TDS s.r.o.

so sídlom: Zlatovska 1904, 911 01 Trenčín, IČO: 44 828 390, DIČ: 2022838653, zapísaná v Obchodnom registri Okresného súdu Trenčín, oddiel: Sro, vložka č. 21760/R

Smernica

pre spracovanie osobných údajov

vyhotovená v súlade so zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov a Všeobecným nariadením o ochrane osobných údajov (GDPR)

Účinnosť od: **25. mája 2018**

Zodpovedný: Ing. Martin Prokša, zodpovedná osoba

Interný firemný predpis č. 1/2018

TDS s.r.o.

Sídlo: Zlatovska 1904

IČO: 44 828 390

DIČ: 2022838653

Zapísané v: Obchodnom registri Okresného súdu Trenčín, oddiel: Sro, vložka č. 21760/R

Obsah a List zmien

Kapitola č.	Názov kapitoly	Zmena č.	Dátum zmeny
1.	Názov informačného systému		
2.	Názov organizácie, ktorá informačný systém prevádzkuje		
3.	Meno zodpovednej osoby		
4.	Rozsah projektu		
5.	Údaje o informačnom systéme – popis informačného systému		
6.	Zásady bezpečnosti a ochrany		
7.	Stupeň bezpečnosti podľa bezpečnostného štandardu		
8.	Bezpečnostný zámer		

Tento dokument bol vytvorený za účelom ochrany osobných údajov zamestnancov a zákazníkov spoločnosti TDS s.r.o. a je jej interným predpisom, ku ktorému majú prístup zainteresované osoby prostredníctvom štatutára spoločnosti. Dokument je pravidelne aktualizovaný v súlade s riadením ochrany osobných údajov spoločnosti.

Platnosť: od 25. mája 2018

TDS s.r.o. je v zmysle ustanovenia § 5 písm. o) zákona č. 18/2018 Z. z. zákona o ochrane osobných údajov a o zmene a doplnení niektorých zákonov prevádzkovateľom. TDS s.r.o. v rámci svojej činnosti spracováva osobné údaje svojich klientov a zamestnancov.

TDS s.r.o. v postavení prevádzkovateľa zodpovedá za bezpečnosť osobných údajov tým, že ich chráni pred náhodným, ako aj nezákonným poškodením a zničením, stratou, odcudzením, zmenou, nedovoleným prístupom, sprístupnením a rozširovaním, ako aj pred akýmikoľvek inými neprípustnými formami spracúvania. Na tento účel TDS s.r.o. prijme primerané technické, organizačné a personálne opatrenia zodpovedajúce spôsobu spracovávania osobných údajov, pričom berie do úvahy najmä použiteľné technické prostriedky, rozsah možných rizík, ktoré sú spôsobilé narušiť bezpečnosť alebo funkčnosť informačného systému a dôvernosť a dôležitosť spracovávania osobných údajov.

ZÁKLADNÉ POJMY

Osobný údaj: sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby (ďalej len „dotknutá osoba“); identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby.

Spracúvanie: je operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov, napríklad získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami.

Informačný systém: je akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe;

Prevádzkovateľ: je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov; v prípade, že sa účely a prostriedky tohto spracúvania stanovujú v práve Únie alebo v práve členského štátu, možno prevádzkovateľa alebo konkrétne kritériá na jeho určenie určiť v práve Únie alebo v práve členského štátu;

Sprostredkovateľ: je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa;

Súhlas dotknutej osoby: je akýkoľvek slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby, ktorým formou vyhlásenia alebo jednoznačného potvrdzujúceho úkonu vyjadruje súhlas so spracúvaním osobných údajov, ktoré sa jej tyká;

Dôvody spracovávanie osobných údajov

Spoločnosť spracováva osobné údaje na základe nasledujúcich dôvodov:

- ***Súhlas dotknutej osoby*** (podľa § 13, ods. 1, písm. a) Zákona č. 18/2018 Z.z. Zákona o ochrane osobných údajov a o zmene a doplnení niektorých zákonov)

- ***Plnenie zmluvy*** (podľa § 13, ods. 1, písm. b) Zákona č. 18/2018 Z.z. Zákona o ochrane osobných údajov a o zmene a doplnení niektorých zákonov)
- ***Právna povinnosť*** (podľa § 13, ods. 1, písm. c) Zákona č. 18/2018 Z.z. Zákona o ochrane osobných údajov a o zmene a doplnení niektorých zákonov)
- ***Ochrana života, zdravia alebo majetku dotknutej osoby*** (podľa § 13, ods. 1, písm. d) Zákona č. 18/2018 Z.z. Zákona o ochrane osobných údajov a o zmene a doplnení niektorých zákonov)
- ***Verejný záujem, resp. výkon verejnej moci*** (podľa § 13, ods. 1, písm. e) Zákona č. 18/2018 Z.z. Zákona o ochrane osobných údajov a o zmene a doplnení niektorých zákonov)
- ***Oprávnený záujem*** (podľa § 13, ods. 1, písm. a) Zákona č. 18/2018 Z.z. Zákona o ochrane osobných údajov a o zmene a doplnení niektorých zákonov)

1. NÁZOV INFORMAČNÉHO SYSTÉMU

Názov informačného systému je:

Personalistika a mzdy - súbor všetkých písomných a elektronických informácií týkajúcich sa osobných údajov o zamestnancoch a ich miezd. V tomto informačnom systéme sa spracovávajú osobné údaje zamestnancov spoločnosti za mzdovými a personálnymi účelmi. Tento informačný systém obsahuje aj osobné údaje uchádzačov o zamestnanie. Tieto osobné údaje sa poskytujú sprostredkovateľovi, ktorým je účtovná kancelária.

Účtovné doklady, účtovníctvo a dane – spracovanie všetkých dokladov, faktúr a objednávok.

GPS – GPS v služobných autách, za účelom ochrany majetku. GPS sa nachádzajú vo vozidlách s ŠPZ: TN554FI, TN632DV,TN849ET,TN969DR,TN104EI;

Kamerový systém v skladových priestoroch – kamery v skladových priestoroch, ktoré sa nachádzajú na ulici: Zlatovská 1904, 911 01 Trenčín. Kamerový systém je v týchto priestoroch za účelom ochrany majetku.

Osobné informácie zamestnancov a subdodávateľov – súbor všetkých písomných a elektronických informácií týkajúcich sa údajov, ktoré sú potrebné na vybavenie vstupov do závodov, prípadne na stavby. Tieto osobné údaje sú poskytované tretej strane – za účelom, aby príslušný zamestnanec, prípadne subdodávateľ bol pustený do objektu (závodu) za účelom plnenia si pracovných, resp. zmluvných povinností.

TDS s.r.o. vo všetkých svojich informačných systémoch spracováva bežné osobné údaje. Pri svojej činnosti neprichádza k spracovávaniu osobitnej kategórie osobných údajov podľa § 16 Zákona o ochrane osobných údajov ani osobných údajov týkajúcich sa uznania viny za spáchanie trestného činu alebo priestupku podľa § 17 Zákona o ochrane osobných údajov.

2. NÁZOV ORGANIZÁCIE, KTORÁ INFORMAČNÝ SYSTÉM PREVÁDZKUJE

TDS s.r.o.
Sídlo: Zlatovská 1904, 911 01 TrenčínIng.Martin Prokša, konateľ
IČO: 44 828 390
DIČ: 20 228 38 653
Zapísané v: Obchodnom registri Okresného súdu Trenčín, oddiel: Sro, vložka č. 21760/N

3. MENO ZODPOVEDNEJ OSOBY

Meno a priezvisko, titul, funkcia: Ing. Martin Prokša, konateľ

4. ROZSAH SMERNICE

1. bezpečnostné opatrenia v oblasti fyzickej ochrany osobných údajov v informačnom systéme v manuálnej písomnej podobe,
2. zásady a zákonný dôvod spracovávanie osobných údajov,
3. organizačné a personálne opatrenia na ochranu osobných údajov,
4. rozsah tejto smernice je zameraný na zabezpečenie nevyhnutnej bezpečnosti informačného systému proti možnému útoku zo strany interných a externých osôb, a to na jeho:

- dôvernosť (ochrana pred neoprávneným prístupom nepovolaných osôb – vlámačov, neoprávneného rozmnožovania a pod.)
- integritu (ochrana proti poškodeniu, zmene, vymazaniu a zničeniu) a
- dostupnosť (ochrana proti výpadkom napájania a iným havarijným stavom)

5. ÚDAJE O INFORMAČNOM SYSTÉME – POPIS INFORMAČNÉHO SYSTÉMU

5.1 Súčasný stav technológie spracúvania a jej zabezpečenie:

Automatizovaná – osobné údaje sú spracované pomocou výpočtovej techniky v rámci počítačovej siete, resp. informačný systém je prevádzkovaný na samostatných PC. Automatizovaný informačný systém je komplexnou programovou agendou s podsystémami. Prístup do PC je zabezpečený heslom. Prístup do konkrétneho PC má iba pracovník, ktorému je konkrétny počítač pridelený – každý zamestnanec má svoj počítač, ktorý má zaheslovaný. Tak isto je pod ochranou heslom aj celý server. Miestnosť, kde sa nachádzajú PC je chránený zabezpečovacím systémom.
Osobné údaje sú spracovávané aj v písomnej forme. Všetky takto spracovávané dokumenty, a akékoľvek dokumenty, ktoré obsahujú osobné údaje, ako aj spomínané PC sú umiestnené v kancelárii, ktorá je uzamknutá a do ktorej majú prístup len zamestnanci spoločnosti a konatelia. Všetky dokumenty v papierovej podobe, na ktorých sa nachádzajú osobné údaje sú umiestnené v zamknutej skrini. Budova, v ktorej je kancelária je tak isto uzamknutá, chránená zabezpečovacím systémom a do priestoru budovy nemajú prístup cudzie osoby.

