

Ochrana osobných údajov

podľa GDPR (General Data Protection Regulation)

Obchodné meno: *Technické služby mesta Partizánske, spol. s r. o.*
Sídlo: Nemocničná 979/1, 958 30 Partizánske
Štatutárny zástupca: *Ing. Jozef Jarošinec, konateľ spoločnosti*
IČO: 36 311 693
DIČ: 2020139902
IČ DPH: SK2020139902
Bankové spojenie: VÚB, a. s. pobočka Partizánske
IBAN: SK48 0200 0000 0013 6602 1759
BIC: SUBASKBX
Registrácia: OR OS Trenčín, odd. Sro, vložka č.19422/R

Kontaktná osoba zodpovedná za výkon dohľadu nad ochranou osobných údajov :

Mgr. Ľubica Ručeková, právnička e-mail: lubica.rucekova@tsmpartizanske.sk
mobil: +421 0918905092

Začiatok spracúvania osobných údajov - 11. 02. 2000, t. j. od zápisu obchodnej spoločnosti do Obchodného registra.

V Partizánskom, dňa 18.05.2018

Ing. Jozef Jarošinec
konateľ spoločnosti

BEZPEČNOSTNÁ SMERNICA

Východiskom pre spracovanie ochrany osobných údajov sú základné princípy ochrany osobných údajov zakotvené v **GDPR (General Data Protection Regulation) - Nariadení Európskeho parlamentu a Rady (EÚ) 2016/679 z 27.04.2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov.**

Bezpečnostná smernica podľa základných princípov ochrany osobných údajov zakotvených v GDPR a v zmysle zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, ktorý nadobudol platnosť dňa 30.01.2018, účinnosť dňa 25.05.2018 vymedzuje a definuje rozsah a spôsob technických, organizačných a personálnych opatrení prevádzkovateľa potrebných na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na informačné systémy z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti.

Bezpečnostná smernica podľa GDPR a v zmysle zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, ktorý sa vzťahuje na informačný systém v oblasti personálnej a mzdovej agendy sa skladá z nasledovných častí:

A/ Bezpečnostný zámer

B/ Analýza bezpečnosti informačného systému

C/ Základné princípy ochrany osobných údajov

Súčasťou bezpečnostnej smernice sú aj:

- záznamy o poučení osôb oprávnených spracúvať osobné údaje v zmysle zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov,
- zoznam súhlasu dotknutých osôb s poskytnutím osobných údajov a poučení o právach dotknutých osôb v zmysle § 14 až 16 a zároveň § 19 až 25 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov,
- zoznam poučení o povinnosti mlčanlivosti oprávnených osôb o spracúvaných osobných údajoch, ktoré majú, alebo môžu mať prístup k osobným údajom v informačných systémoch v oblasti personálnej a v oblasti mzdovej agendy v zmysle § 79 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

A/ BEZPEČNOSTNÝ ZÁMER

Bezpečnostný zámer obsahuje základné bezpečnostné ciele na ochranu informačného systému pred ohrozením jeho bezpečnosti v oblasti personálnej agendy a na ochranu informačného systému v oblasti mzdovej agendy.

1/ Informačný systém v oblasti personálnej agendy

Technológia spracúvania osobných údajov je automatizovaná na samostatnom počítači, ktorý je prepojený k VUC NET – u.

Samostatný počítač na spracovávanie personálnej agendy je z hľadiska technického zabezpečenia chránený voči nepovolaným osobám užívateľským menom a heslom, ktoré pozná len personálna referentka, ktorá spracúva osobné údaje zamestnancov prevádzkovateľa.

Personálna agenda je spracúvaná aj manuálne na osobných kartách zamestnancov prevádzkovateľa. Účelom spracúvania osobných údajov je vedenie personálnej agendy zamestnancov prevádzkovateľa.

Právnym základom spracúvania osobných údajov sú:

- Zákoník práce č. 311/2001 Z. z. v znení neskorších predpisov
- zákon č. 580/2004 Z. z. o zdravotnom poistení a doplnení zákona č. 95/2002 Z. z. o poisťovníctve a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
- zákon č. 5/2004 Z. z. o službách zamestnanosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
- zákon č. 40/1964 Zb. Občiansky zákoník v znení neskorších predpisov
- zákon č. 124/2006 Z. z. o bezpečnosti a ochrane zdravia pri práci a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
- zákon č. 461/2003 Z. z. o sociálnom poistení v znení neskorších predpisov, ktorý zahŕňa:
 - a) nemocenské poistenie
 - b) dôchodkové poistenie a to: - starobné poistenie, - invalidné poistenie
 - c) úrazové poistenie
 - d) garančné poistenie
 - e) poistenie v nezamestnanosti
- zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (Zákon o slobode informácií)

Osobné údaje zamestnancov prevádzkovateľa z oblasti personálnej agendy sa ďalším cudzím osobám neprístupujú, neposkytujú a ani nezverejňujú.

