Borzen

Nina Planinšek

Pravilnik o varovanju osebnih podatkov

družbe Borzen, d.o.o.

Datum	Različica	Avtor	Opis spremembe
17.01.2007	1.0		Akt o varovanju osebnih podatkov
16.05.2018	2.0	Jani Recer	Posodobitev dokumenta in prenehanje veljavnosti Akta o varovanju osebnih podatkov
05.06.2024	2.1	Jani Recer	Posodobitev dokumenta
17.09.2025	3.0	Nina Planinšek	Posodobitev dokumenta
8.10.2025	3.1	Nina Planinšek	Uskladitev s prejetimi pripombami zaposlenih

Uvod in regulatorni okvir

1. člen (predmet urejanja)

Borzen, d.o.o. (v nadaljevanju: družba) se zavezuje k zakoniti, varni in pregledni obdelavi osebnih podatkov, skladno z veljavno zakonodajo in najboljšimi praksami.

Ta pravilnik je pripravljen 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 ter o razveljavitvi Direktive 95/46/ES v nadaljevanju splošna uredba ali GDPR) in Zakona o varstvu osebnih podatkov (Uradni list RS, št. 163/22 in 40/25 – ZInfV-1, v nadaljevanju ZVOP-2), ki je začel veljati 26. 1. 2023 ter nadomestil ZVOP-1. Splošna uredba določa enotna pravila varstva podatkov v EU, ZVOP-2 pa ureja nacionalne posebnosti, pri čemer se določbe ZVOP-2 razlagajo v skladu s Splošno uredbo.

Poleg zakonskih zahtev družba upošteva tudi standarde ISO/IEC 27001 (sistem upravljanja informacijske varnosti) in ISO/IEC 27701 (razširitev za upravljanje zasebnosti), ki zagotavljajo okvir za neprekinjeno obvladovanje varstva podatkov in podporo skladnosti s splošno uredbo.

S tem pravilnikom družba določa pravila, načela, postopke in varnostne ukrepe za obdelavo osebnih podatkov v svojem poslovanju, s ciljem zaščititi pravice posameznikov in zmanjševanja tveganja obdelave. Ta pravilnik opredeljuje tudi dolžnosti vodstva družbe, pooblaščene osebe za varstvo podatkov, vseh zaposlenih ter zunanjih obdelovalcev.

Družba ima sprejeto tudi Politiko zasebnosti, ki jo redno posodablja in je objavljena na spletni strani.

V kolikor posamezno vprašanje ni urejeno s tem pravilnikom se neposredno uporabljata Splošna uredba ter zakon, ki ureja varstvo osebnih podatkov.

2. člen (opredelitev pojmov)

Terminologija uporabljena v tem pravilniku ima enak pomen kot to določa splošna uredba in ZVOP-2, in sicer:

»Osebni podatek« pomeni katerikoli podatek, ki se nanaša na določeno ali določljivo fizično osebo, torej posameznika, ne glede na obliko, v kateri je izražen. **Posameznik** pa je določena ali določljiva fizična oseba, na katero se nanaša osebni podatek, pri čemer je določljiva, če se jo lahko neposredno ali posredno identificira s pomočjo njenih identifikacijskih številk (npr. EMŠO, davčna številka, številka zdravstvenega zavarovanja, telefonska številka), ali s sklicevanjem na dejavnike, ki so značilni za njeno fizično, fiziološko, duševno, ekonomsko, kulturno ali družbeno identiteto (npr. zaposlitev, naslov, funkcijo, položaj ali status v določenem subjektu, ipd.), pri čemer način identifikacije ne povzroča velikih stroškov, nesorazmerno velikega napora ali ne zahteva veliko časa;

»Obdelava« pomeni vsako vrsto dejavnosti (postopek obdelave), ki se izvaja na osebnih podatkih posameznikov ali z njimi. To vključuje zbiranje, beleženje, urejanje, strukturiranje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, poizvedbo, uporabo, razkritje s posredovanjem, razširjanjem ali drugačno omogočanje dostopa, prilagajanje ali kombiniranje, omejitev, izbris ali uničenje osebnih podatkov.

»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 Evropske unije ali pravo države članice, se lahko upravljavec ali posebna merila za njegovo imenovanje določijo s pravom Evropske unije ali pravom države članice;

»Obdelovalec« pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo tele, ki obdeluje osebne podatke v imenu upravljavca (npr. razvijalec aplikacije za dodeljevanje subvencij, zunanji izvajalec psihometričnih testiranj zaposlenih itd.);

»Zunanji izvajalec« je vsaka pravna ali fizična oseba, ki z družbo nima sklenjene pogodbe o zaposlitvi ali druge delovnopravne pogodbe ter za družbo opravlja posamezna opravila na temelju pogodbe civilnega prava in je registriran za opravljanje taksne dejavnosti (pogodbeni obdelovalec);

»Evidenca dejavnosti obdelav« je evidenca informativne narave, ki je namenjen seznanitvi posameznika, na katerega se nanašajo osebni podatki glede podatkov o upravljavcu, pravni podlagi za obdelavo osebnih podatkov, vrste in namen obdelave osebnih podatkov, rok hrambe ter drugih informacij za uresničevanje pravic posameznika, na katerega se nanašajo osebni podatki;

V primeru neskladja z definicijami pojmov po tem pravilniku ter Splošno uredbo, velja definicija pojmov skladno s Splošno uredbo.

3. člen (umestitev v interne akte družbe)

Ta pravilnik se vsebinsko navezuje na obstoječe interne akte družbe, zato se za vsa ravnanja z osebnimi podatki smiselno uporabljajo ostali pravilniki, in sicer:

- *Pravilnik o klasifikaciji podatkov*
- *Pravilnik o upravljanju varnostnih incidentov*
- *Pravila o upravljanju sprememb*

Smiselno se upoštevajo tudi vsi pravilniki s področja IKT-varnosti.

V primeru, da določeno vprašanje v tem pravilniku ni urejeno, se neposredno uporabljajo določbe Splošne uredbe in veljavnega zakona, ki ureja varstvo osebnih podatkov.

Vsi zaposleni in pogodbeni sodelavci družbe se morajo ravnati po tem pravilniku in ga razumeti kot zavezujoč notranji akt.

Vloge in odgovornosti pri varstvu podatkov

4. člen (odgovorne osebe)

Poslovodstvo družbe nosi odgovornost za skladnost obdelave osebnih podatkov. Vodstvo družbe je dolžno zagotoviti ustrezno podporo in kulturo spoštovanja zasebnosti ter omogočiti pogoje za izvajanje tega pravilnika (npr. zagotavljanje virov, orodij in kadrovskih pogojev). Vodstvo družbe imenuje in podpira pooblaščeno osebo za varstvo podatkov (DPO) ter njenega morebitnega namestnika, odloča o ključnih ukrepih upravljanja podatkov in potrjuje ta pravilnik ter morebitne posodobitve. Prav tako je vodstvo družbe odgovorno za vključitev vidikov varstva podatkov v strategijo in procese družbe ter za obravnavo poročil in priporočil DPO. Pri sprejemanju novih projektov ali sprememb procesov, ki vključujejo osebne podatke, vodstvo zagotovi, da se izvede ocena vpliva na varstvo podatkov (DPIA), kadar je to zahtevano in odobri potrebne ukrepe za zmanjšanje tveganj. S svojo zavezanostjo in aktivno udeležbo vodstvo zagotavlja, da družba izpolnjuje obveznosti upravljavca iz Splošne uredbe in ZVOP-2 ter da je vzpostavljen učinkovit sistem varovanja osebnih podatkov.