Opis budovy sídla spoločnosti

Sídlo spoločnosti TDS s.r.o. sa nachádza na ulici Zlatovská, v Trenčíne. Ide o budovu so samostatných vchodom, ktorá je zabezpečená uzamykateľnými dverami a chránená zabezpečovacím systémom. Vstup do budovy nemajú cudzie osoby, nakoľko budova ma samostatný vchod, ktorý je neustále uzamknutý. Ak chce do budovy vstúpiť cudzia osoba, musí zazvoniť na zvonček a do priestorov budovy je vpustený niektorým z pracovníkov.

Rozmiestnenie kancelárií

Spoločnosť TDS s.r.o. disponuje samostatnými kanceláriami na prízemí a prvom poschodí a poschodí budovy, ktoré majú jedny spoločné vchodové dvere, ktoré sú zabezpečené bezpečnostnými dverami s bezpečnostným zámkom. Kľúče od kancelárie majú k dispozícii iba zamestnanci firmy a konatelia. Ak sa v kancelárii nenachádza žiadny zo zamestnancov, vždy je uzamknutá. Po pracovnej dobe je uzamknutá aj celá budova, kde sa kancelária nachádza.
Manuálna – osobné údaje spracovávané v manuálnej podobe vo forme zmlúv, písomností a listín sú zabezpečené v uzamykateľnej kancelárii s plnými dverami v uzamykateľnej skrini, do ktorej majú prístup iba zamestnanci a konatelia spoločnosti.

5. 2 Účel spracúvania osobných údajov:

- *Pre informačný systém „Personalistika a mzdy“*

Vedenie personálnej a mzdovej agendy zamestnancov spoločnosti pre účely pracovnoprávne, mzdové a pre účely zdravotného a sociálneho poistenia, starobného dôchodkového sporenia, doplnkového dôchodkového sporenia, dane z príjmov zo závislej činnosti fyzických osôb zamestnancov spoločnosti v pracovnom pomere a pre osoby pracujúce v spoločnosti na základe dohôd vykonávaných mimo pracovného pomeru v zmysle Zákonníka práce alebo obdobného pomeru.

- *Pre informačný systém „Účtovné doklady, účtovníctvo a dane“*

Vedenie účtovníctva spoločnosti, spracovanie účtovných dokladov, objednávok a faktúr.

➢ *Pre informačný systém „GPS“*

Účelom používania GPS vo vyššie spomenutých vozidlách je 24hodinová ochrana majetku spoločnosti.

➢ *Pre informačný systém „Kamerový systém v skladových priestoroch“*

Účelom používania kamerového systému v skladových priestoroch je 24 hodinová ochrana majetku.

➢ *Pre informačný systém „Osobné údaje zamestnancov a subdodávateľov“*

Spoločnosť TDS s.r.o. na to, aby mohla plniť výkon svojej činnosti, resp. zmluvných povinností voči klientom musí často vstupovať do objektov svojich klientov (Napr.: stavby, závody,..) Keďže sú tieto objekty strážené, je do nich umožnení vstup, len po predchádzajúcom nahlásení konkrétnych osôb, ktoré sa pri vstupe musia legitimovať. Preto spoločnosť TDS s.r.o. musí za týmto účelom získavať a spracovávať osobné údaje nie len svojich zamestnancov ale aj subdodávateľov. Tieto osobné údaje sú poskytované tretej strane – konkrétnemu klientovi, za účelom umožnenia vstupu do spomínaných priestorov.

5. 3 Právny základ spracúvania osobných údajov:

➢ *Pre informačný systém „Personalistika a mzdy“*

Osobné údaje spracovávané v informačnom systéme „*Personalistika a mzdy*“ sa spracovávajú na základe plnenia zákonnej povinnosti stanovenej všeobecne záväzným právnym predpisom na základe čl. 6 ods. 1 písm. c) GDPR, resp. podľa § 13, ods. 1, písm. c) zákona š. 18/2018 Z.z. Zákona o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

Osobné údaje uchádzačov o zamestnanie sú spracovávanie na základe súhlasu so spracovaním osobných údajov na účely uchádzania sa o zamestnanie v súlade s § 13, ods. 1, písm. a) zákona š. 18/2018 Z.z. Zákona o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

Osobitnými predpismi sú najmä:

- *zákon č. 311/2001 Z.z. Zákonník práce v znení neskorších predpisov*
- *zákon č. 580/2004 Z.z. o zdravotnom poistení o zmene a doplnení zákona č. 95/2002 Z.z. o poisťovníctve v znení neskorších predpisov*
- *zákon č. 461/2003 Z.z. o sociálnom poistení 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. 595/2003 Z.z. o dani z príjmov v znení neskorších predpisov*
- *zákon č. 43/2004 Z.z. o starobnom dôchodkovom sporení v znení neskorších predpisov*
- *zákon č. 650/2004 Z.z. o doplnkovom dôchodkovom sporení a o zmene niektorých zákonov v znení neskorších predpisov*
- *zákon č. 462/2003 Z.z. o náhrade príjmu pri dočasnej pracovnej neschopnosti zamestnanca a o zmene a doplnení niektorých zákonov v znení neskorších predpisov*
- *zákon č. 152/1994 Z.z. o sociálnom fonde*
- *zákon č. 355/2007 Z.z. o ochrane, podpore a rozvoji verejného zdravia a o zmene a doplnení niektorých zákonov 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. 283/2002 Z.z. o cestovných náhradách*
- *zákon č. 233/1995 Z.z. o súdnych exekútoroch a exekučnej činnosti (Exekučný poriadok) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov*

➢ *Pre informačný systém „Účtovné doklady, účtovníctvo a dane“*

Osobné údaje spracovávané v informačnom systéme „*Účtovné doklady, účtovníctvo a dane*“ sa spracovávajú na základe plnenia zákonnej povinnosti stanovenej všeobecne záväzným

právnym predpisom na základe čl. 6 ods. 1 písm. c) GDPR, resp. podľa § 13, ods. 1, písm. c) zákona š. 18/2018 Z.z. Zákona o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

Osobitnými predpismi sú najmä:

- *zákon č. 311/2001 Z.z. Zákonník práce v znení neskorších predpisov*
- *zákon č. 563/2009 Z.z. o správe daní v znení neskorších predpisov*
- *zákon č. 595/2003 Z.z. o dani z príjmov v znení neskorších predpisov*
- *zákon č. 582/2004 o miestnych daniach*
- *autorský zákon č. 349/2012 v znení neskorších predpisov*
- *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. 122/2013 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov*
- *zákon č. 145/1995 Z.z. o správnych poplatkoch v znení neskorších predpisov*
- *zákon č. 40/1964 Zb. občiansky zákonník v znení neskorších predpisov*
- *zákon č. 152/1994 Z.z. o sociálnom fonde a o zmene a doplnení zákona č. 286/1992 Zb. o daniach z príjmov v znení neskorších predpisov*
- *zákon č. 618/2003 Z.z. Autorský zákon pre zmluvy o vytvorení autorského diela*

➢ *Pre informačný systém „GPS“*

Osobné údaje spracovávanie v informačnom systéme „*GPS*“ sú spracovávané za účelom ochrany majetku - spracúvanie osobných údajov je nevyhnutné na účel oprávnených záujmov prevádzkovateľa. Tento účel je v súlade s § 13, ods. 1. písm f) zákona š. 18/2018 Z.z. Zákona o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

➢ *Pre informačný systém „Kamerový systém v skladových priestoroch“*

Osobné údaje spracovávanie v informačnom systéme „*Kamerový systém v skladových priestoroch*“ sú spracovávané za účelom ochrany majetku - spracúvanie osobných údajov je nevyhnutné na účel oprávnených záujmov prevádzkovateľa. Tento účel je v súlade s § 13,

ods. 1. písm f) zákona š. 18/2018 Z.z. Zákona o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

➢ *Pre informačný systém „Osobné údaje zamestnancov a subdodávateľov“*

Osobné údaje spracovávanie v informačnom systéme „*Osobné údaje zamestnancov a subdodávateľov*“ sú spracovávané za účelom plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo na vykonanie opatrenia pred uzatvorením zmluvy na základe žiadosti dotknutej osoby. Tento účel je v súlade s § 13, ods. 1. písm b) zákona š. 18/2018 Z.z. Zákona o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

5. 4 Okruh a počet dotknutých osôb:

➢ *Pre informačný systém „Personalistika a mzdy“*

zamestnanci spoločnosti v pracovnoprávnom vzťahu, osoby vykonávajúce činnosť pre prevádzkovateľa na základe dohôd mimo pracovného pomeru v zmysle Zákonníka práce, uchádzači o zamestnanie, zamestnanci klientov, manželia a manželky zamestnancov, vyživované deti zamestnancov, bývalí zamestnanci.

