Na podlagi 19. točke prvega odstavka 28. člena v zvezi z 8. točko prvega odstavka 70. člena in tretjim odstavkom 71. člena ter na podlagi drugega odstavka 83. člena Statuta Zavoda za zdravstveno zavarovanje Slovenije (Uradni list RS, št. 87/01 in 1/02 – popr.) generalna direktorica Zavoda za zdravstveno zavarovanje Slovenije izdaja

PRAVILNIK O VARSTVU OSEBNIH PODATKOV V ZAVODU ZA ZDRAVSTVENO ZAVAROVANJE SLOVENIJE

I. DEL
SPLOŠNE DOLOČBE

1. člen
(predmet pravilnika)

(1) S tem pravilnikom se v Zavodu za zdravstveno zavarovanje Slovenije (v nadaljnjem besedilu: ZZZS) zagotavlja skladnost obdelav osebnih podatkov, ki jih upravlja ZZZS, z Uredbo (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 nadaljnjem besedilu: GDPR), Zakonom o varstvu osebnih podatkov (Uradni list RS, št. 163/22; v nadaljnjem besedilu: ZVOP-2) in drugimi predpisi, ki urejajo varstvo osebnih podatkov ter določa tehnične in organizacijske ukrepe za varno in zakonito obdelavo teh podatkov.

(2) S tem pravilnikom se v ZZZS določa postopek vzpostavitve in evidentiranja obdelav osebnih podatkov, način informiranja in uveljavljanja pravic posameznika v zvezi z obdelavo podatkov, ki se nanašajo nanj ter izvajanje tehničnih in organizacijskih ukrepov, s katerimi ZZZS varuje osebne podatke in njihovo obdelavo v skladu s predpisanimi zahtevami.

(3) ZZZS s tem pravilnikom in z drugimi notranjimi akti, politikami, načrti ter navodili, ki sestavljajo sistem upravljanja varovanja informacij v ZZZS (v nadaljnjem besedilu: SUVI) določa nosilce, organiziranost in postopke ter pristojnosti in odgovornosti za izvajanje ukrepov iz prvega in drugega odstavka tega člena.

(4) Po tem pravilniku se varujejo tudi osebni podatki, ki jih na podlagi pogodbe v smislu 28. člena GDPR za ZZZS obdeluje zunanji izvajalec.

2. člen
(izjava o seznanitvi s predpisi o varstvu osebnih podatkov)

(1) Končni uporabniki morajo biti seznanjeni z GDPR, ZVOP-2 in z drugimi zakoni in podzakonskimi akti, ki urejajo obdelavo osebnih podatkov na področjih poslovanja ZZZS, povezanimi z njihovim delom, ter z vsebino tega pravilnika in drugimi dokumenti SUVI.

(2) Zaposleni v ZZZS in zunanji sodelavci, ki na podlagi študentske napotnice pri svojem delu obdelujejo osebne podatke, ki jih upravlja oziroma obdeluje ZZZS, svojo seznanjenost in zavezanost k ustreznemu varstvu podatkov potrdijo s podpisom izjave na obrazcu iz Priloge 1, ki je sestavni del tega pravilnika.

(3) Zunanji sodelavci ZZZS, ki se v okviru izvajanja pogodbenih del seznanijo ali bi se lahko seznanili z osebnimi podatki, ki jih upravlja ZZZS, pred začetkom izvajanja pogodbenih del podpišejo izjavo na obrazcu iz Priloge 2, ki je sestavni del tega pravilnika.

3. člen
(pomen izrazov)

Izrazi, uporabljeni v tem pravilniku, pomenijo:

1. končni uporabnik je zaposleni v ZZZS oziroma zunanji pogodbeni sodelavec ZZZS oziroma študent, ki delo v ZZZS opravlja preko študentske napotnice, ki zaradi narave svojega dela lahko obdeluje določene osebne podatke, s katerimi upravlja, ali jih v okviru izvajanja poslovnih dejavnosti obdeluje ZZZS;

2. uporabniški račun je tehnološka rešitev za hrambo podatkov o identiteti končnega uporabnika (npr. ime in priimek, identifikacijska številka, uporabniško ime), podatkov za avtentikacijo uporabnika (npr. geslo, PIN) in podatkov o njegovih dostopnih pravicah;

3. vsebinski skrbnik zbirke je zaposleni v ZZZS, odgovoren za obdelavo podatkov določene zbirke osebnih podatkov, vpisane v evidenco dejavnosti obdelave osebnih podatkov;

4. lastnik zbirke je vodja - direktor področja, sektorja, območne enote ZZZS oziroma področne enote Informacijski center (v nadaljnjem besedili: PE IC) v ZZZS, kamor glede na njene naloge in pristojnosti sodi določena zbirka osebnih podatkov;

5. informacijski sistem je programska, strojna, komunikacijska in druga oprema ZZZS, ki deluje samostojno ali v omrežju in je namenjena obdelavi osebnih podatkov;