5. člen (naloge pooblaščene osebe za varstvo osebnih podatkov DPO)

Družba je skladno s 37. členom Splošne uredbe imenovala pooblaščeno osebo za varstvo osebnih podatkov, ki ima ključno svetovalno in nadzorno vlogo pri zagotavljanju skladnosti z zakonodajo o varstvu podatkov. Njene naloge vključujejo naslednje:

- svetovanje in izobraževanje upravljavca in zaposlenih o njihovih obveznostih po Splošni uredbi, ZVOP-2 in tem pravilniku.
- Nadzor skladnosti postopkov obdelave z veljavnimi predpisi in internimi politikami, vključno z nadzorom spoštovanja načel varstva podatkov ter tehničnih in organizacijskih ukrepov.
- Sodelovanje pri presojah učinkov (DPIA): DPO svetuje pri izvedbi ocen učinka na varstvo podatkov in spremlja izvedbo priporočil.
- Sprejemanje pritožb in uresničevanje pravic posameznikov: DPO je kontaktna točka za posameznike in nadzorni organ (Informacijski pooblaščenec RS) glede vprašanj v zvezi z obdelavo osebnih podatkov. Sprejema in obravnava zahteve posameznikov za uresničevanje njihovih pravic ter sodeluje z nadzornim organom.
- Obveščanje o kršitvah: v primeru incidenta DPO svetuje glede obveznosti priglasitve Informacijskemu pooblaščencu in obveščanja posameznikov ter pregleda vsebino teh obvestil.
- Vodenje evidenc: DPO sodeluje pri vodenju evidenc dejavnosti obdelave in evidenc o kršitvah ter spremlja izvajanje politike varstva osebnih podatkov.

Pooblaščena oseba deluje neodvisno. Pri opravljanju nalog ne sme prejeti navodil, vodstvo pa ji mora omogočiti dostop do vseh potrebnih informacij in virov. DPO redno poroča vodstvu o stanju varstva podatkov in morebitnih tveganjih. Družba zagotavlja, da DPO in njen namestnik vzdržujeta strokovnost (tudi z rednim usposabljanjem s področja varstva podatkov) ter da nista v navzkrižju interesov glede svojih drugih nalog. Imenovanje in kontaktni podatki DPO so objavljeni in dostopni posameznikom, katerih podatke družba upravlja.

6. člen (odgovornost zaposlenih)

Vsi zaposleni, pogodbeni sodelavci in druge osebe, ki pri delu prihajajo v stik z osebnimi podatki, so zavezani k spoštovanju pravilnika in varovanju osebnih podatkov. Družba omejuje dostop do osebnih podatkov le na tiste zaposlene, ki jih potrebujejo za svoje delovne naloge (načelo *"need-to-know"*) - vsakemu takemu zaposlenemu ali pogodbeniku se dodeli status *pooblaščene osebe za obdelavo osebnih podatkov* za določena področja dela. Na področjih, kjer omejitve dostopov zaradi informacijskega sistema družbe niso mogoče, se zagotavlja revizijska sled dostopov in beleži dostopanje do osebnih podatkov. Iz evidence dostopa mora biti razvidno ime, priimek, naziv delovnega mesta, datum in čas vpogleda in razlog.

Pooblaščene osebe za obdelavo osebnih podatkov so odgovorne za zakonito obdelavo in varnost podatkov znotraj svojega delovnega področja, njihova obveza varovanja pa traja tudi po prenehanju delovnega razmerja oziroma sodelovanja z družbo.

Zaposleni so dolžni osebne podatke obdelovati izključno v okviru svojih pooblastil in v skladu z internimi postopki. Prav tako morajo nemudoma poročati DPO ali nadrejenim o vsakršnem incidentu ali sumu kršitve varnosti osebnih podatkov. Incidente oz. kršitve morajo dosledno vnašati v sistem, ki je namenjen evidentiranju kršitev.

Zaposleni morajo sodelovati pri usposabljanjih s področja varstva podatkov in se sproti seznanjati s spremembami politik ter varnostnimi navodili. Neupoštevanje določb tega pravilnika ali malomarno ravnanje z osebnimi podatki lahko vodi v disciplinske ukrepe in odškodninsko ali kazensko odgovornost v skladu z zakonodajo.

7. člen (izjava o zaupnosti)

Vsi zaposleni morajo pred začetkom dela podpisati izjavo o zaupnosti in varovanju osebnih podatkov, s katero se zavežejo k varovanju vseh osebnih podatkov, s katerimi se seznanijo pri delu, ter so seznanjeni s posledicami kršitev te zaveze.

8. člen (podobdelovalci)

Družba lahko pri izvajanju določenih dejavnosti najame pogodbene obdelovalce (npr. ponudnike IT-storitev, kadrovske ali druge svetovalce), ki v imenu družbe obdelujejo osebne podatke.

Pred vključitvijo vsakega obdelovalca družba preveri, ali zagotavlja zadostna jamstva za izvajanje ustreznih tehničnih in organizacijskih ukrepov varstva podatkov.

Vsak skrbnih projekta mora pred oddajo javnega naročila pridobiti mnenje DPO o skladnosti obdelave osebnih podatkov s splošno uredbo, ZVOP-2 in pravili družbe. Pred pridobitvijo mnenja naročila ni dopustno oddati.

Z vsakim obdelovalcem je sklenjena pisna pogodba o obdelavi osebnih podatkov, skladna s 28. členom Splošne uredbe, ki določa namen in obseg obdelave, vrste podatkov, ukrepe za varovanje, obveznost zaupnosti, pomoč obdelovalca pri zagotavljanju pravic posameznikov in izpolnjevanju obveznosti upravljavca ter druge zahteve po Splošni uredbi.

Obdelovalec sme osebne podatke obdelovati le po dokumentiranih navodilih družbe in jih ne sme uporabiti za lastne namene. Družba od obdelovalcev zahteva, da ne smejo uporabljati podobdelovalcev (*sub-processors*) brez predhodnega soglasja in da v primeru podobdelovalcev le-ti zagotavljajo enake varnostne standarde.

Poleg obdelovalcev lahko družba osebne podatke posreduje tudi uporabnikom (npr. državnim organom, partnerjem) v skladu z zakonitim (ali drugim z ZVOP-2 skladnim) namenom - vedno na podlagi pravne podlage in ob ustrezni zavarovanosti prenosa. Vsak tak prenos tretjim osebam se zabeleži v ustrezni evidenci iznosov podatkov izven družbe.

Vsi zunanji prejemniki osebnih podatkov so dolžni varovati prejete podatke in jih obdelovati le v okviru namena, za katerega so bili posredovani, ter skladno z vsemi dogovori in zakonodajo na kar morajo biti izrecno opozorjeni in zavezani.

Načela in postopki obdelave osebnih podatkov

9. člen (načela obdelave podatkov)

Obdelava osebnih podatkov v družbi poteka po vnaprej določenih postopkih, ki pokrivajo celoten življenjski cikel podatkov: od zbiranja in klasifikacije, preko shranjevanja in uporabe, do posredovanja, arhiviranja in končnega izbrisa. V vseh fazah se zagotavlja spoštovanje temeljnih načel varstva podatkov in izvajanje ustreznih ukrepov.

10. člen (zakonitost obdelave)

Vsaka obdelava osebnih podatkov mora imeti zakonito podlago in opredeljen namen. Družba osebne podatke zbira in obdeluje izključno za določne, določljive in zakonite

namene, skladne s pristojnostmi in dejavnostjo družbe, ter jih ne obdeluje na načine, nezdružljive s temi nameni (načelo omejitve namena).

Uporabljajo se le tiste pravne podlage, ki jih dovoljuje 6. člen Splošne uredbe in sicer če;

- je posameznik, na katerega se nanašajo osebni podatki, veljavno privolil v obdelavo njegovih osebnih podatkov,
- je obdelava 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,
- je obdelava potrebna za izpolnitev zakonske obveznosti, ki velja za upravljavca,- je obdelava potrebna za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki. ali druge fizične osebe,
- je obdelava potrebna zaradi uresničevanja upravičenih ter zakonitih interesov, ki so opredeljeni v oceni učinka za varstvo osebnih podatkov ter za katere si prizadeva upravljavec ali tretja oseba, razen kadar nad takimi interesi prevladajo interesi ali človekove pravice in temeljne svoboščine posameznika, na katerega se nanašajo osebni podatki, ki zahtevajo varstvo osebnih podatkov.