Počet dotknutých osôb: 20

➢ *Pre informačný systém „Účtovné doklady, účtovníctvo a dane“*

zamestnanci spoločnosti, zamestnanci dodávateľov, tovarov a služieb, obchodné spoločnosti, fyzické a právnické osoby, daňový úrad, sociálna zdravotná poisťovňa.

Počet dotknutých osôb: 20

➢ *Pre informačný systém „GPS“*

Monitorované vozidlá s ŠPZ: TN554FI, TN632DV,TN849ET,TN969DR,TN104EI.

Počet dotknutých osôb: 20

➢ *Pre informačný systém „Kamerový systém v skladových priestoroch“*

zamestnanci spoločnosti, ktorí pracujú v skladových priestoroch na ulici: Bezručova 16

Počet dotknutých osôb: 15

➢ *Pre informačný systém „Osobné údaje zamestnancov a subdodávateľov“*

zamestnanci spoločnosti, zamestnanci subdodávateľov, subdodávatelia, prepravné spoločnosti.

Počet dotknutých osôb: 10

5. 5 Sprístupňovanie a zverejňovanie osobných údajov z informačného systému:

➢ *Pre informačný systém „Personalistika a mzdy “*

Osobné údaje z informačného systému sa nezverejňujú a sprístupňujú sa len dotknutým osobám. Sprístupňujú sa oproti osobnému prevzatiu, resp. poštou v doporučenej zásielke do vlastných rúk. Osobné údaje spracováva aj sprostredkovateľ – účtovná kancelária. Sprostredkovateľovi sú sprístupnené a odoslané požadované informácie na plnenie zmluvy – spracovanie účtovníctva a miezd. So sprostredkovateľom má prevádzkovateľ uzatvorenú zmluvu o spracovaní osobných údajov. Osobné údaje od dotknutých osôb sú získavané na základe ich oslovenia pri uzatváraní pracovnej zmluvy, resp. dohody o vykonaní prác mimo pracovného pomeru. Pravdivosť osobných údajov sa overuje nahliadnutím do preukazu totožnosti dotknutej osoby a dotknutá osoba svojim podpisom zmluvy podpisuje 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, na dobu stanovenú osobitným predpisom a po uplynutí úložnej doby v zmysle registratúrneho poriadku spoločnosti sú osobné údaje zlikvidované.

- *Pre informačný systém „Účtovné doklady, účtovníctvo a dane“*

Osobné údaje z informačného systému sa nezverejňujú a sprístupňujú sa len kontrolným orgánom na základe písomného oznámenia o vykonaní kontroly príslušného daňového subjektu. Doklady si príslušný daňový subjekt prevezme osobne oproti podpisu. Osobné údaje spracováva aj sprostredkovateľ – účtovná kancelária. Sprostredkovateľovi sú sprístupnené a odoslané požadované informácie na plnenie zmluvy – spracovanie účtovníctva a miezd. 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, na dobu stanovenú osobitným predpisom a po uplynutí úložnej doby v zmysle registratúrneho poriadku spoločnosti sú osobné údaje zlikvidované.

- *Pre informačný systém „GPS“*

Osobné údaje z informačného systému „*GPS*“ sa nezverejňujú a nesprístupňujú tretím osobám.
Archivujú sa 15 dní.

- *Pre informačný systém „Kamerový systém v skladových priestoroch“*

Osobné údaje z informačného systému „Kamerový systém v skladových priestoroch“ sa nezverejňujú a nesprístupňujú tretím osobám. Uchovávané sú 15 dní, následne sa záznamy vymazávajú. Sprístupnili by sa iba orgánom činným v trestnom konaní, prípadne inému štátnemu orgánu na ich žiadosť. Pri podozrení zo spáchania trestného činu, by sa kamerový záznam uchoval aj dlhšie ako 15 dní – na nevyhnutne dlhú dobu, v súčinnosti s orgánmi činnými v trestnom konaní.

➢ *Pre informačný systém „Osobné údaje zamestnancov a subdodávateľov“*

Osobné údaje z informačného systému „*Osobné údaje zamestnancov a subdodávateľov*“ sa sprístupňujú len klientom, resp. investorom, za účelom plnenia zmluvy. Aby TDS s.r.o. mohla plniť výkon svojej činnosti, resp. zmluvných povinností voči klientom musí často vstupovať do objektov svojich klientov (Napr.: stavby, závody,..) Keďže sú tieto objekty strážené, je do nich umožnení vstup, len po predchádzajúcom nahlásení konkrétnych osôb, ktoré sa pri vstupe musia legitimovať. Preto spoločnosť TDS s.r.o. musí za týmto účelom získavať a spracovávať osobné údaje nie len svojich zamestnancov ale aj subdodávateľov. Tieto osobné údaje sú poskytované tretej strane – konkrétnemu klientovi, za účelom umožnenia vstupu do spomínaných priestorov.

6. ZÁSADY BEZPEČNOSTI A OCHRANY

Hlavnými zásadami bezpečnosti a ochrany osobných údajov v informačnom systéme spoločnosti sú:

1. Umožnenie prístupu k informačnému systému len oprávneným osobám, ktoré sú poučené o svojich povinnostiach ochrany osobných údajov v zmysle § 79 a ost. zákona č. 18/2018 Z.z. Zákona o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

2. Prístup k získavaným osobným údajom majú len zamestnanci firmy a konatelia – ide o administratívnu pracovníčku a konateľov. Iba tieto osoby majú kľúč od miestnosti, kde sa nachádzajú osobné údaje či už v papierovej forme, alebo elektronicky v PC. Tak isto, iba tieto osoby majú heslo od svojho počítača, kde sa osobné údaje nachádzajú v elektronickej podobe.

3. Oboznámenie všetkých zamestnancov o povinnostiach vyplývajúcich zo zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých údajov, vrátane prípadných externých zamestnancov.

4. Určenie a zabezpečenie miesta uschovávania osobných údajov v manuálnej podobe a primerané zabezpečenie tohto miesta.

5. Určenie termínov a spôsobu likvidácie nepotrebných údajov po skončení účelu, na ktorý boli získavané, a osôb zodpovedných za ich likvidáciu.

7. STUPEŇ BEZPEČNOSTI PODĽA BEZPEČNOSTNÉHO ŠTANDARDU

Fyzická bezpečnosť komponentov informačného systému je štandardná.
Objekt je chránený zabezpečovacím systémom. Budova je mimo pracovnej doby uzamknutá. Do kancelárie a ani do budovy nemajú prístup cudzie osoby. Kľúče od kancelárie majú iba zamestnanci a konatelia. V prípade, že v kancelárii nie je nikto zo zamestnancov, vždy je uzamknutá. Objekt v ktorom sa nachádzajú komponenty IS, je z hľadiska požiarnej bezpečnosti vybavený zodpovedajúcimi hasiacimi prístrojmi, je spracovaný požiarny plán.
Kancelárie v objekte, kde sa nachádzajú miesta uloženia komponentov IS v manuálnej podobe, sú zabezpečené mechanickými zábranami - zámkami na dverách.

