Na podlagi določb 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), 24. in 25. člena Zakona o varstvu osebnih podatkov (Uradni list RS, Uradni list RS, št. 94/07 – uradno prečiščeno besedilo; ZVOP-1) izdaja direktor družbe Strenia IND d.o.o., Matej Kordelič

PRAVILNIK
o obdelavi osebnih in zaupnih podatkov vključno z zagotavljanjem varnosti osebnih podatkov in politiko varstva osebnih podatkov zaposlenih

I. SPLOŠNE DOLOČBE

1. člen

S tem pravilnikom se določajo zaupni podatki v družbi (poslovne skrivnosti in osebni podatki), notranja politika varstva osebnih podatkov zaposlenih in v povezavi s tem pričakovana zasebnost in varstvo osebnih podatkov na delovnem mestu in organizacijski, tehnični in logično-tehnični postopki in ukrepi za zavarovanje in varovanje zaupnih in osebnih podatkov v družbi Strenia d.o.o. (v nadaljevanju: družba), z namenom, da se prepreči slučajno ali namerno nepooblaščeno uničevanje podatkov, njihova sprememba ali izguba, kakor tudi nepooblaščen dostop, obdelava, uporaba, spreminjanje in posredovanje osebnih in drugih zaupnih podatkov.

Zaposleni in zunanji sodelavci družbe (v nadaljevanju: delavci), ki pri svojem delu obdelujejo in uporabljajo osebne in zaupne podatke, morajo biti seznanjeni in spoštovati Uredbo (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, nacionalni zakon o varstvu osebnih podatkov, podzakonske akte in področno zakonodajo, ki ureja posamezno področje njihovega dela ter ta pravilnik.

Ta pravilnik velja za vse zaposlene v družbi, kakor tudi za pogodbene sodelavce, tudi v kolikor pri posameznih členih niso navedene vse oblike dela oziroma sodelovanja z družbo. Kadar je v pravilniku uporabljen izraz "zaposleni" se določilo razteza tudi na pogodbene sodelavce, enako, kadar je uporabljen izraz »delavec«, razen, kadar bi drugačna obravnava izhajala iz narave pogodbenega razmerja ali kadar bi imela družba z njimi drugačen dogovor.

V tem pravilniku uporabljeni nazivi delovnih mest oziroma delavcev so zapisani v moški slovnični obliki in so v skladu z namenom uporabljeni kot nevtralni za ženske in moške.

2. člen

V tem pravilniku uporabljeni izrazi imajo naslednji pomen:

1. *Zaupni podatki* po tem pravilniku so podatki, ki predstavljajo poslovno skrivnost in osebni podatki.
2. *Osebni podatek* je katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen.
3. *Posameznik* je določena ali določljiva fizična oseba, na katero se nanaša osebni podatek. Fizična oseba je določljiva, če se jo lahko neposredno ali posredno identificira, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, ki so značilni za njeno fizično, fiziološko,

duševno, ekonomsko, kulturno, ali družbeno identiteto, pri čemer način identifikacije ne povzroča velikih stroškov, nesorazmerno velikega napora ali ne zahteva veliko časa.
4. *Zbirka osebnih podatkov* je vsak strukturiran niz podatkov, ki vsebuje vsaj en osebni podatek, ki je dostopen na podlagi meril, ki omogočajo uporabo ali združevanje podatkov, ne glede na to, ali je niz centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi, strukturiran niz podatkov je niz podatkov, ki je organiziran na takšen način, da določi ali omogoči določljivost posameznika.
5. *Strukturiran niz podatkov* je vsak niz podatkov, ki je organiziran na tak način, da določi ali omogoči določljivost posameznika.
6. *Obdelava osebnih podatkov* pomeni kakršnokoli delovanje ali niz delovanj, ki se izvaja v zvezi z osebnimi podatki, ki so avtomatizirano obdelani ali ki so pri ročni obdelavi del zbirke osebnih podatkov ali so namenjeni vključitvi v zbirko osebnih podatkov, zlasti zbiranje, pridobivanje, vpis, urejanje, shranjevanje, prilagajanje ali spreminjanje, priklicanje, vpogled, uporaba, razkritje s prenosom, sporočanje, širjenje ali drugo dajanje na razpolago, razvrstitev ali povezovanje, blokiranje, anonimiziranje, izbris ali uničenje; obdelava je lahko ročna ali avtomatizirana (sredstva obdelave).
7. *Upravljavec osebnih podatkov* je fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki sama ali skupaj z drugimi določa namene in sredstva obdelave osebnih podatkov oziroma oseba, določena z zakonom, ki določa tudi namene in sredstva obdelave.
7. *Uporabnik osebnih podatkov* je fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki se ji posredujejo ali razkrijejo osebni podatki.
8. *Posebne vrste osebnih podatkov* so osebni podatki, ki razkrivajo rasno ali etnično poreklo, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu, in obdelava genetskih podatkov, biometričnih podatkov za namene edinstvene identifikacije posameznika, podatkov v zvezi z zdravjem ali podatkov v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo.
9. *Nosilec podatkov* je oprema, preko katere je mogoč dostop do zbirk osebnih podatkov, vse vrste sredstev, na katerih so zapisani ali posneti podatki (listine, gradiva, spisi, računalniška oprema vključno z magnetnimi, optičnimi ali drugimi računalniškimi mediji, fotokopije, zvočno in slikovno gradivo, mikrofilmi, naprave za prenos podatkov ipd.).
10. *Obdelovalec* je fizična ali pravna oseba, ki obdeluje osebne podatke v imenu in na račun upravljavca osebnih podatkov s področja obdelovanja osebnih podatkov.
11. *Pogodbeni podobdelovalec* je pravna ali fizična oseba, ki ji pogodbeni obdelovalec ob soglasju upravljavca poveri določene od zaupanih nalog.
12. *Poslovna skrivnost* so podatki, za katere tako določi družba s pisnim sklepom in podatki, za katere je očitno, da bi družbi nastala občutna škoda, če bi zanje izvedela nepooblaščena oseba.