6. kršitev varnosti osebnih podatkov pomeni kršitev, ki vodi do nezakonitega uničenja, izgube, spremembe, nepooblaščenega razkritja ali dostopa do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani;

7. osebje obdelovalca so zaposleni pri obdelovalcu oziroma zunanji pogodbeni sodelavci obdelovalca oziroma študenti, ki delo pri obdelovalcu opravljajo preko študentske napotnice, ki zaradi narave svojega dela lahko obdelujejo določene osebne podatke, ki jih upravlja ZZZS;

8. vodstvo ZZZS so generalna direktorica ZZZS in delavci s posebnimi pooblastili, določenimi v statutu ZZZS;

9. vodstveni pregled je dokumentiran pregled sistema upravljanja informacijske varnosti in sistema upravljanja neprekinjenega poslovanja ZZZS, ki ga generalna direktorica ZZZS opravi najmanj enkrat letno, da zagotovi skladnost obdelave osebnih podatkov.

II. DEL
NOSILCI VARSTVA IN VARNOSTI OBDELAVE OSEBNIH PODATKOV

1. poglavje
Odgovornosti in organiziranost varstva in varnosti osebnih podatkov

4. člen
(naloge in pristojnosti generalne direktorice ZZZS v zvezi z obdelavo osebnih podatkov)

Za zagotovitev ustreznih in učinkovitih tehničnih in organizacijskih ukrepov za izvajanje obdelave osebnih podatkov v skladu s predpisanimi in pogodbeno dogovorjenimi zahtevami ter za dokazovanje skladnosti dejavnosti obdelave s temi zahtevami, generalna direktorica ZZZS (v nadaljnjem besedilu: generalna direktorica):

- imenuje pooblaščeno osebo za varstvo osebnih podatkov,
- ustanovi strateško skupino za politiko varovanja informacij v ZZZS,
- pooblasti osebo, ki koordinira izvajanje politike varovanja informacij v ZZZS,
- imenuje osebe, ki so odgovorne za posamezne zbirke podatkov in obravnavanje tveganj, povezanih z obdelavo teh zbirk;
- določi vsebino in obseg pravic za dostop do osebnih podatkov, ki jih zaposleni na določenem delovnem mestu nujno potrebuje za izvedbo svojih delovnih obveznosti, ter
- izvaja vodstveni pregled.

5. člen
(imenovanje pooblaščene osebe za varstvo osebnih podatkov)

(1) Generalna direktorica izmed zaposlenih v ZZZS, ki izpolnjujejo v GDPR in ZVOP-2 predpisane pogoje, imenuje pooblaščeno osebo za varstvo osebnih podatkov (v nadaljnjem besedilu: DPO).

(2) Generalna direktorica lahko za pomoč DPO pri opravljanju njegovih nalog izmed zaposlenih ali zunanjih strokovnjakov določi tudi druge osebe, ki pa so pri izvajanju pomoči vezane na navodila DPO.

6. člen
(položaj DPO)

(1) Generalna direktorica zagotovi neodvisno opravljanje nalog in ustrezno umeščenost DPO v organizacijsko shemo ZZZS, da je DPO ustrezno in pravočasno vključen v vse zadeve v zvezi z varstvom osebnih podatkov. Vključevanje DPO v zadeve varstva osebnih podatkov se zagotovi predvsem z:

- neposrednim dostopom do vodstva ZZZS, kadar vodstvo ali DPO ocenita, da določena zadeva varstva osebnih podatkov zahteva tak način obravnave;
- njegovim udeleževanjem sestankov vodstva ZZZS ter sestankov projektnih in delovnih skupin, ki se nanašajo na obdelavo in varstvo osebnih podatkov;

- neposrednim dostopom do zaposlenih v ZZZS in pri morebitnih obdelovalcih, ki obdelujejo osebne podatke, ki jih upravlja ZZZS;
- dostopom do dokumentarnega gradiva, ki obravnava zadeve varstva osebnih podatkov;
- neposrednim dostopom do zbirk osebnih podatkov in zapisov revizijskih sledi oziroma dnevnika obdelave, ki jih potrebuje za izvajanje svojih delovnih nalog.

(2) Generalna direktorica DPO zagotovi vsa sredstva, potrebna za izvajanje njenih nalog, kamor poleg informacijskega sistema in druge opreme sodijo zlasti dostopi do:
- osebnih podatkov in revizijskih sledi oziroma dnevnikov obdelave v zbirkah in drugih oblikah obdelave osebnih podatkov;
- podatkov o kršitvah varnosti osebnih podatkov;
- končnih uporabnikov in osebja obdelovalca, ki izvaja naloge obdelave osebnih podatkov, ki jih upravlja ZZZS;
- virov in oblik usposabljanj oziroma izpopolnjevanj, namenjenih vzdrževanju ustrezne ravni strokovnega znanja DPO.