8. BEZPEČNOSTNÝ ZÁMER

Zámerom bezpečnostného projektu je stanovenie citlivých a rizikových faktorov v rámci IS, kde by mohlo dôjsť k úniku informácií z IS. Takýmito rizikovými oblasťami sú:

1. zabránenie získavania osobných údajov nad rozsah, ako to vyžaduje účel, na ktorý sú získavané,

2. zabezpečenie fyzickej a automatizovanej ochrany kritických miest a rizikových oblastí informačného systému, ktorými sú:
   získavanie osobných údajov,
   manipulácia s nimi a ich spracovávanie,

prenos dát z IS, ich kopírovanie a používanie osobných údajov v rámci výkonu činnosti spoločnosti,

úschova a likvidácia osobných údajov po skončení účelu, na ktoré boli získané

Základnými bezpečnostnými cieľmi spoločnosti TDS s.r.o. sú:

a) zabezpečiť dodržiavanie zákona a súvisiacich právnych noriem

b) chrániť osobné údaje klientov pred ich odcudzením, stratou, poškodením, zničením, neoprávneným prístupom, neoprávneným rozširovaním, resp. zmenou a pod.

c) chrániť osobné údaje zamestnancov, pred ich odcudzením, stratou, poškodením, zničením, neoprávneným prístupom, neoprávneným rozširovaním, resp. zmenou a pod.

d) za účelom ochrany osobných údajov podľa bodu b) a c) vyššie prijať tomu zodpovedajúce bezpečnostné opatrenia (technické, organizačné a personálne), ktoré eliminujú alebo minimalizujú vplyv rizík a hrozieb;

e) zabrániť akejkoľvek diskreditácii klienta v súvislosti so zneužívaním, neoprávneným zverejňovaním alebo sprístupňovaním osobných údajov;

f) včas identifikovať všetky potencionálne narušenia bezpečnosti osobných údajov a urobiť potrebné opatrenia na elimináciu a minimalizáciu následkov.

Minimálne požadované bezpečnostné opatrenia

V TDS s.r.o. musia byť zachované minimálne nasledovné bezpečnostné opatrenia:

- opatrenia na zamedzenie neoprávneného prístupu osôb do priestorov TDS s.r.o.;
- opatrenia na zamedzenie neoprávneného prístupu osôb k chráneným osobným údajom (prostredníctvom počítačovej siete, resp. fyzicky);
- pravidelné vyčleňovanie finančných prostriedkov na realizáciu a zlepšovanie opatrení na ochranu osobných údajov;

- poučiť všetkých zamestnancov a ostatné fyzické osoby a právnické osoby, ktoré majú prístup k informačným systémom TDS s.r.o. o právach a povinnostiach ustanovených zákonom a o zodpovednosti za ich porušenie;
- zabezpečiť dodržanie povinnosti zachovávať mlčanlivosť o osobných údajoch, ktoré TDS s.r.o. spracúva;
- prijať organizačno-riadiace akty na usmerňovanie ochrany osobných údajov;
- minimálne protipožiarne opatrenia.

Opatrenia na zabezpečenie ochrany osobných údajov

Špecifikácia technických opatrení

Mechanické zábrany – okná, dvere a pod.

Objekty slúžiace na úschovu a zabezpečenie:

- trezor, skrine na spisy;
- kľúčový systém – kontrolovaný výdaj uschovania a pohyb kľúčov;
- bezpečnostný systém (elektronický, na senzor pohybu);
- likvidácia nepotrebných údajov, osobných údajov a médií – skartovacie zariadenia;
- elektronický systém ochrany počítačov – kontrolovaný prístup (prihlasovacie procedúry), šifrovanie informácií – softvér, ktorý zabezpečuje dáta pred útokom z vonkajšej siete (firewall, antivirová ochrana), chránené šifrované linky, šifrované lokálne disky serverov; zabezpečenie nepretržitého napájania, zálohovanie napájania rozhodujúcich elektrických zariadení;

– zálohovanie dokumentov obsahujúcich osobné údaje – technické prostriedky s garantovanou odolnosťou.

Špecifikácia organizačných opatrení

Preventívne opatrenia:

– pravidlá prihlasovania sa do počítačových informačných systémov prevádzkovaných TDS s.r.o., pravidlá zmeny hesla, kontrolná činnosť, režimové opatrenia, hodnotenie spoľahlivosti externých firiem poskytujúcich služby TDS s.r.o. (servisné služby);

– opatrenia na zisťovanie bezpečnostných incidentov – systém kontroly zamestnávateľa voči zamestnancom, ktorí spracúvajú osobné údaje, vyhodnocovanie kontrolnej činnosti a prijímanie efektívnych nápravných opatrení.

–

Špecifikácia personálnych opatrení

Personálne opatrenia riešia otázky výberu, riadenia a kontroly ľudských zdrojov zainteresovaných do procesu spracúvania a ochrany osobných údajov.

- optimálny výber pracovníkov spĺňajúcich kritéria spracúvania osobných údajov;
- sankčný postih pracovníkov, ktorí porušili ustanovenia zákona týkajúce sa ochrany osobných údajov;
- jasné vymedzenie právomocí a kompetencií pracovníkov pri spracúvaní osobných údajov;
- vymedzenie kontrolných mechanizmov v TDS s.r.o.;
- poučenie pracovníkov, ktorí spracúvajú osobné údaje;
- vyhodnocovanie kontrolnej činnosti a prijímanie efektívnych nápravných opatrení.

Vymedzenie okolia informačného systému

Okolie informačného systému TDS s.r.o. z hľadiska možných ohrození je tvorené:

a) ľuďmi (zamestnancami a spolupracujúcimi osobami TDS s.r.o., klientmi, zamestnancami poskytovateľov servisných upratovacích a iných služieb, zamestnancami spoločnosti sídliacich v tej istej budove, osobami, ktoré sú v príbuzenskom alebo inom vzťahu so zamestnancami TDS s.r.o., neoprávnenými osobami – cudzími osobami, útočníkmi, narušiteľmi);

b) prostredím – lokalitou (centrum mesta – pomerne frekventovaná časť, prítomnosť viacerých spoločností a firiem v jednej budove);

c) prírodnými vplyvmi (klimatické podmienky, počasie, prírodné energetické polia, vyššia moc) - unikajúca voda, požiar, porucha klimatizačného zariadenia, výpadky elektrického prúdu.

Odhad zvyškových rizík

Ide o riziká, ktoré je veľmi ťažko vopred identifikovať a prijať voči ním účinné preventívne opatrenia.

- vynášanie osobných údajov zamestnancami TDS s.r.o., porušenie lojality voči TDS s.r.o.;
- vandalizmus, teroristický útok, sabotáž;
- akékoľvek iné zlyhanie ľudského faktoru;
- skupina prípadov vis maior.

Na zabezpečenie bezpečnostného zámeru je potrebné prijať opatrenia na stanovenie pravidiel vstupu do objektu, príchodového a odchodového režimu na pracovisko, stanovenie spôsobu udeľovania a rušenia prístupov do informačných systémov, rozsahu údajov potrebných pre jednotlivé kategórie ochrany údajov v informačných systémoch.

9. VÝSLEDKY ANALÝZY BEZPEČNOSTI INFORMAČNÉHO SYSTÉMU

Vykonanou analýzou bezpečnosti informačných systémov obsahujúcich osobné údaje fyzických osôb je odhalenie bezpečnostných rizík, ktorými v rámci IS vedených spoločnosťou môžu byť:

1. Prípadné útoky na jeho dôvernosť – zabezpečenie ochrany pred neoprávneným prístupom nepovolaných osôb – vlámačov, zneužitia, neoprávneného rozmnožovania,
2. Prípadné útoky na integritu IS – ochrana proti ich poškodeniu, zmene a neplánovanému zničeniu,
3. Zabezpečenie dostupnosti IS – ochrana proti požiaru a iným havarijným stavom.

Vykonanou kvalitatívnou analýzou vyššie uvedených rizík, v rámci ktorej boli identifikované hrozby pôsobiace na informačný systém, boli stanovené tieto možné riziká narušenia bezpečnosti IS spracovávaných v tomto subsystéme:

Neoprávnený prístup zo strany nepovolaných osôb – vlámačov – fyzická ochrana objektu je dostatočná. Celý objekt je chránený zabezpečovacím systémom. Budova je zabezpečená uzamykateľnými dverami a tak isto aj kancelária je zabezpečená uzamykateľnými dverami. Kľúče od kancelárie majú iba zamestnanci spoločnosti a konatelia. Kancelária je vždy uzamknutá v prípade neprítomnosti zamestnancov. Do priestorov budovy nemá vstup cudzia osoba.

Zneužitie oprávnenia oprávnenej osoby na neoprávnené rozmnožovanie a rozširovanie osobných údajov – sú prijaté primerané opatrenia vzhľadom na to, že k údajom majú prístup len úzky okruh ľudí - zamestnanci spoločnosti a konatelia.

