INOX CENTER, proizvodnja in trgovina d.o.o., Partizanska ulica 55, 5000 Nova Gorica, matična številka: 5901545000 (v nadaljevanju: »**upravljavec**«) na podlagi 24. in 25. člena Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07 s spremembami, v nadaljevanju: »**ZVOP-1**«) ter zlasti 24., 25. in 32. člena Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (v nadaljevanju: »**Splošna uredba o varstvu podatkov**«)

sprejema naslednji:

P R A V I L N I K

o varovanju osebnih podatkov

I. Uvodno glede obdelave osebnih podatkov

1. člen

Upravljavec je podjetje, ki se ukvarja s trgovino z nerjavečimi in alu materiali (pločevino, cevmi, profili...), polizdelki in sredstvi za njihovo obdelavo.

Glavna gospodarska dejavnost upravljavca je trgovina na debelo z nerjavečimi in alu materiali, pri čemer obdelava osebnih podatkov upravljavca predstavlja zgolj postransko dejavnost delodajalca.

Ta Pravilnik določa ukrepe za zavarovanje pri zbiranju, obdelovanju, shranjevanju, posredovanju in uporabi osebnih podatkov pri upravljavcu.

V zadevah, ki jih ne ureja ta Pravilnik, se neposredno uporabljajo določbe Zakona o varstvu osebnih podatkov ter Splošne uredbe o varstvu podatkov.

Upravljavec podatkov ne posreduje in ne iznaša v tretje države in/ali mednarodne organizacije.

Pri izvajanju navedenih dejavnosti upravljavec obdeluje naslednje osebne podatke: zaposlenih delavcev, strank, ki so fizične osebe, kontaktnih podatkov fizičnih oseb pri strankah, ki so pravne osebe.

Upravljavec ne obdeluje posebnih vrst osebnih podatkov (t.i. občutljive osebne podatke), niti ne obdeluje osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški.

2. člen

V tem Pravilniku uporabljeni izrazi imajo naslednji pomen:

- **ZVOP-1** – Zakon o varstvu osebnih podatkov (Uradni list RS, št. 86/04 in 113/05);

- **Splošna uredba** – Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 26. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov (GDPR);

- **osebni podatek**: katero koli informacija v zvezi z določenim ali določljivim posameznikom; določljiv posameznik je tisti, ki ga je mogoče neposredno ali posredno določiti, zlasti z navedbo identifikatorja, kot je ime, identifikacijska številka, podatki o lokaciji, spletni identifikator, ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, gensko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika;

- **posebna vrsta osebnih podatkov**: podatki, ki razkrivajo rasno ali etnično poreklo, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu, in obdelava genskih podatkov, biometričnih podatkov za namene edinstvene identifikacije posameznika, podatkov v zvezi z zdravjem ali podatkov v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo;

- **posameznik**: je določena ali določljiva fizična oseba na katero se nanaša osebni podatek;

- **obdelava**: vsako dejanje ali niz dejanj, ki se izvaja v zvezi z osebnimi podatki ali nizi osebnih podatkov z avtomatiziranimi sredstvi ali brez njih, kot je zbiranje, beleženje, urejanje, strukturiranje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, prilagajanje ali kombiniranje, omejevanje, izbris ali uničenje;

- **zbirka**: vsak strukturiran niz osebnih podatkov, ki so dostopni v skladu s posebnimi merili, niz pa je lahko centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi;

- **upravljavec**: fizična ali pravna oseba, javni organ, agencijo ali drugo telo, ki samo ali skupaj z drugimi obdeluje osebne podatke in določa namene in sredstva obdelave;

- **obdelovalec**: fizična ali pravna oseba, javni organ, agencijo ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca;

- **uporabnik**: fizična ali pravna oseba, javni organ, agencijo ali drugo telo, ki so mu bili osebni podatki razkriti, ne glede na to, ali gre za posameznika, na katerega se podatki nanašajo ali na tretjo osebo. Javni organi, ki lahko prejmejo osebne podatke v okviru posamezne poizvedbe se ne štejejo za uporabnike.;

- **nosilec podatkov**: vse vrste sredstev, na katerih so zapisani ali posneti podatki, ne glede na obliko, v kateri so izraženi (listina, akt, gradivo, spis, magnetni, optični ali drugi računalniški mediji, prikazovalnik računalnika, fotokopije, zvočno ali slikovno gradivo, mikrofilmi, naprave za prenos podatkov);

- **strojna oprema**: oprema za vnos, obdelavo, prikaz, shranjevanje in posredovanje podatkov;

- **računalniška strojna oprema**: oprema za prenos podatkov, oprema za kriptografijo, oprema za zvočno in slikovno gradivo, merilni instrumenti, mikrofilmska oprema ipd.;

- **sistemska programska oprema**: programi, ki jih računalnik uporablja za krmiljenje svoje opreme in za komunikacije z okoljem (operacijski sistem) in druga programska orodja, ki so del operacijskega sistema in so namenjena vzdrževalcem in uporabnikom računalnika;

- **aplikativna programska oprema**: programi, s katerimi se izvaja obdelava podatkov;

- **zavarovani prostori**: prostori, kjer se nahajajo nosilci podatkov, preko katere je mogoč dostop do zbirk podatkov;

- **pooblaščeni delavec**: s strani odgovorne osebe imenovan delavec, ki skrbi za izvajanje postopkov in ukrepov za izvajanje zavarovanja podatkov;

- **pooblaščena oseba za varstvo osebnih podatkov** – s strani upravljavca imenovana oseba z ustreznimi poklicnimi odlikami in zlasti strokovnim znanjem ter dejanskimi izkušnjami o zakonodaji in praksi na področju varstva osebnih podatkov ali na primerljivem področju, ki upravljavcu ali obdelovalcu na neodvisen način pomaga pri zagotavljanju skladnosti obdelave osebnih podatkov s pravili Splošne uredbe ter določbami zakona, ki ureja področje varstva osebnih podatkov in drugih zakonov, ki urejajo obdelavo in varstvo osebnih podatkov.

