PRAVILNIK
o varovanju osebnih podatkov

I. SPLOŠNE DOLOČBE

1. člen

S tem pravilnikom se določajo organizacijski, tehnični in logično-tehnični postopki in ukrepi za zavarovanje osebnih podatkov v podjetju GRAD d.d z namenom, da se prepreči slučajno ali namerno nepooblaščeno uničevanje podatkov, njihovo spremembo ali izgubo kakor tudi nepooblaščen dostop, obdelava, uporaba ali posredovanje osebnih podatkov.

Zaposleni, ki pri svojem delu obdelujejo in uporabljajo osebne podatke, morajo biti seznanjeni z Zakonom o varstvu osebnih podatkov, s področno zakonodajo, ki ureja posamezno področje njihovega dela ter z vsebino tega pravilnika.

2. člen

V tem pravilniku uporabljeni izrazi imajo naslednji pomen:

1. **Osebni podatek** - pomeni katero koli informacijo v zvezi z določenim ali določljivim posameznikom (v nadaljnjem besedilu: posameznik, na katerega se nanašajo osebni podatki); 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;
2. **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;
3. **Zbirka osebnih podatkov** - 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;
4. **Obdelava osebnih podatkov** - 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;
5. **Upravljavec osebnih podatkov** - pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki samo ali skupaj z drugimi določa namene in sredstva obdelave;
6. **Občutljivi osebni podatki** oz. posebna vrsta osebnih podatkov - so podatki o rasnem narodnem ali narodnostnem poreklu, političnem, verskem filozofskem prepričanju, članstvu v sindikatu, zdravstvenem stanju, spolnem življenju, vpisu ali izbrisu v ali iz kazenske evidence ali prekrškovne evidence ter biometrične značilnosti;
7. **Uporabnik osebnih podatkov** - pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki samo ali skupaj z drugimi določa namene in sredstva obdelave;

8. **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.);
9. **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;

3. člen

Opis zbirk osebnih podatkov, katerih upravljavec je GRAD d.d. , se vodi v katalogu zbirk osebnih podatkov (opisu zbirk osebnih podatkov).

Zaposleni, ki obdelujejo osebne podatke, morejo biti seznanjeni s katalogom zbirk osebnih podatkov, vpogled v katalog zbirk osebnih podatkov pa je potrebno omogočiti tudi vsakomur, ki to zahteva.

GRAD d.d. v matriki Odgovornosti in usposobljenosti vodi 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 osebe, ki je odgovorna za zbirko osebnih podatkov ter osebno ime oseb, ki lahko zaradi narave njihovega dela obdelujejo osebne podatke, ki se nanašajo na zbirko osebnih podatkov.

II. VAROVANJE PROSTOROV IN RAČUNALNIŠKE OPREME

4. člen

Prostori, v katerih se nahajajo nosilci osebnih podatkov, strojna in programska oprema (varovani prostori), morajo biti varovani z organizacijskimi ter fizičnimi in/ali tehničnimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov.

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

Izven delovnega časa morajo biti omare in pisalne mize z nosilci osebnih podatkov zaklenjene, računalniki in druga strojna oprema pa programsko zaklenjeni.

Zaposleni ne smejo puščati nosilcev osebnih podatkov na mizah v prisotnosti oseb, ki nimajo pravice vpogleda vanje.

Občutljivi osebni podatki se ne smejo hraniti izven varovanih prostorov.

5. člen

V prostorih, ki so namenjeni poslovanju s strankami, morajo biti nosilci podatkov in računalniški prikazovalniki nameščeni tako, da stranke nimajo vpogleda vanje.

6. člen

Vzdrževanje in popravila strojne računalniške in druge opreme opravljajo serviserji GRAD d.d. sami, izjemoma je popravilo dovoljeno z vednostjo pooblaščene osebe, izvajajo pa ga lahko samo pooblaščeni servisi in vzdrževalci.

7. člen

Pogodbeni izvajalci del, kot so čistilke, varnostniki idr., se lahko izven delovnega časa gibljejo samo v tistih varovanih prostorih, kjer je onemogočen vpogled v osebne podatke (nosilci podatkov so shranjeni v zaklenjenih omarah in pisalnih mizah, računalniki in druga strojna oprema so izklopljeni ali kako drugače fizično ali programsko zaklenjeni).

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

8. člen

Dostop do programske opreme mora biti varovan tako, da dovoljuje dostop samo za to v naprej določenim zaposlenim.

9. člen

Ker GRAD d.d. uporablja programsko opremo lastne izdelave, lahko servis in dopolnjevanje sistemske in aplikativne programske opreme izvajajo posamezniki, ki so zaposleni v podjetju.