Obdelava osebnih podatkov za druge namene kot za tiste, za katere so bili osebni podatki prvotno zbrani, je dovoljena le, kadar ni nezdružljiva z nameni, za katere so bili osebni podatki prvotno zbrani ali kadar to določa zakon.

Pri posebnih vrstah osebnih podatkov (občutljivi podatki, npr. zdravstveni) družba ravna skladno s posebnimi pogoji iz 9. člena Splošne uredbe in relevantnimi določbami ZVOP-2. Obdelava vedno poteka pošteno in pregledno do posameznika – zagotovljeno je ustrezno obveščanje posameznikov o tem, katere podatke družba zbira, v kakšne namene in na kakšni podlagi, ter druge informacije po členih 13 in 14 Splošne uredbe.

Družba se zaveda načela minimalne količine podatkov (*data minimization*) in zbira le tiste osebne podatke, ki so nujni za določeni namen. Podatki morajo biti tudi točni in ažurni - redno se preverjajo in po potrebi popravijo ali dopolnijo, netočni podatki pa izbrišejo oziroma popravijo brez odlašanja. Vsi takšni posegi morajo biti dokumentirani.

Družba izpolnjuje tudi načelo omejitve shranjevanja, kar pomeni, da podatke hrani le toliko časa, kolikor je potrebno za dosego namena oziroma toliko časa, kolikor to zahtevajo predpisi (*glej tudi* politiko hrambe).

Vsi zaposleni morajo upoštevati tudi načeli zaupnosti in integritete, torej varovati podatke pred nepooblaščenim razkritjem ali spremembo, ter načelo odgovornosti, po katerem mora družba biti sposobna dokazati skladnost z omenjenimi načeli.

Z doslednim izvajanjem teh ukrepov lahko družba izkazuje, da je obdelava skladna z vsemi načeli iz 5. člena Splošne uredbe, vključno z zagotavljanjem zaupnosti, celovitosti,

razpoložljivosti in točnosti osebnih podatkov. Če določeno vprašanje glede obdelave s strani tega pravilnika ni urejeno, se neposredno uporabijo pravila iz Splošne uredbe in ZVOP-2.

11. člen (klasifikacija osebnih podatkov)

Družba vzpostavlja in vzdržuje sistem klasifikacije podatkov, ki vključuje tudi kategorizacijo osebnih podatkov glede na občutljivost in kritičnost. Skladno s *Pravilnikom o klasifikaciji podatkov* so vsi podatki, ki jih družba obdeluje, razvrščeni v ustrezne razrede (npr. interno, zaupno, strogo zaupno, tajno). Osebni podatki so običajno označeni vsaj kot zaupni podatki, posebne vrste (občutljivi) osebni podatki pa se lahko opredelijo kot posebej varovani.

Vsaka zbirka ali evidenca osebnih podatkov ima določeno raven zaupnosti, kar narekuje ustrezne varnostne ukrepe pri ravnanju z njo. Klasifikacija omogoča, da se osebne podatke zaščiti sorazmerno z njihovim pomenom: bolj občutljive kategorije (npr. podatki o zdravju, finančni podatki, identifikacijski podatki) so deležne strožjih varnostnih ukrepov in omejitev dostopa.

V internih evidencah dejavnosti obdelave je posebej označeno, če zbirka vsebuje posebne vrste osebnih podatkov. Vsi zaposleni morajo poznati klasifikacijo podatkov in jo upoštevati pri delu - npr. uporabljati primerne načine shranjevanja, šifriranja in prenosa glede na razred podatkov. Klasifikacija se redno pregleduje in posodablja glede na spremembe v predpisih ali dejavnostih družbe.

12. člen (hramba osebnih podatkov)

Družba hrani osebne podatke v varnih zbirkah in arhivih tako v elektronski obliki (informacijski sistemi, baze podatkov) kot v fizični obliki (dokumentacija v papirni obliki), odvisno od narave podatkov. Vsi mediji, kjer se nahajajo osebni podatki (strežniki, delovne postaje, prenosni mediji, papirni nosilci itd.), so zaščiteni s tehničnimi in fizičnimi ukrepi, opisanimi v nadaljevanju in namenskih pravilnikih.

Roki hrambe osebnih podatkov so določeni glede na namen zbiranja in zakonske obveznosti. Za vsako vrsto evidence osebnih podatkov so opredeljeni roki, kako dolgo se posamezni podatki hranijo, oziroma kdaj morajo biti izbrisani. Pri določanju rokov se upoštevajo zahteve specialnih zakonov (npr. področna zakonodaja energetike, delovna zakonodaja), priporočila Informacijskega pooblaščenca ter notranje potrebe (npr. zastaralni roki za pravne zahtevke).

Podatke, za katere je potekel predpisani ali poslovno potrebni rok hrambe, se izbriše ali anonimizira, razen če je z zakonom določeno drugače (npr. arhiviranje gradiva z zgodovinsko vrednostjo). V času hrambe se zagotavlja integriteta in točnost podatkov - podatki so zaščiteni pred nepooblaščenimi spremembami, redno se izvajajo varnostne

kopije (backup) ključnih zbirk in preverjanje celovitosti shranjenih podatkov. Elektronske evidence se hranijo znotraj EU/EGP oziroma v tretjih državah le ob izpolnjevanju pogojev iz poglavja V. Splošne uredbe (*glej tudi* Prenosi podatkov).

Papirni dokumenti z osebnimi podatki se hranijo v zaklenjenih omarah ali varnih prostorih, do katerih imajo dostop le pooblaščene osebe (*glej tudi* ureditev fizične varnosti).

Posebno pozornost je namenjena shranjevanju občutljivih podatkov (npr. šifrirana baza za gesla, ločeno hranjenje biometričnih podatkov ipd.). Vsi nosilci z osebnimi podatki so označeni skladno s klasifikacijo in se z njimi ravna po predpisanih postopkih.

13. člen (izbris in uničenje osebnih podatkov)

Ko preneha potreba po posameznih osebnih podatkih oziroma ko preteče rok hrambe, je treba podatke trajno in varno izbrisati ali uničiti. Izbris elektronskih podatkov se izvaja na način, ki onemogoča obnovitev (npr. prepis podatkov z naključnimi vrednostmi ali uporaba ustreznih orodij za varno brisanje).

V primerih, ko določene podatke zaradi tehnoloških omejitev ni mogoče izbrisati iz sistema (npr. varnostne kopije na neprepisljivih medijih), se zagotovi njihova ustrezna logična izločitev iz uporabe (npr. šifriranje in hranjenje ločeno) do izteka življenjske dobe medija.

Papirno dokumentacijo ali fizične nosilce (CD, USB ključke ipd.), ki vsebujejo osebne podatke in jih ni več dovoljeno hraniti, se uniči na ustrezen način - dokumente se zmelje (uničevalnik dokumentov z ustrezno stopnjo varnosti) ali razreže, nosilce pa fizično uniči ali preda v industrijsko uničenje.

Uničenje občutljivih dokumentov poteka pod nadzorom odgovorne osebe ali DPO, o uničenju pa se vodi evidenca (zapisnik o uničenju z datumom in obsegom uničenega gradiva).

Družba ima tudi utečen postopek uničenja arhivskega gradiva, ki vključuje tudi kategorizacijo, kaj se uniči interno in kaj preko pogodbenih uničevalcev (ki morajo zagotavljati skladnost s Splošno uredbo kot obdelovalci).