Zoznam osobných údajov zamestnancov pre potreby personálnej agendy sú:

- meno a priezvisko, rodné meno a priezvisko - individuálny identifikátor dotknutej osoby,
- dátum a miesto narodenia - individuálny identifikátor dotknutej osoby,

- rodné číslo, všeobecne použiteľný, trvalý identifikačný osobný údaj dotknutej osoby, ktorý zabezpečuje jej jednoznačnosť v informačnom systéme – osobitná kategória osobných údajov,
- bydlisko, názov ulice, orientačné, prípadne súpisné číslo domu, názov obce, PSČ, názov okresu, názov štátu – adresa dotknutej osoby - individuálny identifikátor dotknutej osoby,
- číslo občianskeho preukazu - individuálny identifikátor dotknutej osoby,
- rodinný stav - doplňujúci identifikátor dotknutej osoby,
- štátna príslušnosť, národnosť - doplňujúci identifikátor dotknutej osoby,
- pracovné zaradenie - doplňujúci identifikátor dotknutej osoby,
- výška dohodnutej mzdy - doplňujúci identifikátor dotknutej osoby,
- osobné údaje o rodinných pomeroch týkajúce sa manžela/manželky, detí - osobitná kategória osobných údajov dotknutej osoby,
- dosiahnuté vzdelanie - doplňujúci identifikátor dotknutej osoby,
- pracovná prax (ak to vyžaduje druh dojednávanej práce) - osobitná kategória osobných údajov dotknutej osoby,
- zdravotný stav (ak to vyžaduje druh dojednávanej práce) - osobitná kategória osobných údajov,
- prípadne ďalšie osobné údaje, ak sú potrebné pre výkon práce (napr. zdravotná spôsobilosť a podobne),
- číslo bankového účtu z dôvodu zasielania mzdy na účet - osobitná kategória osobných údajov dotknutej osoby,
- výpis z registra trestov - osobitná kategória osobných údajov dotknutej osoby,
- telefónne číslo - doplňujúci identifikátor dotknutej osoby.

Správnosť a aktuálnosť osobných údajov zabezpečuje prevádzkovateľ. Osobné údaje, ktoré sú spracovávané manuálne na osobných kartách sú uložené v samostatnej skrinke na samostatný kľúč, ktorý je uschovaný u personálnej referentky. Skrinka je uzamknutá aj počas pracovnej doby, aby sa k osobným údajom nedostali nepovolané osoby. Pracuje s nimi len personálna referentka.

Prevádzkovateľ po splnení účelu spracúvania zabezpečuje likvidáciu osobných údajov v súlade s príslušnými zákonmi.

2/ Informačný systém v oblasti mzdovej agendy

Technológia spracúvania osobných údajov je automatizovaná na samostatnom počítači, ktorý je prepojený k VUC NET - u.

Samostatný počítač na spracovávanie mzdovej agendy je z hľadiska technického zabezpečenia chránený voči nepovolaným osobám užívateľským menom a heslom, ktoré pozná len mzdová referentka, ktorá spracováva osobné údaje zamestnancov prevádzkovateľa.

Účelom spracúvania osobných údajov je vedenie mzdovej agendy zamestnancov prevádzkovateľa.

Právnym základom spracúvania osobných údajov sú:

- Zákoník práce č. 311/2001 Z. z. v znení neskorších predpisov,
- zákon č. 580/2004 Z. z. o zdravotnom poistení a doplnení zákona č. 95/2002 Z. z. o poisťovníctve a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- zákon č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov,
- zákon č. 461/2003 Z. z. o sociálnom poistení v znení neskorších predpisov, ktorý zahŕňa:
 - a) nemocenské poistenie,
 - b) dôchodkové poistenie,
 - c) úrazové poistenie,
 - d) garančné poistenie,
 - e) poistenie v nezamestnanosti,
- zákon č. 36/2005 Z. z. o rodine a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- zákon č. 601/2003 Z. z. o životnom minime a o zmene a doplnení niektorých zákonov,
- zákon č. 280/2002 Z. z. o rodičovskom príspevku v znení neskorších predpisov,
- zákon č. 281/2002 Z. z. o prídavku na dieťa a o príspevku k prídavku na dieťa v znení neskorších predpisov,
- zákon č. 320/1993 Z. z. o úprave náhrady za stratu na zárobku po skončení pracovnej neschopnosti vzniknutej pracovným úrazom alebo chorobou z povolania v znení neskorších predpisov,
- zákon č. 241/1993 Z. z. o štátnych sviatkoch, dňoch pracovného pokoja a pamätných dňoch v znení neskorších predpisov.