3. člen

Za namen identifikacije in popisa vseh vrst osebnih podatkov, katere obdeluje upravljavec, se vodi Seznam evidenc dejavnosti obdelave osebnih podatkov (v nadaljevanju: »**Seznam evidenc**«), katerega namen je omogočiti popoln pregled nad tokom osebnih podatkov. Seznam evidenc je obenem podlaga za sprejem tehničnih, organizacijskih in kadrovskih ukrepov za zavarovanje osebnih podatkov, kot so opisani v tem Pravilniku.

Upravljavec skrbi za točnost in ažurnost Seznama evidenc. Upravljavec bo nadzornemu organu na njegovo zahtevo omogočil dostop do Seznama evidenc.

Delavci, ki pri izvajanju del in nalog za upravljavca obdelujejo osebne podatke, morajo biti seznanjeni s Seznamom evidenc, vpogled vanj pa je potrebno omogočiti tudi vsakomur, ki to zahteva in ima za vpogled zakonit interes (npr. posameznik, na katerega se nanašajo osebni podatki, nadzorni organ, policija na podlagi zakonskih pooblastil).

4. člen

Ob upoštevanju opisane narave, obsega, okoliščin in namena obdelave, kot je razviden iz 1. člena tega Pravilnika in Seznama evidenc, upravljavec zaključuje, da obdelava podatkov ne predstavlja velikega tveganja za pravice in svoboščine posameznikov, zato priprava predhodne ocene učinka v zvezi z obdelavo podatkov ni potrebna.

Pred vsako novo obdelavo osebnih podatkov, zlasti pa pred uporabo novih tehnologij ter pred vsako spremembo narave, obsega, okoliščin in namenov obdelave, ter vedno, ko se spremeni tveganje, ki ga predstavljajo dejanja obdelave, se upravljavec zaveže ponovno opraviti pregled tveganj in oceniti, ali je v zvezi z obdelavo potrebno pripraviti oceno učinka.

II. Splošne določbe

5. člen

Namen tega Pravilnika je zagotoviti zaupnost, celovitost, dostopnost in točnost osebnih podatkov, v interesu

posameznikov, na katere se osebnih podatki nanašajo, in sicer v vsaki fazi obdelave osebnih podatkov. Vsi zaposleni se morajo zavedati tveganj, ki so povezana s tehničnimi in informacijskimi sistemi ter komunikacijsko tehnologijo, ter morajo zato izvajati obdelavo osebnih podatkov z zahtevano skrbnostjo.

6. člen

Upravljavec mora zagotoviti ustrezne tehnične in organizacijske ukrepe, s katerimi se varujejo osebni podatki ter preprečuje njihovo slučajno, namerno ali drugače nezakonito uničenje, spremembo, izgubo, nepooblaščeno razkritje, dostop ali drugo nepooblaščeno obdelavo.

Ukrepi morajo biti primerni glede na stanje najnovejšega tehnološkega razvoja in stroškov, izvajanja ter narave, obsega, okoliščin in namenov obdelave kot tudi tveganj za pravice in svoboščine posameznikov ter zagotavljati ustrezno varnost podatkov glede na morebitna tveganja, ki jih pomeni obdelava podatkov, zlasti v primeru nenamernega ali nezakonitega uničenja, izgube, spremembe, nepooblaščenega razkritja ali dostopa do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani.

Upravljavec mora ozaveščati osebe, udeležene v postopkih obdelave podatkov o varnostnih politikah ter postopkih in ukrepih za zagotavljanje varnosti osebnih podatkov (kot npr.: odjavljanje iz sistema po zaključku dela, uporaba programskega zaklepanja računalnika ob odsotnosti od računalnika, zaklepanje prostorov ali stalni nadzor, politika čiste in urejene delovne mize in delovnega prostora, pomen zagotavljanja sledljivosti obdelave, vsak uporabnik uporablja svoje uporabniško ime in geslo, fizično varovanje gesel, previdnost pri izbiri gesel, občasno spreminjanje gesel, kriptirano pošiljanje podatkov po elektronskih medijih, pazljivost in skrbnost pri posredovanju podatkov po telefonu, takojšnje obveščanje o incidentu, upoštevanje notranjih pravil in aktov,...).

7. člen

Upravljavec pri obdelavi osebnih podatkov upošteva splošna načela v zvezi z obdelavo osebnih podatkov. Upravljavec obdeluje le tiste osebne podatke, za katere ima ustrezno zakonsko podlago na podlagi določb ZVOP-1 in Splošne uredbe o varstvu podatkov.

Osebni podatki se smejo zbirati samo za določene in zakonite namene ter se ne smejo nadalje obdelovati tako, da bi bila njihova obdelava v neskladju s temi nameni, razen če relevantna zakonodaja ne določa drugače.

Pri obdelavi osebnih podatkov upravljavec zagotavlja, da so osebni podatki:

- obdelani zakonito, pošteno in na pregleden način v zvezi s posameznikom, na katerega se nanašajo osebni podatki;
- zbrani za določene, izrecne in zakonite namene ter da se ne obdelujejo dalje na način, ki ni združljiv s temi nameni;
- ustrezni, relevantni in omejeni glede na namene, za katere se obdelujejo;
- točni in kadar je to potrebno posodobljeni;
- hranjeni v obliki, ki dopušča identifikacijo posameznikov, na katere se nanašajo osebni podatki, le toliko časa, kolikor je to potrebno za namene, za katere se obdelujejo, razen če posamezen zakon ne določa česa drugega;

- obdelujejo na način, ki zagotavlja njihovo celovitost in zaupnost, zlasti pa, da so z ustreznimi tehničnimi ali organizacijskimi ukrepi ustrezno varovani pred nedovoljeno ali nezakonito obdelavo ter pred nenamerno izgubo, uničenjem, ali poškodbo.

8. člen

V tem Pravilniku uporabljeni izrazi imajo pomene kot to izhaja iz veljavnega ZVOP-1 ter Splošne uredbe o varstvu podatkov.