Izbris ali uničenje podatkov se izvede brez nepotrebnega odlašanja, ko so izpolnjeni pogoji, da podatkov ni več dopustno hraniti. V zvezi z izbrisom se hrani evidenca izbrisa, ki vključuje najmanj naslednje podatke: podatki, ki so bili izbrisani, datum in čas izbrisa, oseba, ki je izvedla izbris, kje so se podatki nahajali, podatek o morebitnem arhiviranju. V zvezi s fizičnimi dokumenti, ki so bili posredovani v razrez je potrebno evidentirati najmanj naslednje podatke: firma, ki so ji bili dokumenti predani, datum in čas predaje dokumentov in datum in čas razreza dokumentov, kje so se podatki nahajali.

Za določene zbirke (npr. podatki o zaposlenih) lahko obstajajo interni roki rednega pregleda, po katerih se izvajajo izbrisi (npr. enkrat letno). S strogo politiko izbrisa družba zagotavlja spoštovanje pravice do izbrisa (»pravice do pozabe«) posameznikov in zmanjšuje količino shranjenih podatkov na minimalno nujno količino.

14. člen (dostop do osebnih podatkov)

Dostop do osebnih podatkov je dovoljen le pooblaščenim osebam in v obsegu, ki je nujno potreben za opravljanje njihovih delovnih nalog.

Informacijski sistemi družbe so nastavljeni po načelu najmanjših potrebnih pravic (*least privilege*), kar pomeni, da ima vsak uporabnik dodeljene le tiste pravice (dostope), ki jih potrebuje, kar urejajo tudi namenski pravilniki in standardni postopki družbe.

Uporabniški računi in pravice za dostop do zbirk osebnih podatkov so vezani na posameznika; skupinski ali anonimni dostopi niso dovoljeni.

Vsakemu uporabniku se dodeli unikatno uporabniško ime in geslo oziroma drug način avtentikacije za dostop do sistemov, kjer se obdelujejo osebni podatki. Uporabniki so dolžni svoja gesla in certifikate varovati in jih ne smejo deliti. Posojanje gesel med zaposlenimi je prepovedano.

Sistemi zahtevajo močna gesla in njihovo redno menjavo v določenih intervalih ter onemogočajo ponovno uporabo predhodnih gesel.

Vsak dostop do pomembnih informacijskih sistemov je zabeležen (sled dostopa), kar omogoča poznejše preverjanje, kdo je dostopal do katerih podatkov in kdaj. Pravice dostopa se redno pregledujejo - ob organizacijskih spremembah, menjavi delovnih mest ali prenehanju zaposlitve se takoj ukinejo ali prilagodijo dostope (npr. preklic uporabniških računov ob odhodu zaposlenega).

Posebne kategorije osebnih podatkov so lahko dodatno zaščitene z omejitvami dostopa (npr. samo določeni oddelek).

Fizični dostop do prostorov, kjer se hranijo osebni podatki (strežniške sobe, arhivi), je prav tako omejen na pooblaščene uslužbence in varovan.

Če zaposleni ali zunanji sodelavci potrebujejo dostop do osebnih podatkov izven poslovnih prostorov (npr. delo na daljavo), se uporabljajo varni komunikacijski kanali (VPN z večfaktorsko avtentikacijo) ter službene naprave z ustrezno zaščito.

Družba vodi evidenco vseh pooblaščenih oseb za obdelavo (internih in zunanjih), vključno z datumom podelitve in ukinitve posameznih pooblastil ter obsegom podatkov, ki jih lahko obdelujejo.

Vsaka pooblaščena oseba je seznanjena s svojo odgovornostjo varovati podatke, do katerih ima dostop, ta odgovornost pa ostaja tudi po prenehanju njenega delovnega razmerja.

15. člen (posredovanje podatkov izven družbe)

Vsako posredovanje osebnih podatkov izven družbe (bodisi tretjim organizacijam bodisi posameznikom, ki niso zaposleni pri upravljavcu) mora biti strogo nadzorovano in imeti ustrezno pravno podlago.

Osebni podatki se tretjim osebam posredujejo le:

- če tako določa zakon (npr. poročanje predpisanim organom),
- na podlagi pogodbe ali druge pravne osnove (npr. izpolnitev pogodbe s posameznikom zahteva posredovanje podatkov partnerju),
- s privolitvijo posameznika
- v drugih primerih, dovoljenih po Splošni uredbi /ZVOP-2.

Pred posredovanjem se preveri identiteta in pravica prejemnika do prejema podatkov; upravljavec se prepriča, da bo prejemnik podatke uporabil skladno z dogovorjenim namenom in da jih bo ustrezno varoval.

Za vsako redno posredovanje podatkov (npr. posredovanje podatkov o plačah računovodskemu servisu) se dokumentira namen, obseg in prejemnik v *Evidenci dejavnosti obdelave*. Evidenca iznosa podatkov mora vsebovati vsaj naslednje podatke: organ oz. pravno ali fizično osebo, ki so ji bili podatki posredovani, pravno podlago, podatke o pogodbi oz. sporazumu, ki je bil sklenjen z osebo, ki prejema podatke ter lokacijo hrambe le-te, čas in način posredovanja, osebo, ki je podatke posredovala.

Kadar podatke prejema pogodbeni obdelovalec, velja postopek in zahteve iz poglavja *Zunanji obdelovalci* tega pravilnika (pogodba, varnostni ukrepi).

Vsi drugi zunanji prejemniki (t.i. uporabniki v smislu Splošne uredbe), ki prejmejo osebne podatke od družbe (npr. javni organi, partnerji), so praviloma sami upravljavci - odgovorni so, da podatke obdelujejo zakonito in skladno z namenom, zaradi katerega so jim posredovani.

Družba bo posredovala podatke upravičenim uporabnikom le ob predložitvi ustrezne pravne podlage ali dokaza o zakonitem interesu. Pri posredovanju podatkov organom (npr. sodišču, policiji) se vedno preveri uradna zahteva ali pravna obveznost za izročitev podatkov, izvede pa se prenos na varen način in vodi zapis o posredovanju (kaj je bilo posredovano, komu, kdaj).

Osebnih podatkov se ne prenaša v države izven EU/EGP, razen če so izpolnjeni pogoji iz poglavja V. Splošne uredbe. To pomeni, da mora EU za državo uvoznico priznati

ustrezno raven varstva (*ustrezna odločba* Evropske komisije), ali pa morajo biti vzpostavljeni drugi zaščitni mehanizmi (npr. standardne pogodbene klavzule, zavezujoča poslovna pravila, certifikati). Družba pred vsakim takim prenosom oceni morebitna tveganja za pravice posameznikov in zagotovi dodatne ukrepe, če je potrebno (npr. šifriranje podatkov med prenosom in pri hrambi pri prejemniku). Posameznike se vnaprej obvesti o namenih in prejemnikih v tretjih državah, če do takih prenosov prihaja, v skladu z zahtevami Splošne uredbe. Družba vodi evidenco prenosov osebnih podatkov v tretje države in mednarodne organizacije, ki vključuje pravno podlago prenosa in ustrezne zaščitne ukrepe.

Ko se osebni podatki posredujejo izven družbe, se uporabi varen način prenosa. Elektronski prenosi (pošiljanje podatkov po e-pošti, nalaganje na portale ipd.) morajo biti praviloma šifrirani ali zavarovani (npr. šifriranje priponk z geslom, varni protokoli HTTPS/SFTP). Če se podatki prenašajo na fizičnih nosilcih, se uporabljajo priporočene pošiljke s povratnico ali kurirske storitve s sledljivostjo pošiljke. Zaposleni ne smejo sami prenašati osebnih podatkov na osebne naprave ali iznašati fizičnih nosilcev iz prostorov družbe brez izrecne odobritve vodstva. Vsak izreden prenos osebnih podatkov zunaj družbe mora odobriti odgovorna oseba, v nekaterih primerih tudi DPO, in se evidentira (npr. iznos podatkov na zahtevo posameznika ali regulatorja). S takimi postopki družba zagotavlja sledljivost in nadzor nad podatki tudi, ko zapustijo njene sisteme.