7. člen
(naloge DPO)

(1) DPO generalni direktorici na strokovno neodvisen način pomaga pri zagotavljanju skladnosti obdelave osebnih podatkov z GDPR, ZVOP-2 in drugimi predpisi, ki urejajo obdelavo in varstvo osebnih podatkov v ZZZS.

(2) DPO izvaja naslednje naloge:
1. generalno direktorico in ostale zaposlene ZZZS obvešča ter jim svetuje o njihovih obveznostih, ki izhajajo iz GDPR, ZVOP-2 in drugih predpisov o varstvu osebnih podatkov;
2. spremlja skladnost poslovanja ZZZS z zakonodajo in drugimi predpisi s področja obdelave in varstva osebnih podatkov, vključno z dodeljevanjem nalog, ozaveščanjem in usposabljanjem osebja ter s tem povezanimi revizijami;
3. svetuje, kadar je to zahtevano, glede ocene učinka v zvezi z varstvom osebnih podatkov;
4. sodeluje z Informacijskim pooblaščencem glede vprašanj s področja varstva osebnih podatkov v ZZZS;
5. deluje kot kontaktna točka ZZZS za Informacijskega pooblaščenca pri vprašanjih v zvezi z obdelavo osebnih podatkov, vključno s predhodnim posvetovanjem ali posvetovanjem glede katere koli druge zadeve;
6. svetuje razvijalcem novih rešitev za obdelavo osebnih podatkov v ZZZS glede načina obvladovanja tveganj za pravice in svoboščine, ki bi jih glede na uporabljene tehnologije ter naravo, obseg, okoliščine in namen obdelave lahko imela nova rešitev obdelave;
7. obravnava zahteve posameznikov po seznanitvi z lastnimi osebnimi podatki in sodeluje pri obravnavi drugih zahtevkov posameznikov, katerih podatke ZZZS obdeluje, vezanih na varstvo njihovih pravic in svoboščin v zvezi z obdelavo osebnih podatkov;
8. vodi in upravlja evidenco dejavnosti obdelave osebnih podatkov;

9. daje mnenje k oceni učinka v zvezi z varstvom osebnih podatkov, ki jo ZZZS pripravi v okviru priprav na obdelavo, ki bi lahko povzročila veliko tveganje za pravice in svoboščine posameznikov, katerih podatki bodo predmet obdelave;
10. organizira in izvaja usposabljanja in ozaveščanja končnih uporabnikov, ki so vključeni v dejanja obdelave in v zvezi z varstvom osebnih podatkov;
11. izvaja notranje nadzorne preglede s področja varstva osebnih podatkov skladno z letnim načrtom preverjanja skladnosti obdelave s predpisanimi in interno določenimi zahtevami.

8. člen
(ustanovitev in naloge strateške skupine za politiko varovanja informacij)

(1) Generalna direktorica ustanovi strateško skupino za politiko varovanja informacij v ZZZS (v nadaljnjem besedilu: strateška skupina), ki je njen posvetovalni organ na področju varovanja informacij, ki jih upravlja oziroma jih v okviru svojega poslovanja obravnava ZZZS.

(2) Strateška skupina določi smernice za uvajanje politik varovanja informacij v ZZZS. Strateška skupina se sestaja po potrebi, vendar najmanj enkrat letno, ko obravnava poročilo pooblaščene osebe za informacijsko varnost. Na osnovi pripravljenih strokovnih podlag pooblaščene osebe za informacijsko varnost strateška skupina generalni direktorici predlaga izvedbo ukrepov za zmanjšanje tveganj in izboljšanje politike varovanja informacij ZZZS.

9. člen
(imenovanje in naloge koordinatorja za informacijsko varnost)

(1) Generalna direktorica izmed zaposlenih v ZZZS, ki imajo ustrezna znanja s področja informacijske varnosti, za izvajanje funkcije vodenja in koordiniranja izvajanja politike varovanja informacij, imenuje pooblaščeno osebo za informacijsko varnost (v nadaljnjem besedilu: koordinator), ki vodstvu svetuje na področju načrtovanja, organiziranja in izvajanja ukrepov za zagotavljanje zaupnosti, celovitosti, razpoložljivosti in odpornosti rešitev in sistemov obdelave ter operativno koordinira nosilce odgovornosti za izvajanje tehničnih in organizacijskih ukrepov, ki temeljijo na oceni tveganj in s katerimi ZZZS varuje osebne podatke ter preprečuje njihovo naključno, namerno ali drugače nezakonito uničenje, spremembo, izgubo, nepooblaščeno razkritje, dostop ali drugo nepooblaščeno obdelavo.