9. člen

S tem pravilnikom se določajo organizacijski, tehnični in logično tehnični postopki in ukrepi za varovanje osebnih podatkov v družbi INOX CENTER d.o.o. (v nadaljevanju: upravljavcu) z namenom, da se prepreči slučajno ali namerno nepooblaščeno uničevanje podatkov, njihova sprememba ali izguba kakor tudi nepooblaščen dostop, obdelavo, uporabo ali posredovanje osebnih podatkov.

Zaposleni in zunanji sodelavci družbe INOX CENTER d.o.o., ki pri svojem delu obdelujejo in uporabljajo osebne in zaupne podatke, morajo pri svojem delu spoštovati Zakon o varstvu osebnih podatkov (v nadaljevanju: ZVOP - 1) in Splošno uredbo o varstvu podatkov.

Zavarovanje osebnih podatkov obsega kadrovske, organizacijske, tehnične in logistično-tehnične postopke in ukrepe, z namenom, da se izpolnijo zakonske zahteve glede varovanja osebnih podatkov in zaščitijo pravice posameznikov, na katere se nanašajo osebni podatki.

Ti ukrepi sestojijo iz zavezujočih pravil, priporočil oziroma načel iz prakse, internih postopkov, organizacijskih struktur in varnosti informacijske tehnologije, s katerimi se:
- varujejo prostori, oprema in sistemska programska oprema;
- varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki;
- zagotavlja varnost posredovanja in prenosa osebnih podatkov;
- onemogoča nepooblaščenim osebam dostop do naprav, na katerih se obdelujejo osebni podatki in do njihovih zbirk.

III. Kadrovski ukrepi

10. člen

Upravljavec, zaposleni in pooblaščene osebe pri upravljavcu so dolžni izvajati ukrepe za zagotavljanje varovanja osebnih podatkov, s katerimi se seznanijo pri svojem delu, ravnati vestno in skrbno na način in po postopkih, ki jih določa ta Pravilnik.

11. člen

Direktorica upravljavca lahko imenuje pristojno osebo, pooblaščeno za:

- izvajanje postopkov in ukrepov za izvajanje zavarovanja podatkov;
- za obdelavo osebnih podatkov.

Direktorica lahko za posamezne naloge zaposlenim odvzame pooblastilo in pooblasti druge osebe.
Za pravilno izvajanje tega Pravilnika je dokončno pristojen in odgovoren direktorica upravljavca.

12. člen

Ker obdelava osebnih podatkov pri upravljavcu ne zajema rednega in sistematičnega obsežnega spremljanja posameznikov in ker upravljavec ne obdeluje posebnih vrst osebnih podatkov in/ali podatkov v zvezi s kazenskimi obsodbami in prekrški, upravljavec ne bo imenoval posebne pooblaščene osebe za varstvo podatkov, skladno s 37. členom Splošne uredbe o varstvu podatkov.

13. člen

Vsi delavci, ki opravljajo delo pod vodstvom upravljavca in imajo dostop do osebnih podatkov, teh podatkov ne smejo obdelovati brez ali izven navodil upravljavca. Vsi delavci, ki pri svojem delu obdelujejo osebne podatke, so dolžni izvajati predpisane postopke in ukrepe za zavarovanje podatkov in varovati podatke, za katere so izvedeli oziroma bili z njimi seznanjen pri opravljanju svojega dela. Obveza varovanja podatkov ne preneha s prenehanjem delovnega razmerja.

Vsi delavci, ki pri svojem delu obdelujejo osebne podatke, morajo biti seznanjeni z zakonodajo s področja varstva osebnih podatkov ter z vsebino tega Pravilnika. Upravljavec bo v ta namen poskrbel, da bodo taki delavci podpisali posebno Izjavo o varstvu osebnih podatkov, iz katere bo razvidno, da so seznanjeni z določbami tega Pravilnika in zakonodajo s področja varstva osebnih podatkov.

Upravljavec bo skladno z načelom odgovornosti delavcem, ki obdelujejo osebne podatke, po potrebi zagotavljal ustrezna izobraževanja oz. treninge s področja varovanja osebnih podatkov.

Za kršitev določil iz tega člena so delavci disciplinsko, odškodninsko in kazensko odgovorni. Kršitev določil tega Pravilnika se šteje za hujšo kršitev pravic in obveznosti iz delovnega razmerja, zaradi česar se takim delavcem lahko pogodba o zaposlitvi redno odpove iz krivdnih razlogov ali izredno odpove v primeru hujših kršitev.

III. Varovanje prostorov, opreme in sistemsko programske opreme

14. člen

Osebni podatki in informacijski sistemi morajo biti ustrezno zaščiteni.

Prostori, kjer se nahajajo osebni podatki ali nosilci osebnih podatkov, njihove kopije in informacijski sistemi, sodijo v kategorijo "Varovanih prostorov".

Pri upravljavcu so »varovani prostori« vsi pisarniški prostori na sedežu upravljavca. Ti prostori morajo biti varovani z organizacijskimi ter fizičnimi in tehničnimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov in za katere velja naslednji režim:

1. Dostop v varovane prostore je mogoč in dopusten le v delovnem času, izven delovnega časa pa le na podlagi dovoljenja direktorice družbe.

2. Dostop osebam, ki niso zaposlene v varovanih prostorih, je dovoljen le v prisotnosti zaposlenega delavca v teh prostorih.

3. Delavci v varovanih prostorih morajo prostor vestno in skrbno nadzorovati in ob vsaki odsotnosti zakleniti.

4. Nosilcev osebnih podatkov ne smejo izpostavljati nevarnosti nenadzorovanega vpogleda ali iznosa.

5. Vsi računalniki, na katerih se nahajajo osebni podatki morajo biti v času vsake odsotnosti delavca zadolženega za delo z osebnimi podatki fizično ali programsko zaklenjeni. Izven delovnega časa morajo biti omare in pisalne mize z nosilci osebnih podatkov zaklenjene, računalniki in druga strojna oprema izklopljeni in fizično ali programsko zaklenjeni.

6. Nosilci osebnih podatkov, hranjeni izven aktivnih delovnih prostorov oziroma izven varovanih prostorov (hodniki, skupni prostori, aktivni in pasivni arhivi ipd.), morajo biti stalno zaklenjeni.