16. člen (ukrepi za varovanje osebnih podatkov)

Za zaščito osebnih podatkov družba izvaja nabor tehničnih in organizacijskih ukrepov, ki so namenjeni preprečevanju nepooblaščenega dostopa, razkritja, spreminjanja ali izgube podatkov. Ukrepi so sorazmerni glede na ocenjena tveganja in občutljivost podatkov, upoštevaje sodobne standarde in priporočila in podrobneje opredeljeni v namenskih pravilnikih; ne glede na to, pa morajo upravljavec in obdelovalci v skladu z 32. členom Splošne uredbe izvajati ustrezne ukrepe, da zagotovijo raven varnosti, primerno tveganjem pri obdelavi. Ti ukrepi med drugim vključujejo:

- Fizična varnost: poslovni prostori in prostori, kjer se nahajajo sistemi ali nosilci z osebnimi podatki (strežniška soba, arhiv), so zaklenjeni in dostopni le pooblaščenim osebam. Med delovnim časom je zagotovljen nadzor nad obiskovalci, izven delovnega časa pa so prostori alarmno varovani in pod video-nadzorom (kjer je to ustrezno in skladno z zakonodajo). Nosilci podatkov (papirni dokumenti, prenosni diski) se hranijo v ognjevarnih omarah ali sefih. Čistilno osebje in vzdrževalci nimajo dostopa do občutljivih gradiv. Osebni podatki na vidnih mestih (na mizah, zaslonih) ne smejo ostati nenadzorovani - zaposleni izvajajo politiko čiste mize in zaslona (zaklepanje računalnika ob odsotnosti, pospravljanje dokumentov). Vzpostavljeni so postopki za obiskovalce in tretje

osebe, ki vključujejo spremstvo po prostorih in prepoved nedovoljenega fotografiranja ali kopiranja informacij.

- Logično-tehnična varnost: informacijski sistemi so zaščiteni pred zunanjimi in notranjimi grožnjami. Družba uporablja požarne pregrade (firewall) za nadzor omrežnega prometa ter sisteme za zaznavanje vdora (IDS/IPS) za odkrivanje morebitnih napadov. Vsi strežniki in delovne postaje imajo nameščeno antivirusno in protivohunsko programsko opremo, ki se dnevno posodablja in redno pregleduje sisteme glede zlonamerne kode. Operacijski sistemi in aplikacije se posodabljajo (nameščanje varnostnih popravkov) v skladu s procesom upravljanja sprememb IKT, tako da se ranljivosti odpravijo pravočasno. Družba uporablja tudi SIEM orodja (Security Information and Event Management) za centralni nadzor varnostnih dogodkov - sumljive aktivnosti in odkloni se spremljajo v realnem času ter ustrezno obravnavajo. Za občutljive podatke se uporabljajo šifrirni mehanizmi: prenosni računalniki in drugi mobilni mediji so šifrirani, komunikacija po omrežju (VPN, https) poteka šifrirano, občutljivi nabori podatkov v zbirkah pa so lahko dodatno kriptografsko zaščiteni (npr. šifriranje gesel, kreditnih kartic). Kjer je mogoče, se osebni podatki psevdonimizirajo ali anonimizirajo, da se zmanjša tveganje pri obdelavah (npr. uporaba identifikatorjev namesto imen v testnih bazah). Zagotovljena je tudi razpoložljivost podatkov in odpornost sistemov: pomembni strežniki imajo redundančne sisteme, vzpostavljeni so redni *backupi* podatkov (varnostne kopije), ki se hranijo ločeno in se občasno testira njihovo obnovitev. V primeru fizičnega ali tehničnega incidenta (okvara strojne opreme, izpad elektrike ipd.) ima družba načrt za obnovitev podatkov in delovanja (disaster recovery plan), ki omogoča pravočasno povrnitev dostopnosti do osebnih podatkov. Informacijska infrastruktura je nameščena v varovanem podatkovnem centru z nadzorovanim okoljem (klimatizacija, UPS napajanje, gasilni sistem).

- Kontrola dostopa in sledljivost: vsak uporabnik ima svoje prijavne podatke, uporaba teh je zabeležena. Dnevniški zapisi (log datoteke) se vodijo za vpogled v vse osebne podatke in za vse pomembne aktivnosti v informacijskih sistemih. Zapisuje se, kdo je dostopal ali spreminjal podatke, kdaj in v kakšnem obsegu. Te dnevnike se redno pregleduje v okviru notranjih kontrol, nepravilnosti pa se preiskujejo. Sistematično beleženje aktivnosti obdelave zagotavlja sledljivost (t. i. audit trail) in dokazovanje skladnosti. ZVOP-2 uvaja obveznost zagotavljanja sledljivosti dostopov do določenih zbirk (npr. pri videonadzoru, evidencah v javnem sektorju), kar družba implementira tam, kjer je to zahtevano.

- Varovanje podatkov pri razvoju in zunanjih izvajalcih: pri razvoju ali nabavi novih IT-rešitev družba upošteva načeli privzete in vgrajene zasebnosti (privacy by design & by default) v skladu s 25. členom Splošne uredbe. To pomeni, da se že pri načrtovanju sistemov predvidijo minimalna zbiranja podatkov, ustrezne

omejitve dostopa in možnosti anonimizacije. Zunanji izvajalci, ki razvijajo ali vzdržujejo sisteme, lahko dostopajo do osebnih podatkov le pod strogimi pogoji - praviloma v nadzorovanem okolju in ob navzočnosti pooblaščene osebe družbe. Pred vzdrževalnimi deli se podatke, če je mogoče, psevdonimizira ali uporabi testne anonimizirane nize. Vsak poseg v informacijski sistem (servis, nadgradnja) mora biti odobren in nadzorovan, DPO pa po potrebi spremlja potek posega, da prepreči nepooblaščeno kopiranje ali prenos podatkov.

- Preprečevanje izgube podatkov in drugih incidentov: družba uporablja mehanizme DLP (Data Loss Prevention) za zaznavo in preprečevanje nenamernih odtekanj podatkov (npr. opozorila ob pošiljanju zaupnih podatkov izven organizacije). Prav tako so uvedeni postopki za ravnanje s sumljivimi elektronskimi sporočili (protivirusni in antiphishing filtri ter osveščanje zaposlenih, da prijavijo poskuse socialnega inženiringa). Vzpostavljena je politika varne uporabe prenosnih naprav (prepoved nešifriranih USB ključkov, nadzor nad prenosom podatkov na prenosnike ipd.). Redno se izvajajo tudi testiranja varnosti (penetracijski testi, pregledne varnostne ocene sistemov) s ciljem odkriti in odpraviti morebitne ranljivosti.

- Organizacijski ukrepi: sem spadajo vsi postopki, pravila in nadzorni mehanizmi, ki zagotavljajo skladnost. Družba vodi predpisane evidence dejavnosti obdelav in sezname pooblaščenih oseb, sklepa ustrezne pogodbe z obdelovalci, ter redno ozavešča in usposablja zaposlene o pomenu varstva podatkov. Za vsako novo obdelavo ali projekt, ki vključuje osebne podatke, se izvede ocena tveganja in po potrebi DPIA. Procesi ravnanja s podatki so opisani v notranjih navodilih, ki jih morajo zaposleni upoštevati (npr. pravilnik o uporabi e-pošte in interneta, pravilnik o upravljanju gesel, načrt zagotavljanja neprekinjenega poslovanja). Določene situacije urejajo posebna pravila - npr. uporaba video-nadzora, sledenje vstopom/izstopom v prostore in druge posebne obdelave so skladne z zahtevami ZVOP-2. Vsi ti organizacijski ukrepi so dokumentirani in dostopni odgovornim deležnikom.

Ti tehnični in organizacijski ukrepi so podrobneje opisani v Strategiji kibernetske varnosti in notranjih aktih IKT, zato jih ta pravilnik zgolj povzema.