Zoznam osobných údajov zamestnancov pre potreby mzdovej agendy:

- meno a priezvisko, rodné meno a priezvisko - individuálny identifikátor dotknutej osoby,
- dátum a miesto narodenia - individuálny identifikátor dotknutej osoby,
- rodné číslo, všeobecne použiteľný, trvalý identifikačný osobný údaj dotknutej osoby, ktorý zabezpečuje jej jednoznačnosť v informačnom systéme – osobitná kategória osobných údajov,
- bydlisko, názov ulice, orientačné, prípadne súpisné číslo domu, názov obce, PSČ, názov okresu - individuálny identifikátor dotknutej osoby,
- číslo občianskeho preukazu - individuálny identifikátor dotknutej osoby,
- rodinný stav - doplňujúci identifikátor dotknutej osoby,
- pracovné zaradenie - doplňujúci identifikátor dotknutej osoby,
- výška dohodnutej mzdy - doplňujúci identifikátor dotknutej osoby,
- osobné údaje o rodinných pomeroch týkajúce sa manžela/manželky, detí - osobitná kategória osobných údajov dotknutej osoby,
- informácie o priznaní dôchodku - osobitná kategória osobných údajov dotknutej osoby,
- číslo bankového účtu z dôvodu zasielania mzdy na účet - osobitná kategória osobných údajov dotknutej osoby,
- telefónne číslo - doplňujúci identifikátor dotknutej osoby.

Po splnení účelu spracúvania osobných údajov prevádzkovateľ zabezpečí ich likvidáciu. Ak osobitný zákon ustanovuje lehotu, ktorá neumožňuje osobnú údaje bezodkladne zlikvidovať, prevádzkovateľ zabezpečí uschovanie osobných údajov v archíve, ktorý je uzamknutý (aj počas pracovnej doby), čím je tiež chránený proti vstupu nepovoláných osôb.

Osobné údaje uschované v archíve sú súčasťou archívnych dokumentov. Osobné údaje v archíve a v predarchívnej starostlivosti sa uchovávajú z dôvodu zákonom ustanovených lehôt a využívajú sa len na účely občiansko-právneho, trestného alebo správneho konania.

Po uplynutí zákonom ustanovenej lehoty zabezpečí prevádzkovateľ likvidáciu osobných údajov skartáciou.

Dohľadom nad ochranou osobných údajov najmä v oblasti personálnej a mzdovej, ktoré sú spracovávané v zmysle zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov zodpovedá prevádzkovateľ.

Kľúčovými ustanoveniami tohto zákona sú ustanovenia §§ 6 až 18, týkajúce sa zásad spracúvania osobných údajov. Týmto ustanoveniami sa zabezpečuje vylúčenie možnosti spracúvania takých osobných údajov, ktoré sú s danými zásadami a účelom nezlučiteľné. Z týchto ustanovení zároveň vyplýva povinnosť prevádzkovateľa vyžadovať od dotknutej osoby len také údaje, ktoré zodpovedajú vymedzenému účelu spracúvania osobných údajov.

Okruh a počet dotknutých osôb pre informačný systém personálnej a mzdovej agendy:

- zamestnanci prevádzkovateľa v pracovnoprávnom vzťahu k prevádzkovateľovi v počte okolo 150 osôb,
- osoby vykonávajúce činnosti pre prevádzkovateľa na základe dohôd o vykonávaní prác mimo pracovného pomeru v zmysle jednotlivých ustanovení Zákonníka práce,
- členovia orgánov spoločnosti - dozorná rada.