10. člen

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

11. člen

Vsebina diskov mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo osebni podatki, se sprotno preverja glede na prisotnost računalniških virusov. Ob pojavu računalniškega virusa se tega čimprej odpravi s pomočjo ustrezne strokovne službe GRAD d.d, obenem pa se ugotovi vzrok pojava virusa v računalniškem informacijskem sistemu GRAD d.d. .

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

12. člen

Dostop do podatkov preko aplikativne programske opreme se varuje s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov in podatkov.
Pooblaščena oseba določi režim dodeljevanja hranjenja in spreminjanja gesel. Pooblaščena oseba je opredeljena v matriki Odgovornosti in usposobljenosti.

13. člen

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

Te kopije se hranijo v zato določenih mestih, ki morajo biti ognjevarna, zavarovana proti poplavam in elektromagnetnim motnjam, v okviru predpisanih klimatskih pogojev ter zaklenjena.

IV. SPREJEM IN POSREDOVANJE OSEBNIH PODATKOV

14. člen

Delavec, ki je zadolžen za sprejem in evidenco pošte, odpira in pregleduje vse poštne pošiljke in pošiljke, ki na drug način prispejo v podjetje - prinesejo jih stranke ali kurirji, ali prispejo v podjetje na elektronski naslov info@grad.si.

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.

Vse pošiljke, naslovljene na GRAD d.d. so uradna pošta podjetja, ne glede na dodano osebno ime delavca.

15. člen

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.

Osebni podatki se pošiljajo priporočeno.

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.

16. člen

Podatki iz prejšnjega odstavka se smejo posredovati preko telekomunikacijskih omrežij.

17. 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.

Nikoli se ne posredujejo originali dokumentov, razen v primeru pisne odredbe sodišča. Originalni dokument se mora v času odsotnosti nadomestiti s kopijo.

V. BRISANJE PODATKOV

18. člen

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

19. 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, register, seznam, ...) se uničijo na način, ki onemogoča čitanje vseh ali dela uničenih podatkov.

VI. UKREPANJE OB SUMU NEPOOBLAŠČENEGA DOSTOPA

20. 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.

VII. ODGOVORNOST ZA IZVAJANJE VARNOSTNIH UKREPOV IN POSTOPKOV

21. člen

Za izvajanje postopkov in ukrepov za zavarovanje osebnih podatkov so odgovorni vodje organizacijskih enot in pooblaščene osebe, ki jih imenuje direktor GRAD d.d.

Nadzor nad izvajanjem postopkov in ukrepov, določenih s tem pravilnikom, opravlja oseba, določena v matriki Odgovornosti in usposobljenosti.

22. 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.

Varovanje osebnih podatkov, njihovo nerazkrivanju in kazenska odgovornost so opredeljeni v individualni Pogodbi o zaposlitvi, ki jo podpiše vsak zaposleni delavec.

23. člen

Osebne podatke, ki jih GRAD d.d. prejme od pogodbenih strank (strank, ki imajo s podjetjem GRAD d.d. podpisano pogodbo o vzdrževanju programske opreme) GRAD d.d. obdeluje le toliko in le tiste vrste osebnih podatkov, kot je sorazmerno glede na zakonit namen obdelave in namen krovne pogodbe.
V skladu s Splošno uredbo o varstvu podatkov (EU 2016/679) GRAD d.d. kot pogodbeni obdelovalec s tem pravilnikom upravljavcu osebnih podatkov zagotavlja tako varovanje osebnih podatkov, da se preprečuje slučajno ali namerno nepooblaščeno uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščena obdelava tako, da se:

- Varujejo prostori, oprema in sistemska programska oprema
- Varuje aplikativna programska oprema, s katero se osebni podatki obdelujejo
- Preprečuje nepooblaščen dostop do osebnih podatkov ter njihovem prenosu
- Zagotavlja učinkovit način uničenja ali izbrisa osebnih podatkov po prenehanju dejavnosti obdelave
- Omogoča poznejše ugotavljanje, kdaj so bili posamezni podatki obdelovani in kdo je to storil.

GRAD d.d. v matriki Odgovornosti in usposobljenosti vodi seznam, iz katerega je jasno razvidno, katera oseba ima dostop do osebnih podatkov pridobljenih od pogodbenih strank ter katere osebe lahko zaradi narave svojega dela obdelujejo osebne podatke.

24. člen

Za kršitev določil iz prejšnjega člena so zaposleni disciplinsko odgovorni in odgovorni na temelju pogodbenih obveznosti.

VIII. KONČNE DOLOČBE:

25. člen

Ta pravilnik prične veljati 24.5.2018

Direktor:
Tomaž Kukovec

V Ljubljani, 1.3.2018