7. Delavec, ki pri svojem delu uporablja osebne podatke ali jih kakorkoli obdeluje, ne sme med delovnim časom puščati nosilcev osebnih podatkov na pisalnih mizah ali jih kako drugače izpostavljati nevarnosti vpogleda vanje nepooblaščenim osebam oziroma delavcem (t.i. politika čiste mize).

8. V prostorih, v katere imajo vstop stranke oziroma osebe, ki niso zaposlene v družbi, morajo biti nosilci podatkov in računalniški prikazovalniki nameščeni v času obdelave ali dela na njih tako, da je strankam onemogočen vpogled vanje. V odsotnosti z delovnega mesta morajo zaposleni ekran računalnika izklopiti ali kako drugače fizično ali programsko zakleniti (t.i. politika čistega ekrana).

Nosilci osebnih podatkov, ki se nahajajo izven zavarovanih prostorov (hodniki, skupni prostori) morajo biti stalno zaklenjeni.

15. člen

Varovani prostori ne smejo ostajajo nenadzorovani, oziroma se zaklepajo ob odsotnosti delavcev, ki jih nadzorujejo. Izven delovnega časa se varovani prostori zaklepajo. Ključi se ne puščajo v ključavnici v vratih od zunanje strani.

16. člen

Vzdrževalci prostorov, strojne in programske opreme, obiskovalci in poslovni partnerji se smejo gibati v varovanih prostorih samo ob prisotnosti vsaj enega delavca, ki v teh prostorih opravlja delo. Zaposleni tehnično-vzdrževalni delavci in čistilke se lahko gibljejo v varovanih prostorih izven delovnega časa in

brez prisotnosti odgovornega delavca le, če so nosilci podatkov shranjeni v zaklenjenih omarah na način, ki ga določa ta pravilnik za čas izven delovnega časa.

17. člen

Obdelovanje osebnih podatkov iz zbirk osebnih podatkov je dovoljeno le v prostorih družbe.

Nosilcev osebnih podatkov delavci družbe ne smejo odnašati izven družbe brez izrecnega dovoljenja direktorice družbe. Direktorica lahko dovoli iznos nosilcev osebnih podatkov iz družbe, ko predhodno delavec vpiše namen in razlog za iznos podatkov iz družbe v seznam evidenc v zvezi z varstvom osebnih podatkov.

V primeru obdelovanja osebnih podatkov po pogodbenem obdelovalcu, režim varovanja osebnih podatkov določa 36. čl. tega Pravilnika.

18. člen

Posredovanje osebnih podatkov pooblaščenim zunanjim institucijam in drugim, ki izkažejo zakonsko podlago za pridobitev osebnih podatkov, dovoli direktorica in posredovanje vpiše v seznam evidenc v zvezi z varstvom osebnih podatkov.

19. člen

Vzdrževanje in popravilo strojne računalniške in druge opreme, s katero se obdelujejo osebni podatki, je dovoljeno samo z vednostjo in odobritvijo direktorice ali od nje pooblaščene osebe, izvajajo pa ga lahko samo pooblaščeni servisi in njihovi vzdrževalci (obdelovalci osebnih podatkov), ki imajo z upravljavcem sklenjeno pogodbo o servisiranju računalniške oziroma strojne opreme ter pogodbo o obdelavi osebnih podatkov.

Zunanji dostopi, ki so namenjeni vzdrževanju, se aktivirajo le za čas trajanja vzdrževanja in jih je potrebno dokumentirati. Po prenehanju vzdrževalnih del tako dostopi za vzdrževanje deaktivirajo.

IV. Varovanje aplikativne programske opreme, s katero se obdelujejo osebni podatki

20. člen

Dostop do računalniške programske opreme mora biti varovan na način, ki omogoča dostop samo zaposlenim pri upravljavcu ali pooblaščenim osebam pri upravljavcu in tretjim, ki za upravljavca po pogodbi opravljajo servisiranje računalniške strojne in programske opreme ali drugih pogodbenih storitev.

21. člen

Vsaka operacija s podatki se beleži v sistemskih dnevniških datotekah (t.i. *logih*). Beleženje mora izvesti administrator v skladu z zahtevami in možnostmi operacijskih sistemov in aplikacij.

Revizijska sled mora zagotavljati, da se da ugotoviti, kdaj so bili posamezni osebni podatki vneseni v zbirko podatkov, uporabljeni ali drugače obdelovani oziroma spremenjeni ter kdo je to storil. Vsi dogodki se morajo opremiti s časovnim žigom.

22. člen

Strojna oprema in sistemska programska oprema, vključno z vhodno-izhodnimi enotami, mora biti zaščitena na način, da se zavaruje integriteta in zaupnosti podatkov.

Vse delovne postaje in prenosni računalniki in druga oprema morajo biti opremljeni z aktualno antivirusno zaščito. Vsi računalniki na delovnem mestu morajo biti opremljeni s kombinacijo iz lokalnega požarnega zidu in lokalnega sistema za zaznavanje in preprečevanje vdorov. Vsi prenosni računalniki in druga oprema morajo biti opremljeni z lokalnim požarnim zidom.

23. člen

Za potrebe restavriranja računalniškega sistema ob okvarah in ob drugih izjemnih situacijah se zagotavlja redna izdelava kopij vsebine mrežnega strežnika in lokalnih postaj, če se podatki tam nahajajo (tj. izdelava varnostnih kopij podatkov).

Za podatke, za katere velja visoka zahteva po razpoložljivosti, se mora varnostna kopija (*backup*) vzpostaviti redno, tako da se lahko v primeru izpada ene ali več komponent ponovno vzpostavi pripravljenost za obratovanje celotnega sistema.

24. člen

Ob izpadu sistema mora biti zagotovljeno, da se ne izgubijo nobene kritične informacije.

Mediji za varnostno shranjevanje se morajo hraniti na krajih, ki izpolnjujejo zahteve zaupnosti, integritete in razpoložljivosti zadevnih informacij. To vključuje tudi zadostno prostorsko ločevanje med mediji za varnostno shranjevanje in varnostnim virom (npr. skladiščenje v drugih prostorih).