Sprístupňovanie a zverejňovanie osobných údajov z informačného systému

Osobné údaje z personálneho a mzdového informačného systému prevádzkovateľ neposkytuje žiadnemu sprostredkovateľovi. Prevádzkovateľ osobné údaje svojich zamestnancov nezverejňuje a sprístupňuje len dotknutým osobám. Sprístupňujú sa oproti osobnému prevzatíu, resp. poštou v doporučenej zásielke do vlastných rúk. Osobné údaje od dotknutých osôb sú získavané na základe ich oslovenia pri uzatváraní pracovnej zmluvy, dohody o vykonávaní prác mimo pracovného pomeru. Pravdivosť osobných údajov sa overuje nahliadnutím do preukazu totožnosti dotknutej osoby a dotknutá osoba podpisom zmluvy potvrdzuje pravdivosť osobných údajov. Previerka aktuálnosti a správnosti údajov sa vykonáva každoročne pri ročnom zúčtovaní dane z príjmov zo závislej činnosti. Osobné údaje po splnení účelu ich spracovania sú založené pre potrebu evidencie a archivácie príslušných dokladov, ktoré sa v danom systéme nachádzajú, v mieste na to zvlášť určenom - v archíve a po

uplynutí úložnej doby v zmysle registratúrneho poriadku sú osobné údaje zlikvidované.

Fyzická bezpečnosť organizácie - štandardná (strážna služba na vrátnici pri vstupe do objektu organizácie).

Celý areál prevádzkovateľa je nepretržite chránený strážnou službou. V areáli prevádzkovateľa sa nachádza vrátnica, kde je strážna služba, ktorá dohliada nepretržite, t. j. cez pracovnú dobu aj po pracovnej dobe na vstup cudzích osôb do areálu spoločnosti (okrem vlastných zamestnancov). Vstup cudzích osôb je povolený len po zapísaní mena, priezviska, čísla občianskeho preukazu, alebo služobného preukazu. Strážna služba požaduje od každej fyzickej osoby na účely identifikácie : meno, priezvisko, titul a číslo občianskeho preukazu, alebo číslo služobného preukazu.

Personálny aj mzdový informačný systém, v ktorých sa spracúvajú osobné údaje, sú umiestnené v uzamykateľných miestnostiach v hlavnej budove prevádzkovateľa. Vstup do hlavnej jednopodlažnej budovy prevádzkovateľa je cez hlavné vchodové dvere , ktoré sú uzamykateľné. Taktiež vchody do bočnej prízemnej budovy, kde sa nachádzajú kancelárie a dielne sú uzamykateľné. Kancelárske priestory sa nachádzajú najmä na prvom nadzemnom podlaží.

Informačné systémy podliehajúce ochrane sú situované v miestnostiach so samostatnými vchodmi, ktoré sú chránené uzamykateľnými dverami. Objekt, v ktorom sa nachádzajú komponenty IS, je z hľadiska požiarnej bezpečnosti vybavený zodpovedajúcimi hasiacimi prístrojmi, je spracovaný požiarne plán a určené požiarne hliadky v zmysle zákona o ochrane pred požiarom a spĺňa požiadavky týmto zákonom stanovené.

Ochrana v rámci automatizovanej formy IS a to Hardware a Software je štandardná. Je zabezpečená ochrana vstupných bodov do IS pomocou hesiel. Automatizovaný systém pracuje v systéme WINDOWS a je zabezpečený proti vírusom antivírusovou ochranou ESET Smart Security.

Informačný systém je zabezpečený pred zničením zálohovaním a archiváciou dát štandardným spôsobom.

Organizačná a personálna bezpečnosť informačných systémov je zabezpečená:

- vypracovaním bezpečnostnej smernice
- poverením zodpovednej osoby za dodržiavanie bezpečnosti IS
- poučením oprávnených osôb a užívateľov IS o povinnostiach vyplývajúcich zo zákona o ochrane osobných údajov
- poučením o právach dotknutej osoby
- poučením o povinnosti mlčanlivosti o spracúvaných osobných údajoch

B/ ANALÝZA BEZPEČNOSTI INFORMAČNÉHO SYSTÉMU

S rozvojom nových informačných technológií a sprístupnením internetu, ako aj ďalších počítačových sietí je potrebné venovať zvýšenú pozornosť ochrane osobných údajov.