Družba redno pregleduje učinkovitost ukrepov ter jih prilagaja glede na tehnološki razvoj in nove grožnje. Upošteva se načelo stanja tehnike, stroškov izvajanja ter narave in obsega podatkov pri odločanju o tem, kateri varnostni ukrepi so primerni.

S kombinacijo navedenih ukrepov družba zagotavlja ustrezno raven varnosti osebnih podatkov glede na tveganja, kot to zahteva 32. člen Splošne uredbe, in tako varuje pravice posameznikov ter interese družbe.

17. člen (pravice posameznika na katerega se podatki nanašajo)

Posamezniki, na katere se nanašajo osebni podatki, imajo po Splošni uredbi in ZVOP-2 določene pravice, ki jim omogočajo nadzor nad njihovimi podatki. Družba spoštuje vse pravice posameznikov in je vzpostavil postopke, kako omogočiti njihovo učinkovito uresničevanje. Pravice posameznikov po Splošni uredbi vključujejo:

- Pravica do obveščenosti - posameznik ima pravico prejeti jasne informacije o tem, kako in zakaj se njegovi osebni podatki obdelujejo (to zajema obveznosti upravljavca po členih 13 in 14 Splošne uredbe glede posredovanja informacij ob zbiranju podatkov).
- Pravica dostopa - posameznik ima pravico pridobiti potrditev, ali družba obdeluje njegove osebne podatke, in dostop do teh podatkov ter informacij o obdelavi (namen, vrste podatkov, uporabniki, rok hrambe itd.).
- Pravica do popravka - posameznik lahko doseže, da družba brez nepotrebnega odlašanja popravi netočne osebne podatke, ki se nanašajo nanj, ter dopolni nepopolne podatke.
- Pravica do izbrisa (*»pravica do pozabe«*) - posameznik lahko zahteva, da upravljavec izbriše njegove osebne podatke, če so izpolnjeni določeni pogoji (npr. podatki niso več potrebni, privolitev je preklicana in ni druge podlage, nezakonita obdelava ipd.). Družba bo v takih primerih brez odlašanja izbrisal podatke, razen če obstajajo zakonski razlogi za zavrnitev izbrisa (npr. pravna obveznost hrambe, uveljavljanje pravnih zahtevkov).
- Pravica do omejitve obdelave - posameznik lahko doseže začasno omejitev obdelave (npr. v času preverjanja točnosti podatkov ali reševanja ugovora). V obdobju omejitve družba podatke le shranjuje in z njimi ne izvaja drugih obdelav, razen če posameznik da privolitev ali gre za nujne razloge.
- Pravica do prenosljivosti - posameznik ima pravico prejeti svoje osebne podatke, ki jih je posredoval upravljavcu, v strukturirani, splošno uporabljani strojno berljivi obliki, in pravico te podatke prenesti drugemu upravljavcu, kadar je to tehnično izvedljivo in če se obdelava izvaja avtomatizirano na podlagi privolitve ali pogodbe.
- Pravica do ugovora - posameznik lahko kadar koli ugovarja obdelavi osebnih podatkov, ki temelji na zakonitih interesih upravljavca ali na opravljanju nalog v javnem interesu. V primeru ugovora mora upravljavec prenehati obdelovati podatke, razen če dokaže nujne legitimne razloge, ki prevladajo nad interesi posameznika, ali za vzpostavitev oziroma obrambo pravnih zahtevkov. Kadar se podatki obdelujejo za namene neposrednega trženja, ima posameznik pravico kadar koli ugovarjati in upravljavec nato takoj preneha obdelavo v te namene.

- Pravica v zvezi z avtomatiziranim odločanjem - posameznik ima pravico, da zanj ne velja izključno avtomatizirano sprejeta odločitev (brez človekovega vpliva), ki ima pravne ali podobno pomembne učinke zanj, vključno z oblikovanjem profilov. Če družba v svojih procesih uporablja avtomatizirano odločanje (trenutno ne uporablja), mora zagotoviti ustrezne varovalke, vključno vsaj s pravico do človeškega posredovanja pri odločitvi.

Družba je vzpostavila postopek za uresničevanje pravic posameznikov. Zahteve glede katerekoli od zgoraj navedenih pravic lahko posameznik naslovi na družbo pisno (po pošti na sedež družbe) ali preko elektronske pošte na uradni kontakt (DPO ali *dpo@borzen.si*).

Na spletni strani družbe so objavljene osnovne informacije o uresničevanju pravic in kontaktni podatki DPO. Zahteva je lahko neformalna, družba pa lahko za lažjo obravnavo ponudi tudi obrazce (npr. pripravljene obrazce za dostop, izbris ipd. na podlagi vzorcev IP-RS). Posameznika, na katerega se nanašajo osebni podatki, katerih obdelava temelji na zakonski podlagi, pogodbeni podlagi oz. je za obdelavo izkazan zakonit Interes, se z javno objavo tega pravilnika na spletni strani družbe wvwv.borzen.si obvesti, s čimer je posameznik seznanjen s pravicami, ki mu gredo po tem pravilniku, zakonu, ki ureja varstvo osebnih podatkov in Splošni uredbi o varstvu podatkov.

Pri vlaganju zahteve mora posameznik zagotoviti razumljivo identifikacijo; če družba upravičeno dvomi v identiteto, lahko pred izpolnitvijo zahteve zahteva dodatne podatke za potrditev identitete.

Družba bo na zahtevo odgovorila brez nepotrebnega odlašanja, najpozneje v enem mesecu od prejema zahteve. V primeru kompleksnih ali številnih zahtev se lahko rok za odgovor podaljša za največ dva dodatna meseca, o čemer bo posameznik obveščen v enem mesecu od prejema zahteve, skupaj z razlogi za zamudo.

Odgovor se praviloma posreduje na način, kot je bila zahteva podana (pisno ali elektronsko), če ni drugače dogovorjeno, in v jasnem in razumljivem jeziku.

Izvrševanje pravic posameznika je načeloma brezplačno; družba lahko zaračuna razumno pristojbino ali zahtevo zavrne le, če je zahteva očitno neutemeljena ali pretirana (zlasti če se ponavlja), pri čemer mora takšno odločitev obrazložiti.

Če družba zahteve posameznika ne namerava ugoditi (npr. zavrne izbris zaradi zakonskih obveznosti hrambe), bo v odgovoru pojasnila razloge za zavrnitev in posameznika poučila o možnosti pritožbe pri Informacijskem pooblaščencu oz. uveljavljanja sodnega varstva.

Vse prejete zahteve in ukrepi, ki so bili v zvezi z njimi izvedeni, se evidentirajo (hrani se vsaj vsebina zahteve, datum prejema, datum odgovora in izid), da lahko družba izkaže skladnost z zahtevami Splošne uredbe o uresničevanju pravic.

18. člen (incidenti v zvezi z osebnimi podatki)

Kljub vsem preventivnim ukrepom obstaja možnost, da pride do varnostnega incidenta, povezanega z osebnimi podatki. Družba ima vzpostavljen postopek upravljanja incidentov (v skladu s posebnim pravilnikom o upravljanju incidentov IKT in varnostnih dogodkov), ki vključuje tudi ravnanje ob kršitvah varnosti osebnih podatkov (»personal data breach« po Splošna uredba). Za namen tega pravilnika kršitev varnosti pomeni vsak dogodek, ki privede do nenamernega ali nezakonitega uničenja, izgube, spremembe, nepooblaščenega razkritja ali dostopa do osebnih podatkov. To lahko vključuje tako naključne incidente (npr. izgubljen prenosnik s podatki, pomotoma poslan e-mail napačnemu prejemniku, izbris podatkov brez varnostne kopije) kot zlonamerna dejanja (npr. vdor v sistem, kraja podatkov, ransomware šifriranje podatkov).

