Na podlagi določil:

- Splošne uredbe o varstvu podatkov – SUVP, Uredba (EU) 2016/679 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov – GDPR,
- Zakon o varstvu osebnih podatkov – ZVOP-2, (Ur.l. RS, št. 163/22, 40/25 – ZinfV-1, 10/26 – ZP-1L),

izdaja direktor družbe

HONESTAS, DRUŽBA ZA ZAVAROVALNO ZASTOPANJE, d.o.o.,

Beloruska ulica 7, 2000 Maribor,

naslednji

PRAVILNIK
O VARSTVU OSEBNIH PODATKOV

SPLOŠNE DOLOČBE

1. člen

S tem pravilnikom se določajo nameni obdelave osebnih podatkov, vrste osebnih podatkov, ki se lahko obdelujejo, rok njihove hrambe, arhiviranja ali izbrisa osebnih podatkov, organizacijski, tehnični postopki in ukrepi za zavarovanje osebnih podatkov v podjetju, z namenom, da se prepreči slučajno ali namerno nepooblaščeno uničevanje podatkov, njihovo spremembo ali izgubo, kakor tudi nepooblaščen dostop, obdelava, uporaba ali posredovanje podatkov v podjetju HONESTAS d.o.o. (upravljavec).

Določbe tega Pravilnika, kakor tudi veljavne zakonodaje na področju varstva osebnih podatkov, morajo spoštovati odgovorna oseba podjetja, vodstvo, zaposleni, delavci in vse osebe, ki so vključene v delovni proces podjetja na podlagi pogodbe o zaposlitvi ali na podlagi drugega pogodbenega razmerja, ki pri svojem delu v podjetju oziroma za ime in račun podjetja na kakršenkoli način obdelujejo, uporabljajo ali dostopajo do osebnih podatkov, drugih zaupnih podatkov in se seznanjajo s poslovno skrivnostjo podjetja (na primer vajenci, študentje, dijaki na praktičnem izobraževanju/usposabljanju/delu preko študentske napotnice, člani raznih odborov, delovnih teles v podjetju, zunanji izvajalci storitev…).

V zadevah, ki jih ne ureja ta pravilnik, se neposredno uporabljajo določbe veljavnih predpisov.

2. člen

Izrazi, ki so uporabljeni v tem pravilniku, imajo v skladu z veljavnimi predpisi naslednji pomen:

1. »osebni podatki« pomeni katero koli informacijo v zvezi z določenim ali določljivim posameznikom (v nadaljnjem besedilu: posameznik, na katerega se nanašajo osebni podatki);

2. »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, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika;

3. »obdelava« pomeni 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;

4. »omejitev obdelave« pomeni označevanje shranjenih osebnih podatkov zaradi omejevanja njihove obdelave v prihodnosti;

5. »psevdonimizacija« pomeni obdelavo osebnih podatkov na tak način, da osebnih podatkov brez dodatnih informacij ni več mogoče pripisati specifičnemu posamezniku, na katerega se nanašajo osebni podatki, če se take dodatne informacije hranijo ločeno ter zanje veljajo tehnični in organizacijski ukrepi za zagotavljanje, da se osebni podatki ne pripišejo določenemu ali določljivemu posamezniku;

6. »zbirka« pomeni 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;

7. »nosilec podatkov« pomeni vse vrste sredstev, na katerih so zapisani ali posneti podatki (listine, akti, gradiva, spisi, računalniška oprema vključno s magnetnimi, optičnimi ali drugimi računalniškimi mediji, fotokopije, zvočno ali slikovno gradivo, mikrofilmi, naprave za prenos podatkov, in podobno;

8. »upravljavec« pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki samo ali skupaj z drugimi določa namene in sredstva obdelave; kadar namene in sredstva obdelave določa pravo Unije ali pravo države članice, se lahko upravljavec ali posebna merila za njegovo imenovanje določijo s pravom Unije ali pravom države članice;

9. »obdelovalec« pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca;

10. »uporabnik« pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki so mu bili osebni podatki razkriti, ne glede na to, ali je tretja oseba ali ne. Vendar pa se javni organi, ki lahko prejmejo osebne podatke v okviru posamezne poizvedbe v skladu s pravom Unije ali pravom države članice, ne štejejo za uporabnike; obdelava teh podatkov s strani teh javnih organov poteka v skladu z veljavnimi pravili o varstvu podatkov glede na namene obdelave;

11. »tretja oseba« pomeni fizično ali pravno osebo, javni organ, agencijo ali telo, ki ni posameznik, na katerega se nanašajo osebni podatki, upravljavec, obdelovalec in osebe, ki so pooblaščene za obdelavo osebnih podatkov pod neposrednim vodstvom upravljavca ali obdelovalca;

12. »privolitev posameznika« na katerega se nanašajo osebni podatki pomeni vsako prostovoljno, izrecno, informirano in nedvoumno izjavo volje posameznika, na katerega se nanašajo osebni podatki, s katero z izjavo ali jasnim pritrdilnim dejanjem izrazi soglasje z obdelavo osebnih podatkov, ki se nanašajo nanj;

13. »kršitev varstva osebnih podatkov« pomeni kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščeno razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani;

14. »biometrični podatki« pomeni osebne podatke, ki so rezultat posebne tehnične obdelave v zvezi s fizičnimi, fiziološkimi ali vedenjskimi značilnostmi posameznika, ki omogočajo ali potrjujejo edinstveno identifikacijo tega posameznika, kot so podobe obraza ali daktiloskopski podatki;

15. »podatki o zdravstvenem stanju« pomeni osebne podatke, ki se nanašajo na telesno ali duševno zdravje posameznika, vključno z zagotavljanjem storitev in razkrivajo informacije o njegovem zdravstvenem stanju;

16. »posebne vrste osebnih podatkov« pomeni osebne podatke, ki razkrivajo rasno ali etično poreklo, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu in obdelava genetskih podatkov, biometrični podatki za namene edinstvene identifikacije posameznika, podatkov v zvezi z zdravjem ali podatkov v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo;

13. »podjetje« pomeni fizično ali pravno osebo, ki opravlja gospodarsko dejavnost, ne glede na njeno pravno obliko, vključno s partnerstvi ali združenji, ki redno opravljajo gospodarsko dejavnost;

14. »nadzorni organ« pomeni Informacijskega pooblaščenca, določenega z zakonom, ki ureja informacijskega pooblaščenca;

