PRAVILNIK O POSTOPKIH IN UKREPIH ZA ZAVAROVANJE OSEBNIH PODATKOV

Verzija dokumenta : 1.0.

Datum veljavnosti : od 25.5.2018

Skrbnik dokumenta : Jerica Lebar

Zgodovina dokumenta

Verzija dokumenta	Status	Bistvene spremembe glede na prejšnjo verzijo	Datum začetka veljave
1.0.	Končna		25.5.2018

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 (Uradni list RS, v nadaljevanju: ZVOP-2) izdaja zakonita zastopnica podjetja Jerica Lebar s.p.

I. Splošne določbe

1. ČLEN

S tem pravilnikom se določajo organizacijski, tehnični in logično-tehnični postopki in ukrepi za zavarovanje osebnih podatkov v družbi Jerica Lebar s.p.

z namenom, da se zagotovi, da:

- so osebni podatki obdelani zakonito, pošteno in na pregleden način;
- so osebni podatki zbrani za določene, izrecne in zakonite namene, in se ne obdelujejo na način, ki ni združljiv s temi nameni;
- se privzeto obdelajo samo osebni podatki, ki so potrebni za vsak poseben namen obdelave; ta obveznost velja za količino zbranih osebnih podatkov, obseg njihove obdelave, obdobje njihove hrambe in njihovo dostopnost;
- se spoštujejo in zaščitijo pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki;
- se zagotovi varnost osebnih podatkov, vključno z zaščito pred nedovoljeno ali nezakonito obdelavo ter pred nenamerno izgubo, uničenjem ali poškodbo;
- lahko družba dokaže skladnost z zakonodajo s področja varstva osebnih podatkov.

Določbe tega pravilnika veljajo tudi za druge osebe, ki v družbi opravljajo delo na podlagi pogodb, ki niso pogodbe o zaposlitvi.

V primeru dvoma glede pomena katere izmed določb tega dokumenta se obrnite na Jerico Lebar.

2. ČLEN

V tem pravilniku uporabljeni izrazi imajo naslednji pomen:

1. Osebni podatek - je katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen;

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 – 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;

4. 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, priklica, 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);

5. 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;

6. Občutljivi osebni podatki – 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 – je fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki se ji posredujejo ali razkrijejo osebni podatki;

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. Zaposleni - pomeni osebe, ki imajo z družbo sklenjeno pogodbo o zaposlitvi, osebe, ki opravljajo delo v družbi kot dijaki ali študenti, osebe, ki opravljajo delo v družbi na podlagi pogodbe med družbo in njihovim delodajalcem, ki opravlja dejavnost zagotavljanja dela drugim delodajalcem, ter osebe, ki opravljajo delo za družbo na podlagi pogodb civilnega prava;

10. Varnostni incident - 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;

11. Poslovna skrivnost - so podatki, ki so označeni z oznako zaupnosti v skladu z Zakonom o gospodarskih družbah.

3. ČLEN[1]

Družba vodi in vzdržuje evidenco dejavnosti obdelave osebnih podatkov s predpisani sestavinami, skladno z določbo 30. člena GDPR.
Evidenca dejavnosti obdelave se vodi v elektronski obliki, dostop je na poslovnem računalniku.

4. ČLEN

V družbi oziroma za potrebe družbe se lahko obdelujejo le tisti osebni podatki, za katere obstaja ustrezna pravna podlaga po določbah GDPR ali druge zakonodaje. Če pravna podlaga za obdelavo ne obstaja, je potrebno osebne podatke takoj prenehati aktivno obdelovati in onemogočiti dostop do njih.

Osebni podatki se smejo zbirati samo za določene in zakonite namene ter se ne smejo nadalje obdelovati tako, da bi bila njihova obdelava v neskladju s temi nameni, če zakon ne določa drugače. Kadar namerava družba nadalje obdelovati osebne podatke za namen, ki ni namen, za katerega so bili osebni podatki zbrani, je potrebno predhodno preveriti, ali je nov namen združljiv s prvotnim in izdelati o tem pisno poročilo.

Ukrepe za zagotovitev varnosti konkretnih (zbirk) osebnih podatkov, kot so med drugim psevdonimizacija in šifriranje, omejitev roka hrambe in dostopa, omejitev obdelave, omejitev namenov ipd., ter način izvedbe določi Jerica Lebar.