Ochrana proti poškodeniu, zmene, vymazaniu a zničeniu osobných údajov v IS – keďže prístup k OU majú iba zamestnanci spoločnosti, riziko zneužitia je minimálne. Tak isto je dostatočne zabezpečené, aby k OU nemali prístup nepovolané osoby – uzamknutá kancelária , zaheslovaný počítač, zabezpečovací systém.

Ochrana IS v manuálnej podobe – sú stanovené bezpečné miesta na uloženie písomností, zabezpečené pred odcudzením uzamykaním zámkou na kancelárii a uzamykateľnou skriňou.

Ochrana spracúvaných údajov pri likvidácii – je dostatočne zabezpečená, likvidujú je samotný konateľ spoločnosti.

Ochrana proti požiaru – je dostatočná, spĺňa náležitosti zákona o ochrane pred požiarmi č. 341/2001 Z. z. v zmysle vypracovaného požiarneho plánu ochrany objektu.

Nepokrytými rizikami sú udalosti, ktoré môžu nastať, a to z objektívnych alebo subjektívnych príčin a ktoré v súčasnosti nie je možné dostatočne objektívne predpovedať.

ANALÝZA BEZPEČNOSTI INFORMAČNÝCH SYSTÉMOV

1. Súpis aktív informačných systémov (automatizované prostriedky spracúvania, neautomatizované – dokumentárne prostriedky spracúvania osobných údajov)

a) automatizované prostriedky spracúvania:
- informačné aktíva – dokumenty (zmluvy, požiadavky klienta, jednostranné právne úkony, archivované údaje na elektronických médiách),
- fyzické aktíva: počítačové vybavenie – server, pracovná stanica, komunikačná infraštruktúra, periférie,
- zálohovacie zariadenia, zdroje nepretržitého napájania,
- komunikačné zariadenia – zariadenia na prenos údajov, sieťová LAN infraštruktúra,
- softwarové aktíva, systémový software (komunikačný software i operačné systémy), aplikačný software (MS office),

b) neautomatizované prostriedky spracúvania
- informačné aktíva:
  - ➢ údaje o klientoch, údaje o zamestnancoch, dokumenty (v dokumentárnej podobe – zmluvy, jednostranné právne úkony),

➢ archivované údaje – papierová forma,

c) spoločné aktíva

- ľudský faktor:
  - ➢ zamestnanci,
  - ➢ návštevníci (klienti, zamestnanci externých firiem poskytujúcich spoločnosti služby, zamestnanci iných firiem sídliacich v tej istej budove, osoby, ktoré sú v príbuzenskom alebo inom vzťahu so zamestnancami a na druhej strane ostatní – narušitelia, cudzie osoby, neoprávnené osoby),
- služby:
  - ➢ logistika: poplachová signalizácia, nahlásenie narušenia, riadiaca a monitorovacia ústredňa, detekčné a iné periférne prvky, ovládacie panely a prvky, identifikačný predmet, identifikačný kód, elektrická protipožiarna signalizácia (riadiaca jednotka, detekčné prvky), úschovné objekty (identifikačný predmet, trezorový mechanický zámok),
  - ➢ zabezpečenie dodávky elektrickej energie, osvetlenie, prívod a odvod vody, klimatizácia, vykurovanie, prevádzková dokumentácia (manuály).

KVALITATÍVNA ANALÝZA JEDNOTLIVÝCH AKTÍV INFORMAČNÝCH SYSTÉMOV A ODHAD PRAVDEPODOBNOSTI NARUŠENIA

a) automatizované prostriedky spracúvania

Aktívum informačné systému	**faktor ohrozenia**	**pravdepodobný spôsob ohrozenia**	**Odhad pravdepodobnosti, že ohrozenie nastane**	**Odhad miery negatívneho dopadu**

Dokumenty (na pamäťovom médiu) Archivované údaje	Dôvernosť	Zamestnanec alebo návštevník vyhotoví neautorizovanú kópiu a vynesie ju mimo TDS s.r.o.	Vysoká	Vysoká
	Dôvernosť	Zamestnanec alebo návštevník si zapamätá dôležitý údaj a vynesie ho mimo TDS s.r.o.	Vysoká	Vysoká
	Integrita	Neoprávnená modifikácia údajov	Nízka	Vysoká
		Poškodenie vírusom pri neoprávnenej modifikácie údajov	Stredná	Vysoká
	Dostupnosť	Nekontrolovaná zmena uloženia databázy súboru alebo archívneho média	Nízka	Nízka
		Zablokovanie účtu po neúspešných prihláseniach	Nízka	Nízka
		Zavírený systém	Stredná	Vysoká
		Zabudnutie prístupových kódov do systému aplikácie súboru	Nízka	Nízka
	Autentickosť	Vloženie nesprávneho údaja do databázy (úmyselné, neúmyselné)	Stredná	Vysoká
		Neoprávnená modifikácia záznamov databázy alebo dokumentu	Nízka	Vysoká

		Zneužitie elektronického podpisu	Nízka	Vysoká
Počítačové vybavenie	Dôvernosť	Úmyselná alebo neúmyselná manipulácia s pamäťovými médiami zamestnancom servisnej organizácie s následkom úniku osobných údajov	Nízka	Vysoká
		Inštalácia neželaného HV (modifikácia HV) s následkom nekontrolovaného úniku údajov	Vysoká	Vysoká
		Zabudnutý dokument v scanneri alebo na tlačiarni	Stredná	Nízka
		Neoprávnené získanie prístupových práv do počítača	Nízka	Nízka
	Dostupnosť	Technická porucha na zariadení	Nízka	Nízka
Zálohovacie zariadenia	Dôvernosť	Vyhotovenie neautorizovanej kópie záložného média, zneužitie mimo TDS s.r.o.	Nízka	Vysoká
	Integrita	Modifikácia záznamu na archívnom médiu a zámena médií	Nízka	Vysoká
	Dostupnosť	Nepoužiteľnosť archívneho média v prípade potreby	Nízka	Vysoká

		Nefunkčnosť zdroja nepretržitého napájania v prípade potreby	Nízka	Vysoká
	Autentickosť	Modifikácia záznamu na archívnom médiu	Nízka	Vysoká
Komunikačné zariadenia	Dôvernosť	Nekontrolované pripojenie sa do infraštruktúry s následným vyťažovaním údajov	Nízka	Vysoká
		Neoprávnené získanie prístupových práv do siete	Nízka	Vysoká
	Integrita	Nekontrolované pripojenie sa do infraštruktúry s následným poškodzovaním alebo modifikovaním údajov	Nízka	Vysoká
	Dostupnosť	Mechanické poškodenie systému	Nízka	Nízka
	Autentickosť	Nekontrolované pripojenie sa do infraštruktúry s následným modifikovaním údajov	Nízka	Vysoká
Systémový software	Dôvernosť	Neoprávnené získanie prístupových práv do systémového software SW	Nízka	Vysoká

		Neznalosť bezpečnostných parametrov systémového SW s následkom straty dôvernosti údajov na nich spracúvaných	Nízka	Nízka
	Integrita	Poškodenie vírusom	Stredná	Vysoká
	Dostupnosť	Poškodenie SW následkom odmietnutia	Nízka	Nízka
	Autentickosť	SW generuje používateľovi neznáme funkcie	Nízka	Stredná
Aplikačný software	Dôvernosť	Neoprávnené získanie prístupových práv do systémového SW	Nízka	Vysoká
		Neznalosť bezpečnostných parametrov systémového SW s následkom straty dôvernosti údajov na ňom spracúvaných	Nízka	Stredná
	Integrita	Poškodenie vírusom	Stredná	Stredná
	Dostupnosť	Poškodenie SW s následkom odmietnutia	Nízka	Nízka
	Autentickosť	SW generuje používateľovi neznáme funkcie	Nízka	Vysoká

b) neautomatizované prostriedky spracúvania

Aktívum informačné systému	**faktor ohrozenia**	**pravdepodobný spôsob ohrozenia**	**Odhad pravdepodobnosti, že ohrozenie nastane**	**Odhad miery negatívneho dopadu**
Dokumenty Archivované údaje	Dôvernosť	Zamestnanec alebo návštevník vyhotoví neautorizovanú kópiu a vynesie ju mimo TDS s.r.o.	Vysoká	Vysoká
		Zamestnanec alebo návštevník si zapamätá dôležitý údaj a vynesie ho mimo TDS s.r.o.	Vysoká	Vysoká
	Integrita	Neoprávnená modifikácia údajov	Nízka	Vysoká
	Dostupnosť	Nekontrolovaná zmena uloženia	Nízka	Nízka
	Autentickosť	Vloženie nesprávneho údaja do databázy	Stredná	Vysoká
		Neoprávnená modifikácia záznamov databázy alebo dokumentu	Nízka	Vysoká
		Zneužitie alebo sfalšovanie elektronického podpisu	Nízka	Vysoká

c) spoločné aktíva

Aktívum informačné systému	**faktor ohrozenia**	**pravdepodobný spôsob ohrozenia**	**Odhad pravdepodobnosti, že ohrozenie nastane**	**Odhad miery negatívneho dopadu**
Zamestnanci	Dôvernosť	Neúmyselné porušenie zásad ochrany	Vysoká	Vysoká
		Úmyselné porušovanie zásad ochrany	Nízka	Vysoká
		Dočasná indispozícia	Nízka	Vysoká
		Skrytá psychická porucha	Nízka	Vysoká
		Neplánovaná neprítomnosť	Stredná	Nízka
		Neschopnosť plniť povinnosti	Nízka	Vysoká
	Autentickosť	Schopnosť klamať	Vysoká	Vysoká
Návštevníci	Dôveryhodnosť	Neúmyselné porušovanie zásad ochrany	Nízka	Vysoká
		Úmyselné porušovanie zásad ochrany	Nízka	Vysoká
	Autentickosť	Schopnosť klamať	Vysoká	Vysoká
Hrozby (bombový útok, vydieranie a pod.)	Dôvernosť Integrita Dostupnosť Autentickosť	Môžu vzniknúť podmienky pre uplatnenie všetkých typov ohrození	Stredná	Vysoká