(2) Koordinator izvaja zlasti naslednje naloge:
1. skrbi za posodabljanje krovne politike na področju varovanja informacij v ZZZS in aktov, sprejetih za izvedbo te politike;
2. skrbi za učinkovito delovanje in nenehno izboljševanje SUVI;
3. sodeluje pri pripravi postopkov za učinkovito delovanje in nenehno izboljševanje sistema upravljanja neprekinjenega delovanja informacijskega sistema ZZZS;
4. sodeluje pri preverjanju in izboljševanju sistema upravljanja neprekinjenega poslovanja ZZZS;
5. skrbi za učinkovito obravnavanje ter dokumentiranje varnostnih dogodkov in incidentov, kar obsega tudi pripravo oceno učinkov posameznih varnostnih dogodkov oziroma incidentov na

poslovanje ZZZS, oziroma zagotavljanje zakonsko skladne obdelave podatkov ter sprejetje ustreznih popravnih ukrepov;

6. skrbi, da so pri razvoju novih rešitev za obdelavo osebnih podatkov upoštevana varnostna tveganja, ki bi jih glede na uporabljene tehnologije ter naravo, obseg, okoliščine in namen obdelave lahko imela nova rešitev obdelave, ter da so privzeto izvedeni oziroma vgrajeni ustrezni tehnični in organizacijski ukrepi za odpravo ali zmanjšanje tveganj;
7. v sodelovanju z DPO in skrbniki zbirk ocenjuje varnostne dogodke in incidente, v okviru katerih je bila kršena varnost osebnih podatkov, če iz informacije o varnostnem dogodku ali incidentu izhaja, da so s kršitvijo bile ali bi lahko bile ogrožene pravice in svoboščine posameznikov, na katere se nanašajo podatki, ki so bili predmet kršitve;
8. daje mnenje na oceno učinka v zvezi z varstvom osebnih podatkov;
9. za strateško skupino pripravlja gradiva, vezana na informacijsko varnost in varnost obdelave osebnih podatkov.

10. člen

(imenovanje in naloge lastnikov in vsebinskih skrbnikov zbirk osebnih podatkov)

(1) Vse zbirke oziroma obdelave osebnih podatkov (v nadaljnjem besedilu: zbirke), ki jih upravlja ZZZS, morajo biti vpisane v evidenco dejavnosti obdelave osebnih podatkov (v nadaljnjem besedilu: evidenca dejavnosti obdelave). Za vsako zbirko mora biti v evidenci dejavnosti obdelave določen lastnik zbirke in odgovorna oseba (v nadaljnjem besedilu: vsebinski skrbnik zbirke), ki sta odgovorna za zakonito obdelavo osebnih podatkov v tej zbirki.

(2) Lastnike in vsebinske skrbnike posameznih zbirk, vpisanih v evidenco dejavnosti obdelave, imenuje generalna direktorica.

(3) Lastnik in vsebinski skrbnik zbirke sta odgovorna zlasti za:

1. sodelovanje z DPO z namenom vzpostavitve, upravljanja in posodabljanja posamezne zbirke;
2. pripravo opisa posamezne zbirke in pripravo ter objavo obvestil posameznikom glede obdelave osebnih podatkov, kot je določeno v Prilogi 3, ki je sestavni del tega pravilnika;
3. obdelavo osebnih podatkov le za namene, za katere so bili zbrani;
4. pridobitev predhodnega mnenja DPO v primeru obdelave osebnih podatkov za drug (dodaten) namen, zagotovitev informacije posamezniku o tem drugem namenu in za pridobitev privolitve posameznika za obdelavo, kadar je pravna podlaga za obdelavo privolitev;
5. zbiranje najmanjšega možnega obsega osebnih podatkov, ki jih ZZZS potrebuje za uresničitev namena obdelave podatkov v zbirki;
6. sodelovanje z DPO pri obravnavi zahtev posameznikov po seznanitvi z lastnimi osebnimi podatki, ki jo posameznik vloži tudi na obrazcu iz Priloge 4, ki je sestavni del tega pravilnika;
7. obravnavanje zahtev posameznikov, ki uveljavljajo pravice v zvezi z obdelavo njihovih osebnih podatkov (popravek, izbris, preklic ali ugovor obdelavi), ki jo posameznik lahko vloži tudi na obrazcu iz Priloge 5, ki je sestavni del tega pravilnika;
8. ustrezno obravnavanje podatkov v zbirki po poteku roka hrambe;

9. opredelitev vsebine pogodbenega razmerja v primeru, da podatke iz zbirke obdeluje obdelovalec v smislu 28. člena GDPR;
10. sodelovanje z DPO ali koordinatorjem pri obravnavi sumov kršitev varnosti osebnih podatkov;
11. sprotno oziroma najmanj enkrat v obdobju enega leta posodabljanje opisa zbirke v evidenci dejavnosti obdelave;
12. obveščanje DPO o vseh potrebnih dopolnitvah in posodobitvah opisa zbirke.

(4) DPO najmanj enkrat letno vse skrbnike zbirk pisno pozove k pregledu in pripravi ter posredovanju posodobitev opisa zbirk v evidenci dejavnosti obdelave osebnih podatkov.

11. člen
(obveznosti končnega uporabnika)

(1) Končnemu uporabniku mora biti dodeljen uporabniški račun, ki mu omogoča dostop do tistih osebnih podatkov v posameznih zbirkah, ki jih nujno potrebuje za izvedbo svojih delovnih oziroma pogodbenih obveznosti.