Posebne vrste osebnih podatkov se lahko obdelujejo le v skladu z določbami GDPR in druge zakonodaje. Pri obdelavi morajo biti ti podatki posebej označeni in zavarovani tako, da se nepooblaščenim osebam onemogoči dostop do njih.

O obdelavi osebnih podatkov mora biti posameznik obveščen v skladu z določbami 12., 13. in 14. člena GDPR.

Pooblaščeni obdelovalci morajo biti pred obdelavo osebnih podatkov seznanjeni z določbami GDPR ter z vsebino tega pravilnika, o čemer so dolžni podpisati posebno izjavo: Dodatek k pogodbi. Upravljalec-obdelovalec osebnih podatkov.

5. ČLEN

Posameznik ima pravico od družbe dobiti potrditev, ali se obdelujejo njegovi osebni podatki, in če se, pravico dobiti dostop do osebnih podatkov (vpogled) in informacije iz 1. odstavka 15. člena GDPR.

Posameznik ima pravico doseči, da družba brez nepotrebnega odlašanja popravi netočne oziroma dopolni nepopolne osebne podatke v zvezi z njim.

Posameznik ima pravico doseči, da družba brez nepotrebnega odlašanja izbriše osebne podatke v zvezi z njim, kadar velja eden od naslednjih razlogov:

- osebni podatki niso več potrebni v namene, za katere so bili zbrani ali kako drugače obdelani;
- posameznik prekliče privolitev, na podlagi katere poteka obdelava in za obdelavo ne obstaja nobena druga pravna podlaga;
- posameznik obdelavi ugovarja, za njihovo obdelavo pa ne obstajajo nobeni prevladujoči zakoniti razlogi;
- osebni podatki so bili obdelani nezakonito;
- osebne podatke je treba izbrisati za izpolnitev pravne obveznosti zaradi izpolnitve zakonskih obveznosti;
- osebni podatki so bili zbrani v zvezi s ponudbo storitev informacijske družbe od mladoletnega posameznika.

Posameznik ima pravico doseči, da družba omeji obdelavo, kadar velja en od naslednjih primerov:

- posameznik oporeka točnosti podatkov, in sicer za obdobje, ki družbi omogoča preveriti točnost osebnih podatkov;
- je obdelava nezakonita in posameznik nasprotuje izbrisu osebnih podatkov ter namesto tega zahteva omejitev njihove uporabe;
- družba osebnih podatkov ne potrebuje več za namene obdelave, temveč jih posameznik potrebuje za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov;
- je posameznik vložil ugovor v zvezi z obdelavo, dokler se ne preveri, ali zakoniti razlogi upravljavca prevladajo nad razlogi posameznika, na katerega se nanašajo osebni podatki.

Posameznik ima pravico, da prejme osebne podatke ki jih je posredoval družbi, v strukturirani, splošno uporabljani in strojno berljivi obliki, in pravico, da te podatke posreduje drugemu upravljavcu, ne da bi ga družba pri tem ovirala, kadar:

- obdelava temelji na privolitvi in
- se obdelava izvaja z avtomatiziranimi sredstvi.

Zastopnica podjetja je dolžna poskrbeti za to, da so posamezniki na primeren način, ki je skladen z zahtevami GDPR, obveščeni o pravicah iz prejšnjih odstavkov tega člena. Zastopnica podjetja tudi poskrbi za enotno kontaktno točko, na katero se lahko obrnejo posamezniki pri uveljavljanju svojih pravic.

6. ČLEN

Osebni podatki se na zahtevo uporabnika posredujejo samo tistim uporabnikom, ki se izkažejo z ustrezno zakonsko 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 zakonsko podlago.

Posredovanje osebnih podatkov iz prvega odstavka tega člena lahko uporabnik zahteva pisno ali ustno. Ob vložitvi pisne vloge mora uporabnik jasno navesti določbo zakona, ki ga pooblašča za pridobitev osebnih podatkov, ali pa mora k vlogi priložiti pisno zahtevo oziroma privolitev posameznika, na katerega se podatki nanašajo. Če uporabnik zahteva posredovanje osebnih podatkov ustno, sme odgovorna oseba ali pooblaščeni obdelovalec v primeru dvoma o obstoju pisne zahteve oziroma privolitve posameznika, na katerega se podatki nanašajo, od uporabnika zahtevati, naj jih predloži.

Posredovanje občutljivih osebnih podatkov iz prvega odstavka tega člena lahko uporabnik zahteva le pisno. Pisna vloga mora biti po vsebini enaka pisni vlogi iz prejšnjega odstavka.