Elektrická protipožiarna signalizácia	Dostupnosť	Následkom technickej poruchy zariadenie vyhlasuje falošný požiarny poplach	Nízka	Nízka
Bezpečnostné zariadenie na prístup do informačného systému automatizovaného spracúvania	Dôvernosť	Zneužitie identifikačného média alebo prístupového kódu	Stredná	Vysoká
	Integrita	Odchytenie prihlasovacieho hesla	Nízka	Vysoká
	Dostupnosť	Následkom technickej poruchy zariadenia odmietnutie prístupu oprávneným osobám	Nízka	Nízka
	Autentickosť	Následkom technickej poruchy nebol zistený neoprávnený pokus o ovládanie systému	Nízka	Vysoká
Úschovné objekty	Dôvernosť	Zneužitie kľúča alebo identifikačného média alebo prístupového kódu	Stredná	Vysoká
	Integrita	Odpozorovanie prístupového kódu	Nízka	Vysoká
	Dostupnosť	Následkom technickej poruchy zariadenie odmieta prístup oprávneným osobám	Nízka	Stredná

		Zabezpečenie dodávky elektrickej energie – môže mať negatívny vplyv na dostupnosť	Nízka	Nízka
	Integrita	Náhlym vypnutím dodávky elektrickej energie môže dôjsť aj k porušeniu integrity súborov v automatizovanom systéme spracúvania	Stredná	Stredná
Prívod a odvod vody, klimatizácia, vykurovanie	Dôvernosť Integrita Dostupnosť Autentickosť	Pri poruche zariadení môže dôjsť k narušeniu dôvernosti hasičmi, servisnými technikmi, záchranármi a pod., záchranárske práce, evakuácia, servisný zásah, hasenie môžu byť podmienkou pre narušenie integrity údajov, údaje môžu byť následkom vyššie uvedených prác aj zničené – stanú sa nedostupnými	Nízka	Vysoká
Osvetlenie	Dôvernosť Integrita Dostupnosť Autentickosť	Pri poruche osvetlenia môžu vzniknúť podmienky pre uplatnenie sa uvedených ohrození	Nízka	Stredná

Vyššia moc	Dôvernosť Integrita Dostupnosť Autentickosť	Môžu vzniknúť podmienky pre uplatnenie sa všetkých typov ohrození	Nízka	Vysoká

Vlastnosti osobných údajov:

Dôvernosť: je vlastnosť informácie, ktorá zabezpečuje, že informácie sú dostupné len tým subjektom, ktoré majú k nim autorizovaný prístup; informácie nebudú poskytnuté neoprávneným subjektom, pričom subjektom sa rozumie nielen používateľ, ale aj technické prostriedky a software

Integrita: je definovaná ako zabezpečenie presnosti a úplnosti informácií a metód spracúvania; zaisťuje, aby informácia nebola zmenená neautorizovaným subjektom

Dostupnosť: je definovaná ako zabezpečenie toho, aby autorizovaní používatelia mali prístup k informáciám vtedy, keď to potrebujú; zaisťuje ochranu proti odmietnutiu alebo zadržaniu služieb a zdrojov v systéme

Autentickosť: vlastnosť informácií, ktorá zabezpečuje jej pravosť a hodnovernosť

Nízka pravdepodobnosť, že príslušné ohrozenie nastane, znamená, že toto ohrozenie môže nastať iba výnimočne a je dostatočne eliminované základnými opatreniami použitím mechanických zábran a základných režimových opatrení.

Stredná pravdepodobnosť znamená takú intenzitu hrozby, ktorej je potrebné venovať zvýšenú pozornosť a eliminovať dôsledky je možné špecifickými opatreniami.

Vysoká pravdepodobnosť je tak závažná, že vyžaduje relatívne preverenie všetkých opatrení na elimináciu. Opatrenia na elimináciu vyžadujú nadštandardné aktivity.

Nízka miera negatívneho dopadu znamená, že nežiaduce dopady je možné odstrániť bežne dostupnými prostriedkami, nedôjde k porušeniu zákonov a hlavné procesy súvisiace s použitím informačného systému nebudú znateľne ohrozené.

Stredná miera negatívneho dopadu znamená, že odstránenie nežiaducich dopadov vyžaduje použitie plánovaných neštandardných prostriedkov a výpadok projektovanej funkcie informačného systému môže znamenať prekážku.

Vysoká miera nežiaduceho dopadu znamená, že došlo k porušeniu zákona, katastrofálnym dôsledkom, obnova projektovanej funkcie informačného systému vyžaduje neplánované prostriedky (finančné a časové), záujmy klienta sú nedostupné na dobu prevyšujúcu 1 deň.

NÁVRH OPATRENÍ NA ELIMINÁCIU NEŽIADÚCICH DOPADOV

Návrh opatrení na elimináciu nežiaducich dopadov v automatizovaných informačných systémov

Typ opatrenia	**Skupina**	**Realizácia**
Fyzické	Mechanické zábranné prostriedky	Zámkové vložky, pevné dvere, bezpečnostné dvere, pevné okná
	Úschovné objekty	Zámkové systémy, drevené skrine, trezor, skrinky na kľúče
	Bezpečná likvidácia	Skartovacie zariadenia
Technické	Elektronické detekčné systémy	Poplachový systém nahlásenia narušenia, elektrická požiarna signalizácia, kamerový systém
	Prístupové systémy	Riadenie prístupu, evidencia dochádzky
	Záložné systémy	Zálohovanie údajov, zálohovanie napájania
	Prostriedky proti pozorovaniu a neoprávnenému monitorovaniu	Zatemnenie okien, aktívne rušiče
Programové opatrenia	Kontrola prístupu	Heslo pre prístup do siete, heslo do aplikácie, heslo do emailovej schránky

	Audit činnosti	Záznamy do log súborov, automatizované hlásenie pokusov o neoprávnený prístup
	Opatrenia na ochranu súborov	Antivírusová ochrana, zálohovanie údajov, šifrovanie údajov
Režimové opatrenia	Zodpovednosť a riadenie	Vytvorenie pracovnej pozície, útvaru povereného riadením procesov bezpečnosti
	Určenie	Určenie technických prostriedkov, určenie oprávnených osôb a ich oprávnení, realizácia priestorov pre styk so stránkami
	Pravidlá	Pre prístup k informačnému systému, pre prácu s informačným systémov, pre prácu s heslami a prístupovými procedúrami, pre fyzickú ochranu
	Výber a príprava	Výber pracovníkov, príprava pracovníkov
	Kontrolný systém	Realizácia pravidelnej kontroly, nepravidelnej kontroly
	Havarijné plánovanie	Havarijné plány, plány obnovy
Personálne opatrenia	Výber a príprava	Výber pracovníkov, príprava pracovníkov, hodnotiaci a sankčný systém

Návrh opatrení na realizáciu nežiaducich dopadov v neautomatizovaných systémoch

Typ opatrenia	**Skupina**	**Realizácia**
Fyzické	Mechanické zábranné prostriedky	Zámkové vložky, pevné dvere, bezpečnostné dvere, pevné okná
	Úschovné objekty	Zámkové systémy, drevené skrine, trezor, skrinky na kľúče
	Bezpečná likvidácia	Skartovacie zariadenia

Technické	Elektronické detekčné systémy	Poplachový systém nahlásenia narušenia, elektrická požiarna signalizácia, kamerový systém
	Prístupové systémy	Evidencia dochádzky
	Záložné systémy	Zálohovanie údajov, zálohovanie napájania
	Prostriedky proti pozorovaniu a neoprávnenému monitorovaniu	Zatemnenie okien, aktívne rušiče
Režimové opatrenia	Zodpovednosť a riadenie	Vytvorenie pracovnej pozície, útvaru povereného riadením procesov bezpečnosti
	Určenie	Určenie technických prostriedkov, určenie oprávnených osôb aj ich oprávnení
	Pravidlá	Pre prístup do miestnosti, pre prístup s informačným systémom, priestorov pre styk so stránkami, pre fyzickú ochranu
	Kontrolný systém	Realizácia pravidelnej kontroly, nepravidelnej kontroly
	Havarijné plánovanie	Havarijné plány, plány obnovy
Personálne opatrenia	Výber a príprava	Výber pracovníkov, príprava pracovníkov, hodnotiaci a sankčný systém

BEZPEČNOSTNÁ SMERNICA
Popis technických, organizačných a personálnych opatrení

Poznámka: na účely tejto smernice pojem „zamestnanec“ zahŕňa i osoby pracujúci pre TDS s.r.o. na základe dohody o brigádnickej práci študentov, dohody o vykonaní práce alebo dohody o pracovnej činnosti.