Zásady bezpečnosti ochrany

Hlavnými zásadami bezpečnosti ochrany osobných údajov v informačných systémoch prevádzkovateľa sú:

1. Umožnenie prístupu k informačnému systému len oprávneným osobám, ktoré sú poučené o svojich povinnostiach ochrany osobných údajov v zmysle zákona č. 18/2018 Z. z. a o povinnosti mlčanlivosti.
2. Zabezpečenie riešenia prístupových práv do personálneho a mzdového informačného systému zabezpečujúcich nemožnosť tlačenia, resp. kopírovania dokumentov obsahujúcich osobné údaje neoprávnenou osobou. Dokument môžu vytlačiť, resp. kopírovať len tí zamestnanci, ktorí majú na to oprávnenie a sú v zmysle organizačného zabezpečenia oprávnení s údajmi pracovať. V automatizovanej forme vedenia IS formou vstupného hesla na otvorenie informačného systému prideleného oprávnenej osobe.
3. Preškolenie všetkých oprávnených osôb k spracovaniu osobných údajov v IS v zmysle zákona č. 18/2018 Z. z. a stanovenie zodpovednosti za porušenie povinnosti pri manipulácii s osobnými údajmi a porušenia povinnosti mlčanlivosti.
4. Oboznámenie všetkých zamestnancov o povinnostiach vyplývajúcich zo zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.
5. Určenie a zabezpečenie miesta uschovávaní osobných údajov v manuálnej podobe a zabezpečenie oddelenia v automatizovanej forme prvkov IS obsahujúcich osobné údaje od iných prvkov automatizovaných systémov, ktoré sú prístupné v rámci siete aj iným než oprávneným osobám, je riešené daným systémom bezpečnosti Hardware a Software.
6. Určenie termínov a spôsobu likvidácie nepotrebných údajov po skončení účelu, na ktoré boli získavané a osôb zodpovedných za ich likvidáciu.
7. Zabezpečenie ochrany osobných údajov a automatizovanej podobe v PC proti zničeniu vírusom, proti neoprávnenému prístupu iných ako poverených osôb a neautorizovanému prístupu k údajom IS.
8. Stanovenie zásad zálohovania dát z IS a okruhu oprávnených osôb na zálohovanie s určením miesta a zodpovedného pracovníka za uloženie pred zneužitím neoprávnenou osobou.

Kontrola spracúvania osobných údajov

1/ Kontrolu spracúvania osobných údajov, kontrolu dodržiavania kódexu správania u prevádzkovateľa môže vykonávať úrad prostredníctvom kontrolného orgánu zloženého zo zamestnancov úradu.

2/ Každý člen kontrolného orgánu vykonáva kontrolu na základe písomného poverenia vedúceho zamestnanca, členovia kontrolného orgánu vykonávajú kontrolu na základe písomného poverenia predsedu úradu.

- 3/ Kontrola je začatá dňom doručenia oznámenia o kontrole prevádzkovateľovi alebo sprostredkovateľovi, zástupcovi prevádzkovateľa alebo zástupcovi sprostredkovateľa, ak bol poverený, alebo monitorujúcemu subjektu alebo certifikačnému subjektu.
- 4/ Pri výkone kontroly je kontrolný orgán povinný postupovať tak, aby neboli dotknuté práva a právom chránené záujmy kontrolovanej osoby.

Kontrolný orgán je v zmysle § 92 zákona povinný vopred písomne oznámiť kontrolovanej osobe predmet kontroly, dátum a čas výkonu kontroly v lehote najmenej desiatich dní pred vykonaním kontroly. Pred začatím výkonu kontroly a kedykoľvek na požiadanie kontrolovanej osoby sa preukázať poverením a služobným preukazom. Kontrolný orgán je povinný vypracovať zápisnicu o priebehu výkonu kontroly. Okrem iného je kontrolný orgán povinný písomne potvrdiť kontrolovanej osobe prevzatie kópií dokladov, písomných dokumentov, kópií pamäťových médií a iných materiálov a zabezpečiť ich riadnu ochranu pred stratou, zničením, poškodením a zneužitím. To znamená, že kontrolný orgán môže prevziať a odnieť k ďalšiemu kontrolnému zisťovaniu od prevádzkovateľa alebo inej kontrolovanej osoby iba kópie všetkých dokumentov a relevantných materiálov.

Kontrolovaná osoba je v zmysle § 94 zákona povinná strpieť výkon kontroly a vytvoriť kontrolnému orgánu primerané podmienky na výkon kontroly a spracovanie kontrolných zistení, poskytnúť kontrolnému úradu súčinnosť nevyhnutnú na riadny výkon kontroly.

Výsledkom kontroly je protokol alebo záznam o kontrole.

Ak boli kontrolou zistené nedostatky pri spracúvaní osobných údajov, kontrolný orgán vypracuje protokol. Kontrolovaná osoba je po oboznámení sa s kontrolnými zisteniami v protokole oprávnená podať písomné námietky v lehote 21 dní odo dňa doručenia protokolu. Na neskôr podané námietky kontrolný orgán neprihliada.