Zagotoviti se mora, da ima administracijsko osebje v nujnem primeru dostop do varnostnih medijev.

Varnostne kopije se shranjujejo dnevno, izbrišejo pa se po preteku 14 dni.

25. člen

Vsi osebni računalniki, na katerih je možen dostop do osebnih podatkov, so varovani z uporabniškim imenom in geslom.

Programska oprema inštalirana na računalniku, ki omogoča dostop do osebnih podatkov, je varovana z uporabniškim imenom in geslom, različnim od uporabniškega imena in gesla računalnika.

Dostop do informacijskih sistemov je omejen na pravice, ki so potrebne za izvajanje določene naloge (npr. pravice do branja, spreminjanja, administratorski dostop). Pri podelitvah pravic dostopa upravljavec sledi načelo »*need-to-know*«, kar pomeni, da uporabniki ne smejo prejeti več pravic, kot bi bile potrebne za izvajanje njihovih nalog ali za dostop do podatkov.

Dostop do podatkov prek aplikativne programske opreme mora biti varovan s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov in podatkov. Politika (režim) dodeljevanja, hranjenja in spreminjanja gesel:

Vsakemu uporabniku se dodeliti jasno (osebno) uporabniško ime (ID oznaka uporabnika). To velja tudi za privilegirane pravice do dostopa (npr. za administratorje). Dolžina gesel je 8-mestna (8 znakov). Gesla se menjujejo vsakih 6 mesecev. Nameščeni računalniški sistem samodejno opozarja uporabnika na potek veljavnosti gesla.

Vsa gesla in postopki, ki se uporabljajo za dostop in za administriranje v mreži osebnih računalnikov, administriranje z elektronsko pošto in administriranje prek aplikativnih programov, se hranijo pri IT administratorju.

Če določeni delavec zamenja delovno mesto, se mora preveriti pravice do dostopa. Tudi sicer se morajo pravice do dostopa redno preverjati.

Če delavec preneha opravljati delo za upravljavca, se mora najpozneje ob koncu zadnjega delovnega dne odvzeti vsa izdana dovoljenja za dostop. Enako velja za vse zunanje ponudnike storitev.

26. člen

Popravljanje, spreminjanje in dopolnjevanje sistemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve direktorice oziroma z njene strani pooblaščene osebe, izvajajo pa ga lahko samo pooblaščeni servis in organizacije oziroma njihovi delavci, ki imajo z družbo sklenjeno ustrezno pogodbo.

Upravljavec mora spremembe in dopolnitve sistemske in aplikativne programske opreme ustrezno dokumentirati.

Zaposleni delavci ne smejo brez izrecnega dovoljenja direktorice inštalirati programske opreme.

27. člen

Za shranjevanje in varovanje aplikativne programske opreme veljajo enaka določila kot za ostale podatke iz tega pravilnika.

Delavec, pooblaščen za obdelavo in ravnanje z osebnimi podatki na računalniku, mora skrbeti, da se v primeru servisiranja, popravila, spreminjanja ali dopolnjevanja sistemske ali aplikativne programske opreme ob morebitnem kopiranju osebnih podatkov, po prenehanju potrebe po kopiji, kopija uniči.

Delavec, pooblaščen za obdelavo in ravnanje z osebnimi podatki na računalniku, mora biti v času servisiranja

računalnika in programske opreme ves čas prisoten in mora nadzirati, da ne pride do nedopustnega ravnanja z osebnimi podatki.

V primeru, če se pokaže potreba po popravilu računalnika, na čigar disku se nahajajo osebni podatki, izven družbe in brez kontrole pooblaščenega delavca družbe, se morajo podatki iz diska računalnika izbrisati na način, ki onemogoča restavracijo. Če tak izbris ni mogoč, se mora popravilo opraviti v poslovnih prostorih družbe v prisotnosti pooblaščenega delavca.

28. člen

Vsebina diskov mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo osebni podatki, se preverja glede na prisotnost računalniških virusov dvakrat letno. Ob pojavu računalniškega virusa je potrebno storiti vse, da se s pomočjo strokovnjakov virus odpravi in da se ugotovi vzrok pojava virusa ter odpravi nevarnost zlorabe osebnih podatkov.

Vsi podatki in programska oprema, ki so namenjeni uporabi na računalnikih družbe in v računalniškem informacijskem sistemu družbe in prispejo na medijih za prenos računalniških podatkov ali prek telekomunikacijskih kanalov, morajo biti pred uporabo preverjeni glede prisotnosti računalniških virusov.

29. člen

Računalniške kopije vsebin zbirk osebnih podatkov na disketah, kompaktnih diskih ali drugih medijih se hranijo v zavarovanih zaklenjenih omarah v varovanih prostorih.

30. člen

Pred nedovoljenimi dostopi in manipulacijami morajo biti zaščitene tudi pisarniške naprave za komunikacijo kot so tiskalniki, faks naprave, kopirni stroji idr.

V. Pravice dostopa posameznika, na katerega se nanašajo osebni podatki

31. člen

Vsak posameznik od upravljavca lahko za svoje podatke v skladu s pogoji iz zakona in Uredbe zahteva sledeče:

- vpogled,
- popravek,
- popoln izbris,
- prenos drugemu ponudniku sorodnih storitev,
- prekinitev obdelave in hranjenja oz. preklic soglasja za obdelavo in hranjenje, ne da bi to vplivalo na zakonitost obdelave, ki se je na podlagi privolitve oz. soglasja izvajala do njegovega preklica
- omejitev obdelave.

Upravljavec v zvezi z zahtevami posameznika iz zgornjega odstavka tega člena postopa skladno z določili veljavne zakonodaje.

Vsako posredovanje osebnih podatkov se beleži v evidenco posredovanih osebnih podatkov, iz katere mora biti razvidno, kateri osebni podatki so bili posredovani, komu, kdaj in na kakšni podlagi (22. člen ZVOP-1).