Vsak zaposleni ali obdelovalec, ki zazna ali sumi na incident v zvezi z osebnimi podatki, mora o tem takoj obvestiti pristojno osebo (npr. službo za informatiko in DPO) v skladu z internim protokolom. Družba zagotavlja, da so zaposleni ozaveščeni o tej obveznosti in vedo, kako prepoznati potencialno kršitev (npr. izgubljena naprava, nenavaden dostop, virus na računalniku ipd.). Obvestilo mora vsebovati čim več informacij o naravi incidenta in prizadetih podatkih.

Po prijavi se sproži postopek odziva na incident. Odgovorna ekipa (običajno IKT-oddelek skupaj z DPO in drugimi relevantnimi člani) najprej oceni, ali gre za osebne podatke in ali dogodek pomeni kršitev varnosti le-teh. Če incident ne vključuje osebnih podatkov, se obravnava v okviru splošnih varnostnih postopkov. Če gre za osebne podatke, se tak dogodek dokumentira v interni evidenci kršitev, ne glede na resnost. Ekipa nato oceni tveganja za pravice in svoboščine posameznikov, ki izhajajo iz incidenta - upošteva se vrsta in količina prizadetih podatkov, narava incidenta (zaupnost, celovitost ali razpoložljivost podatkov je bila prizadeta), število in kategorije prizadetih posameznikov, možne posledice (npr. finančna škoda, kraja identitete, poseg v zasebnost). Na podlagi te ocene se odloči o nadaljnjih ukrepih: zajezitev in odprava posledic (npr. onemogočanje dostopa, obnova podatkov iz backupa, sprememba gesel, popravilo varnostne pomanjkljivosti) ter ukrepi za preprečitev ponovitve (npr. nadgradnja varnosti, dodatno usposabljanje zaposlenih).

Če obstaja verjetnost, da bo kršitev varnosti ogrozila pravice in svoboščine posameznikov (tj. predstavlja tveganje zanje), mora družba o tem obvestiti Informacijskega pooblaščenca RS (kot pristojni nadzorni organ) brez nepotrebnega odlašanja, najpozneje v 72 urah po tem, ko je za kršitev izvedel. V praksi DPO pripravi prijavo za IP, ki vključuje predpisane informacije: opis narave kršitve (kategorije in približno število prizadetih posameznikov ter zapisov podatkov), kontaktne podatke DPO, opis verjetnih posledic kršitve in opis ukrepov, ki jih je upravljavec sprejel ali predlaga za obravnavo kršitve (vključno z omilitvenimi ukrepi). Če vseh informacij ni mogoče zbrati v 72 urah, se poda

začetna prijava z utemeljitvijo zamude, manjkajoče informacije pa se posredujejo naknadno. Prijava IP ni potrebna, če ocena pokaže, da je malo verjetno, da incident predstavlja tveganje za posameznike (npr. podatki so bili šifrirani in neberljivi za napadalca). Vendar tudi v teh primerih družba vodi evidenco o incidentu in utemeljitev, zakaj ni bil priglašen.

Če je verjetno, da bo kršitev povzročila visoko tveganje za pravice in svoboščine posameznikov, bo družba poleg IP obvestila tudi prizadete posameznike brez nepotrebnega odlašanja. Obvestilo posameznikom je pripravljeno v razumljivem jeziku in vsebuje bistvene informacije o kršitvi (opis, možne posledice) ter kontakt za dodatne informacije, priporočila za posameznike (npr. zamenjavo gesla, pazljivost na poskuse goljufij) in informacije o tem, katere ukrepe je upravljavec že sprejel za ublažitev škode. Obvestilo posameznikom ni potrebno, če so bili ob uporabi ukrepov podatki postali nerazumljivi za nepooblaščenega (npr. šifrirani), ali če je upravljavec že sprejel ukrepe, ki odpravijo visoko tveganje, ali če bi obveščanje zahtevalo nesorazmeren napor (v tem primeru se izda javno obvestilo).

Družba vodi Evidenco vseh kršitev varnosti osebnih podatkov, ne glede na to, ali so bile priglašene IP ali ne. V evidenci se zabeleži čas in narava incidenta, kategorije prizadetih podatkov, ugotovljeni vzroki, posledice, izvedeni ukrepi ter ali je bil incident priglašen IP in/ali posameznikom. DPO skrbi za ažurnost te evidence in jo na zahtevo predloži nadzornemu organu. Redno (npr. letno) se opravi analiza zabeleženih incidentov, da se ugotovijo vzorci ali sistemske pomanjkljivosti in predlagajo izboljšave (npr. dodatni ukrepi ali usposabljanja za preprečevanje ponovitev).

Družba ima imenovan interno (ali pogodbeno) odzivno skupino za incidente, ki vključuje strokovnjake iz IT, DPO, pravne službe in po potrebi vključuje tudi vodstvo. Ta ekipa ima pripravljene načrte odzivanja na različne scenarije (kibernetski napad, izguba naprave, notranja zloraba podatkov itd.) in redno vadi postopke (simulacije incidentov) za zagotavljanje pripravljenosti.

Z doslednim izvajanjem navedenih postopkov družba zagotavlja hitro ukrepanje ob morebitnih kršitvah, zmanjševanje škode in izpolnjevanje zakonskih obveznosti glede priglasitve in obveščanja. S tem se tudi varujejo interesi posameznikov in ohranja zaupanje v družbo.

19. člen (usposabljanje zaposlenih)

Varstvo osebnih podatkov je učinkovito le takrat, ko se vsi zavedajo njegovega pomena, zato je stalno usposabljanje in ozaveščanje zaposlenih ključen del sistema varovanja osebnih podatkov pri družbi.

Novozaposleni so ob nastopu dela deležni temeljitega seznanjenja z določbami tega pravilnika, osnovami Splošne uredbe /ZVOP-2 in internimi varnostnimi politikami; prav

tako morajo podpisati izjavo o zavezanosti varovanju podatkov določeno v 7. členu tega pravilnika.

Vsaj enkrat letno (ali po potrebi pogosteje) se za vse zaposlene organizirajo osvežitvena usposabljanja in delavnice, kjer se obravnavajo posodobitve zakonodaje, nove notranje politike, primeri dobrih praks in dejanski incidenti ter ugotovitve notranjih in zunanjih pregledov. Posebna pozornost je namenjena usposabljanju zaposlenih, ki delajo z občutljivimi osebnimi podatki (npr. HR, IT, klicni center), da dobro razumejo svoje obveznosti.

Družba zaposlene tudi ozavešča skozi različne kanale: redna obvestila po e-pošti o nasvetih za varno ravnanje s podatki, plakati v pisarnah s ključnimi pravili (npr. zaklepanje zaslona, prepoznavanje phishinga), intranetne strani z viri (pogosta vprašanja, vodiči, kontakt DPO) ter občasne kampanje (npr. ob Evropskem mesecu kibernetske varnosti). Vsi, ki obdelujejo osebne podatke na podlagi pooblastil upravljavca, so ob dodelitvi pooblastila informirani o relevantnih določilih tega pravilnika ter svojih obveznostih in odgovornostih pri varstvu podatkov. To vključuje razumevanje posledic kršitev - tako za posameznike kot za družbo (možne globe, škoda ugleda, ipd.). Po potrebi družba organizira tudi specializirana usposabljanja (npr. tehnične delavnice za IT osebje o varnosti sistemov, pravni seminarji za HR glede delovnopravnih vidikov varstva podatkov).

Usposabljanje zajema tudi postopke za uresničevanje pravic posameznikov in ravnanje ob incidentih, da zaposleni vedo, kako reagirati in koga obvestiti. DPO ima pomembno vlogo pri pripravi vsebin usposabljanj in lahko izvede interna predavanja po področjih oz. službah ali Q&A seje za zaposlene. Poleg notranjih virov se zaposlene spodbuja k udeležbi na zunanjih izobraževanjih, konferencah ali spletnih seminarjih o varstvu podatkov, še posebej DPO in ključne osebe, ki morajo ohranjati strokovno znanje posodobljeno.