(2) Ustrezen uporabniški račun končnemu uporabniku na predlog njegovega nadrejenega določi oziroma odobri lastnik oziroma skrbnik zbirke, aktivira pa administrator-informacijski skrbnik uporabniških računov v ZZZS, in sicer v skladu z organizacijskim navodilom, s katerim se v ZZZS ureja upravljanje pooblastil za dostop do informacijskih virov ZZZS.

(3) Končni uporabnik mora posamične dostope do osebnih podatkov izvrševati v skladu z navodili za obdelavo oziroma uporabo določene zbirke. Pri tem mora zlasti paziti, da:
1. ne razkriva osebnih podatkov, s katerimi se je seznanil pri svojem delu, sodelavcem, ki niso pooblaščeni za delo z osebnimi podatki, ali drugim osebam;
2. ne opušča ravnanj, s katerim bi lahko preprečil:
   - nepooblaščen vpogled v nosilce osebnih podatkov,
   - nedovoljeno odnašanje nosilcev osebnih podatkov iz prostorov ZZZS,
   - ogrožanje integritete, zaupnosti in razpoložljivosti osebnih podatkov,
   - postopke in ukrepe za evidentiranje vseh dejavnosti obdelav osebnih podatkov;
3. o zlorabi osebnih podatkov ali vdoru v zbirko osebnih podatkov obvesti službo za podporo uporabnikov PE IC.

(4) Ob dodelitvi računalnika oziroma ob prvi dodelitvi uporabniškega računa končni uporabnik podpiše izjavo na obrazcu iz Priloge 6, ki je sestavni del tega pravilnika. Te izjave ni potrebno podpisovati zunanjim sodelavcem ZZZS, ki so predhodno že podpisali izjavo na obrazcu iz Priloge 2.

(5) Končni uporabnik je dolžan na zaprosilo DPO posredovati vse zaprošene podatke in informacije v zvezi z obdelavami osebnih podatkov, ki so potrebne v postopkih izvajanja nadzorov nad izvajanjem postopkov in ukrepov varstva osebnih podatkov ter varnosti obdelave, v postopkih

priprave odgovorov na zahteve po seznanitvi z lastnimi osebnimi podatki ter v drugih postopkih vezanih na uveljavljanja pravic posameznikov in zagotavljanja varstva osebnih podatkov.

2. poglavje
Dokazila o skladnosti obdelave

12. člen
(dokazovanje skladnosti obdelave osebnih podatkov)

(1) ZZZS za potrebe dokazovanja skladnosti obdelave osebnih podatkov s predpisanimi zahtevami, pogodbenimi obveznostmi in tem pravilnikom vodi ustrezno dokumentacijo, s katero je sposoben dokazati, da obdelava poteka v skladu z določbami GDPR, ZVOP-2 in drugih relevantnih predpisov.

(2) Vsi tehnični in organizacijski ukrepi za izvajanje obdelave v skladu s predpisanimi in pogodbeno dogovorjenimi zahtevami morajo biti dokumentirani tako, da je omogočeno njihovo učinkovito izvajanje, spremljanje in nadziranje ter dokazovanje skladnosti obdelave v sodnih in drugih uradnih postopkih oziroma na zahtevo Informacijskega pooblaščenca ali drugih pristojnih organov.

(3) Dokumentacija iz prejšnjega odstavka obsega tako dokazila o razvoju, upravljanju in vzdrževanju informacijske infrastrukture ZZZS, dokumentacijo rešitev, storitev in sistemov za obdelavo, evidenco dejavnosti obdelave, ocene tveganj, ocene učinkov, poročila o obravnavanju kršitev varnosti osebnih podatkov, informacijske varnostne politike in politike neprekinjenega delovanja ter njune priloge kakor tudi revizijski sledi oziroma dnevnike obdelave in poročila o notranjih presojah in zunanjih revizijah, inšpekcijskih nadzorih in drugih preverjanjih skladnosti poslovanja ZZZS s strani pristojnih organov oziroma pooblaščenih organizacij.

III. DEL
EVIDENTIRANJE OBDELAVE OSEBNIH PODATKOV

1. poglavje
Vzpostavitev zbirke in evidentiranje dejavnosti obdelave

13. člen
(vzpostavitev zbirke)

(1) Zbirko s sklepom, na predlog vodje - direktorja organizacijske enote v ZZZS, v katerega vsebinsko sodi nova zbirka in po predhodno pridobljenem mnenju DPO, vzpostavi generalna direktorica.

(2) V sklepu iz prejšnjega odstavka generalna direktorica določi:
1. naziv zbirke;

2. lastnika zbirke;
3. vsebinskega skrbnika zbirke;
4. pravno podlago za obdelavo podatkov v zbirki;
5. namene obdelave;
6. opis kategorij posameznikov, na katere se nanašajo osebni podatki;
7. vrste osebnih podatkov;
8. kategorije uporabnikov, ki jim bodo razkriti osebni podatki, vključno z uporabniki v tretjih državah ali mednarodnih organizacijah;
9. kadar je mogoče, predvidene roke za izbris različnih vrst podatkov.