Osebni podatki, ki se posredujejo uporabniku v fizični obliki, morajo biti posredovani v skladu z določbami predpisov, ki urejajo upravno poslovanje z dokumentarnim gradivom, oziroma v ovojnici, ki ne omogoča, da bi bila ob normalni svetlobi ali pri osvetlitvi ovojnice z običajno lučjo vidna vsebina ovojnice. Ovojnica mora tudi zagotoviti, da odprtja ovojnice in seznanitve z njeno vsebino ni mogoče opraviti brez vidne sledi odpiranja ovojnice.

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

Občutljive osebne podatke je dovoljeno posredovati preko komunikacijskih omrežij samo, če so posebej zavarovani s kriptografskimi metodami in elektronskim podpisom tako, da je zagotovljena nečitljivost podatkov med njihovim prenosom.

Originalni dokument, ki vsebuje osebne podatke, se lahko posreduje uporabniku samo na podlagi pisne odredbe sodišča. Posredovani originalni dokument mora biti v času odsotnosti nadomeščen s fizično (fotokopijo) ali elektronsko (skenirano) kopijo.

II. Varovanje prostorov in računalniške opreme

7. 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.

Dostop je mogoč le v rednem delovnem času, izven tega časa pa samo na podlagi dovoljenja.

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.

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

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

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

Občutljivi osebni podatki se ne smejo hraniti izven varovanih prostorov.

Zaposleni, ki pri svojem delu uporablja osebne podatke ali jih kakorkoli obdeluje, ne sme med delovnim časom nenadzorovano puščati nosilcev osebnih podatkov na pisalni mizi ali jih kako drugače izpostavljati nevarnosti, da bi nepooblaščene osebe dobile vpogled v osebne podatke.

Ključe, kartice, gesla in ostala sredstva, ki omogočajo dostop do varovanih prostorov, je treba varovati, upravljati in hraniti vestno in skrbno. Vsako izgubo ali odtujitev ali sum o zlorabi, mora zaposleni takoj sporočiti.

8. ČLEN

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

9. ČLEN

Vzdrževanje in popravila strojne računalniške in druge opreme je dovoljeno samo z vednostjo pooblaščene osebe, izvajajo pa ga lahko samo pooblaščeni servisi in vzdrževalci.

10. ČLEN

Vzdrževalci prostorov, strojne in programske opreme, obiskovalci in poslovni partnerji se smejo gibati v zavarovanih prostorih samo z vednostjo pooblaščene osebe. Zaposleni, 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

11. ČLEN

Dostop do programske opreme mora biti varovan tako, da dovoljuje dostop samo za to v naprej določenim zaposlenim ali pravnim ali fizičnim osebam, ki v skladu z naročilom opravljajo dogovorjene storitve.

12. ČLEN

Popravljanje, spreminjanje in dopolnjevanje sistemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve pooblaščene osebe, izvajajo pa ga lahko samo pooblaščeni servisi in organizacije in posamezniki.

13. ČLEN

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

14. 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, obenem pa se ugotovi vzrok pojava virusa v računalniškem informacijskem.

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

15. ČLEN

Zaposleni ne smejo inštalirati programske opreme brez vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema. Prav tako ne smejo odnašati programske opreme iz poslovnih prostorov brez dovoljenja.

16. ČLEN

Pristop do 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 vneseni v zbirko podatkov, uporabljeni ali drugače obdelovani ter kdo je to storil.

17. ČLEN

Vsa gesla in postopki, ki se uporabljajo za vstop in administriranje mreže osebnih računalnikov (supervisorska oziroma nadzorna gesla), administriranje elektronske pošte in administriranje aplikativnih programov se hranijo v zapečatenih ovojnicah in se jih varuje pred dostopom nepooblaščenih oseb. Uporabi se jih samo v izrednih okoliščinah oziroma ob nujnih primerih.

18. ČLEN

Osebni podatki se lahko zgolj izjemoma, kadar je to glede na naravo dela nujno potrebno, shranjujejo in obdelujejo lokalno (na lokalnih računalnikih in drugih podobnih napravah). Po prenehanju potrebe po takem shranjevanju in obdelavi osebnih podatkov, se morajo osebni podatki prenesti v centralizirane baze podatkov ali pa se trajno izbrisati.

Morebitne kopije vsebin zbirk osebnih podatkov na lokalnih nosilcih (zunanji diski, USB-ključi in drugo) se hranijo v zaklenjenih omarah.