Družba beleži udeležbo na obveznih usposabljanjih (podpisi ali elektronska evidenca) in vodi evidenco o izvedenih aktivnostih ozaveščanja. Tako lahko spremlja, ali so vsi relevantni zaposleni opravili potrebna usposabljanja. Če se ugotovi pomanjkljivo znanje ali neskladnosti v praksi, se organizirajo dodatna ciljna izobraževanja. Ozaveščanje in znanje zaposlenih je tudi predmet rednih notranjih pregledov.

Z vzpostavljeno kulturo, kjer vsak zaposleni razume svojo vlogo pri varstvu podatkov in ima znanje za pravilno ravnanje, družba bistveno zmanjšuje verjetnost človeških napak in krepi skladnost. Varstvo osebnih podatkov je redna tema internih komunikacij in sestankov, vodstvo pa z zgledom spodbuja pomembnost te teme, s čimer se gradi zavedanje, da je zaščita osebnih podatkov odgovornost vseh v organizaciji - ne le DPO, kadrovskega ali IT oddelka.

20. člen (notranji pregledi s področja varstva osebnih podatkov)

Družba je v svojo kulturo vgradila mehanizme nadzora in nenehnega izboljševanja skladnosti s Splošno uredbo, ZVOP-2 ter povezanimi standardi.

Družba izvaja redne notranje preglede oziroma kontrole ravnanja z osebnimi podatki. To pomeni, da v določenih časovnih intervalih (predvidoma vsako leto, lahko pa tudi pogosteje) pregledamo, kako zaposleni in sistemi dejansko obdelujejo osebne podatke ter ali se upoštevajo vse varnostne zahteve. Notranje kontrole lahko izvaja DPO ali posebej pooblaščena notranja revizijska služba oz. funkcija, pooblaščena za skladnost poslovanja. Ti pregledi zajemajo preverjanje evidenc dostopov, pregled spoštovanja politik (ali zaposleni zaklepajo zaslone, ali uporabljajo odobrene prenosne medije), preizkus odzivnosti na testne uveljavitve pravic posameznikov, pregled urejenosti dokumentacije ipd. Ugotovitve kontrol se dokumentirajo, morebitne neskladnosti pa se razvrstijo po resnosti in spremljajo do odprave.

Ker je družba certificirana v skladu s standardom ISO/IEC, se izvajajo notranje revizije sistema vodenja varnosti in zasebnosti. V okviru teh revizij se sistematično preverjajo tudi vidiki varstva osebnih podatkov. Pregledano je, ali so vsi zahtevanji dokumenti in zapisi na voljo (politike, evidence obdelav, DPIA, pogodbe z obdelovalci), ali je vodstvo vključeno v ključne procese, kako se obvladujejo tveganja, itd. Notranje revizije izvede usposobljena oseba, ki je neodvisna od revidiranega področja. Rezultati vsake revizije so predstavljeni vodstvu, ki sprejme korektivne in preventivne ukrepe, kjer je potrebno.

Informacijski pooblaščenec RS kot nadzorni organ ima pooblastila za inšpekcijski nadzor nad družbo. Družba je dolžna sodelovati z nadzornim organom, mu omogočiti dostop do informacij in mu na zahtevo posredovati dokazila o skladnosti (npr. ta pravilnik, evidence obdelav, pogodbe). Družba bo aktivno sodelovala v morebitnih nadzorih ter upoštevala priporočila oziroma odločbe nadzornega organa.

Družba si prizadeva za stalno izboljševanje sistema varstva osebnih podatkov, kar je v skladu z načelom odgovornosti in zahtevami ISO standardov. To dosega prek več mehanizmov:

- Letni pregled skladnosti: vodstvo skupaj z DPO vsaj enkrat letno opravi celovit pregled stanja varstva osebnih podatkov (*management review*). Pregled obsega analizo vseh relevantnih kazalnikov: poročila o incidentih in kršitvah (koliko jih je bilo, vzroki), poročila notranjih in zunanjih revizij, prejete zahteve posameznikov in kako so bile rešene, morebitne nove pravne ali poslovne spremembe, ki vplivajo na obdelavo podatkov, povratne informacije zaposlenih in uporabnikov itd. Na podlagi pregleda vodstvo sprejme strateške usmeritve (npr. potreba po dodatnem usposabljanju, posodobitvi politike, investicija v novo opremo).

- Kazalniki in spremljanje uspešnosti: DPO lahko vzpostavi ključne kazalnike uspešnosti (KPI) varstva podatkov - npr. odstotek zaposlenih, ki so opravili usposabljanje, povprečni čas odziva na zahteve posameznikov, število incidentov glede na resnost, skladnost z roki izbrisa itd. Te kazalnike se spremlja skozi čas in ob negativnih trendih sproži ukrepe.

Z opisanimi mehanizmi se družba trudi ne le vzdrževati skladnost, temveč jo nenehno nadgrajevati. Varstvo podatkov je vpet v splošni sistem vodenja kakovosti in informacijske varnosti podjetja in podvrženo ciklu načrtovanja, izvajanja, preverjanja in ukrepanja (PDCA). Tak pristop je tudi v skladu z ISO standardi in pričakovanji regulatorjev, saj le sprotno prilagajanje zagotavlja učinkovitost v spreminjajočem se okolju.

Sklepne določbe

21. člen (spremljanje področja)

Ta pravilnik se posodablja ob vsakršnih pomembnih spremembah okolja: kadarkoli se spremeni zakonodaja (npr. nove smernice EDPB, sprememba ZVOP-2) ali pride do organizacijskih sprememb v družbi (npr. novi procesi, uvedba novih tehnologij kot je umetna inteligenca). V primeru nejasnosti pri razlagi posameznih določb pravilnika se lete razlaga v skladu z namenom Splošne uredbe, ZVOP-2 in sorodnih predpisov, ob upoštevanju smernic Informacijskega pooblaščenca in EDPB.

DPO spremlja razvoj predpisov in prakse ter predlaga spremembe. Vse spremembe mora odobriti vodstvo, zaposleni pa so z njimi seznanjeni (praviloma pisno ali na usposabljanju).

Če notranje ali zunanje preverjanje odkrije neskladnost (npr. nezadostno zavarovan postopek, neustrezno hranjenje podatkov dlje od dovoljenega), družba izvede korektivni ukrep. To lahko pomeni dopolnitev navodil, dodatno tehnično rešitev ali sankcioniranje neustreznega ravnanja posameznika, odvisno od narave neskladnosti. O korektivnih ukrepih se vodi evidenca, DPO pa spremlja njihovo uresničitev.

Družba prav tako spodbuja zaposlene, da predlagajo izboljšave ali opozorijo na pomanjkljivosti pri varstvu podatkov.

22. člen (sprejem pravilnika)

Ta pravilnik začne veljati z dnem, ko ga potrdi direktor družbe, in se uporablja neposredno od dneva objave v notranjem informacijskem sistemu.

Z dnem uveljavitve tega pravilnika prenehajo veljati prejšnji Pravilnik o varovanju osebnih podatkov in vsa interna pravila oziroma navodila v zvezi z varovanjem osebnih podatkov v družbi.

Vsi organizacijski deli družbe morajo uskladiti svoje postopke s tem pravilnikom v roku 30 dni po začetku veljavnost pravilnika.

DPO in vodstvo sta odgovorna, da se pravilnik implementira v praksi in da se o njegovi vsebini obvesti vse zaposlene.

23. člen (objava pravilnika)

Pred sprejemom pravilnika je ta posredovan vsem zaposlenim, ki lahko v roku 8 dni nanj podajo pripombe in komentarje. Vse prejete pripombe in komentarje bo poslovodstvo obravnavalo in se do njih opredelilo.

Ta pravilnik se objavi na spletni strani družbe in začne veljati naslednji dan po objavi.

Ljubljana, dne 8.10.2025

Mojca Kert
Direktorica

Borzen
Borzen, d.o.o., Dunajska c. 156, 1000 Ljubljana