(3) Sklep iz prvega odstavka tega člena je podlaga za prvi vpis zbirke v evidenco dejavnosti obdelave.

14. člen
(spisek osebnih podatkov)

(1) ZZZS lahko za namen organizacije in izvedbe različnih oblik enkratnih dogodkov, kot so konference, srečanja, predavanja, obiski in izleti in podobno, v obliki spiska zbira osebne podatke, ki jih ob prijavi na dogodek sporočijo potencialni udeleženci. Prijavnica na enkratni dogodek mora vsebovati eksplicitno navedbo, da se bodo zahtevani osebni podatki udeležencev uporabili izključno za namen organiziranja in izvedbe tega dogodka. Spisek osebnih podatkov ZZZS sestavi za vsak posamezni enkratni dogodek.

(2) Spisek osebnih podatkov je po končanem dogodku, ki obsega tudi morebitno pošiljanje gradiv oziroma obvestil o izvedenem dogodku po zaključku dogodka, treba takoj uničiti. Če je osebne podatke v obliki spiska treba posredovati uporabniku, ki sodeluje pri izvedbi dogodka, mora ta spisek po koncu dogodka uničiti.

(3) Če je treba katere od osebnih podatkov udeležencev dogodka iz spiska osebnih podatkov shraniti za nadaljnjo uporabo in so za to podane ustrezne pravne podlage, se jih vključi v obstoječo zbirko ali vzpostavi novo zbirko.

(4) Za izvedbo ukrepov iz prvih treh odstavkov tega člena je odgovoren zaposleni v ZZZS, ki organizira dogodek, v okviru katerega bo oziroma je nastal spisek osebnih podatkov.

15. člen
(vodenje evidence dejavnosti obdelave)

(1) ZZZS za namen pregleda nad vsemi dejavnostmi obdelave osebnih podatkov in z namenom dokazovanja skladnosti obdelav z GDPR vodi evidenco dejavnosti obdelav osebnih podatkov, ki jih upravlja. Skrbnik evidence dejavnosti obdelave je DPO.

(2) Evidenca dejavnosti obdelave osebnih podatkov obsega najmanj naslednje podatke:
a) kontaktne podatke ZZZS;
b) naziv zbirke;

c) skrbnika zbirke;
d) lastnika zbirke;
e) pravno podlago za obdelavo podatkov v zbirki;
f) namen obdelave;
g) opis kategorij posameznikov, na katere se nanašajo osebni podatki, in vrst obdelovanih podatkov;
h) kategorije uporabnikov, ki jim bodo razkriti osebni podatki, vključno z uporabniki v tretjih državah ali mednarodnih organizacijah;
i) informacije o prenosih osebnih podatkov v tretjo državo ali mednarodno organizacijo, vključno z identifikacijo te tretje države ali mednarodne organizacije, v primeru prenosov v tretjo državo ali mednarodno organizacijo, za katero še ni bil izdan sklep o skladnosti pa tudi dokumentacijo o ustreznih zaščitnih ukrepih;
j) predvidene roke za hranjene oziroma izbris podatkov;
k) splošni opis tehničnih in organizacijskih varnostnih ukrepov.

(3) Vsebina opisa in način opisa posamezne zbirke se izvede v skladu s Prilogo 3, ki je sestavni del tega pravilnika.

(4) Ob vzpostavitvi nove zbirke oziroma obdelave osebnih podatkov je vodja - direktor področja oziroma organizacijske enote v ZZZS, ki bo lastnik zbirke oziroma obdelave osebnih podatkov, odgovoren za pripravo popisa te zbirke v skladu s prejšnjim odstavkom.

2. poglavje
Obdelovalec osebnih podatkov

16. člen
(pogodbena obdelava osebnih podatkov)

(1) ZZZS lahko obdelavo osebnih podatkov zaupa obdelovalcu, ki zagotovi ustrezne organizacijske in tehnične ukrepe za varno obdelavo osebnih podatkov v skladu z zahtevami GDPR, ZVOP-2 in notranjih aktov ZZZS ter drugih predpisov s področja varstva osebnih podatkov.

(2) V zvezi z obdelavo osebnih podatkov, ki jo ZZZS zaupa obdelovalcu, ZZZS z obdelovalcem sklene pisno pogodbo o obdelavi osebnih podatkov, s katero določi vrsto in način izvajanja obdelave ter druge obveznosti in pravice obeh strank, v skladu z zahtevami GDPR.

(3) Z namenom zagotovitve, da so zahtevane določbe glede pogodbene obdelave osebnih podatkov vključene v vse relevantne pogodbe, ki jih ZZZS sklepa z zunanjimi izvajalci, pripravljavci pogodb osnutke le-teh posredujejo v predhodno mnenje DPO.