VI. Zagotavljanje varnosti posredovanja in prenosa osebnih podatkov

32. člen

Delavec, ki je zadolžen za sprejem in evidenco pošte, odpira in pregleduje vse poštne pošiljke in pošiljke, ki na drug način prispejo k upravljavcu, razen pošiljk iz drugega in tretjega odstavka tega člena.

Delavec, ki je zadolžen za sprejem in evidenco pošte, ne odpira tistih pošiljk, ki so naslovljene na drug organ ali organizacijo in so pomotoma dostavljena ter pošiljk, ki so označene kot osebni podatki ali za katere iz označb na ovojnici izhaja, da se nanašajo na natečaj ali razpis.

Delavec, ki je zadolžen za sprejem in evidenco pošte, ne sme odpirati pošiljk, naslovljenih na delavca, na katerih je na ovojnici navedeno, da se vročijo osebno naslovniku, ter pošiljk, na katerih je najprej navedeno osebno ime delavca brez označbe njegovega uradnega položaja in šele nato naslov upravljavca.

33. člen

Osebni podatki se pošiljajo s priporočeno pošto ali osebno preko kurirja.

Ovojnica, v kateri se posredujejo osebni podatki, mora biti izdelana na takšen način, da ovojnica ne omogoča, da bi bila ob normalni svetlobi ali pri osvetlitvi ovojnic z običajno lučjo vidna vsebina ovojnice. Prav tako mora ovojnica zagotoviti, da odprtja ovojnice in seznanitve z njeno vsebino ni mogoče opraviti brez vidne sledi odpiranja ovojnice.

34. člen

Osebne podatke je dovoljeno prenašati z informacijskimi, telekomunikacijskimi in drugimi sredstvi le ob izvajanju ustreznih postopkov in ukrepov, ki nepooblaščenim preprečujejo prilaščanje ali uničenje podatkov ter neupravičeno seznanjanje z njihovo vsebino.

V primeru elektronskega pošiljanja sporočil z osebnimi podatki upravljavec zagotavlja tehnične postopke, ki onemogočijo prestrezanje, kopiranje, spreminjanje, preusmerjanje ali uničenje prenesenih informacij. Ti postopki so npr.: šifriranje priponk (ZIP) in se geslo naslovnikom posreduje ločeno (npr. po telefonu), ali kriptiranje e-sporočila in priponk, s posredovanim geslom.

VII. Redno testiranje, ocenjevanje in vrednotenje ukrepov

35. člen

Upravljavec se zaveže, da bo redno testiral, ocenjeval in vrednotil učinkovitost tehničnih in organizacijskih ukrepov za zagotavljanje varnosti obdelave.

Upravljavec bo v ta namen vsaj enkrat letno preveril zakonitost obdelave osebnih podatkov. Za namen oprave notranje kontrole bo upravljavec pregledal dnevnike v zvezi z delovanji obdelav osebnih podatkov (t.i. dnevniške datoteke oz. loge) in se posvetoval z ustreznimi strokovnjaki za informacijsko varnost.

IX. Storitve, ki jih opravljajo zunanje pravne ali fizične osebe (obdelovalci osebnih podatkov)

36. člen

Upravljavec lahko posamezna dejanja obdelave podatkov zaupa tudi zunanji pravni ali fizični osebi, ki opravlja posamezna opravila v zvezi z obdelovanjem osebnih podatkov in je registrirana za opravljanje takšne dejavnosti (v nadaljevanju: »**obdelovalec**«), ki zagotavlja zadostna jamstva za izvedbo ustreznih tehničnih in organizacijskih ukrepov za zagotavljanje skladnosti prevzetih opravil obdelave s Splošno uredbo o varstvu podatkov, zakonom, ki ureja področje varstva osebnih podatkov in tem Pravilnikom. Obdelovalec, ki opravlja dogovorjene storitve izven prostorov upravljavca, mora imeti vsaj enako strog način varovanja osebnih podatkov, kakor ga predvideva ta Pravilnik.

V kolikor pogodbena obdelava pri zunanji osebi ni določena na podlagi izrecnega zakonskega pooblastila, mora upravljavec z obdelovalcem skleniti pogodbo ali drug ustrezni pisni dogovori o pogodbeni obdelavi osebnih podatkov, v katerih bo določil pravice in obveznosti obeh strank. V takšnem dogovoru morajo biti obvezno predpisani pogoji in ukrepi za zagotovitev varstva osebnih podatkov in njihovega zavarovanja ter obveznosti obdelovalca napram upravljavcu. Zunanje osebe smejo opravljati storitve obdelave osebnih podatkov samo v okviru namena, določenega v pogodbi oziroma v okviru naročnikovih pooblastil in osebnih podatkov ne smejo obdelovati ali drugače uporabljati za noben drug namen.

Omenjeno velja tudi za obdelovalce, ki vzdržujejo strojno in programsko opremo ter izdelujejo in instalirajo novo strojno ali programsko opremo.

X. Rok hrambe in brisanje podatkov

37. člen

Osebni podatki se lahko vodijo v zbirki osebnih podatkov skladu z zakonskimi, pogodbenimi in poslovnimi zahtevami. V kolikor rok hrambe ni zakonsko določen, se osebni podatki hranijo le toliko časa, kolikor je potrebno, da se doseže namen, za katerega se zbirajo in vodijo.

Po preteku roka hranjenja, se podatki zbrišejo oziroma nosilci podatkov uničijo, blokirajo ali anonimizirajo, razen če zakon ali drug akt ne določa drugače.

Arhivski podatki se morajo skladiščiti ali shranjevati na krajih, ki izpolnjujejo zahteve razpoložljivosti, integritete in zaupnosti.

38. člen

Brisanje osebnih podatkov na računalniških medijih se opravi na način, po postopku in metodi, ki onemogoča restavriranje brisanih podatkov. Brisanje mora biti popolno in nepovratno. Poleg nosilca takih podatkov je torej potrebno uničiti tudi podatke v mapi »Izbrisano« ali »Koš« oziroma drugi ustrezni mapi / direktoriju, tako da vsebine ni več moč obnoviti.