Technické opatrenia:

- vstup do budovy umožnený len na základe osobitných kľúčov, ktoré vydáva konateľ oproti podpisu, kľúč vlastní každý zamestnanec,
- monitory počítačov sú otočené tak, že nie je možné do nich nazerať cez okno,
- dvere do priestorov TSD s.r.o. sú uzavreté, kľúče sú osobitné, bezpečnostné, prideľované zamestnancom oproti podpisu; dvere sú mimo pracovnej doby uzamykané, do priestorov budovy nemá vstup cudzia osoba ani počas pracovnej doby;
- každý zamestnanec TDS s.r.o. má k dispozícii jeden kľúč od priestorov kancelárie, evidencia je vedená u zodpovednej osoby,
- v prípade straty kľúča je vymenený zámok od vchodových dverí od TDS s.r.o., kľúč je pridelený každému zamestnancovi kancelárie,
- osoba, ktorá odchádza z TDS s.r.o. ako posledná, je povinná priestory zamknúť,
- skartácia osobných údajov sa vykonáva v súlade s požiadavkami zákona za prítomnosti minimálne dvoch osôb
- zálohovanie dokumentov je zabezpečené na dátovom serveri,
- elektrická požiarna signalizácia je v kompetencii správcu budovy,
- v uzamykateľnej skrini sa uschovávajú vyčlenené osobné údaje v pracovnej a mimopracovnej dobe, pričom kľúč má k dispozícii len konateľ firmy

Organizačné opatrenia:

- do priestorov budovy, v ktorej sídli TDS s.r.o., sa dostanú zamestnanci a návštevy len cez vstupný vchod ktorý je uzamknutý,
- zamestnanci, ktorí zatiaľ nemajú pridelené kľúče od budovy a priestorov a takisto návštevy môžu do budovy vstúpiť po preverení na základe ohlásenia poverenou osobou - zväčša niektorým z pracovníkov TDS s.r.o.
- návšteva je oprávnená vstúpiť do priestorov TDS s.r.o. len za účelom služobného rokovania a nikdy sa v priestoroch nezdržiava bez prítomností pracovníka TDS s.r.o. návšteva je povinná pri príchode do priestorov kancelárie TDS s.r.o. prihlásiť sa priamo u zamestnanca,
- vstupné dvere do priestorov TDS s.r.o. sú neustále pod dohľadom pracovníka TDS s.r.o. a sú neustále uzamknuté,

- pobyt zamestnancov v objekte je daný obsahom pracovnej činnosti, resp. pracovnou náplňou,
- mimo pracovnej doby sa môžu zamestnanci TDS s.r.o. zdržiavať v objekte len z dôvodov plnenia pracovných povinností so súhlasom konateľa TDS s.r.o.,
- servisné opravy zariadení, ktoré sú zabezpečené externými poskytovateľmi služieb, sa vykonávajú len za prítomnosti aspoň jedného zamestnanca TDS s.r.o.,
- pred skončením pracovnej doby je každý zamestnanec TDS s.r.o. povinný vypnúť počítač a uložiť dokumenty obsahujúce osobné údaje do príslušných spisov tak, aby sa nenachádzali na voľne prístupnom mieste,
- posledný zamestnanec TDS s.r.o., ktorý opúšťa priestory, je povinný uzamknúť vstupné dvere do priestorov kancelárie a celú budovu.
- v celej budove platí zákaz fajčenia.

Personálne opatrenia:

- podľa ust. § 79 zákona sú osoby, ktoré spracúvajú osobné údaje povinné zachovávať mlčanlivosť,
- oprávnené osoby nesmú využiť informácie a osobné údaje pre vlastnú potrebu, bez súhlasu prevádzkovateľa tieto nesmú zverejniť a nikomu poskytnúť, ani sprístupniť,
- TDS s.r.o. je povinná zaviazať mlčanlivosťou aj pracovníkov servisných a iných dodávateľských firiem,
- povinnosti mlčanlivosti trvá aj po skončení pracovného pomeru,
- všetci zamestnanci TDS s.r.o. boli v zmysle zákona poučení o právach a povinnostiach ustanovených zákonom a o zodpovednosti za ich porušenie zodpovednou osobou,
- zamestnanci TDS s.r.o., ktorí spracúvajú osobné údaje, sú povinní zúčastniť sa poučenia a všetkých preškolení, ktoré v predmetnej veci organizuje zodpovedná osoba TDS s.r.o..

Rozsah oprávnení a popis povolených činností jednotlivých oprávnených osôb:

- všetci zamestnanci TDS s.r.o. pracujúci v trvalom pracovnom pomere majú neobmedzený prístup na server, na ktorom sú uložené dokumenty, v ktorých sa spracúvajú osobné údaje,

- všetci zamestnanci majú prístup do všetkých priestorov TDS s.r.o., mimo pracovnej doby len so súhlasom konateľa TDS s.r.o.,
- mzdový a účtovný informačný systém spracúva externá firma AT consulting, s.r.o.
- kľúč od uzamykateľnej skrinky na archiváciu osobných údajov má iba administratívna pracovníčka
- prideľovanie a evidencia kľúčov je v kompetencii konateľa;
- všetci zamestnanci TDS s.r.o. sú oprávnení spracúvať osobné údaje za použitia všetkých foriem spracúvania osobných údajov podľa ust. § 13 zákona – rozsah spracúvania osobných údajov závisí od príslušnej pracovnej pozície, resp. pracovnej náplne.

Rozsah zodpovednosti oprávnených osôb a osoby zodpovednej za dohľad nad ochranou osobných údajov:

- všetci zamestnanci TDS s.r.o. pracujúci v trvalom pracovnom pomere a zamestnanci pracujúci pre TDS s.r.o. na základe dohody o brigádnickej práci študentov, dohody o vykonaní práce a dohody o pracovnej činnosti zodpovedajú za porušenie práv a povinností vyplývajúcich zo zákona, o ktorých boli riadne poučení v zmysle zákona zodpovednou osobou,
- všetci zamestnanci TDS s.r.o. pracujúci v trvalom pracovnom pomere a zamestnanci pracujúci pre TDS s.r.o. na základe dohody o brigádnickej práci študentov, dohody o vykonaní práce a dohody o pracovnej činnosti spolupracujúce osoby sú povinní dodržiavať mlčanlivosť o osobných údajoch, ktoré v rámci svojho pracovnoprávneho vzťahu s TDS s.r.o. spracovávajú,
- všetci zamestnanci TDS s.r.o. pracujúci v trvalom pracovnom pomere a zamestnanci pracujúci pre TDS s.r.o. na základe dohody o brigádnickej práci študentov, dohody o vykonaní práce a dohody o pracovnej činnosti sú povinní sa riadiť smernicou o spracovaní osobných údajov, so znením ktorého boli riadne oboznámení v rámci poučenia vykonaného v zmysle zákona zodpovednou osobou,
- všetci zamestnanci TDS s.r.o. pracujúci v trvalom pracovnom pomere a zamestnanci pracujúci pre TDS s.r.o. na základe dohody o brigádnickej práci študentov, dohody

o vykonaní práce a dohody o pracovnej činnosti zodpovedajú za splnenie povinnosti likvidácie osobných údajov po splnení účelov ich spracúvania,