3. člen

Opis zbirk osebnih podatkov, katerih upravljavec je družba, se vodi v evidenci dejavnosti obdelav v skladu z določbami 30. člena Splošne uredbe.

V evidenco dejavnosti obdelave se vpisujejo naslednji podatki: naziv zbirke osebnih podatkov, vrste osebnih podatkov v zbirki, vir osebnih podatkov, pravni temelj za obdelavo osebnih podatkov, osebno ime in delovno mesto osebe, ki je odgovorna za določeno zbirko osebnih podatkov ter nazivi delovnih mest oseb, ki lahko zaradi narave njihovega dela obdelujejo osebne podatke, rok hrambe, drugi uporabnike osebnih podatkov (morebitne pogodbene obdelovalce, zunanje sodelavce), ukrepi za zavarovanje osebnih podatkov.

II. ZAUPNI PODATKI

4. člen

Za zaupne podatke v družbi štejejo poslovne skrivnosti in osebni podatki.

Kot poslovna skrivnost štejejo podatki, za katere tako določi družba s pisnim sklepom oziroma drugim aktom. Ne glede na to se za poslovno skrivnost štejejo tudi podatki, za katere je očitno, da bi nastala občutna škoda, če bi zanje izvedela nepooblaščena oseba. Za poslovno skrivnost štejejo tudi sledeči podatki:

- vsak podatek, ki ga stranka zavestno posreduje drugi stranki v zvezi z opravljanjem storitev, ki so opredeljene s Pogodbo o zaposlitvi,
- vsak podatek, ki ga ena stranka pridobi od druge stranke v pogovorih, povezanih z deli in nalogami ali ki ga stranka pridobi v povezavi s posameznimi podatki, pridobljenimi v takšnih pogovorih,
- vsak podatek, ki ga ena stranka pridobi od druge za potrebe opravljanja del in nalog ali ki ga posamezna stranka posreduje drugi stranki zaradi opravljanja delovnih nalog zaradi sodelovanja z naročniki;
- vsak poslovni podatek delodajalca, izvajalcev, njegovih naročnikov in naročnikovih pogodbenih strank, ki je opredeljen kot poslovna skrivnost ali bi lahko bil opredeljen kot poslovna skrivnost v skladu z ustreznimi določbami Zakona o gospodarskih družbah in ki ga stranka pridobi neposredno od druge stranke ali pa tretje osebe.

Za poslovno skrivnost se ne morejo določiti podatki, ki so po zakonu javni ali podatki o kršitvi zakona ali dobrih poslovnih običajev.

V primeru dvoma je delavec dolžan pred razkritjem od delodajalca pridobiti informacijo, ali se posamezen podatek šteje za poslovno skrivnost.

Za varovanje poslovne skrivnosti se poleg določb tega pravilnika uporabljajo tudi določbe Zakona o gospodarskih družbah (Url RS št. 65/2009 – UPB, 33/2011, 91/2011, 32/2012, 57/2012, 44/2013, 82/2013, 55/2015 in 15/2017; v nadaljevanju: ZGD-1).

Dolžnost varovanja poslovne skrivnosti velja za vse zaposlene v družbi in druge osebe, ki za družbo na podlagi pogodbe opravljajo posamezne storitve, in sicer tudi še 2 leti po prenehanju funkcije oziroma delovnega ali pogodbenega razmerja.