15. »čezmejna obdelava osebnih podatkov« pomeni bodisi: a) obdelavo osebnih podatkov, ki poteka v Uniji v okviru dejavnosti sedežev upravljavca ali obdelovalca v več kot eni državi članici, kadar ima upravljavec ali obdelovalec sedež v več kot eni državi članici, bodisi b) obdelavo osebnih podatkov, ki poteka v Uniji v okviru dejavnosti edinega sedeža upravljavca ali obdelovalca, vendar obdelava znatno vpliva ali bi lahko znatno vplivala na posameznike, na katere se nanašajo osebni podatki, v več kot eni državi članici;

16. »povezovanje zbirk« pomeni povezavo vsaj dveh zbirk, tako, da se omogoči, da se vsebina osebnih podatkov v različnih zbirkah samodejno posodablja na način, da so osebni podatki v zbirki osebnih podatkov posodobljeni ali da je avtomatično navedena oznaka, da je osebni podatek spremenjen.

NAMEN OBDELAVE OSEBNIH PODATKOV IN ZBIRKE

3. člen

V podjetju se lahko na podlagi določil GDPR obdelujejo osebni podatki, v kolikor je izpolnjen vsaj eden od naslednjih pogojev:

- posameznik, na katerega se nanašajo osebni podatki, je privolil v obdelavo njegovih osebnih podatkov v enega ali več določenih namenov,
- obdelava je potrebna za izvajanje pogodbe, katere pogodbena stranka je posameznik, na katerega se nanašajo osebni podatki, ali za izvajanje ukrepov na zahtevo takega posameznika pred sklenitvijo pogodbe,
- obdelava je potrebna za izpolnitev zakonske obveznosti, ki velja za upravljavca,
- obdelava je potrebna za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge fizične osebe,
- obdelava je potrebna za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti dodeljene upravljavcu;
- obdelava je potrebna zaradi zakonitih interesov, za katere si prizadeva upravljavec ali tretja oseba, razen, kadar nad takimi interesi prevladajo interesi ali temeljne pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, ki zahtevajo varstvo osebnih podatkov, zlasti kadar je posameznik, na katerega se nanašajo osebni podatki, otrok.

Osebni podatki se smejo obdelovati samo za določene in zakonite namene ter se ne smejo nadalje obdelovati tako, da bi bila njihova obdelava v neskladju s temi nameni, če zakon ne določa drugače. Pri obdelavi posebnih vrst podatkov morajo biti zaposleni še posebej vestni in skrbni. Posebne vrste osebnih podatkov morajo biti varovane tako, da se nepooblaščenim osebam prepreči dostop do njih.

O obdelavi osebnih podatkov mora biti posameznik obveščen v skladu z določbo 13. in 14. člena oziroma mu morajo iti predstavljene pravice iz 15. in naslednjih členov GDPR.

4. člen

Posameznik, na katerega se nanašajo osebni podatki, ima pravico od podjetja dobiti potrditev, ali se v zvezi z njim obdelujejo osebni podatki in kadar je temu tako, mu podjetja nudi dostop do osebnih podatkov in informacije iz 15/I. čl. GDPR ter zagotavlja naslednje pravice, v kolikor je to v skladu s GDPR:

- pravica dostopa do svojih osebnih podatkov
- pravica do popravka netočnih oziroma do dopolnitve osebnih podatkov,
- pravica do izbrisa t.i. »pravica do pozabe«,
- pravica do omejitve obdelave osebnih podatkov,
- pravica do obveščanja v zvezi s popravkom ali izbrisom osebnih podatkov ali omejitvijo obdelave,
- pravica do prenosljivosti podatkov,
- pravica do ugovora obdelave osebnih podatkov.

5. člen

Odgovorna oseba podjetja je dolžna poskrbeti za to, da so posamezniki na primeren način, ki je skladen z zahtevami GDPR, obveščeni o pravicah. Prav tako odgovorna oseba poskrbi za enotno kontaktno točko, na katero se lahko obrnejo in s podjetjem komunicirajo posamezniki pri uveljavljanju svojih pravic.

Posamezniki imajo naslednje pravice iz varstva osebnih podatkov:

- zahtevajo lahko informacije o tem, ali ima podjetje osebne podatke o njih in če jih ima, katere podatke ima ter na kakšni podlagi jih ima in zakaj jih uporablja,
- zahtevajo lahko dostop do svojih osebnih podatkov, kar jim omogoča, da prejmejo kopijo osebnih podatkov, ki jih imajo o njih ter preverijo, ali jih podjetje obdeluje zakonito,
- zahtevajo lahko popravek osebnih podatkov, kot je popravek nepopolnih ali netočnih osebnih podatkov,
- zahtevajo lahko izbris osebnih podatkov, kadar ni razloga za nadaljnjo obdelavo oziroma kadar uveljavljajo svojo pravico do ugovora glede nadaljnje obdelave,
- ugovarjajo lahko nadaljnji obdelavi osebnih podatkov, kjer se zanašamo na zakoniti poslovni interes (tudi v primeru zakonitega interesa tretje osebe), kadar obstajajo razlogi, povezani z njihovim osebnim položajem, na glede na določilo prejšnjega stavka imajo pravico kadarkoli ugovarjati, če obdeluje podjetje njihove osebne podatke za namene neposrednega trženja,
- zahtevajo lahko omejitev obdelave lastnih osebnih podatkov, kar pomeni prekinitev obdelave osebnih podatkov o njih, na primer, če želijo, da podjetje ugotovi njihovo točnost ali preveri

razloge za njihovo nadaljnjo obdelavo,
- zahtevajo lahko prenos osebnih podatkov v strukturirani elektronski obliki k drugemu upravljavcu, v kolikor je to mogoče in izvedljivo,
- prekličejo lahko privolitev oziroma soglasje, ki so ga podali za zbiranje, obdelavo in prenos osebnih podatkov za določen namen, po prejemu obvestila, da so umaknili svojo privolitev, bo podjetje prenehalo obdelovati njihove osebne podatke za namene, ki so jih prvotno sprejeli, razen če podjetje nima druge zakonite pravne podlage za to, da to stori zakonito.

Če želi posameznik uveljavljati katero koli od prej navedenih pravic, lahko pošlje zahtevek po elektronski pošti ali z redno pošto na naslov družbe.

