov a prijímateľov korešpondencie za účelom evidencie odoslanej a došlej pošty. Údaje o došlej počte manuálne zapisuje do Registratúrneho denníka. Osobné údaje sa získavajú z obálok došlej pošty a obsahu korešpondencie.

Osobné údaje sa spracúvajú v informačnom systéme na základe zákona č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov.

**Registratúra**

Písomné dokumenty určené na dlhodobé uloženie – registratúrne záznamy sú uložené v Registratúrnom stredisku. Správu registratúry vykonáva generálny sekretár, postup určuje Registratúrny poriadok.

**Autentizácia a identifikácia**

Každý oprávnený používateľ sa musí identifikovať a autorizovať - musí sa prihlásiť používateľským menom a príslušným heslom. Autorizácia používateľa môže byť viac úrovňová, pri prihlásení sa do operačného systému, pred vstupom do určitej aplikácie, prípadne pred vykonaním určitej činnosti v rámci aplikácie.

Na každej úrovni je oprávnený používateľ povinný používať iné heslo. Heslá pre prihlásenie do siete a do ďalších aplikácií musia byť rôzne.

Prvotné heslo musí oprávnený používateľ zmeniť pri prvom prihlásení sa do siete alebo do aplikácie. Heslo musí obsahovať minimálne 7 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 180 dní. 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.

**Kontrolná činnosť**

Generálny sekretár vykoná minimálne jeden krát ročne kontrolu zameranú na dodržiavanie ochrany osobných údajov. Cieľom kontroly sú doporučenia pre úpravu pracovných postupov, aktualizáciu interných predpisov a prípadne návrh na realizáciu ďalších bezpečnostných opatrení. Manažér vykoná kontrolu:

* interných predpisov – presnosť a jednoznačnosť pracovných postupov pri spracúvaní osobných údajov, aktuálnosť Bezpečnostného projektu a smernice Ochrana osobných údajov,
* uzamykania miestností a fungovania EZS – ochrana pred prístupom nepovolaných osôb do administratívnych priestorov,
* uloženia písomných dokumentov – vhodnosť podmienok na archivovanie,
* záloh APS – v spolupráci s oprávnenými osobami.

**Bezpečnostné incidenty**

Generálny sekretár je zodpovedný za správu bezpečnostných incidentov – udalostí, ktoré sa týkajú porušenia ochrany osobných údajov, informuje predsedu SRZ a písomne eviduje bezpečnostné incidenty, ich následky a použité riešenia.

**Havarijné postupy**

V prípade zistenia poruchy akéhokoľvek prostriedku APS je potrebné na túto skutočnosť upozorniť predsedu SRZ. Predseda rozhodne o ďalšom postupe opravy, s ohľadom na zabezpečenie osobných údajov.

Na predchádzanie vzniku požiaru je potrebné dodržiavať preventívne protipožiarne opatrenia v súlade s Požiarnym štatútom. V prípade požiaru sa postupuje podľa poplachových a evakuačných smerníc.