5. člen

Podatkov, ki v skladu s prejšnjim členom tega pravilnika štejejo za poslovno skrivnost in osebnih podatkov ni dovoljeno razkrivati oz. omogočiti dostopa do njih ali jih posredovati nepooblaščenim tretjim osebam, razen če delavec za to predhodno pridobi pisno soglasje direktorja družbe.

6. člen

Zaposleni oziroma pogodbeni sodelavci so dolžni o aktivnostih, ki so povezane z odkrivanjem ali nepooblaščenim uničenjem oziroma kakršnokoli zlorabo zaupnih podatkov, zlonamerni ali nepooblaščeni uporabi, prilaščanju, spreminjanju ali poškodovanju, takoj obvestiti direktorja, sami pa poskušajo takšno aktivnost preprečiti.

7. člen

Za izvajanje postopkov in ukrepov za varovanje zaupnih podatkov je odgovoren direktor oziroma oseba, ki jo v ta namen pooblasti direktor družbe.

Nadzor nad izvajanjem postopkov in ukrepov, določenih s tem pravilnikom, opravlja direktor družbe oziroma z njegove strani pooblaščena oseba.

8. člen

Vsak, ki obdeluje zaupne podatke, je dolžan izvajati v skladu s tem pravilnikom predpisane postopke in ukrepe za zavarovanje podatkov in varovati podatke, za katere je izvedel oziroma bil z njimi seznanjen pri opravljanju svojega dela.

9. člen

Kršitev dolžnosti varovanja zaupnih podatkov v skladu z določili tega pravilnika šteje za hujšo kršitev obveznosti iz delovnega razmerja, zaradi katere lahko delodajalec delavcu redno iz krivdnega razloga ali v primeru kršitve, ki ima vse znake kaznivega dejanja, tudi izredno odpove pogodbo o zaposlitvi, poleg tega pa je delavec dolžan delodajalcu povrniti tudi vso škodo, ki bi mu nastala zaradi delavčeve kršitve varovanja zaupnih podatkov (poslovne skrivnosti ali osebnih podatkov). Če višine odškodnine ne bo mogoče ugotoviti oziroma bi z ugotavljanjem nastali nesorazmerno visoki stroški, je delavec dolžan delodajalcu plačati pavšalno odškodnino v višini 3-kratnika njegove osnovne bruto plače, kot je določena v delavčevi pogodbi o zaposlitvi, kolikor se delodajalec z delavcem ne dogovori drugače.

Za kršitev določil o varovanju zaupnih podatkov oziroma poslovne skrivnosti so delavci, ki so zaposleni v družbi, lahko tudi disciplinsko odgovorni.

Pristojnost odločitve, katera sankcija se uporabi za kršitev varovanja zaupnih podatkov, je na strani delodajalca oziroma direktorja družbe in se presoja glede na težo storjene kršitve oziroma posledice storjene kršitve ter ob upoštevanju eventualnih olajševalnih okoliščin posamezne kršitve.

Dolžnost varovanja poslovnih skrivnosti družbe velja za vse zaposlene tudi še 2 leti po prenehanju delovnega razmerja iz kakršnegakoli razloga. Delavec je osebne podatke dolžan varovati tudi po prenehanju delovnega razmerja – neomejeno. Za zlorabo zaupnih podatkov ali nepooblaščeno oziroma nezakonito posredovanje le teh tretjim osebam je delavec odškodninsko in kazensko odgovoren.

III. VAROVANJE PROSTOROV IN RAČUNALNIŠKE OPREME

10. člen

Zagotavljanje varnosti osebnih podatkov obsega organizacijske, tehnične in logično-tehnične postopke in ukrepe, s katerimi se varujejo osebni podatki v skladu z Splošno uredbo, ZVOP-1 in nacionalnim predpisom, sprejetim za izvedbo Splošne uredbe, 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.

11. člen

Prostori, v katerih se nahajajo nosilci zaupnih podatkov, strojna in programska oprema (varovani prostor), sodijo v kategorijo varovanih prostorov in morajo biti zavarovani z ustreznimi organizacijskimi ter fizičnimi in/ali tehničnimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov. Pri družbi so to prostori direktorja, prostori tajništva in serverska soba. Ti prostori so varovani s fizičnimi in tehničnimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov in za katere velja naslednji režim:

1. Pisarne so izven delovnega časa zaklenjene in varovane z alarmom.
2. Serverska soba je zaklenjena ves čas, razen v času vzdrževalnih del s strani pooblaščene osebe, izven delovnega časa varovana z alarmom.