Ak sú proti kontrolným zisteniam podané námietky alebo vyšli najavo nové skutočnosti, týkajúce sa predmetu kontroly, kontrolný orgán posúdi ich obsah z hľadiska ich opodstatnenosti a vypracuje o nich dodatok, ktorý je neoddeliteľnou súčasťou protokolu. Ak kontrolný orgán neakceptuje námietky kontrolovanej osoby, je povinný to v dodatku zdôvodniť. Kontrola je ukončená dňom podpísania zápisnice o prerokovaní protokolu, dňom odmietnutia podpísať zápisnicu o prerokovaní protokolu, o čom kontrolný orgán vyhotoví v zápisnici o prerokovaní protokolu záznam.

Správne delikty pri nedodržaní jednotlivých ustanovení zákona

1/ Úrad môže podľa § 104 zákona uložiť pokuty až do 20 000 000 Eur v zmysle tohto zákona:

- prevádzkovateľovi, vrátane orgánu verejnej moci a verejnoprávnym inštitúciám, za neplnenie alebo porušenie niektorej z povinností v zmysle zákona,
- sprostredkovateľovi vrátane orgánu verejnej moci a verejnoprávnej inštitúcie v postavení sprostredkovateľa, za neplnenie alebo porušenie niektorej z povinností podľa jednotlivých ustanovení zákona,
- certifikačnému subjektu za neplnenie alebo porušenie niektorej z povinností podľa zákona,

- monitorujúcemu subjektu za neplnenie alebo porušenie niektorej z povinností podľa zákona

Pokutu podľa § 104 možno uložiť do dvoch rokov odo dňa, keď úrad porušenie povinnosti zistil, najneskôr však do piatich rokov odo dňa, keď k porušeniu povinnosti došlo. Poriadkovú pokutu podľa § 105 úrad uloží opakovane, ak povinnosť nebola splnená v určenej lehote. Poriadkovú pokutu podľa § 105 možno uložiť do 6 mesiacov odo dňa, keď k porušeniu povinnosti došlo.

C/ ZÁKLADNÉ PRINCÍPY OCHRANY OSOBNÝCH ÚDAJOV

Nový zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov nadobudol platnosť dňa 30.01.2018.

Účinnosť nového zákona č. 18/2018 Z. z. o ochrane osobných údajov nastáva dňom 25.05.2018.

Základné princípy ochrany osobných údajov sú zakotvené v **GDPR (General Data Protection Regulation) - Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27.04.2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov:**

GDPR - (General Data Protection Regulation) - Nariadenie Európskeho parlamentu a Rady (EÚ) predstavuje také opatrenia, ktoré sa priamo dotýkajú ochrany základných ľudských práv jednotlivca a bola vydaná priamo za účelom ochrany základných ľudských práv a slobôd fyzických osôb pri spracúvaní osobných údajov občanov Európskej únie.

Okrem GDPR - (General Data Protection Regulation) - Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27.04.2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov medzi významné dokumenty, týkajúce sa automatizovaného spracovávania osobných údajov patria:

"Pokyny pre spracovávanie osobných údajov v automatizovaných informačných systémoch"

V nich sú formulované základné princípy a zásady spracúvania osobných údajov:

1/ Zásada zákonnosti - Osobné údaje možno spracúvať len zákonným spôsobom a tak, aby nedošlo k porušeniu základných práv dotknutej osoby.

2/ Zásada obmedzenia účelu - Osobné údaje sa môžu získavať len na konkrétne určený, výslovne uvedený a oprávnený účel a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmto účelom; ďalšie spracúvanie osobných údajov na účel archivácie, alebo na štatistický účel, ak je v súlade s osobitným predpisom a ak sú dodržané primerané záruky ochrany práv dotknutej osoby podľa § 78 ods. 8, sa nepovažuje za nezlučiteľné s pôvodným účelom.

3/ Zásada minimalizácie osobných údajov - Spracúvané osobné údaje musia byť primerané, relevantné a obmedzené na nevyhnutný rozsah daný účelom, na ktorý sa spracúvajú.

4/ Zásada správnosti - Spracúvané osobné údaje musia byť správne a podľa potreby aktualizované; musia sa prijať primerané a účinné opatrenia na zabezpečenie toho, aby sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bez zbytočného odkladu vymazali alebo opravili.

5/ Zásada minimalizácie uchovávanía - Osobné údaje musia byť uchovávané vo forme, ktorá umožňuje identifikáciu dotknutej osoby najneskôr dovtedy, kým je to potrebné na účel, na ktorý sa osobné údaje spracúvajú.