- všetci zamestnanci TDS s.r.o. pracujúci v trvalom pracovnom pomere a zamestnanci pracujúci pre TDS s.r.o. na základe dohody o brigádnickej práci študentov, dohody o vykonaní práce a dohody o pracovnej činnosti zodpovedajú za správnosť a aktuálnosť osobných údajov, ktoré v informačnom systéme spracúvajú,
- zodpovedná osoba je zodpovedná za výkon dohľadu nad ochranou osobných údajov,
- zodpovedná osoba zabezpečuje:
  a) potrebnú súčinnosť s úradom na ochranu osobných údajov pri plnení úloh patriacich do je pôsobnosti,
  b) pred začatím spracúvania osobných údajov v informačných systémoch TDS s.r.o. posúdi či spracúvaním osobných údajov nevzniká nebezpečenstvo narušenia práv a slobôd dotknutých osôb, a prípadné zistenie narušenia práv a slobôd dotknutých osôb bezodkladne písomne oznámi prevádzkovateľovi resp. sprostredkovateľovi. Ak TDS s.r.o. nevykoná nápravu, bezodkladne písomne oznámi narušenie práv a slobôd dotknutých osôb v súvislosti so spracúvaním ich osobných údajov úradu na ochranu osobných údajov,
  c) dohľad nad plnením základných povinností prevádzkovateľa a sprostredkovateľa,
  d) poučenie oprávnených osôb,
  e) vybavovanie žiadostí dotknutých osôb,
  f) realizácia technických, organizačných a personálnych opatrení a dohliada na ich aplikáciu v praxi,
  g) zabezpečuje vypracovanie bezpečnostného projektu,
  h) dohľad pri výbere sprostredkovateľa,
  i) dohľad nad cezhraničným tokom osobných údajov,
  j) registrácia resp. odhlásenie informačných systémov, evidencia informačných systémov, ktoré nepodliehajú registrácii.

Spôsob identifikácie a autentizácie pri prístupe k informačnému systému:

- zamestnanci TDS s.r.o. používajú na prístup do kancelárie kľúč, ktorý je im prideľovaný konateľom,
- zamestnanci TDS s.r.o. pristupujú do informačného systému vedeného automatizovaným spôsobom prostredníctvom zadania prideleného hesla,
- zamestnanci vstupujú do svojej e-mailovej schránky prostredníctvom zvoleného hesla.

Kontrolná činnosť:

- kontrolná činnosť na úseku ochrany osobných údajov vykonávajú v TDS s.r.o. konatelia TDS s.r.o.,
- pri zistení nedostatkov uloží konateľ zamestnancovi TDS s.r.o. lehotu na nápravu, ak nedôjde v určenej lehote k náprave, stane sa zamestnanec TDS s.r.o. subjektom sankčného postihu,
- kontroly sa vykonávajú pravidelne, najmenej jedenkrát za rok.

Postupy pri haváriách, poruchách a iných mimoriadnych situáciách

V TDS s.r.o. existujú viaceré spôsoby ohrozenia, resp. mimoriadne situácie, najmä krádež, teroristický útok, sabotáž, vydieranie s cieľom získať prístup do objektu, únos spoločníkov s cieľom získať prístup do objektu, hrozba uložením nástražného výbušného systému.

Pri krádeži v objekte sú prijaté tieto organizačné opatrenia:

Opatrenie	**Kto vykoná**	**Spôsob vykonania**
Zadržanie páchateľa, krádeže a pokus o krádež	V závislosti od situácie zamestnanec TDS s.r.o.	Fyzické zadržanie a ohlásenie konateľom TDS s.r.o. polícii,
Zabezpečenie miesta krádeže pred vniknutím neoprávnených a nepovolaných osôb	Poverená osoba z radov zamestnancov TDS s.r.o.	Fyzické stráženie

Oznámenie krádeže osobných údajov v objekte	Konatelia	Policajnému orgánu na č. 158

Pri teroristickom útoku na objekt sú na objekte prijaté tieto organizačné opatrenia:

Opatrenie	**Kto vykoná**	**Spôsob vykonania**
Privolanie pomoci	Zamestnanec TDS s.r.o., správca budovy	telefonicky
Privolanie policajného zboru	Zamestnanec TDS s.r.o., správca budovy	telefonicky

Pri sabotáži sú na objekte prijaté tieto organizačné opatrenia:

Opatrenie	**Kto vykoná**	**Spôsob vykonania**
Miesto narušenia objektu	Správca budovy	Obhliadkou miesta v objekte, obhliadkou chráneného priestoru
Zadržanie páchateľa	Správca budovy , príslušníci policajného zboru	Vyhľadanie páchateľa,
Oznámenie sabotáže v objekte	Správca budovy alebo zamestnanec TDS s.r.o.	Telefonicky na tel. č. 155
Zabezpečenie miesta sabotáže pred vniknutím neoprávnenej a nepovolenej osoby	Správca budovy	Strážením

Pri vydieraní zamestnancov spoločnosti sú na objekte prijaté tieto organizačné opatrenia:

Opatrenie	Kto vykoná	Spôsob vykonania
Povinnosť oznámiť vydieranie	Každý vydieraný pracovník	Oznámenie konateľom TDS s.r.o. a policajnému zboru
Zvýšenie ochrany objektu a chráneného priestoru	Správca budovy, príslušníci policajného zboru	Posilnením ochrany objektu

Pri hrozbe uloženia nástražného výbušného systému sú na objekte prijaté tieto organizačné opatrenia:

Opatrenie	Kto vykoná	Spôsob vykonania
Evakuácia zamestnancov TDS s.r.o. z objektu	Konateľ TDS s.r.o. alebo poverený zamestnanec TDS s.r.o.	Osobne alebo telefonicky
Povinnosť oznámiť uloženie nástražného výbušného systému	Ktorýkoľvek zamestnanec TDS s.r.o.	Telefonicky na č. 155
Ochrana priestorov a objektu z vonka	Správca budovy,	Strážením
Obhliadka objektu políciou	Policajný zbor	Obhliadka

Ďalšie mimoriadne udalosti: Požiar

Vzhľadom na možnosť vzniku požiaru v objekte sú prijaté tieto organizačné opatrenia:

Postup	Spôsob	Určené osoby	Určený materiál
Varovanie všetkých zamestnancov TDS s.r.o.	Osobne, signálmi civilnej ochrany	Správca budovy, zamestnanec TDS s.r.o.	Tabuľka signálov CO
Oznámenie požiaru na tel. č. 150	Osobne alebo telefonicky	Prijímateľ správy o mimoriadnej situácii	Telefón

Likvidácia požiaru	Hasením podľa požiarnej smernice	Prítomní zamestnanci TDS s.r.o.	Hasiace prístroje, hydranty
Evakuácia písomností a vecí	Vynesenie mimo objekt	Zamestnanci TDS s.r.o. prítomní na pracovisku	
Ochrana počas vynesenia písomností a vecí	Strážením	Dve osoby určí v danom čase konateľ TDS s.r.o.	Ochrana nepremokavým materiálom

Spôsob výkonu kontroly organizačných opatrení:

- požiarne prehliadky,
- kontrola výkonu strážnej služby,
- kontrolné nácviky činností na jednotlivé spôsoby narušenia alebo mimoriadne situácie.

10. EKONOMICKÉ A ORGANIZAČNÉ ZABEZPEČENIE BEZPEČNOSTI INFORMAČNÉHO SYSTÉMU

Vzhľadom na súčasný stav a spôsob prevádzky informačného systému nevzniká pre spoločnosť potreba ďalšieho financovania, ktoré by vyplývalo z navrhovaných opatrení a prijatých bezpečnostných smerníc.

Organizačné zabezpečenie spočíva v doplnení zmlúv a vypracovaní smernice o spracovaní osobných údajov, a vedení záznamu o spracovateľských činnostiach tak, aby boli v súlade so zákonom č. 18/2018 Z. z. Zákona o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

11. ZÁVEREČNÉ USTANOVENIA

1. Smernica o spracovaní osobných údajov predstavuje výsledný produkt analytickej časti riešenia bezpečnosti informačného systému ochrany osobných údajov.

Sumarizuje výsledky analýz a spoločne s bezpečnostnými smernicami predkladá spôsoby riešenia pre všetky úrovne zabezpečenia s popisom bezpečnostných opatrení.

2. Smernica o spracovaní osobných údajov z týchto dôvodov je potrebné považovať za dôverný dokument, ktorého obsah je nevyhnutné chrániť pred neoprávneným prístupom rovnako ako najcitlivejšie osobné údaje spracúvané v informačnom systéme.

3. Sprístupnenie jeho obsahu neoprávneným osobám a nepovolaným osobám môže mať za následok eliminovanie bezpečnostných mechanizmov informačného systému a ohrozenie jeho dôvernosti. Z uvedených dôvodov spoločnosť stanovuje, že s obsahom tohto bezpečnostného projektu sa môže okrem spracovateľa oboznamovať len osoba poverená dohľadom nad ochranou osobných údajov a oprávnené osoby.