Osebni podatki, vsebovani na klasičnih nosilcih (listine, kartoteke, register, seznam) se brišejo z uničenjem nosilcev. Nosilci se fizično uničijo (pokurijo, razrežejo) v prostorih družbe ali pod nadzorom zakonitega zastopnika upravljavca ali s predajo dokumentacije v uničenje organizaciji, ki se ukvarja z uničevanjem zaupne dokumentacije in ima z upravljavcem sklenjeno ustrezno pogodbo o izvajanju storitev, s podanim jamstvom upravljavca storitve, da bo ravnal skladno s pravili o varstvu osebnih podatkov. Na enak način se uničuje pomožno gradivo (npr. matrice, izračune in grafikone, skice, poskusne oziroma neuspešne izpise ipd.).

39. člen

Z vso vestnostjo in skrbnostjo, določeno s tem pravilnikom, se mora brisati in uničevati tudi pomožna dokumentacija ali računalniški produkti oziroma predloge, ki vsebujejo posamezne osebne podatke.

Uničevanje osebnih podatkov na nosilcih iz predhodnega odstavka se mora izvajati tekoče in ažurno.

XI. Ukrepanje ob ugotovitvi zlorabe osebnih podatkov ali vdoru v zbirke osebnih podatkov

40. člen

Upravljavec zagotavlja dosleden in učinkovit sistem za ravnanje z varnostnimi incidenti, vključno z dokumentiranjem in obveščanjem o varnostnih dogodkih.

V ta namen upravljavec zagotovi informacijski sistem, ki je sposoben izvajati nadzor za prepoznavanje dogodkov (npr. požarni zid, zaznavanje vdorov, sistem nadzora). Informacijski sistemi nadalje omogočajo dokumentiranje vseh varnostno relevantnih ali sistemsko kritičnih dogodkov. Za spremljanje teh beleženj je odgovoren administrator upravljavca (podjetje Business Solutions d.o.o.)

Vsi zaposleni so dolžni izvajati ukrepe za preprečevanje zlorabe osebnih podatkov.
Vsak zaposleni, ki izve ali opazi, da je prišlo do zlorabe osebnih podatkov (odkrivanje osebnih podatkov, nepooblaščeno uničenje, nepooblaščeno spreminjanje, poškodovanje zbirke, prilaščanje osebnih podatkov) ali do vdora v zbirko osebnih podatkov, mora takoj o tem obvestiti direktorico ter pooblaščenega delavca, ki vodi in ureja zbirko osebnih podatkov, ki so bili zlorabljeni ali v katero se je vdrlo, sam pa mora poskušati takšno aktivnost preprečiti.

41. člen

Direktorica mora zoper tistega, ki je zlorabil osebne podatke ali je nepooblaščeno vdrl v zbirko osebnih podatkov, ustrezno ukrepati.

Če obstaja sum pri vdoru v zbirko osebnih podatkov, da je ta storjen z naklepom in namenom zlorabiti osebne podatke ali jih uporabiti v nasprotju z nameni, za katere so zbrani, ali če je do zlorabe osebnih podatkov že prišlo, mora direktorica poleg uvedbe disciplinskega postopka zoper storilca ali poleg izreka opomina pred redno odpovedjo pogodbe o zaposlitvi ali poleg redne odpovedi pogodbe o zaposlitvi iz krivdnih razlogov ali poleg izredne odpovedi pogodbe o zaposlitvi, če je zlorabil ali poskusil zlorabiti osebne podatke delavec družbe, vdor ali zlorabo oziroma poskus zlorabe, prijaviti organom pregona.

Za zlorabo osebnih podatkov šteje vsaka uporaba osebnih podatkov v namene, ki niso v skladu z nameni zbiranja, določenimi v zakonu, na podlagi katerega se zbirajo ali nameni določenimi v katalogu zbirk osebnih podatkov. Za poskus zlorabe šteje poskus uporabe osebnih podatkov v nedovoljene namene.

42. člen

Upravljavec v evidenco varnostnih incidentov beleži vsako kršitev varstva osebnih podatkov, iz katere morajo biti razvidna dejstva v zvezi s kršitvijo varstva osebnih podatkov, učinki take kršitve in sprejeti popravni ukrepi.

V evidenco varnostnih incidentov se po kronološkem vrstnem redu vpisujejo vsi varnostni incidenti, ne glede na stopnjo in vrsto tveganja za pravice in svoboščine posameznikov. Upravljavec zlasti beleži kršitve zaupnosti podatkov (npr. nepooblaščeno razkritje podatkov), kršitve v zvezi z možnostjo dostopa do podatkov in kršitve integritete podatkov (npr. nepooblaščena sprememba podatkov).

43. člen

V primeru kršitve varstva osebnih podatkov mora upravljavec brez neposrednega odlašanja, najkasneje pa v roku 72 ur po seznanitvi s kršitvijo, o njej uradno obvestiti pristojni nadzorni organ (Informacijskega pooblaščenca), skladno s 33. in 55. členom Splošne uredbe o varstvu podatkov, razen če ni verjetno, da bi bile s kršitvijo varstva osebnih podatkov ogrožene pravice in svoboščine posameznikov.

Kadar je verjetno, da kršitev varstva osebnih podatkov povzroči veliko tveganje za pravice in svoboščine posameznikom, mora upravljavec skladno z določbo 34. člena Splošne uredbe o varstvu podatkov brez nepotrebnega odlašanja obvestiti tudi posameznike, na katere se nanašajo osebni podatki, da je prišlo do kršitve varstva osebnih podatkov.

XII. Odgovornost za izvajanje ukrepov zavarovanja osebnih podatkov

44. člen

Upravljavec je dolžan zagotoviti, da se pred nastopom dela zaposlenega na delovnem mestu, kjer se zbirajo, urejajo, obdelujejo, spreminjajo, shranjujejo, posredujejo ali uporabljajo osebni podatki ali nosilci osebnih podatkov, zaposleni seznani s pravili o varovanju osebnih podatkov in v ta namen podpiše tudi ustrezno izjavo, ki ga opozarja na posledice kršitve pravil o varovanju osebnih podatkov (Priloga št. 1). Iz podpisane izjave mora biti razvidno, da je podpisnik seznanjen z določbami tega Pravilnika ter določbami zakona, ki ureja področje varstva osebnih podatkov ter vsebine Splošne uredbe, izjava pa mora vsebovati tudi pouk o posledicah kršitve.