6/ Zásada integrity a dôvernosti - Osobné údaje musia byť spracúvané spôsobom, ktorý prostredníctvom primeraných technických a organizačných opatrení zaručuje primeranú bezpečnosť osobných údajov vrátane ochrany pred neoprávneným spracúvaním osobných údajov, nezákonným spracúvaním osobných údajov, náhodnou stratou osobných údajov, výmazom osobných údajov alebo poškodením osobných údajov.

7/ Zásada zodpovednosti - Prevádzkovateľ je zodpovedný za dodržiavanie základných zásad spracúvania osobných údajov, za súlad spracúvania osobných údajov so zásadami spracúvania osobných údajov a je povinný tento súlad so zásadami spracúvania osobných údajov na požiadanie úradu preukázať.

Smernica pre jednotlivé informačné systémy určuje:

- a/ - spracúvať osobné údaje, alebo súbor operácií s osobnými údajmi, napr. ich získavanie, zhromažďovanie, zaznamenávanie, usporadúvanie, prepracúvanie, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, premiestňovanie, využívanie, uchovávanie, likvidáciu, ich prenos, poskytovanie, sprístupňovanie, alebo zverejňovanie v súlade so zákonom o ochrane osobných údajov,
- b/ - získavať osobné údaje za účelom vopred vymedzeným, ktorý sa viaže na určitú činnosť (personálna agenda, mzdová agenda),
- c/ - získavať osobné údaje so súhlasom dotknutej osoby, ktorým je výslovný a zrozumiteľný prejav vôle (dotknutá osoba je každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovného pomeru alebo obdobného pracovného vzťahu),
- d/ - neposkytovať a nesprístupňovať osobné údaje iným fyzickým ani právnickým osobám,
- f/ - nezverejňovať osobné údaje publikovaním, ich vystavením verejne prístupných počítačových sietí, prostredníctvom masovo komunikačných prostriedkov, verejným vyhlásením, uvedením vo verejnom zozname, ich umiestnením na úradnej tabuli alebo na inom verejne prístupnom mieste,
- g/ - likvidovať osobné údaje v súlade s príslušnými zákonnými ustanoveniami (vymazaním, fyzickým zničením hmotných nosičov tak, aby sa z nich osobné údaje nedali reprodukovať).

Zakazuje sa spracúvať osobné údaje:

- ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženskú vieru alebo svetonázor, členstvo v politických stranách alebo politických hnutiach, členstvo v odborových organizáciách (ak k takému spracovaniu nedala dotknutá osoba súhlas) a údaje týkajúce sa zdravia alebo pohlavného života sa zakazuje,
- pri spracúvaní osobných údajov možno využiť na účely určenia fyzickej osoby všeobecne použiteľný identifikátor ustanovený osobitným zákonom len vtedy, ak jeho použitie je nevyhnutné na dosiahnutie daného účelu spracúvania. Spracúvať iný identifikátor, ktorý v sebe skrýva charakteristiky dotknutej osoby, alebo zverejňovať všeobecne použiteľný identifikátor sa zakazuje,
- spracúvanie biometrických údajov možno vykonávať len za podmienok ustanovených v osobitnom zákone,

Zakazuje sa zhromažďovanie a rozmnožovanie osobných údajov mimo zákonom stanovených prípadov, poskytovanie osobných údajov telefonicky, internetom a poskytovanie osobných údajov bez overenia oprávnenosti osoby. Zakazuje sa zhromažďovať iné osobné údaje ako je stanovené zákonom.

V zmysle § 21 zákona o ochrane osobných údajov prevádzkovateľ preukázateľne poučil fyzické osoby - oprávnené osoby, ktoré majú alebo môžu mať prístup k jeho informačným systémom, o právach a povinnostiach ustanovených týmto zákonom a o zodpovednosti za ich porušenie.

Prevádzkovateľ pred začatím spracúvania jednoznačne vymedzí účel a zabezpečí, aby sa nespracúvali osobné údaje, ktoré sú nezlučiteľné s daným účelom.

Prevádzkovateľ je povinný zachovávať mlčanlivosť o osobných údajoch, ktoré spracováva. Povinnosť mlčanlivosti trvá aj po skončení spracúvania. Oprávnená osoba je povinná zachovávať mlčanlivosť o osobných údajoch s ktorými príde do styku, tie nesmie využiť ani pre osobnú potrebu a bez súhlasu prevádzkovateľa ich nesmie zverejniť a nikomu poskytnúť ani sprístupniť.