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. Storitve, ki jih opravljajo zunanje pravne ali fizične osebe

19. ČLEN

Z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezna opravila v zvezi z zbiranjem, obdelovanjem, shranjevanjem ali posredovanjem osebnih podatkov in je registrirana za opravljanje takšne dejavnosti (pogodbeni oziroma naročeni obdelovalec), se sklene pisna pogodba, predvidena v drugem odstavku 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 pod pogodbenih obdelovalcev, vključno z njihovimi nazivi in sedeži.

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

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

Pooblaščena pravna ali fizična oseba, ki za družbo Jerica Lebar s.p. opravlja dogovorjene storitve izven prostorov upravljavca, mora imeti vsaj enako strog način varovanja osebnih podatkov, kot ga predvideva ta pravilnik.

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 pod pogodbenih obdelovalcev družbi ne sme zaračunati.

V. Sprejem in posredovanje osebnih podatkov

20. ČLEN

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

Oseba, ki je zadolžena za sprejem in evidenco pošte, odpira in pregleduje vse poštne pošiljke in pošiljke, ki na drug način prispejo v upravni organ prinesejo jih stranke ali kurirji, razen pošiljk iz tretjega in četrtega odstavka tega člena.

Oseba, ki je zadolžena 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.

Oseba, ki je zadolžena 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 upravnega organa.

21. 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.

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

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.

22. ČLEN

Obdelava občutljivih osebnih podatkov mora biti posebej označena in zavarovana.

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

23. 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.

V primeru pridobivanja in posredovanja osebnih podatkov med organi javne uprave, je potrebno upoštevati tudi določbe uredbe o, ki ureja upravno poslovanje.

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

VI. Brisanje podatkov

24. ČLEN

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

O izbrisu, uničenju ali anonimizaciji osebnih podatkov odloči zakonita zastopnica podjetja. O uničenju, izbrisu ali anonimizaciji osebnih podatkov se napravi zapisnik, ki ne sme vsebovati osebnih podatkov posameznikov, katerih podatki so se izbrisali, uničili ali anonimizirali.

25. 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 branje vseh ali dela uničenih podatkov. Točen način uničenja za posamezne tipe osebnih podatkov ali nosilcev določi direktor družbe.

Na enak način se uničuje pomožno gradivo (npr. matrice, izračune in grafikone, skice, poskusne oziroma neuspešne izpise ipd.).

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.

VII. Ukrepanje ob varnostnih incidentih v zvezi z osebnimi podatki

26. ČLEN

Zaposleni so dolžni izvajati ukrepe za preprečevanje zlorabe osebnih podatkov in morajo z osebnimi podatki, s katerimi se seznanijo pri svojem delu, ravnati vestno in skrbno na način in po postopkih, ki jih določa ta pravilnik.

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.

Direktor družbe mora ob vsakem sumu kršitve varstva osebnih podatkov takšno kršitev sporočiti Informacijskemu pooblaščencu v 72 urah. Kadar je verjetno, da kršitev varstva osebnih podatkov povzroči veliko tveganje za pravice in svoboščine posameznikov, mora direktor družbe poskrbeti za to, da so prizadeti posamezniki brez nepotrebnega odlašanja obveščeni o tem, da je prišlo do kršitve varstva osebnih podatkov.

27. ČLEN

Zakonita zastopnica podjetja je dolžna poskrbeti za to, da se po varnostnem incidentu opravi analiza vzrokov in predlog ukrepov, ki naj zmanjšajo ali izničijo tveganje za take in bodoče varnostne incidente, ter da se, če je to smiselno in mogoče, predlagani ukrepi tudi izvedejo.

VIII. Odgovornost za izvajanje varnostnih ukrepov in postopkov

28. ČLEN

Za izvajanje postopkov in ukrepov za zavarovanje osebnih podatkov je odgovorna zakonita zastopnica podjetja in pooblaščene osebe, ki niso zaposlene v 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 podjetju.

29. 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.

Iz podpisane izjave mora biti razvidno, da je podpisnik seznanjen z določbami tega pravilnika ter določbami. Splošne uredbe o varstvu podatkov, izjava pa mora vsebovati tudi pouk o posledicah kršitve.

30. ČLEN

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

IX. Končne določbe

30. ČLEN

Ta pravilnik začne veljati dne 25.5.2018.

Pripravila: Jerica Lebar