IV. DEL
OBVEŠČANJE O OBDELAVAH IN UVELJAVLJANJE PRAVIC POSAMEZNIKA

17. člen
(obveščanje o obdelavi osebnih podatkov)

(1) ZZZS na svoji spletni strani posameznike, v zvezi s katerimi obdeluje osebne podatke, obvesti o obstoju izvajanja obdelav in namenih obdelav z objavo potrebnih informacij o obdelavi osebnih podatkov v skladu s 13. in 14. členom GDPR.

(2) Obvestila iz prejšnjega odstavka morajo obsegati najmanj obvestila o:
1. imenu in kontaktnih podatkih ZZZS kot upravljavca osebnih podatkov;
2. kontaktnih podatkih DPO;
3. namenih, za katere se osebni podatki obdelujejo in pravni podlagi za njihovo obdelavo;
4. vrsti zadevnih osebnih podatkov;
5. uporabnikih ali kategorijah uporabnikov osebnih podatkov;
6. roku hrambe osebnih podatkov;
7. morebitnih prenosih osebnih podatkov v tretje države ali mednarodne organizacije;
8. obstoju pravice posameznika, da lahko zahteva dostop do osebnih podatkov in popravek ali izbris osebnih podatkov ali omejitev, ali obstoj pravice do ugovora obdelavi in pravice do prenosljivosti podatkov;
9. pravici do preklica privolitve, kadar obdelava temelji na privolitvi;
10. pravici do vložitve pritožbe pri Informacijskem pooblaščencu in njegove kontaktne podatke;
11. obstoju avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov ter vsaj v takih primerih smiselne informacije o razlogih zanj, kot tudi pomen in predvidene posledice take obdelave za posameznika, na katerega se nanašajo osebni podatki.

(3) Za pripravo informacij posameznikom iz prvega odstavka tega člena je odgovoren lastnik oziroma vsebinski skrbnik zadevne zbirke osebnih podatkov, ki v sodelovanju s Sektorjem za informiranje in odnose z javnostmi v ZZZS in DPO zagotovi tudi ustrezno objavo teh informacij.

18. člen
(varstvo zasebnosti uporabnikov spletne strani ZZZS)

ZZZS za namen varstva zasebnosti uporabnikov njegove spletne strani na tej spletni strani objavi politiko, s katero se v ZZZS ureja varstvo podatkov pri uporabi spletnih strani ZZZS.

19. člen
(postopek uveljavljanja pravic posameznika)

Zahteve za uveljavljanje pravic posameznikov iz 16. do 22. člena GDPR posameznik lahko poda ZZZS na obrazcu iz Priloge 5. Te zahteve rešuje lastnik oziroma vsebinski skrbnik zbirke osebnih podatkov, na katere se zahteve posameznikov nanašajo.

V. DEL
VARSTVO INFORMACIJSKE IN KOMUNIKACIJSKE ZASEBNOSTI KONČNIH UPORABNIKOV

20. člen
(varstvo službenega predala elektronske pošte)

(1) Predal elektronske pošte, ki je končnemu uporabniku dodeljen v zvezi z izvajanjem delovnih oziroma pogodbenih nalog v ZZZS je njegov osebni službeni elektronski naslov, ki se uporablja v službene namene (v nadaljnjem besedilu: predal e-pošte).

(2) Ne glede na prejšnji odstavek lahko končni uporabnik predal e-pošte uporablja v omejenem obsegu in razumnih mejah tudi v zasebne namene.

(3) Končni uporabnik predala e-pošte ne sme uporabljati:
- za namene različnih pridobitnih dejavnosti, razpošiljanje komercialnih informacij in podobno;
- za zasipanje drugih uporabnikov elektronske pošte z elektronskimi sporočili (angl. spam, junk e-mail; nenaročena reklamna gradiva, napadalna sporočila, verižna sporočila);
- za kreiranje in razpošiljanje kakršnih koli motečih ali žaljivih sporočil, ki vsebujejo žaljive komentarje glede rasne ali nacionalne pripadnosti, spola, barve kože, starosti, spolne usmerjenosti, verskega ali političnega prepričanja, ali imajo pornografsko ali kakšno drugo neprimerno vsebino oziroma vsebino, katere distribucija je kazniva;
- za prijave na elektronske poštne sezname (angl. mailing list), če ti niso vsebinsko povezani z delom, ki ga opravlja v okviru ZZZS;
- za pošiljanje sporočil z obvestili o virusih in drugi škodljivi programski opremi.

(4) V primeru prejema motečega ali žaljivega e-sporočila oziroma e-sporočila s škodljivo programsko opremo ali e-sporočila z opozorilom o škodljivi programski opremi mora končni uporabnik o tem nemudoma obvestiti službo za podporo uporabnikom na PE IC.

