Na podlagi 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 (Splošna uredba o varstvu podatkov, v nadaljevanju: GDPR), in Zakona o varstvu osebnih podatkov izdaja direktor podjetja LSC GROUP celostne rešitve d.o.o., Kranjska cesta 4, 4240 Radovljica (v nadaljevanju: LSC GROUP d.o.o.)

Pravilnik o varstvu osebnih podatkov

I. SPLOŠNE DOLOČBE

1. člen

S tem pravilnikom se določajo tehnični in organizacijski postopki in ukrepi za zavarovanje osebnih podatkov v družbi LSC GROUP d.o.o. z namenom, da se prepreči nezakonit in nepooblaščen dostop, obdelava, uporaba ali posredovanje osebnih podatkov, slučajno ali namerno nepooblaščeno uničevanje podatkov, njihovo spremembo ali izgubo. Ukrepi se pregledujejo in dopolnjujejo, kadar je to potrebno.

Zaposleni in zunanji sodelavci, ki pri svojem delu obdelujejo in uporabljajo osebne podatke, morajo biti seznanjeni z:

- Splošno uredbo EU o varstvu osebnih podatkov (GDPR),
- Zakonom o varstvu osebnih podatkov, skupaj s področno zakonodajo, ki ureja posamezno področje njihovega dela,
- NA 101 Politike informacijske varnosti,
- ter z vsebino tega pravilnika.

2. člen

V tem pravilniku uporabljeni izrazi imajo naslednji pomen:

- **GDPR** - Splošna uredba o varstvu podatkov (Uredba (EU) 2016/679)
- **ZVOP-2** - Zakon o varstvu osebnih podatkov (Uradni list RS, št. 163/22);
- **Osebni podatek** - je katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen;
- **Posameznik** - je določena ali določljiva fizična oseba, na katero se nanaša osebni podatek; fizična oseba je določljiva, če se lahko neposredno ali posredno identificira, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, ki so značilni za njegovo fizično, fiziološko, duševno, ekonomsko, kulturno ali družbeno identiteto, pri čemer način identifikacije ne povzroča velikih stroškov ali ne zahteva veliko časa;
- **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;
- **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);
- **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;
- **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;

- **Obdelovalec osebnih podatkov** - pravna ali fizična oseba ali druga oseba javnega ali zasebnega sektorja, ki obdeluje osebne podatke v imenu upravljavca osebnih podatkov;
- **Uporabnik osebnih podatkov** - je fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki se ji posredujejo ali razkrijejo osebni podatki;
- **Občutljivi osebni podatki** - so podatki o rasnem narodnem ali narodnostnem poreklu, političnem, verskem filozofskem prepričanju, zdravstvenem stanju, spolnem življenju, vpisu ali izbrisu v ali iz kazenske evidence ali prekrškovne evidence ter biometrične značilnosti;
- **Nosilec podatkov** - so vse vrste sredstev, na katerih so zapisani ali posneti podatki (listine, akti, gradiva, spisi, računalniška oprema vključno s magnetni, optični ali drugi računalniški mediji, fotokopije, zvočno in slikovno gradivo, mikrofilmi, naprave za prenos podatkov, ipd.);

3. člen

Opis zbirk osebnih podatkov, katerih upravljavec je LSC GROUP d.o.o. se vodi v katalogu zbirk osebnih podatkov (opisu zbirk osebnih podatkov), ki se vodi v skladu z določbami 30. člena GDPR. Katalog zbirk osebnih podatkov se dopolnjuje ob vsaki spremembi vrste osebnih podatkov v posamezni zbirki.

Zaposleni, ki obdelujejo osebne podatke, morajo biti seznanjeni s katalogom zbirk osebnih podatkov, vpogled v katalog zbirk osebnih podatkov pa je potrebno na zahtevo omogočiti tudi posameznikom, na katere se osebni podatki nanašajo.

Direktor je dolžan voditi ažuren seznam, iz katerega je za vsako zbirko osebnih podatkov jasno razvidno, katera oseba je odgovorna za posamezno zbirko osebnih podatkov ter katere osebe lahko zaradi narave svojega dela obdelujejo osebne podatke, ki se nanašajo na posamezno zbirko osebnih podatkov. V seznam se vpisujejo sledeči podatki: naziv zbirke osebnih podatkov, osebno ime in delovno mesto osebe, ki je odgovorna za zbirko osebnih podatkov ter osebno ime in delovno mesto oseb, ki lahko zaradi narave njihovega dela obdelujejo osebne podatke, ki se nanašajo na zbirko osebnih podatkov.

II. ZAKONITA OBDELAVA PODATKOV

4. člen

Osebni podatki se obdelujejo, le če to določa zakon ali če je za obdelavo določenih osebnih podatkov podana osebna privolitev posameznika. Osebni podatki, ki se obdelujejo morajo biti točni in ažurni.

III. VAROVANJE PROSTOROV, RAČUNALNIŠKE OPREME, VAROVANJE SISTEMSKE IN APLIKATIVNO PROGRAMSKE RAČUNALNIŠKE OPREME TER PODATKOV, KI SE OBDELUJEJO Z RAČUNALNIŠKO OPREMO

5. člen

Varovanje prostorov in računalniške opreme oz. vsi organizacijski, ter fizični in/ali tehnični ukrepi se izvajajo v skladu z ***Politike varovanja informacij*** (ISO 27001).

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

6. člen

Z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezna opravila v zvezi z zbiranjem, obdelovanjem, shranjevanjem ali posredovanjem osebnih podatkov (obdelovalec), se sklene pisna pogodba, predvidena v 28. členu Splošne uredbe o varstvu podatkov. V takšni pogodbi morajo biti obvezno predpisani tudi pogoji in ukrepi za zagotovitev varstva osebnih podatkov in njihovega zavarovanja. Pred sklenitvijo pogodbe z obdelovalcem je odgovorna oseba (praviloma vodja oddelka) dolžna od njega pridobiti podatke, ki omogočajo preveritev, ali obdelovalec izpolnjuje zahteve zakonodaje s področja varstva osebnih podatkov; to vključuje tudi razkritje vseh podpogodbenih obdelovalcev, vključno z njihovimi nazivi in sedeži.

Že zgolj možnost dostopa do podatkov, četudi na izrecno zahtevo družbe (npr. v okviru servisnega posega na strojni opremi ipd.), se šteje za pogodbeno obdelavo v smislu 1. odstavka tega člena.

Obdelovalci smejo opravljati storitve obdelave osebnih podatkov samo v okviru naročnikovih pooblastil in podatkov ne smejo obdelovati ali drugače uporabljati za noben drug namen, k čemur se jih zaveže s pogodbo.

Pooblaščena pravna ali fizična oseba, ki za LSC GROUP d.o.o. opravlja dogovorjene storitve izven prostorov upravljavca, mora imeti vsaj enako strog način varovanja osebnih podatkov, kakor ga predvideva ta pravilnik ter ***Politike varovanja informacij*** (ISO 27001).

Poleg drugih zahtev si mora družba v pogodbah z obdelovalci zagotoviti pravico, da najmanj enkrat letno pri pogodbenem obdelovalcu izvede pregled ali revizijo na področju varstva osebnih podatkov. Pregled ali revizijo je potrebno izvesti ob vsakem sumu ali indicu, da obdelovalec krši sklenjeno pogodbo ali da ne zagotavlja zadostne ravni varstva osebnih podatkov. Revizija se izvede na stroške družbe, pri čemer obdelovalec morebitnega angažmaja svojih ljudi in/ali podpogodbenih obdelovalcev družbi ne sme zaračunati.

V. SPREJEM IN POSREDOVANJE OSEBNIH PODATKOV

7. člen

Delavec, ki je zadolžen za sprejem in evidenco pošte, mora izročiti poštno pošiljko z osebnimi podatki direktno posamezniku, ali službi, na katero je ta pošiljka naslovljena.

Delavec, ki je zadolžen za sprejem in evidenco pošte, odpira in pregleduje vse poštne pošiljke in pošiljke, ki na drug način prispejo v LSC GROUP d.o.o. jih prinesejo stranke ali kurirji, razen pošiljk iz tretjega in četrtega 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 LSC GROUP d.o.o.

8. člen

Osebne podatke in občutljive osebne podatke je dovoljeno prenašati z informacijskimi, telekomunikacijskimi in drugimi sredstvi le ob izvajanju postopkov in ukrepov, ki nepooblaščenim preprečujejo prilaščanje ali uničenje podatkov ter neupravičeno seznanjanje z njihovo vsebino (ustrezne kriptografske metode in zaščita z gesli).

Občutljivi osebni podatki se v fizični obliki pošiljajo naslovnikom v zaprtih ovojnicah proti podpisu v dostavni knjigi ali z vročilnico. 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.

9. člen

Obdelava občutljivih osebnih podatkov mora biti posebej označena in zavarovana skladno z ***Politike varovanja informacij*** (ISO 27001).

Podatki iz prejšnjega odstavka se smejo posredovati preko telekomunikacijskih omrežij samo, če so posebej zavarovani s kriptografskimi metodami in tako, da je zagotovljena nečitljivost podatkov med njihovim prenosom.

10. člen

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

Za vsako posredovanje osebnih podatkov mora upravičenec vložiti pisno vlogo, v kateri mora biti jasno navedena določba zakona, ki uporabnika pooblašča za pridobitev osebnih podatkov, ali pa mora k vlogi priložena pisna zahteva oziroma privolitev posameznika, na katerega se podatki nanašajo.

Vsako posredovanje osebnih podatkov se beleži v evidenco posredovanj, iz katere mora biti razvidno, kateri osebni podatki so bili posredovani, komu, kdaj in na kakšni podlagi (41. člen ZVOP-2).

VI. BRISANJE PODATKOV

11. člen

Osebni podatki se shranjujejo le toliko časa, dokler je potrebno za dosego namena, po izpolnitvi namena obdelave se osebni podatki izbrišejo, uničijo, blokirajo ali anonimizirajo, če niso na podlagi zakona, ki ureja arhivsko gradivo opredeljeni kot arhivsko gradivo oziroma, če zakon za posamezne vrste osebnih podatkov ne določa drugače.

Roki, po katerih se osebni podatki izbrišejo iz zbirke podatkov, so razvidni iz dokumenta ***Katalog zbirk osebnih podatkov*** (sedma alineja v tabeli 2. Podatki o zbirki osebnih podatkov – Rok hrambe).

12. člen

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

Podatki na klasičnih medijih (listine, kartoteke, ipd.) se uničijo na način, ki onemogoča branje vseh ali dela uničenih podatkov. Na enak način se uničuje pomožno gradivo (npr. potrdila o ogledu, naročilnica o ogledu, ipd.).

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 direktor ali od njega pisno pooblaščena oseba, ki o uničenju sestavi tudi ustrezen zapisnik.

VII. UKREPANJE OB SUMU NEPOOBLAŠČENEGA DOSTOPA

13. člen

Zaposleni so dolžni o aktivnostih, ki so povezane z odkrivanjem ali nepooblaščenim uničenjem zaupnih podatkov, zlonamerni ali nepooblaščeni uporabi, prilaščanju, spreminjanju ali poškodovanju takoj obvestiti pooblaščeno osebo ali predstojnika, sami pa poskušajo takšno aktivnost preprečiti.

V primeru kršitve varstva osebnih podatkov upravljavec brez nepotrebnega odlašanja, po možnosti pa najpozneje v 72 urah po seznanitvi s kršitvijo, o njej uradno obvesti pristojni nadzorni organ, razen, če ni verjetno, da bi bile s kršitvijo varstva osebnih podatkov ogrožene pravice in svoboščine posameznikov. Kadar uradno obvestilo nadzornemu organu ni podano v 72 urah, se mu priloži navedbo razlogov za zamudo.

VIII. ODGOVORNOST ZA IZVAJANJE VARNOSTNIH UKREPOV IN POSTOPKOV

14. člen

Za nadzor nad izvajanjem postopkov in ukrepov za zavarovanje osebnih podatkov je odgovoren direktor družbe, ki lahko za posamezne naloge pooblasti druge osebe, ki niso zaposlene pri družbi.

Nadzor iz 1. odstavka tega člena vključuje tudi postopke rednega testiranja, ocenjevanja in vrednotenja učinkovitosti tehničnih in organizacijskih ukrepov za zagotavljanje varnosti obdelave. Pri tem so dolžni sodelovati vsi zaposleni in druge osebe v družbi.

15. člen

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

Pred nastopom dela na delovno mesto, kjer se obdelujejo osebni podatki, mora zaposleni podpisati posebno izjavo, ki ga zavezuje k varovanju osebnih podatkov. Izjava je lahko tudi del pogodbe o zaposlitvi.

Iz podpisane izjave mora biti razvidno, da je podpisnik seznanjen z določbami tega pravilnika ter določbami GDPR in vsakokrat veljavnega zakona o varstvu osebnih podatkov, izjava pa mora vsebovati tudi pouk o posledicah kršitve.

16. člen

Za kršitev določil iz prejšnjega člena so zaposleni disciplinsko odgovorni, ostali pa na temelju pogodbenih obveznosti.

IX. KONČNE DOLOČBE

17. člen

Ta pravilnik velja in se uporablja od 20.3.2024 naprej.

18. člen

Ta pravilnik se nahaja v dokumentnem sistemu podjetja, vsem zaposlenim pa je na vpogled tudi pri vodstvu podjetja.