3. Fizične zbirke osebnih podatkov so v zaklenjenih omarah, ki morajo biti izven delovnega časa obvezno zaklenjene.
4. Elektronske zbirke osebnih podatkov so zaščitene z uporabniškimi imeni in gesli. Računalniki morajo biti izven delovnega časa obvezno izključeni.
5. Dostop v varovane prostore je mogoč le v rednem delovnem času, izven tega časa pa samo za pooblaščene osebe.
6. Dostop osebam, ki niso zaposlene v varovanih prostorih, je dovoljen le ob prisotnosti zaposlenih v teh prostorih.
7. Delavci nosilcev zaupnih podatkov ne smejo izpostavljati nevarnosti nenadzorovanega vpogleda ali iznosa.
8. Delavci ne smejo puščati nosilcev zaupnih podatkov na mizah, kadar na delovnem mestu niso prisotni, ali jih drugače izpostavljati vpogledu vanje nepooblaščenim osebam.
9. V prostorih, v katere imajo vstop stranke oz. osebe, ki v družbi niso zaposlene oziroma v družbi ne delajo, morajo biti nosilci podatkov in računalniški prikazovalniki nameščeni v času obdelave ali dela na njih tako, da je strankam oz. osebam, ki v družbi niso zaposlene oziroma v družbi ne delajo, onemogočen vpogled vanje.

Posebne vrste osebni podatki se ne smejo hraniti izven varovanih prostorov.

12. člen

Obdelovanje osebnih podatkov iz zbirk osebnih podatkov je dovoljeno le v prostorih družbe oziroma s potrebno skrbnostjo, ki se od delavca zahteva za zavarovanje in varstvo osebnih podatkov na delovnem mestu, tudi ob opravljanju dela na domu oziroma neposredno pri stranki, pri čemer mora delavec zagotoviti vse ustrezne ukrepe, ki preprečujejo in onemogočajo nepooblaščenim osebam dostop do teh podatkov.

Nosilcev podatkov z oznako " poslovna skrivnost " zaposleni oz. delavci ne smejo odnašati izven prostorov družbe, ostale nosilce podatkov, ki vsebujejo osebne podatke, pa samo s predhodno odobritvijo oziroma z dovoljenjem direktorja oziroma ob opravljanju dela na domu oziroma neposredno pri stranki.

13. člen

Posredovanje osebnih podatkov pooblaščenim zunanjim institucijam in drugim, ki izkažejo pravno podlago za pridobitev osebnih podatkov (enega od pravnih temeljev iz 6/I člena Splošne uredbe), je večinoma definirano v Evidenci dejavnosti obdelave podatkov, v preostalih primerih pa dovoli direktor družbe ali od njega pooblaščena oseba.

14. člen

Vzdrževanje in popravila strojne računalniške in druge opreme so dovoljena samo z vednostjo in odobritvijo direktorja ali z njegove strani pooblaščene osebe, izvajajo pa ga lahko samo za to pooblaščeni servisi in vzdrževalci, ki imajo z družbo sklenjeno ustrezno pogodbo o servisiranju in vzdrževanju računalniške oz. strojne opreme - pogodbeni obdelovalci, če pride pri njihovem delu tudi do obdelave osebnih podatkov.

15. člen

Vzdrževalci prostorov, strojne in programske opreme, obiskovalci, poslovni partnerji in druge osebe se smejo gibati v varovanih prostorih samo z vednostjo in ob prisotnosti direktorja oziroma pooblaščene osebe.

Zaposleni in poslovni partnerji, kot so čistilke, varnostniki in tehnično-vzdrževalni delavci, se lahko izven delovnega časa gibljejo samo v tistih varovanih prostorih, kjer je onemogočen vpogled v zaupne podatke (nosilci podatkov so shranjeni v sefu, na mizah ni nobene dokumentacije, ki bi vsebovala zaupne ali osebne podatke, računalniki in druga strojna oprema so izklopljeni ali kako drugače fizično ali programsko zaklenjeni) oz. le z dovoljenjem direktorja ali od njega pooblaščene osebe.

IV. VAROVANJE SISTEMSKE IN APLIKATIVNE PROGRAMSKE IN RAČUNALNIŠKE OPREME TER PODATKOV, KI SE OBDELUJEJO Z RAČUNALNIŠKO OPREMO

16. člen

Dostop do programske opreme mora biti varovan tako, da omogoča dostop samo za to vnaprej določenim zaposlenim ali pravnim ali fizičnim osebam, ki v skladu s pogodbo opravljajo dogovorjene storitve, pri katerih je potrebna obdelava osebnih podatkov.

17. člen

Popravljanje, spreminjanje in dopolnjevanje sistemske ali aplikativne programske opreme je dovoljeno samo na podlagi odobritve direktorja oz. pooblaščene osebe, izvajajo pa ga lahko samo za to pooblaščeni servisi in organizacije in posamezniki, ki imajo z družbo sklenjeno ustrezno pogodbo.