21. člen
(vpogled v službeno elektronsko pošto)

(1) Dostop do prometnih podatkov ali sporočil v predalu e-pošte je mogoč le v primeru predhodne in nedvoumne pisne privolitve končnega uporabnika predala e-pošte.

(2) Ob odsotnosti predhodne svobodne in nedvoumne osebne privolitve končnega uporabnika sme ZZZS v njegovo komunikacijsko zasebnost z vpogledom v prometne podatke in sporočila njegovega predala e-pošte poseči le:
- kadar je to nujno za izpolnitev zakonskih in pogodbenih obveznosti ZZZS, ki jih ni mogoče izpolniti na drug način;
- ob odsotnosti končnega uporabnika, ki traja več kot trideset delovnih dni in končni uporabnik za podajo soglasja ni dosegljiv ali ga zaradi zdravstvenega stanja ne more podati;

- v primeru smrti končnega uporabnika in v primeru prenehanja delovnega oziroma pogodbenega razmerja, kolikor ZZZS ocenjuje, da so v predalu e-pošte končnega uporabnika pomembna elektronska sporočila, izguba katerih bi ZZZS povzročila večjo škodo.

(3) ZZZS sme v primerih iz prejšnjega odstavka vpogledati le v prometne podatke predala e-pošte. Če je iz prometnih podatkov mogoče identificirati za ZZZS pomembno elektronsko sporočilo, se ZZZS z vsebino konkretnega elektronskega sporočila iz predala e-pošte lahko seznani le ob pisni privolitvi končnega uporabnika, ki je uporabnik predala, brez njegove privolitve pa le, če tega elektronskega sporočila ne more pridobiti od pošiljatelja oziroma naslovnika.

(4) Vpogled oziroma dostop do prometnih podatkov in sporočil v predalu e-pošte končnega uporabnika ob odsotnosti predhodne svobodne in nedvoumne pisne privolitve končnega uporabnika v izrednih primerih opravi tričlanska komisija, katere sestavo vsakokrat s sklepom določi generalna direktorica.

(5) ZZZS o vsakem dostopu do prometnih podatkov predala e-pošte določenega končnega uporabnika napiše zapisnik, ki vsebuje najmanj:
- obrazložen razlog za dopustnost dostopa do prometnih podatkov;
- zapis poteka dostopa s seznamom oseb, ki so pri tem sodelovale, morebitnimi pripombami končnega uporabnika, pri čemer mora biti ta zapis podpisan s strani vseh sodelujočih;
- izpis prometnih podatkov službenih elektronskih sporočil v predalu e-pošte.

(6) ZZZS o vsakem dostopu do vsebine elektronskega sporočila v predalu e-pošte končnega uporabnika napiše zapisnik, ki vsebuje najmanj:
- obrazložen razlog za dopustnost dostopa do vsebine konkretnega sporočila v predalu e-pošte; če ni bilo izrecne pisne privolitve končnega uporabnika, tudi izkaz dejstva, da sporočila ni bilo mogoče pridobiti od pošiljatelja oziroma naslovnika;
- zapis poteka dostopa s seznamom oseb, ki so pri tem sodelovale, morebitnimi pripombami končnega uporabnika, pri čemer moram biti ta zapis podpisan s strani vseh sodelujočih;
- izpis vsebine elektronskega sporočila, do katerega je bilo dostopano.

(7) ZZZS je končnemu uporabniku, razen v primeru, ko se ukrepi iz tega člena izvajajo po smrti končnega uporabnika, dolžan omogočiti prisotnost pri dostopu do prometnih podatkov njegovega predala e-pošte in do sporočil v njegovem osebnem predalu službene pošte. ZZZS je dolžan o nameri za izvedbo tega ukrepa končnega uporabnika obvestiti vsaj en delovni dan prej in mu zaradi prisotnosti pri izvedbi ukrepa po potrebi tudi prilagoditi delovne obveznosti. Končni uporabnik ima pravico do vpogleda v celotno dokumentacijo, ki se navezuje na dostop do prometnih podatkov in do sporočil svoje e-pošte. Če je pri ukrepu prisoten, ima kočni uporabnik pravico, da na zapisnik o poteku dostopa doda tudi svoje pripombe.

(8) Način izpisa prometnih podatkov oziroma sporočil iz predalov e-pošte v navodilu podrobneje določi generalna direktorica.

22. člen
(zaprtje predala e-pošte)

Ob prenehanju pogodbe o zaposlitvi delavca ZZZS, prenehanju pogodbenega razmerja zunanjega sodelavca ZZZS ali prenehanju dela na podlagi študentske napotnice, mora biti predal e-pošte tega končnega uporabnika zaprt, vsebina predala pa izbrisana skladno z organizacijskim predpisom, s katerim se v ZZZS ureja uporabo storitev interneta in elektronske pošte ZZZS ter v skladu s politiko, s katero se v ZZZS ureja revizijske sledi v informacijskem sistemu ZZZS.

23. člen
(dostop končnih uporabnikov do interneta)

(1) