IZSEK IZ

PRAVILNIKA O POSTOPKIH IN UKREPIH ZA ZAVAROVANJE OSEBNIH PODATKOV

UVELJAVLJANJE PRAVIC POSAMEZNIKA

4.člen
Temeljna načela v zvezi z zbiranjem in obdelavo osebnih podatkov

Osebni podatki morajo biti obdelani zakonito in v razmerju do posameznika, na katerega se nanašajo, pošteno in na pregleden način (načelo zakonitosti, pravičnosti in preglednosti).

Osebni podatki se lahko zbirajo le za določene, izrecne in zakonite namene ter se ne smejo nadalje obdelovati na način, ki ni združljiv s temi nameni (načelo omejitve namena)

Osebni podatki morajo biti ustrezni, relevantni in omejeni le na tisto, kar je potrebno za namene, za katere se obdelujejo (načelo najmanjšega obsega podatkov).

Osebni podatki morajo biti točni in, kadar je to potrebno, posodobljeni (načelo točnosti in ažurnosti).

Osebni podatki se morajo hraniti v obliki, ki dopušča identifikacijo posameznikov, na katere se nanašajo, le toliko časa, kolikor je potrebno za namene, za katere se osebni podatki obdelujejo; osebni podatki se lahko shranjujejo za daljše obdobje, če bodo obdelani zgolj za namene arhiviranja v javnem interesu, za znanstveno- ali zgodovinsko raziskovalne namene ali statistične namene v skladu z ZVOP-1 in Uredbo (načelo omejitve shranjevanja);

Osebni podatki se lahko obdelujejo na način, ki zagotavlja ustrezno varnost osebnih podatkov, vključno z zaščito pred nedovoljeno ali nezakonito obdelavo ter pred nenamerno izgubo, uničenjem ali poškodbo z ustreznimi tehničnimi ali organizacijskimi ukrepi (načelo celovitosti in zaupnosti).

5. člen
Zbirka osebnih podatkov in njen opis v seznamu zbirk

Če se v družbi z določenim namenom zbirajo in obdelujejo osebni podatki, je potrebno te podatke vključiti v eno izmed zbirk osebnih podatkov. Vsako zbirko osebnih podatkov je potrebno opisati v seznamu zbirk osebnih podatkov. Seznam zbirk osebnih podatkov je v prilogi tega pravilnika in je njegov sestavni del.

Posamezna zbirka osebnih podatkov vključuje vse osebne podatke, ki se zbirajo in obdelujejo z istim namenom, ne glede na pravno podlago za njihovo zbiranje in obdelavo.

Opis zbirke osebnih podatkov v seznamu zbirk vsebuje njeno zaporedno številko, njen naziv, podatke o upravljavcu, pravno podlago za zbiranje in obdelavo osebnih podatkov, kategorije posameznikov, na katere se ti podatki nanašajo, vrste osebnih podatkov, namen obdelave, rok hrambe, morebitne omejitve posameznikov po 30. ali 32.členu ZVOP-1, ali se in če, katerim

uporabnikom se osebni podatki prenašajo, dejstvo, ali se osebni podatki iznašajo v tretjo državo in če se, kam, komu in pravno podlago za iznos, nadalje splošen opis tehničnih in organizacijskih ukrepov za varovanje osebnih podatkov, ali se zbrani osebni podatki povezujejo s kakšnimi drugimi zbirkami iz uradnih evidenc ali javnih knjig ter navedbo, da družba kot upravljavec osebnih podatkov nima zastopnika iz 3.odstavka 5.člena ZVOP-1.

Iz opisa zbirke osebnih podatkov mora biti razvidno, na katerem delovnem mestu je v skladu z internim Pravilnikom o sistemizaciji delovnih mest zaposlen njen skrbnik, oziroma, kakšno funkcijo njen skrbnik v družbi opravlja.

Opis zbirke osebnih podatkov se za vsako posamezno zbirko zagotovi najkasneje 15 dni pred vzpostavitvijo zbirke osebnih podatkov. Opis zbirk osebnih podatkov se dopolnjuje ob vsaki spremembi vrste osebnih podatkov v posamezni zbirki.
Vpogled v seznam zbirk osebnih podatkov z opisi posameznih zbirk je potrebno omogočiti vsakomur, ki to zahteva, najkasneje v roku 15 dni od dneva prejema zahteve.

Seznam zbirk osebnih podatkov, z opisom posameznih zbirk, je javno objavljen na spletnih straneh SDH.

8. člen
Podlaga in namen obdelave osebnih podatkov

Zaradi spoštovanja načela zakonitosti obdelave (prvi odstavek 3.člena tega pravilnika) lahko družba v zbirki osebnih podatkov obdeluje le tiste osebne podatke:

- katerih obdelavo določa zakon ali
- če je obdelava potrebna za izvajanje pogodbe, katere pogodbena stranka je posameznik ali
- če je za obdelavo določenih osebnih podatkov podana privolitev posameznika, na katerega se podatki nanašajo ali
- za druge namene, določene v Uredbi oz. veljavni zakonodaji.

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 (načelo omejitve namena; drugi odstavek 4.člena tega pravilnika).

Občutljive podatke se lahko obdeluje le, če so v družbi na voljo pogoji za posebno zaščito teh podatkov in vzpostavljeni primerni dodatni ukrepi za varstvo pravic, svoboščin in interesov posameznika, na katerega se ti podatki nanašajo. Ali so pogoji za posebno zaščito in dodatni ukrepi zagotovljeni, podata mnenje direktor Oddelka za informacijsko tehnologijo in pooblaščenec za varstvo osebnih podatkov, ki tudi določita način izvajanja dodatnih varnostnih ukrepov.

Če zbiranje in obdelavo osebnih podatkov določa zakon, mora ta določati tudi namen obdelave in vrste osebnih podatkov, ki se obdelujejo, kategorije posameznikov, na katere se nanašajo osebni podatki in rok hrambe.

Če zbiranje in obdelava osebnih podatkov temelji na privolitvi posameznika, mora skrbnik zbirke osebnih podatkov poskrbeti, da je posameznik ob privolitvi seznanjen s pravicami, ki mu gredo po zakonu, Uredbi in tem pravilniku. Skrbnik mora za namene dokazovanja zakonitosti obdelave nadalje poskrbeti, da bo posameznikova privolitev v pisni ali elektronski obliki vsebovana v zbirki ali v prilogi zbirke, katere skrbnik je.

9.člen
Pravice posameznika, na katerega se podatki nanašajo

S tem pravilnikom se posamezniku, na katerega se osebni podatki nanašajo, zagotavljajo vse pravice, ki jih ima v skladu s Poglavjem III Uredbe in III. delom ZVOP-1.

Posameznik, na katerega se osebni podatki nanašajo, se ima pravico seznaniti z vsemi podatki, ki jih o njem zbira in obdeluje družba, z informacijami o virih teh podatkov in metodi obdelave, namenu obdelave in vrsti podatkov ter vsa pojasnila s tem v zvezi.

Pojasnila o načinu uveljavljanja pravic posameznika so dostopna na spletnih straneh SDH. Za komunikacijo je posamezniku na voljo elektronski naslov dpo@sdh.si.

V primeru zahteve po uveljavljanju pravic posameznik SDH-ju pošlje zahtevo na predpisanem obrazcu GDPR_1 (»Zahteva za seznanitev z informacijo, ali Slovenski državni holding d.d. zbira in obdeluje osebne podatke, ki se nanašajo name oziroma na osebo pod mojim skrbništvom«), ki je dostopen na spletnih straneh SDH. Na podlagi izražene zahteve posameznik od SDH, najkasneje v 15 dneh od vložitve formalne zahteve, pridobi potrditev, bodisi o tem, da se njegovi osebni podatki ne zbirajo in ne obdelujejo, bodisi o tem, da se njegovi osebni podatki res zbirajo in obdelujejo.

SDH posamezniku posreduje informacijo, v kateri posamezni zbirki osebnih podatkov se ti podatki vodijo, ne posreduje pa konkretnih podatkov oziroma vsebine podatkov, ki jih o posamezniku oziroma o osebi pod skrbništvom posameznika vsebujejo zbirke osebnih podatkov v upravljanju SDH.

Če se želi posameznik seznaniti s konkretnimi podatki oziroma z vsebino osebnih podatkov, ki se nanašajo nanj oziroma na osebo pod njegovim skrbništvom, posameznik po pridobitvi informacije o številki in naslovu posamezne zbirke podatkov, v kateri so vsebovani takšni podatki, izpolni obrazec GDPR_2. Če želi posameznik v zvezi s konkretnimi podatki, ki jih v posamezni zbirki podatkov o njemu ali o osebi pod njegovim skrbništvom zbira in obdeluje SDH, uveljavljati pravico do izbrisa, popravka ali omenitve njihove obdelave, posreduje zahtevo na obrazcu GDPR_3.

Posameznik lahko po predhodni najavi vpogleda, prepiše ali fotokopira svoje osebne podatke neposredno pri družbi v terminu, ki ga za posamezen primer določi skrbnik v roku 15 dni od dneva prejema zahteve za vpogled, prepis ali fotokopiranje. V tem primeru se skrbnik prepriča o posameznikovi istovetnosti z vpogledom v njegov uradni osebni dokument.

Če skrbnik meni, da ni pogojev za vpogled, prepis ali fotokopiranje po prejšnjem odstavku, zahtevo za izdajo potrdila oziroma za vpogled, prepis ali fotokopiranje zavrne. Skrbnik zbirke o razlogih za zavrnitev v 15 dneh od dneva prejema zahteve pisno obvesti vložnika zahteve in ga opozori na možnost sodnega varstva.

Posameznik, na katerega se osebni podatki nanašajo, ima pravico zahtevati posredovanje izpisa osebnih podatkov, posredovanje seznama uporabnikov, katerim so bili podatki posredovani, skupaj z informacijo kdaj, na kakšni podlagi in za kakšen namen so bili posredovani, kakor tudi posredovanje informacije o virih, na katerih temeljijo zapisi, ki jih o posamezniku vsebuje zbirka osebnih podatkov in informacije o namenu in vrsti osebnih podatkov ter vsa potrebna pojasnila s tem v zvezi.

Skrbnik mu izpis, seznam uporabnikov oziroma druge informacije in pojasnila posreduje na nosilcu osebnih podatkov ali preko informacijskega sistema v skladu s 13. členom tega pravilnika, najkasneje v roku 30 dni od prejema zahteve.

Za pravilen postopek in način posredovanja ter nabor posredovanih podatkov posameznikom, na katere se ti podatki nanašajo, je odgovoren skrbnik zbirke, ki o tem, kdaj, komu ter kateri podatki so bili posredovani in pravno podlago za posredovanje, ustrezno evidentira.

Če posameznik, na katerega se osebni podatki nanašajo, meni, da so ti podatki netočni, nepopolni, neažurni ali da so zbrani in obdelani v nasprotju z zakonom, ali če se ne strinja z obdelavo svojih osebnih podatkov, za katero je predhodno dal privolitev, ima pravico zahtevati njihov izbris, dopolnitev, popravo ali blokiranje oziroma ugovarjati njihovi obdelavi.

O zahtevi za izbris, dopolnitev, popravo ali blokiranje najkasneje v 15 dneh od dneva, ko je zahtevo prejel, odloči skrbnik zbirke, na katero se zahteva nanaša. Če zahtevo zavrne, v 15 dneh pisno obvesti vložnika zahteve o razlogih za zavrnitev in ga pouči o možnosti sodnega varstva.

O ugovoru zoper obdelavo odloči pooblaščenec iz 7.člena tega pravilnika v 15 dneh od dneva, ko je ugovor prejel. Če ugovoru ne ugodi, v 15 dneh pisno obvesti vložnika ugovora in ga pouči o možnosti sodnega varstva oziroma vložitve zahteve pri Informacijskem pooblaščencu.

Vse odgovore na zahteve posameznikov, vezane na vsebino osebnih podatkov, pripravi skrbnik ustrezne zbirke. Pred pošiljanjem odgovorov ali pošiljanjem konkretnih osebnih podatkov posamezniku skrbnik zbirke pridobi predhodno pisno potrditev pooblaščenca za varstvo osebnih podatkov.

Skrbniki so dolžni obveščati pooblaščenca o celotni komunikaciji, vezani na uveljavljanje pravic posameznikov. Pri pooblaščencu se vzpostavi centralna evidenca vseh posredovanih zahtev posameznikov in posredovanih odgovorov.

Vsak naslovnik tega pravilnika, ki prvi pride v neposreden stik s posameznikom, ki želi v zvezi s svojimi osebnimi podatki pri družbi uveljavljati kakšne pravice iz tega člena, mu je dolžan takoj sporočiti kontaktne podatke pooblaščenca iz 7.člena tega pravilnika.

15. člen
Hramba in izbris osebnih podatkov

Osebni podatki se lahko shranjujejo le toliko časa, kolikor je to potrebno zaradi namena, za katerega se zbirajo ali če je tako določeno z zakonom. Rok hrambe osebnih podatkov posamezne zbirke je razviden iz opisa, ki je v prilogi.

Po preteku roka hranjenja se osebni podatki zbrišejo, uničijo, blokirajo ali anonimizirajo, razen če zakon ali drug predpis za posamezne vrste osebnih podatkov ne določa drugače (npr. arhivsko gradivo).

Za brisanje osebnih podatkov zaradi preteka roka njihove hrambe ali zaradi zahteve posameznika, na katerega se nanašajo, se uporabi takšna metoda brisanja, da je onemogočena rekonstrukcija vseh ali dela brisanih podatkov. Nosilci osebnih podatkov se uničijo na način, s katerim se zagotovi, da postane osebni podatek nerazpoznaven in neobnovljiv.

Na način in pod pogoji iz prejšnjega odstavka lahko izbriše oziroma odredi izbris osebnih podatkov le skrbnik zbirke, v kateri se ti podatki zbirajo in obdelujejo.

Za ustrezno hrambo in pravočasen ter ustrezen izbris osebnih podatkov je zadolžen skrbnik zbirke osebnih podatkov.

16.člen
Ukrepanje ob zaznavi sumljivih aktivnosti, nevarnosti ali incidenta

Naslovniki tega pravilnika so dolžni o aktivnostih, ki bi lahko bile povezane z nepooblaščenim razkrivanjem ali nepooblaščenim uničevanjem osebnih podatkov, zlonamerni ali nepooblaščeni uporabi, prilaščanju, spreminjanju ali poškodovanju osebnih podatkov oziroma nosilcev osebnih podatkov (sumljive aktivnosti), takoj obvestiti skrbnika zbirke osebnih podatkov in pooblaščenca.

Naslovniki tega pravilnika so dolžni ob zaznavi kakršnekoli nevarnosti zaradi pomanjkljivosti v sistemu varovanja osebnih podatkov oziroma o tem, da organizacijski, tehnični in logično tehnični ukrepi ali postopki ne zagotavljajo optimalnega zavarovanja osebnih podatkov, takoj obvestiti skrbnika zbirke osebnih podatkov, ki so v nevarnosti. Če nevarnost izvira iz pomanjkljivosti informacijskega sistema, so dolžni takoj obvestiti tudi direktorja Oddelka za informacijsko tehnologijo. Skrbnik oziroma direktor Oddelka za informacijsko tehnologijo sta dolžna nemudoma poskrbeti, da se nevarnost odpravi oz. postopati skladno z določili Krovne politike varovanja informacij in upravljanja z incidenti informacijske varnosti.

Naslovnik tega pravilnika, ki je zaznal kršitev, mora o kršitelju in naravi kršitve takoj obvestiti skrbnika zbirke osebnih podatkov, na katero se kršitev nanaša in pooblaščenca za varstvo osebnih podatkov. Če je kršitelj skrbnik se o tem obvesti pooblaščenca za varstvo osebnih podatkov. Skrbnik oziroma pooblaščenec nemudoma poskrbita, da kršitev preneha.

Če naslovnik tega kodeksa ugotovi, da je prišlo do nenamernega ali nezakonitega uničenja, izgube, spremembe, nepooblaščenega razkritja ali dostopa do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani (incident na področju varovanja osebnih podatkov), o tem takoj obvesti direktorja Oddelka za informacijsko tehnologijo in pooblaščenca za varstvo osebnih podatkov, ki v sodelovanju s skrbnikom zbirke incident obravnavata in nemudoma sprejmeta najbolj nujne ukrepe za preprečitev širitve incidenta. O incidentu pooblaščenec nemudoma obvesti tudi upravo družbe.

V primeru iz prejšnjega odstavka je pooblaščenec dolžan poskrbeti, da je o incidentu najkasneje v 72 urah od njegove zaznave v skladu s 33.členom Uredbe uradno obveščen Informacijski pooblaščenec. Prav tako je pooblaščenec dejstvo, da se je incident zgodil, dolžan sporočiti posamezniku, katerega osebni podatki so bili udeleženi v incidentu, če gre za primer iz 34.člena Uredbe.