Povinnosť mlčanlivosti platí aj pre iné fyzické osoby, ktoré v rámci svojej činnosti (údržba, servis technických prostriedkov) prídu do styku s osobnými údajmi u prevádzkovateľa.

Povinnosť mlčanlivosti trvá aj po zániku funkcie oprávnenej osoby, alebo po skončení jej pracovného pomeru, alebo obdobného pracovného vzťahu.

Kontrolné činnosti zamerané na dodržiavanie bezpečnosti IS

Spôsob, forma a periodicita výkonu kontrolných činností

Zásady spracovania osobných údajov sa kontrolujú minimálne jedenkrát za rok. Kontrola prevádzky automatizovaného IS sa prevádza nepretržite a to technickými a programovými prostriedkami. V pracovnej dobe sa prevádza podľa potreby povereným správcom siete.

Kontrola zabezpečenia miestností pred nepovolaným vstupom počas pracovnej doby, ale i v mimopracovnom čase je vykonávaná vedúcimi pracovníkmi prevádzkovateľa.

Informačné systémy sú chránené užívateľskými menami a heslami tak, aby k nim nemali prístup nepovolané osoby.

Oprávnené osoby sú povinné osobné údaje chrániť pred zneužitím tretou osobou. Pokiaľ bezprostredne nepracujú s osobnými údajmi tieto držať v trezorovej skrini, resp. v zabezpečenej uzamykateľnej skrini, príp. skrinke.

Oprávnenými osobami spracovávať osobné údaje sú hlavne personálny referent, mzdový referent, referent bezpečnosti práce a ostatné určené oprávnené osoby prevádzkovateľa v rozsahu svojej pracovnej náplne.

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 a ak prevádzkovateľ po upozornení bezodkladne nevykoná nápravu, oznámi to zodpovedná osoba úradu na ochranu osobných údajov.

Informačné systémy personálnej a mzdovej agendy sú chránené heslami tak, aby k nim nemali prístup nepovolané osoby. Oprávnené osoby, ktoré pracujú s jednotlivými informačnými systémami sú povinné uplatňovať pri svojej práci bezpečnostné opatrenia na zamedzenie vstupu nepovolaných osôb v rámci pracovnej činnosti do počítača (opatrenie počítača heslom, uzamykanie skriniek s osobnými dokladmi, uzamykanie kancelárie). Taktiež po skončení pracovnej činnosti sú povinné vypnúť počítače, uzamknúť skrine, skrinky, aby boli osobné údaje chránené nielen po technickej stránke, ale aj mechanicky.

Oprávnenými osobami spracovávať osobné údaje sú hlavne personálny referent, mzdový referent a ostatné oprávnené osoby prevádzkovateľa v rozsahu svojej pracovnej náplne.

Uloženie sankcií kontrolným orgánom za nedodržiavanie a porušovanie zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

Porušenie nakladania s osobnými údajmi je obsiahnuté v §§ 247, 247a, 247b a v § 374 Trestného zákona č. 300/2005 Z. z. v znení neskorších predpisov. Predmetom týchto ustanovení sú sankcie za neoprávnené nakladanie s osobnými údajmi (neoprávnené poskytnutie alebo zverejnenie osobných údajov je kvalifikované ako trestný čin).

Neoprávnený prístup do počítačového systému

Kto prekoná bezpečnostné opatrenie neoprávneným vkladáním, prenášaním, poškodením, vymazaním, zhoršením kvality, pozmenením, potlačením alebo znepriístupnením počítačových údajov, alebo tým, že urobí neoprávnený zásah do technického alebo programového vybavenia počítača a získané informácie neoprávnene zničí, poškodí, vymaže, pozmení alebo zníži ich kvalitu a tým získa neoprávnený prístup do počítačového systému alebo jeho časti dopustí sa trestného činu. Taktiež sa dopustí trestného činu ten, kto úmyselne poškodí, vymaže, pozmení, potlačí alebo znepriístupní počítačové údaje alebo zhorší ich kvalitu v rámci počítačového systému alebo jeho časti.

Neoprávnené nakladanie s osobnými údajmi

Kto neoprávnene poskytne, sprístupní alebo zverejní osobné údaje o inom zhromaždené v súvislosti s výkonom verejnej moci alebo uplatňovaním ústavných práv osoby, alebo osobné údaje o inom získané v súvislosti s výkonom svojho povolania, zamestnania alebo funkcie a tým poruší všeobecne záväzným právnym predpisom ustanovenú povinnosť bude potrestaný v zmysle trestného zákona.