18. člen

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

Delavci, pooblaščeni za obdelavo in ravnanje z osebnimi podatki na računalniku, morajo skrbeti, da se v primeru servisiranja, popravila, spreminjanja ali dopolnjevanja sistemske oziroma aplikativne programske opreme ob morebitnem kopiranju osebnih podatkov, po prenehanju potrebe po kopiji, kopija uniči, enako tudi drugi, za lažje delo pripravljeni delovni pripomočki (kot so excel tabele z uvoženimi osebni podatki iz zbirke ipd).

19. člen

Vsebina diskov mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo pomembni podatki, se vsakodnevno preveri glede na prisotnost računalniških virusov. Ob pojavu računalniškega virusa se tega nemudoma (čimprej) odpravi s pomočjo ustrezne strokovne službe v družbi oziroma zunanjega sodelavca, obenem pa se ugotovi vzrok pojava virusa v računalniškem informacijskem sistemu.

20. člen

Nihče ne sme instalirati programske opreme brez vednosti direktorja oz. osebe, zadolžene za delovanje računalniškega informacijskega sistema. Prav tako nihče ne sme odnašati programske opreme iz prostorov družbe brez odobritve direktorja oziroma z njegove strani pooblaščene osebe.

21. člen

Dostop do osebnih podatkov preko aplikativne programske opreme se varuje s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov in podatkov, sistem gesel pa mora omogočati tudi možnost naknadnega ugotavljanja, kdaj so bili posamezni osebni podatki vnešeni v zbirko podatkov, uporabljeni ali kako drugače obdelovani in s strani koga.

Direktor oziroma z njegove strani pooblaščena oseba določi režim dodeljevanja, hranjenja in spreminjanja gesel.

22. člen

Za potrebe restavriranja računalniškega sistema ob okvarah in ob drugih izjemnih situacijah se zagotavlja redna izdelava kopij vsebine mrežnega strežnika in lokalnih postaj, kjer se nahajajo vsebine zbirk osebnih podatkov.

Takšne kopije vsebine oziroma delov zbirk ali zbirk osebnih podatkov se hranijo na ustreznih medijih, ti pa na za to določenih mestih, v okviru predpisanih klimatskih pogojev ter zaklenjena.

V. STORITVE, KI JIH OPRAVLJAJO ZUNANJE PRAVNE ALI FIZIČNE OSEBE

23. člen

Z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezna opravila v zvezi z obdelovanjem osebnih podatkov - zbiranjem, shranjevanjem, posredovanjem ali drugačno obdelavo osebnih podatkov za družbo in je registrirana za opravljanje takšne dejavnosti (obdelovalec), se sklene pisna pogodba, predvidena v 28. členu Splošne uredbe. V takšni pogodbi morajo biti predpisani tudi pogoji in ukrepi za zagotovitev varnosti osebnih podatkov, zagotavljanje njihove celovitosti in avtentičnosti ves čas obdelave. Obdelovalci so tudi zunanji sodelavci, ki vzdržujejo strojno in programsko opremo ter izdelujejo in instalirajo novo strojno ali programsko opremo, kolikor imajo pri svojem delu dostop do osebnih podatkov.

Zunanje pravne ali fizične osebe smejo opravljati storitve obdelave osebnih podatkov samo v okviru pooblastil družbe in osebnih podatkov ne smejo obdelovati za noben drug namen.

Pooblaščena pravna ali fizična oseba, ki za družbo opravlja dogovorjene storitve izven prostorov upravljavca, mora imeti vsaj enako strog način zagotavljanja varnosti osebnih podatkov, kakor ga predvideva ta pravilnik.

24. člen

Obdelovalec sme določene aktivnosti v zvezi z osebnimi podatki, ki mu jih je zaupala družba prepustiti v pod-obdelavo enemu ali večim izvajalcem le ob predhodnem pisnem soglasju družbe.

Če družba ocenjuje, da nameravani pod-obdelovalec ne uživa njenega zaupanja, soglasje odkloni.

VI. POLITIKA VARSTVA OSEBNIH PODATKOV ZAPOSLENIH

25. člen

Delavec, ki je zadolžen za sprejem in evidence pošte v družbi, odpira in pregleduje vse poštne pošiljke in pošiljke, ki na drug način prispejo v družbo – prinesejo jih stranke ali kurirji, razen pošiljk iz 2. in 3. odstavka tega člena.

Delavec, ki je zadolžen za sprejem in evidence pošte, ne odpira tistih pisemskih pošiljk, ki so naslovljene na drug organ ali organizacijo in so pomotoma dostavljena v družbo.