Dostop do lastnih osebnih podatkov in uveljavljanje pravic je za posameznika brezplačno. V kolikor prepis zahteva večji obseg dela, ki za seboj potegne materialne stroške se posamezniku ti materialni stroški zaračunajo. Če je posameznikova zahteva za dostop očitno neutemeljena ali pretirana, lahko v takšnem primeru podjetje zahtevo tudi zavrne.

V primeru uveljavljanja pravic posameznika po tem določilu Pravilnika, podjetje mora od posameznika zahtevati določene informacije, ki bodo omogočale preverjanje identitete posameznika, kar predstavlja varnostni ukrep, ki zagotavlja, da se osebni podatki ne razkrijejo nepooblaščeni osebi.

V primeru, da posameznik meni, da so njegove pravice s področja varstva osebnih podatkov, kršene, se lahko za zaščito ali pomoč obrne na nadzorni organ oziroma na informacijskega pooblaščenca: GP.IP@IP-RS.SI ali poišče informacije na spletni strani WWW.IP-RS.SI .

6. člen

Osebni podatki se na zahtevo uporabnika posredujejo samo tistim uporabnikom, ki se izkažejo z ustrezno pravno podlago ali s pisno zahtevo oziroma privolitvijo posameznika, na katerega se podatki nanašajo.

Osebni podatki se po uradni dolžnosti posredujejo samo tistim uporabnikom, ki imajo ustrezno pravno podlago.

Posredovanje osebnih podatkov lahko uporabnik zahteva pisno ali ustno. Ob podajanju zahteve po posredovanju osebnih podatkov mora uporabnik jasno navesti določbo zakona, ki ga pooblašča za pridobitev osebnih podatkov, ali pa mora uporabnik k zahtevi za posredovanje osebnih podatkov priložiti zahtevo ali pisno privolitev posameznika, na katerega se osebni podatki nanašajo.

Če uporabnik zahteva posredovanje osebnih podatkov ustno, sme odgovorna oseba ali pooblaščeni

obdelovalec v primeru dvoma obstoja pisne zahteve oziroma pisne privolitve posameznika, na katerega se osebni podatki nanašajo, od uporabnika zahtevati, da predloži ustrezno in primerno zahtevo posameznika ali njegovo privolitev.

Posredovanje posebnih vrst osebnih podatkov lahko uporabnik zahteva le s pisno vlogo, ki mora biti po vsebini vlogi iz prejšnjega odstavka.

Osebni podatki, ki se posredujejo uporabniku v fizični obliki, morajo biti posredovani v ovojnici, ki ne omogoča, da bi bila ob normalni svetlobi ali pri osvetlitvi ovojnice z običajno lučjo, vidna vsebina ovojnice. Ovojnica mora tudi zagotavljati, da odprtje ovojnice in seznanitve z njeno vsebino ni mogoče odpraviti brez vidne sledi odpiranja ovojnice.

Osebne podatke je dovoljeno 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.

Posebne vrste osebnih podatkov se v fizični obliki pošilja naslovnikom v zaprtih ovojnicah proti podpisu v dostavni knjigi ali z vročilnico. V primeru, da se posebne vrste osebnih podatkov pošilja v elektronski obliki, mora biti med prenosom zagotovljena njihova nečitljivost, tako da so šifrirani in zavarovani z geslom.

7. člen

Delavec je zadolžen za sprejem in evidenco pošte v podjetju, mora izročiti poštno pošiljko z osebnimi podatki direktno posamezniku ali službi, na katero je ta pošiljka naslovljena. Ravno tako odpira in pregleduje vse poštne pošiljke in pošiljke naslovljene na podjetje, ki na drug način prispejo v podjetje, 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 dostavljene 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, sme odpirati pošiljke, naslovljene na naslov podjetja in obenem delavca, razen v primerih, ko je iz ovojnice razvidno, da je delavcu treba pismo vročiti osebno.

8. člen

Podjetje vodi evidenco dejavnosti obdelave osebnih podatkov v okviru svoje odgovornosti in v skladu z 30.čl. GDPR.

Zaposleni, ki obdeluje osebne podatke, morajo biti seznanjeni z evidenco dejavnosti obdelave, vpogled v evidenco dejavnosti obdelave je omogočen vsakemu zaposlenemu na zahtevo. Seznanjenost se izkazuje z izjavo iz priloge tega pravilnika.

Evidenca dejavnosti obdelave osebnih podatkov vsebuje:

- naziv zbirke osebnih podatkov z navedbo kontaktnih podatkov upravljavca, predstavnika upravljavca in pooblaščene osebe za varstvo podatkov;
- namene obdelave;
- pravna podlaga obdelave;
- opis kategorij posameznikov, na katere se nanašajo osebni podatki;
- vrste osebnih podatkov;
- kategorije uporabnikov, ki so jim bili ali jim bodo razkriti osebni podatki,
- prenosi osebnih podatkov v tretjo državo;
- rok hrambe osebnih podatkov,
- splošen opis tehničnih in organizacijskih varnostnih ukrepov;
- podatek o lokaciji, obliki podatka in dostop do evidence – informacijska podpora.

9. člen

Kadar je možno, da bi lahko načrtovana obdelava osebnih podatkov, zlasti z uporabo novih tehnologij, ob upoštevanju narave, obsega, okoliščin in namenov obdelave osebnih podatkov, povzročilo veliko tveganje za pravice in svoboščine posameznikov, se na to opozori vodstvo podjetja.

V navedenem primeru se izvede ocena učinka v zvezi z varstvom podatkov, kot jo predvideva 35.čl. GDPR.

10. člen

Za namene dokumentiranja aktivnosti in obveščanja javnosti o delu in dogodkih v in v zvezi s podjetjem, kot so prireditve, srečanja, tekmovanja, izobraževanja in podobno, lahko podjetje takšen dogodek delno ali v celoti snema oziroma fotografira in izdelani material objavi na spletnih straneh, tiskovinah in družabnih omrežjih podjetja.

Obvestilo o tem, da bo dogodek sneman, fotografiran, se zapiše na vabilo oziroma na obvestilo o dogodku. Navede se tudi namen snemanja oziroma fotografiranja. Šteje se, da so udeleženci, obiskovalci dogodka obveščeni o snemanju oziroma fotografiranju dogodka.

Ob dogodkih z manjšim številom udeležencev, dogodki, ki niso odprti za javnost, se snemanje ali fotografiranje lahko napove ustno in udeležencem pusti možnost, da izrazijo svojo voljo glede zajema

njihove podobe s kamero.

11. člen

Podjetje redno obvešča zaposlene o pomenu in novostih s področja varstva osebnih podatkov in izvaja izobraževanje s tega področja ter s področja informacijske varnosti.

Podjetje zaposlenim predstavlja:

- pravice in dolžnosti zaposlenih na področju varstva osebnih podatkov,
- nevarnosti in najpogostejša tveganja za varovanje osebnih podatkov,
- možne posledice za podjetje in zaposlene v primeru kršitve varstva podatkov,
- varovanje gesel in upravljanje z gesli,
- varovanje opreme in prostorov,
- varno ravnanje v primeru iznosa podatkov izven prostorov podjetja (na prenosnikih, telefonih, nosilcih podatkov…)
- politiko čiste mize,
- politiko čistega ekrana,
- druge politike, prakse in primere s področja varstva osebnih podatkov.

Podjetje redno izvaja varnostne politike na področju informacijske varnosti, ki so opredeljene v internih aktih, sklepih vodstva podjetja oziroma drugih navodilih.

POOBLAŠČENA OSEBA ZA VARSTVO PODATKOV

12. člen

Podjetje ni zavezanec za imenovanje pooblaščene osebe za varstvo osebnih podatkov. Za namene posvetovanja s področja varstva osebnih podatkov se podjetje posvetuje z zunanjimi strokovno usposobljenimi izvajalci.

POGODBENA OBDELAVA OSEBNIH PODATKOV

13. člen

Z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezna opravila v zvezi z obdelavo osebnih podatkov za podjetje, se sklene pisna pogodba o opravljanju storitev, katera vsebuje tudi določila o predmetu obdelave, zlasti vsebino in trajanje obdelave, naravo in namen obdelave, vrste osebnih podatkov in kategorije posameznikov, o pravicah in obveznostih pogodbenega obdelovalca in upravljavca ter postopke in ukrepe za zavarovanje osebnih podatkov skladno z GDPR in ZVOP-2.

Obdelovalci so tudi zunanji sodelavci, ki oziroma če vzdržujejo programsko opremo ter izdelujejo in inštalirajo novo programsko opremo, v kolikor imajo pri svojem delu dostop do osebnih podatkov.

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

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

BRISANJE PODATKOV

14. člen

Osebni podatki se lahko obdelujejo le toliko časa, kolikor je določen rok hrambe oziroma dokler obstaja pravna podlaga iz 6. čl. GDPR. Po preteku roka hranjenja se osebni podatki zbrišejo, uničijo, blokirajo ali anonimizirajo, razen če zakon ali drug akt ne določa drugače.

Osebne podatke, ki jih podjetje obdeluje na osnovi pogodbenega odnosa s posameznikom, podjetje hrani za obdobje, ki je potrebno za izvršitev pogodbe in še 10 let po njenem prenehanju, razen v primerih, ko pride med posameznikom in podjetjem do spora v zvezi s pogodbo, do sodne izterjave ali varovanja pravic upnika v postopkih prenehanja, izbrisa, stečaja ali prisilne poravnave. V takem primeru hrani podjetje podatke še 5 let po zaključeni poravnavi obveznosti oziroma še 5 let po odločitvi o prenehanju obveznosti.

Tiste podatke, ki jih podjetje obdeluje na podlagi osebne privolitve posameznika ali zakonitega interesa, bo podjetje hranilo do preklica te privolitve oziroma do zahteve za izbris. Po prejemu preklica ali zahteve za izbris se podatki izbrišejo najkasneje v 15 dneh. Podjetje lahko te podatke izbriše tudi pred preklicem, kadar je bil dosežen namen obdelave osebnih podatkov ali če tako določa zakon.

Izjemoma lahko podjetje zavrne zahtevo za izbris osebnih podatkov iz razlogov iz GDPR in sicer zaradi uresničevanja pravice do svobode izražanja in obveščanja, zaradi izpolnjevanje pravne obveznosti obdelave, zaradi razlogov javnega interesa na področju javnega zdravja, zaradi namena arhiviranja v javnem interesu, zaradi znanstveno- ali zgodovinsko- raziskovalnih namenov ali zaradi statističnih namenom ali zaradi izvajanja pravnih zahtevkov ali zaradi obrambe pred pravnimi zahtevki.

15. člen

Za brisanje podatkov iz nosilcev podatkov se uporabi takšna metoda brisanja, da je nemogoča restavracija vseh ali dela brisanih podatkov.

Podatki na klasičnih medijih, kot so listine, kartoteke, registri, … se uničijo na način, ki onemogoča

branje vseh ali dela uničenih podatkov. Na enak način se uniči pomožno gradivo, kot so to matrice, izračuni in grafikoni, skice, poskusne in/ali neuspešne izpise

Prepovedano je odmetavati odpadne nosilce podatkov z osebnimi podatki v koše za smeti.

Pri prenosu nosilcev osebnih podatkov na mesto uničenja je potrebno zagotoviti ustrezno zavarovanje tudi v času prenosa. Prenos nosilcev podatkov na mesto uničenja ter uničevanje nosilcev osebnih podatkov nadzoruje posebna komisija, ki o uničenju sestavi tudi ustrezen zapisnik ozirom se uničenje preda ustrezni zunanji službi na osnovi sklenjene pogodbe. Zapisniki o uničenju nosilcev osebnih podatkov se hranijo pri osebi, pooblaščeni za arhiviranje.

INFORMACIJSKA VARNOSTNA POLITIKA

16. člen

Zaposleni uporabljajo različno informacijsko tehnologijo – računalnik, telefon, tablica… ter različne elektronske storitve – dostop do interneta, elektronska pošta, dostop do oblaka, skupni imeniki in mape ter druga programska oprema oziroma storitve, odvisno od tega, kar od tega jim dodeli podjetje, izključno za službene namene.

V omejenem obsegu in razumnih mejah se s strani podjetja dodeljena informacijska tehnologija in elektronske storitve lahko uporabljajo tudi v zasebne namene, vendar morajo pri tem zaposleni varovati ugled podjetja, tehnologije in storitve pa se ne sme uporabljati za neprimerne ali žaljive namene. Vodstvo lahko po lastni presoji delavcu kadarkoli prepove uporabo v zasebne namene.

17. člen

Dostop do svetovnega spleta je omogočen zaposlenim za njihovo delo, izobraževanje in informiranje.

Zaposleni v podjetju morajo uporabljati svetovni splet v skladu z etičnimi in moralnimi normami. Vsi uporabniki informacijskih sistemov se morajo zavedati, da se v medmrežju izkazujejo z mrežnim naslovom podjetja (IP naslov).

Posredovanje službenih elektronskih naslovov na zunanje spletne strežnike za namene prijave določene storitve – na primer pošta…, ni dovoljeno, razen če je povezano s poslovnim procesom podjetja.

V omrežju podjetja se na zahtevo odgovorne osebe lahko izdeluje statistika obiskanih spletnih strani, ki mora biti anonimizirana in ni za javno objavo. Statistika se lahko uporablja izključno za načrtovanje in varovanje informacijskega sistema.

Vodstvo podjetja lahko zaradi zagotavljanja informacijske varnosti in razpoložljivosti informacijskih virov ter zaradi preprečevanja kršitev s posebno odredbo odredi blokado določenih spletnih strani. Blokado dostopa do spletnih strani izvede oseb, zadolžena za delovanje računalniškega informacijskega sistema, na podlagi pisne odredbe odgovorne osebe. O blokadi se obvesti vse zaposlene po elektronski pošti.

18. člen

Službena elektronska pošta se v podjetju lahko uporablja kot orodje za komunikacijo s posamezniki, strankami, zaposlenimi in zunanjimi izvajalci. Zaposleni se pri tej komunikaciji morajo ravnati po strogih etičnih in moralnih normah ter popravilih bontona. Vsak pošiljatelj sporočila se mora zavedati, da se vsako sporočilo poslano s službenega elektronskega naslova, pri prejemniku lahko tolmači kot mnenje ozirom stališče podjetja, v katerem je pošiljatelj zaposlen.

Zaposleni po elektronski pošti ne smejo pošiljati verižnih pisem in obsežnih datotek (glasba, filmi, predstavitve, zagonske datoteke, skripte in podobno), razen, če so namenjen delu ali postopkom v podjetju.

Zaposleni svojega službenega elektronskega naslova ne sme uporabljati v marketinške namene in iz njega ne sme pošiljati oglasne pošte na znani in/ali neznane naslove. Prav tako se zaposleni ne smejo prijavljati na oglasno pošto ali novice z elektronskimi naslovi podjetja, razen če je to povezano s potrebami delovnega mesta.

Zaposleni morajo biti previdni pri odpiranju elektronske pošte s priponkami neznanih pošiljateljev. Če zaposlen sum, da gre za nezaželeno pošto, ki bi bila lahko škodljiva, je ne sme odpreti, temveč o prejemu takšne pošte obvesti za to pristojno osebo, zadolženo za delovanje računalniškega informacijskega sistema.

Zaposleni nikakor ne smejo pošiljati posebnih vrst osebnih podatkov ali gesel po elektronski pošti razen v ustrezno akreditiranih sistemih oziroma mora biti podatkom med prenosom zagotovljena njihova nečitljivost, tako da so šifrirani in zavarovani z geslom.

Uporaba zasebne elektronske pošte – na primer Gmail, Hotmail, Yahoo… za službene namene je prepovedana, saj potencialno predstavlja neupravičeno obdelavo osebnih podatkov. Izjemoma je izključno za namene komuniciranja med zaposlenimi na osnovi dovoljenja odgovorne osebe dovoljeno uporabljati zasebno elektronsko pošto.

Mobilnim telefonom, ki so v lasti podjetja in v uporabi posameznega delavca, se ne sme slediti in v ta namen se v te mobilne naprave ne sme namestiti naprav oziroma aplikacije za sledenje.

19. člen

Oddaljeni dostop do informacijskega sistema podjetja je dovoljen na podlagi odobrene metode z ustrezno ravnjo varnosti in sicer za tiste delavce, ki dostop potrebujejo zaradi opravljanja delovnih nalog, vendar le v omejenem obsegu. Treba je upoštevati tudi načelo praznega zaslona. Po končanem delu se je potrebno obvezno odjaviti iz sistema in zagotoviti, da katerikoli podatki in sledi ne ostanejo nezavarovani na delovni postaji.

Za uvedbo oddaljenega varnega dostopa mora biti na strojni opremi zagotovljena prepoznava ustrezne programske opreme, ki omogoča zaščito končne točke pred internetnimi grožnjami. Za zagotavljanje zaupnosti se ves promet iz končne točke oddaljenega omrežja do omrežja podjetja šifrira.

20. člen

Oseba, zadolžena za delovanje informacijskega sistema v podjetju, lahko na posebej utemeljeno pisno zahtevo pooblaščene osebe v prisotnosti tri članske komisije v izrednih primerih vpogleda v informacijsko tehnologijo ali druge elektronske storitve delavca le, če je to nujno potrebno za izpolnjevanje zakonskih, pogodbenih in drugih obvez podjetja oziroma za vodenje delovnega procesa.

Vpogled opravi tri članska komisija, ki jo vsakokrat imenuje odgovorna oseba podjetja. V njej mora biti vsaj en predstavnik zaposlenih, ki ni vodstveni delavec. O vpogledu mora komisija napisati zapisnik, ki vsebuje:

- obrazložitev vpogleda,
- zapisnik o vstopu z morebitnimi pripombami delavca, če je navzoč,
- navedbe prisotnih oseb,
- seznam oziroma izpis pridobljenih podatkov.

Če se pojavi utemeljen sum, da zaposleni ne spoštuje določil informacijsko varnostne politike tega pravilnika, lahko oseba, zadolžena za delovanje računalniškega informacijskega sistema, na posebej utemeljeno pisno zahtevo, odgovorne osebe podjetja opravi nadzor uporabe elektronskih storitev, a zgolj z vidika pregleda dnevniških zapisov o količini prometa in shranjenih podatkov, ki obremenjujejo strežnik. Ob tem se ne sme pregledovati vsebin.

Vpogled v telefonske prometne podatke priključkov, katerih lastnik je podjetje, lahko podjetje zahteva od operaterja telekomunikacijskih storitev le takrat, kadar pride med podjetje in zaposlenim do kakršnega koli spora glede višine stroškov porabe konkretnega telefonskega priključka.

O namenu porabe informacijske tehnologije in elektronskih storitev iz tega člena ter možnosti

vpogleda mora biti zaposleni pisno obveščen. Kot zadostno obvestilo se šteje obvestilo skupaj s temi pravili poslano vsem zaposlenim po e-pošti.

21. člen

Ob prenehanju delovnega razmerja oziroma ob prenehanju temelja za opravljanje dela v podjetju, je zaposleni dolžan vrniti službeno informacijsko tehnologijo, ki jo je uporabljal v službene namene, pri čemer mora pred vrnitvijo delavec sam poskrbeti, da so iz uporabljene informacijske tehnologije in elektronskih storitev očiščene oziroma izbrisane vse njegove zasebne vsebine, službene pa ohranjene v celoti. Zaposleni in podjetje se lahko dogovorita o odkupu računalniške opreme.

22. člen

Zaposleni lahko za namene opravljanja dela poleg službene opreme uporablja svojo zasebno opremo in druge tehnične naprave, če takšno uporabo odobri odgovorna oseba in delavec poda prostovoljno pisno soglasje, da lahko delodajalec za namene izvajanja delovnega procesa pri tem obdeluje njegovo zasebno telefonsko številko oziroma zasebni elektronski naslov.

V primeru prenehanja delovnega razmerja je delavec dolžan z zasebne opreme ali drugih naprav in njihovih nosilcev podatkov, ki jih je v soglasju z delodajalcem uporabljal za službene namene, izbrisati vse osebne podatke, ki so bili preneseni v okviru opravljanja delovnega procesa, in vse datoteke, ki jih je zaposleni uporabljal v službene namene, ne glede na to, ali vsebujejo osebne podatke.

VAROVANJE PROSTOROV IN RAČUNALNIŠKE OPREME

23. člen

V prostorih, v katerih se nahajajo nosilci osebnih podatkov, programska oprema, morajo biti varovani z organizacijskimi ter fizičnimi in/ali tehničnimi ukrepi, ki ne omogočajo nepooblaščenim osebam dostop do osebnih podatkov.

Kot varovani prostor so opredeljeni prostori vodstva, tajništva, strežniške sobe, pisarne, arhivski prostori, kabineti in drugi prostori, v katere nepooblaščene osebe nimajo vstopa.

Dostop do varovanih prostorov je mogoč le v rednem delovnem času, izven tega časa pa samo na podlagi dovoljenja odgovorne osebe podjetja.

Ključi se ne puščajo v ključavnici v vratih od zunanje strani.

Varovani prostori ne smejo ostajati nenadzorovani oziroma se morajo zaklepati ob odsotnosti delavcev, ki jih nadzorujejo.

Zaposleni svojega delovnega mesta ne smejo zapustiti nenadzorovanega oziroma morajo poskrbeti, da so takrat originalne listine in nosilci osebnih podatkov shranjeni tako, da nepooblaščene osebe do njih nimajo dostopa. Izven delovnega časa morajo biti omare in pisalne mize z nosilci osebnih podatkov zaklenjene, na delovnih površinah ne sme biti listin in drugih nosilcev z osebnimi podatki (politika čiste mize). Če to ni mogoče, se prostori zaklepajo, vstop tretjim osebam pa je zagotovljen zgolj ob prisotnosti osebe, ki prostor sicer nadzoruje.

Računalniki in druga informacijska tehnologija oziroma oprema, ki omogoča dostop do osebnih podatkov morajo biti v času odsotnosti zaposlenega, bodisi izklopljeni, bodisi fizično ali programsko zaklenjeni (politika čistega zaslona).

Zaposleni ne smejo puščati nosilcev z osebnimi podatki na mizah v prisotnosti oseb, ki nimajo pravice vpogleda vanje.

Nosilci osebnih podatkov, ki se nahajajo izven varovanih prostorov, morajo biti stalno zaklenjeni v omarah.

Posebne vrste osebnih podatkov se ne sme hraniti izven varovanih prostorov.

24. člen

V prostorih, ki so namenjeni poslovanju s strankami oziroma nimajo statusa varovanega prostora in je vanje dovoljen dostop nezaposlenim, morajo biti nosilci podatkov in računalniški zasloni nameščeni tako, da stranke nimajo neposrednega vpogleda vanje. V takšnih prostorih na oglasni deski ali kakorkoli drugače ne smejo biti izpostavljeni takšni podatki, na osnovi katerih bi se lahko nepooblaščene osebe seznanile z osebnimi podatki posameznika in za katere podjetja nima pravne podlage za njihovo objavo oziroma obdelavo.

25. člen

Vzdrževanje in popravila informacijske tehnologije in elektronskih storitev ter druge opreme je dovoljeno samo z vednostjo odgovorne osebe oziroma ga lahko izvajajo pooblaščeni servisi ali vzdrževalci, ki imajo s podjetjem sklenjeno ustrezno pogodbo.

26. člen

Vzdrževalci prostorov, informacijske tehnologije oziroma strojne in programske opreme, obiskovalci in poslovni partnerji se smejo gibati v varovanih prostorih samo z vednostjo odgovorne osebe. Delavci, kot so čistilke, varnostniki, hišniki, se lahko izven delovnega časa gibljejo samo v tistih varovanih prostorih, kjer je onemogočen vpogled v osebne podatke (nosilci osebnih podatkov so zaklenjeni v omarah, pisalnih mizah, računalniki in druga strojna oprema pa so izklopljeni ali kako

drugače fizično ali programsko zaklenjeni.

VAROVANJE SISTEMSKE IN APLIKATIVNE PROGRAMSKE OPREME

27. člen

Dostop do elektronskih storitev oziroma do programske opreme mora biti varovan tako, da dovoljuje dostop samo za to vnaprej določenim zaposlenim v podjetju ali zunanjim sodelavcem, ki v skladu s pogodbo opravljajo dogovorjene storitve.

28. člen

Popravljanje, spreminjanje in dopolnjevanje sistemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve odgovorne osebe ali od nje pooblaščene osebe, izvajajo ga lahko samo pooblaščeni servisi ali vzdrževalec, ki ima s podjetjem sklenjeno ustrezno pogodbo, izvajalci morajo izvedene spremembe in dopolnitve sistemske in aplikativne programske opreme ustrezno dokumentirati. V primeru, da je potrebno za delo izdelati kopije, morajo biti le-te po prenehanju namena, s katerim si bule izdelane, ustrezno uničene. Enako velja za ostale zapise, izvoze podatkov ali druge pripomočke za izvedbo storitev servisiranja.

29. člen

Vsebine na nosilcih podatkov na mrežnih strežnikih in lokalnih delovnih postajah, kjer se nahajajo osebni podatki, se mora redno preverjati zaradi potencialne prisotnosti računalniških virusov in druge oblike zlonamerne kode. V primeru odkritja virusa, se ta odpravi s strani ustrezne strokovne službe oziroma pristojne osebe, zadolžene za delovanje računalniškega informacijskega sistema, obenem pa se skuša ugotoviti tudi vzrok pojava virusa.

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

30. člen

Zaposleni ne smejo inštalirati programske opreme brez odobritve osebe, zadolžene za delovanje računalniškega informacijskega sistema. Prav tako ne smejo odnašati programske opreme iz podjetja brez odobritve odgovorne osebe podjetja in vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema.

31. člen

Dostop do podatkov in uprava sistemske in aplikativne programske opreme se varuje s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programske opreme in podatkov. Vsak uporabnik

ima svoje geslo za dostopanje do posameznih elektronskih storitev. Posojanje gesel in uporaba skupinskih gesel je prepovedana.

Pri generiranju oziroma določanju gesel je potrebno spoštovati naslednja pravila:

- gesla morajo biti dolžine minimalno 8 znakov ali ustrezno daljša, v kolikor je to določeno za posamezno uporabniško rešitev,
- gesla ne smejo vsebovati smiselnih alfa numeričnih zaporedij znakov,
- gesla morajo biti kvalitetna (ustrezne dolžine, posebni znaki, velike in male črte, številke),
- gesla ne smejo vsebovati besed iz različnih slovarjev,
- gesla naj ne bodo ciklična in naj se ne ponavljajo iz predhodnih obdobij,
- uveljavljeno mora biti obvezno redno spreminjanje gesel (najmanj na 6 mesecev),
- začetna gesla se ob prvi prijavi zamenja,
- gesla, ki jih je generiral zunanji dobavitelj, je potrebno takoj spremeniti ob prvi uporabi v produkcijskem okolju,
- uporabniško ime ne sme kazati posebnih pooblastil uporabnika.

Pri ravnanju z gesli je potrebno obvezno spoštovati napotke:

- pooblaščena oseba, ki dodeljuje gesla, jih mora obravnavati zaupno, preprečiti mora možnost nepooblaščenega vpogleda in jih posredovati na varen način,
- uporabnikom mora biti omogočeno, da kadar koli spremenijo svoje uporabniško geslo,
- geslo ne sme biti nikdar prikazano na zaslonu,
- gesla morajo biti obvezno shranjena v šifrirani obliki,
- vsak uporabnik mora imeti svoje uporabniško ime in geslo izključno za osebno rabo,
- geslo je potrebno hraniti na način, ki drugi osebi popolnoma onemogoči možnost vpogleda,
- vsak uporabnik je odgovoren za zaupnost gesla in ga ne sme v nobenem primeru zaupati drugi osebi,
- v nobenem primeru uporabnik ne sme izdati gesla nadrejenemu, podrejenemu ali osebi, ki ga nadomešča ali IT osebju,
- v primeru razkritja gesla ali suma razkritja gesla mora to nemudoma sporočiti pooblaščeni osebi za dodeljevanje gesel.

Vsa gesla in postopki, ki se uporabljajo za vstop in administriranje mreže osebnih računalnikov (supervizorska oziroma nadzorna gesla), administriranje elektronske pošte in administriranje aplikativnih organov, se hranijo v sefu, v zaprti kuverti ali na drug ustrezen način, tako da je dostop nepooblaščenim osebam onemogočen. Uporabi se jih samo v izrednih okoliščinah oziroma ob nujnih primerih. Vsako uporabo teh gesel sme dovoliti odgovorna oseba podjetja. Po vsaki takšni uporabi se določi nova vsebina gesel.

32. člen

Za potrebe restavriranja računalniškega sistema ob okvarah in ob drugih izjemnih situacijah se redni izdelujejo varnostne kopije podatkov.

Varnostne kopije podatkov se hranijo zaklenjene v zavarovanih ognjevarnih omarah, zaščitene pred poplavami in elektromagnetnimi motnjami.

UKREPANJE OB SUMU NEPOOBLAŠČENEGA DOSTOPA

33. člen

Zaposleni so dolžni o aktivnostih, ki so povezane z odkrivanjem, nepooblaščenim dostopom ali uničenjem podatkov, zlonamerni ali nepooblaščeni uporabi, prilaščanju, spreminjanju ali poškodovanju podatkov takoj obvestiti odgovorno osebo v podjetju in v primeru elektronskih podatkov tudi osebo zadolženo za informatiko, sami pa poskušajo takšno aktivnost preprečiti.

Kršitev varstva osebnih podatkov pomeni kršitev varnosti, ki povzroča nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščeno razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani. Kršitev je lahko storjena nehote – iz malomarnosti ali pa je načrtovana – naklep. Na splošno vsaka kršitev pomeni varnostni incident, ki ogroža zaupnost, celovitost in dostopnost osebnih podatkov.

Zaposleni so dolžni pri svojem delu spremljati in biti pozorni na morebitne varnostne incidente ter v skladu s tem pravilnikom ustrezno ravnati.

34. člen

Zaposleni morajo nemudoma, potem ko zaznajo varnostni incident, o tem obvestiti odgovorno osebo v podjetju.

Odgovorna oseba v podjetju mora najprej izvedeti, kaj se je zgodilo, oceniti, kakšne so potencialno škodljive posledice za pravice in svoboščine posameznikov in sprejeti ustrezne ukrepe za odpravo posledic ali vsaj zmanjšanje tveganj. Priporočljivo je, da se vodstvo za pripravo ocene verjetnosti in resnosti posledic za pravice in svoboščine posameznikov posvetuje z zunanjo strokovno usposobljeno osebo.

V primeru, da vodstvo podjetja oceni, da bo zaradi incidenta nastalo tveganje za pravice in svoboščine posameznikov, mora o tem obvestiti informacijskega pooblaščenca brez odlašanja, najkasneje pa v 72 urah po zaznani kršitvi. V primeru, da se je incident zgodil v zvezi s podatki, pri katerih je podjetje v vlogi obdelovalca, mora o kršitvi obvestiti upravljavca v najkrajšem možnem času po zaznavi kršitve.

Za prijavo se uporabi obrazec, ki ga priporoča informacijski pooblaščenec in predstavlja del dokumentacije podjetja. Ob prijavi mora informacijski pooblaščenec pridobiti vsaj naslednje informacije, skladno z GDPR:

- opis vrste kršitve, kategorije in približno število posameznikov, na katere se nanašajo osebni podatki, vrste in približno število evidenc osebnih podatkov,
- kontaktne podatke pooblaščene osebe za varstvo podatkov,
- opis verjetnih posledic kršitve varstva osebnih podatkov,
- opis ukrepov, ki jih je upravljavec sprejel ali pa predvidenih ukrepov za ublažitev tveganja za kršitve.

35. člen

Za obveščanje informacijskega pooblaščenca o kršitvah varstva osebnih podatkov po 33.čl. GDPR je zadolžena odgovorna oseba podjetja.

ODGOVORNOST ZA IZVAJANJE VARNOSTNIH UKREPOV IN POSTOPKOV

36. člen

Za izvajanje postopkov in ukrepov za zavarovanje osebnih podatkov so odgovorni vsi zaposleni v podjetju, kot tudi zunanji izvajalci, ki imajo s podjetjem podpisan dogovor o sodelovanju.

Določbe o obveznosti zaposlenih se smiselno uporabljajo tudi za osebe, ki s podjetjem sodelujejo na drugih pogodbenih pravnih podlagah (dijaki, študentje,…).

37. člen

Vsak zaposleni, ki obdeluje osebne podatke, je dolžan izvajati predpisane postopke in ukrepe za zavarovanje podatkov in varovati podatke, za katere je izvedel oziroma bil z njimi seznanjen pri opravljanju svojega dela. Obveza varovanja podatkov ne preneha s prenehanjem delovnega razmerja oziroma druge pogodbene pravne podlage s podjetjem.

38. člen

V primeru kršitev določil tega pravilnika, je delavec disciplinsko in odškodninsko odgovoren podjetju za škodo, ki je nastala podjetju oziroma fizičnim ali pravnim osebam, s katerimi podjetje sodeluje.

Z zunanjimi sodelavci ni dovoljeno sklepati pogodb, v katere bi se vnesle klavzule o omejitvi odškodninske odgovornosti iz naslova kršitev pravil na področju varovanja osebnih podatkov. V primeru odškodninske odgovornosti zunanjega sodelavca za kršitve pravil na področju varovanja osebnih podatkov, za škodo, ki nastane podjetju, le ti odgovarjajo v skladu z načeli odškodninskega prava in za celotno povzročeno škodo.

Kršitev določil tega Pravilnika predstavlja hujšo kršitev delovnih obveznosti po pogodbi o zaposlitvi oziroma bistveno kršitev druge pogodbe, zaradi katere lahko podjetje uvede postopek za odpoved pogodbe o zaposlitvi oziroma te druge pogodbe, ki je podlaga za opravljanje dela za podjetje.

Kršitev določil Pravilnika ima lahko za osebo, ki krši določila tega pravilnika, za posledico kazensko, prekrškovno, odškodninsko ter tudi disciplinsko odgovornost

39. člen

Kot kršitev varovanja osebnih podatkov se obravnavajo zlasti:

- opustitev vestnega in skrbnega nadzorovanja varovanja prostorov,
- opustitev ravnanja za preprečitev vpogleda v ali na nosilce osebnih podatkov,
- opustitev uničenja nepotrebne kopije osebnih podatkov,
- nepooblaščeno izdelovanje kopij osebnih podatkov,
- opustitev prisotnosti v času servisiranja računalniška in programske opreme,
- opustitev izvajanja preventive v zvezi z računalniškimi virusi,
- opustitev obvestila vodje organizacijske enote, osebe pooblaščene za informatiko in odgovorne osebe podjetja v primeru zlorabe osebnih podatkov ali vdora v zbirko osebnih podatkov,
- sporočanje osebnih podatkov, s katerimi se je uporabnik seznanil pri svojem delu, sodelavcem ali drugim nepooblaščenim osebam oziroma organizacijam,
- opustitev skrbi in nadzor nad nosilci osebnih podatkov med delovnim časom in s tem dopustitev možnosti vpogleda vanje nepooblaščenim osebam,
- odnašanje nosilcev osebnih podatkov iz podjetja brez izrecnega dovoljenja,
- posredovanje osebnih podatkov pooblaščenim osebam zunanjim institucijam brez dovoljenja vodstva podjetja,
- popravljanje, spreminjanje ali dopolnjevanje sistemske ali aplikativne programske opreme v nasprotju s tem pravilnikom,
- inštaliranje ali iznos programske opreme iz podjetja brez izrecnega dovoljenja vodstva podjetja in/ali brez vednosti pooblaščenega delavca za informatiko,
- opuščanje izdelovanja rednih kopij vsebine osebnih podatkov,
- opustitev hranjena računalniških kopij vseh zbirk osebnih podatkov v skladu s tem pravilnikom,
- opustitev evidentiranja aktivnosti posameznih pooblaščenih oseb do računalniško podprtih baz osebnih podatkov,
- druge opustitve oziroma kršitve dolžnosti ali prepovedi iz tega pravilnika.

PREHODNE IN KONČNE DOLOČBE

40. člen

Ta Pravilnik velja za zaposlene v podjetju, za osebe, ki v podjetju opravljajo dela na podlagi pogodbe o delu ali druge pogodbe, za dijake in študente, ki v družbi opravljajo dela preko študentskih napotnic oziroma so v družbi na praksi. Pojem zaposleni se smiselno uporabljajo za vse delavce, ki na kakršnih koli pravni podlagi sodelujejo z družbo.

Ta Pravilnik se objavi na spletni strani podjetja. Z objavo Pravilnika se šteje, da so z njegovo vsebino, določili seznanjeni vse zaposleni v podjetju in drugi delavci, ki opravljajo delo za podjetje.

Oseba, ki zaradi narave svojega dela zbira, ureja, obdeluje, spreminja, shranjuje, posreduje ali uporablja osebne podatke ali nosilce osebnih podatkov, mora podpisati izjavo, da je seznanjena z določbami GDPR, ZVOP-2 in vsebino tega Pravilnika.

41. člen

Ta pravilnik začne veljati z dnem 01.07.2026.

Maribor, 29.06.2026

HONESTAS d.o.o.
Rok Rotovnik, direktor