Izjavo morajo podpisati tudi zaposleni, ki prihajajo posredno v stik z obdelavo osebnih podatkov pri upravljavcu, to so študentje, pripravniki, dijaki na praksi in drugi delavci, ki se izobražujejo pri upravljavcu (Priloga št. 2).

Obveza varovanja osebnih podatkov, s katerimi se delavec seznani pri svojem delu v družbi, traja tudi po prenehanju delovnega razmerja v družbi ter po prenehanju funkcije v organih družbe.

Za kršitev določil iz prejšnjega odstavka so zaposleni disciplinsko odgovorni, zunanje osebe pa na podlagi pogodbenih obveznosti.

45. člen

Ravnanje zaposlenega v nasprotju z določili tega Pravilnika pomeni kršitev delovnih obveznosti,

Kot lažja kršitev delovnih obveznosti se šteje kršitev zaposlenega:

1. če opusti vestno in skrbno nadzorovanje varovanih prostorov,

2. če opusti ravnanja za preprečitev vpogleda v ali na nosilce osebnih podatkov,

3. če ne uniči kopije osebnih podatkov v za to določenih primerih,

4. če ni ves čas servisiranja računalnika in programske opreme prisoten,

5. če ne izvaja preventive v zvezi z računalniškimi virusi,

6. če ne vodi evidence kopij vsebin zbirk osebnih podatkov v seznamu evidenc v zvezi z varstvom osebnih podatkov,

7. če ne obvesti direktorice ali pooblaščenega delavca v primeru zlorabe osebnih podatkov ali vdora v zbirko osebnih podatkov.

46. člen

Kot hujša kršitev delovnih obveznosti se šteje kršitev zaposlenega:

- če razkriva osebne podatke, s katerimi se je seznanil pri svojem delu, nepooblaščenim osebam,

- če opusti skrb in nadzor nad nosilci osebnih podatkov med delovnim časom in tako dopusti možnost vpogleda vanje nepooblaščenim osebam,

- če brez izrecnega dovoljenja odnaša iz prostorov upravljavca nosilce osebnih podatkov,

- če posreduje osebne podatke pooblaščenim zunanjim institucijam brez dovoljenja zakonitega zastopnika upravljavca,

- če ne vpiše v knjigo evidenc o ravnanju z osebnimi podatki dejstva o posredovanju osebnih podatkov zunanjim institucijam,

- če popravlja, spreminja ali dopolnjuje sistemsko ali aplikativno programsko opremo,

- če inštalira ali odnese programsko opremo iz prostorov upravljavca brez izrecnega dovoljenja zakonitega zastopnika upravljavca,

- če ne izdeluje redno kopije vsebine osebnih podatkov,

- če ne hrani računalniških kopij vsebin zbirk osebnih podatkov v zavarovanih zaklenjenih omarah.

47. člen

V primeru zlorabe ali suma zlorabe osebnih podatkov, vodenih v zbirkah osebnih podatkov družbe, upravljavec o tem obvesti organe, pooblaščene za pregon.

XIII. Posebne ureditve za zbirke osebnih podatkov vodenih v družbi

48. člen

Za vzpostavitev, vodenje, ažuriranje in ravnanje z zbirkami osebnih podatkov, vodenih v družbi, so odgovorni direktorica in s strani direktorice pisno pooblaščene osebe.

49. člen - Zbirke osebnih podatkov, za katere je potrebno soglasje

Za vzpostavitev in vodenje zbirk osebnih podatkov, ki se nanašajo na stranke in za katere ni pravne podlage v zakonih, mora družba pridobiti pisno soglasje strank. To stori tako, da pogodbe, ki jih ponudi strankam v podpis vsebujejo tudi izjavo stranke, da s podpisom pogodbe dovoli tudi uporabo osebnih podatkov, ki so na pogodbi, izključno za namene sklenitve in izvajanja te pogodbe.

Pisno soglasje zaposlenih oziroma oseb, na katere se nanašajo osebni podatki, mora družba pridobiti tudi za vzpostavitev in vodenje zbirke osebnih podatkov ali osebnega podatka, ki jo ali ga namerava družba voditi, pa taka zbirka ali osebni podatek ni predpisana oziroma predpisan z zakonom.

Pisno soglasje mora vsebovati:
- jasno opredeljeno voljo za izdajo soglasja,
- navedbo podatkov, ki se zbirajo,
- natančno opredeljen namen zbiranja podatkov,
- zagotovilo, da se bodo podatki uporabljali le za namen za katerega so zbrani,
- čas shranjevanja podatkov,
- seznanitev z možnostjo preklica soglasja,
- datum podpisa izjave in podpis osebe.

XIV. Vodenje in ažuriranje zbirk osebnih podatkov

50. člen

Zbirke osebnih podatkov strank se ažurirajo (brisanje, dopolnjevanje) najmanj ob začetku vsakega koledarskega leta.
V zbirki osebnih podatkov strank podatke vzpostavijo in ažurirajo pooblaščeni delavci za obdelavo osebnih podatkov.

XVI. Prehodni in končni določbi

51. člen

Vse spremembe in dopolnitve tega Pravilnika se sprejmejo na enak način kot Pravilnik in v pisni obliki.

52. člen

Z določbami tega pravilnika morajo biti seznanjeni vsi delavci družbe.

53. člen

Pravilnik se objavi na pri upravljavcu običajen način, in sicer se objavi na oglasni deski, tako da se z njegovo vsebino lahko seznanijo vsi delavci pri upravljavcu.

Ta pravilnik začne veljati in se uporablja naslednji dan po dnevu objave na oglasni deski.

Z dnem, ko prične veljati ta pravilnik, preneha veljati Pravilnik o varovanju osebnih podatkov z dne 1.10.2006.

V Novi Gorici, dne 1.6.2019

INOX CENTER d.o.o.
Direktorica: Orijana Zimic

INOX CENTER d.o.o. 5000 NOVA GORICA