Delavec, ki je zadolžen za sprejem in evidence 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 družbe.

26. člen

Elektronska pošta, računalnik (prenosni in stacionarni), tablice, mobilni telefon in druge elektronske naprave, ki jih delavcu za potrebe opravljanja dela dodeli delodajalec, se s strani zaposlenih uporabljajo v službene namene. V omejenem obsegu in razumnih mejah se lahko elektronska pošta in računalnik ter telefon uporabljata tudi v zasebne namene delavcev, pri čemer so se uporabniki na strani družbe dolžni v smislu skrbi za ugled družbe izogibati pošiljanju elektronskih sporočil z neprimerno in žaljivo vsebino.

V računalnik (delovno postajo), drugo tehnično sredstvo (na primer mobilni telefon), dano v uporabo s strani družbe, ali v elektronsko pošto delavca, ki je angažiran bodisi na podlagi pogodbe o zaposlitvi bodisi na drugem pogodbenem temelju (v nadaljevanju: uporabnik opreme), sme družba poseči le v izjemnih primerih, opredeljenih v tem pravilniku, in sicer v primeru nepričakovane, nenadne in dalj časa trajajoče ali trajne odsotnosti uporabnika opreme, na primer v primeru odpovedi delovnega razmerja s strani zaposlenega brez odpovednega roka, v primeru odpovedi delovnega razmerja iz krivdnih razlogov zaradi neopravičene odsotnosti, v primeru, da zaradi svojega zdravstvenega stanja uporabnik ni sposoben izraziti svoje volje, pa takšno stanje traja dlje časa ali se upravičeno domneva, da bo trajalo dlje časa, smrt uporabnika in podobni izredni primeri, kadar:
- je to nujno potrebno za izpolnitev zakonskih obveznosti družbe;
- je to nujno in neogibno potrebno za izpolnitev pogodbenih obveznosti družbe, katerih neizpolnitev ali izpolnitev z zamudo bi za družbo pomenila izgubo ugleda ali nastanek premoženjske škode.

Uporabnika opreme se pred posegom v njegov računalnik (delovno postajo), drugo tehnično sredstvo ali elektronsko pošto pozove k prostovoljni predložitvi gesel in/ali potrebnih dokumentov ter se mu za izpolnitev zahteve postavi primeren rok. Tako v primeru prostovoljnega posredovanja dostopnih gesel, kot tudi v primeru, da se uporabnik na poziv družbe ne odzove ali ga zavrne, se vstop v računalnik (delovno postajo), drugo tehnično sredstvo ali elektronsko pošto opravi s strani osebe, ki jo vsakokrat imenuje direktor družbe, delavcu/uporabniku pa se omogoči, da dejanju osebno prisostvuje, tako da se ga obvesti o kraju in času dejanja, razen če to iz objektivnih razlogov ni mogoče ali če zaposleni s svojim ravnanjem očitno onemogoča vstop.

O vsakem vstopu v računalnik, drugo tehnično sredstvo in/ali elektronsko pošto po tem členu se vodi dokumentacija, ki vsebuje najmanj:

- obrazložen razlog za dopustnost vstopa,
- zapisnik o vstopu v računalnik ali elektronsko pošto z morebitnimi pripombami delavca, če je ta navzoč,
- navedbo prisotnih oseb,
- seznam oziroma izpis pridobljenih podatkov.

Šteje se, da je o namenu uporabe elektronske pošte in ostale programske opreme, ki jo uporabniku za namene opravljanja dela nudi družba, ter o možnostih nadzora po določbah tega člena tega pravilnika uporabnik predhodno obveščen, ko mu družba izroči izvod tega pravilnika ali mu ga pošlje na e-naslov, ki ga delavcu/uporabniku da družba, ali ga za namen komunikacije z družbo posreduje uporabnik sam.

27. člen

Vpogled v telefonske prometne podatke mobilnih naročniških številk v lasti družbe in uporabi posameznega uporabnika, lahko od operaterjev telekomunikacijskih storitev zahteva le direktor družbe ali od njega pooblaščena oseba in le v primeru spora med uporabnikom in družbo o višini stroškov porabe za sporno mobilno naročniško številko za določeno obračunsko obdobje, pri čemer to stori

skladno z določili Zakona o elektronskih komunikacijah in nikakor ne sme preverjati identitete oziroma lastništva klicanih ali klicočih številk, razen kadar bi to zaradi ugotavljanja, ali so bili klici opravljeni v službene namene, zahteval delavec/uporabnik sam.

Družba mobilnim napravam v njeni lasti in uporabi posameznega uporabnika ne sme slediti in v ta namen v svoje mobilne naprave ne sme namestiti naprave oziroma aplikacije za sledenje uporabniku.

28. člen

Ob prenehanju delavnega razmerja je delavec družbi dolžan vrniti službeni računalnik, drugo tehnično sredstvo in/ali službeni mobilni telefon, ki ga je uporabljal v službene namene, pri čemer mora pred vrnitvijo delavec sam poskrbeti, da so s službenih računalniških, tehničnih in mobilnih naprav očiščene oziroma izbrisane vse njegove zasebne vsebine, službene pa ohranjene v celoti.

29. člen

Delavec lahko za namene opravljanja dela poleg službene opreme in naprav v lasti družbe uporablja svoje zasebne računalnike in/ali mobilne telefone in druge tehnične naprave, če takšno uporabo odobri direktor ali od njega pooblaščena oseba.

V primeru prenehanja delovnega razmerja je delavec dolžan s zasebnih računalnikov in/ali mobilnih telefonov ali drugih naprav (tudi USB ključev ipd.), ki jih je v soglasju z delodajalcem uporabljal za službene namene, izbrisati vse osebne podatke, ki so bili preneseni s službenega omrežja, in vse datoteke, ki jih je zaposleni uporabljal v službene namene, ne glede na to, ali vsebujejo osebne podatke.

VII. POSREDOVANJE ZAUPNIH PODATKOV

30. člen

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

Ovojnica, v kateri se posredujejo zaupni podatki, mora biti izdelana na takšen način, da 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 ni mogoče opraviti brez vidne sledi odpiranja ovojnice.

31. člen

Zaupne podatke, ki se prenašajo po komunikacijskih kanalih ali fizično na računalniških medijih, je potrebno zaščititi s ustreznimi standardiziranimi kriptografskimi metodami tako, da je zagotovljena njihova nečitljivost oziroma neprepoznavnost med prenosom, ali zavarovano z gesli.

VIII. BRISANJE ZAUPNIH PODATKOV

32. člen

Po preteku roka hranjenja se osebni podatki zbrišejo, uničijo, blokirajo ali anonimizirajo, razen če zakon ali drug predpis ne določa drugače.

Osebni podatki, ki so del pogodb, se izbrišejo iz zbirke podatkov uničijo, blokirajo ali anonimizirajo po izteku absolutnih zastaralnih rokov, ki so določeni v zvezi s posamezno obveznostjo ali upravičenjem.

Osebni podatki, ki se obdelujejo na podlagi privolitve, se izbrišejo, uničijo, blokirajo ali anonimizirajo najkasneje 15. dan po prejemu preklica.

33. člen

Za brisanje podatkov z nosilcev podatkov se uporabi takšna metoda brisanja, da je nemogoča restavracija vseh ali dela brisanih podatkov.
Podatki na klasičnih medijih (listine, kartoteke, register, seznam,...) se uničijo na način, ki onemogoča branje vseh ali dela uničenih podatkov.
Na enak način se uničuje pomožno gradivo (npr. matrice, izračune in grafikone, skice, poskusne oziroma neuspešne izpise ipd.).
Prepovedano je odmetavati odpadne nosilce zaupnih podatkov v koše za smeti.
Pri prenosu nosilcev zaupnih podatkov na mesto uničenja je potrebno zagotoviti ustrezno zavarovanje tudi v času prenosa/prevoza.
Prenos nosilcev podatkov na mesto uničenja ter uničevanje nosilcev zaupnih podatkov nadzoruje posebna komisija, ki o uničevanju sestavi tudi ustrezen zapisnik.

IX. UKREPANJE OB SUMU NEPOOBLAŠČENEGA DOSTOPA

34. člen

Vsi zaposleni so dolžni izvajati ukrepe za preprečevanje zlorabe osebnih podatkov in morajo z osebnimi podatki, s katerimi se seznanijo pri svojem delu, ravnati odgovorno, vestno in skrbno.
Zaposleni so dolžni o aktivnostih, ki so povezane z odkrivanjem ali nepooblaščenim uničenjem zaupnih in osebnih podatkov, zlonamerni ali nepooblaščeni uporabi, prilaščanju, spreminjanju ali poškodovanju, takoj obvestiti direktorja oziroma pooblaščeno osebo, sami pa poskušajo takšno aktivnost preprečiti.

35. člen

Družba mora zoper tistega, ki je zlorabil osebne podatke ali je nepooblaščeno vdrl v zbirko osebnih podatkov, ustrezno ukrepati.
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 podpisanih dogovorih družbe s strankami.

36. člen

Za obveščanje Informacijskega pooblaščenca o kršitvah varstva osebnih podatkov po 33. členu Splošne uredbe je odgovoren direktor.

X. ODGOVORNOST ZA IZVAJANJE VARNOSTNIH UKREPOV IN POSTOPKOV

37. člen

Za izvajanje postopkov in ukrepov za zavarovanje zaupnih podatkov so odgovorni vsi zaposleni v družbi, kot tudi zunanji izvajalci, ki imajo z družbo podpisan dogovor o sodelovanju.

Nadzor nad izvajanjem postopkov in ukrepov, določenih s tem pravilnikom, opravlja direktor družbe oziroma od njega pooblaščena oseba.

38. člen

Oseba, ki ima dostop do zaupnih podatkov, mora pred nastopom dela podpisati pisno izjavo, s katero se zaveže k varovanju zaupnih podatkov ves čas trajanja delovnega razmerja, pri čemer se delavca opozori, da obveznost varovanja osebnih podatkov ne preneha s prenehanjem delovnega razmerja in da bo kršitev te obveznosti šteta tudi kot kršitev njegovih zavez iz pogodbe o zaposlitvi. Vzorec pisne izjave je priloga pravilnika (priloga 1).

39. člen

Za kršitev določil tega pravilnika je oseba, ki ima dostop do zaupnih podatkov, lahko kazensko, odškodninsko in disciplinsko odgovorna oziroma odgovorna na podlagi pogodbene obveznosti oziroma v skladu z določbami tega pravilnika.

XI. VIDEO NADZOR

40. člen

Odločitev o uvedbi videonadzora sprejme direktor. V odločitvi, ki je lahko v obliki sklepa ali zaznamka, direktor opredeli namen videonadzora in opredeli prostore, v katerih se izvaja videonadzor ter namestitev obvestil v skladu z zakonom, ki ureja varstvo osebnih podatkov.

Obvestilo vsebuje informacije o tem:
- da se izvaja videonadzor,
- naziv osebe javnega ali zasebnega sektorja, ki ga izvaja,
- telefonsko številko za pridobitev informacije, kje in koliko časa se shranjujejo posnetki iz video nadzornega sistema.

Obvestilo mora biti nameščeno na mestih, ki posamezniku omogočajo, da se seznani z izvajanjem videonadzora najkasneje, ko se ta nad njim začne izvajati – torej najkasneje ob vstopu v video nadzorovani prostor.
Direktor ali z njegove strani pooblaščena oseba za delovanje video nadzornega sistema lahko v upravičenih primerih, kadar je prizadeta dobrina, ki jo družba varuje z video nadzornim sistemom, vpogleda v posnetke video nadzornega sistema (zlasti ugotovljena materialna škoda, poškodba ljudi, sum nepooblaščenega vstopa v prostore, ki so video nadzorovani, oziroma v prostorih, do katerih dostopa skozi prostore, ki so video nadzorovani, sprožitev alarma, nevklop ali zatajitev alarma itd.).

Videonadzori posnetki se hranijo najdlje 12 mesecev, potem se izbrišejo.

XII. KONČNE DOLOČBE

41. člen

Ta pravilnik začne veljati dne 1.12.2018

Matej Kordelič, direktor Ljubljana, dne 19.11.2018

Priloga:
1. Izjava o varovanju zaupnih podatkov

Priloga 1

**Izjava o seznanjenosti z varstvom osebnih podatkov,
s Pravilnikom o obdelavi osebnih in zaupnih podatkov vključno z zagotavljanjem varnosti osebnih podatkov in politiko varstva osebnih podatkov zaposlenih družbe Strenia, d.o.o. in z morebitnimi posledicami nespoštovanja**

Spodaj podpisani _____
potrjujem, da sem prebral **Pravilnik o obdelavi osebnih in zaupnih podatkov vključno z zagotavljanjem varnosti osebnih podatkov in politiko varstva osebnih podatkov zaposlenih** družbe *Strenia d.o.o.*, ga razumem in se zavezujem k njegovemu izrecnemu uveljavljanju ves čas mojega dela oziroma sodelovanja z družbo *Strenia d.o.o.*, kakor tudi po prenehanju mojega dela oziroma sodelovanja s to družbo.

Prav tako potrjujem, da sem seznanjen z določbami zakona in uredbe, ki ureja področje varstva osebnih podatkov in s posledicami morebitnega neupoštevanja prej navedenega pravilnika oziroma zakona – kršitev pogodbe o zaposlitvi. Seznanjen sem tudi, da bom regresno odgovoren v primeru, da bo *družba Strenia d.o.o.*, morala izplačati odškodnino zaradi protipravnih posegov v varstvo osebnih podatkov, ki jih bom s svojim ravnanjem povzročil namenoma ali iz hude malomarnosti.

Podpis: _____ Datum in kraj: _____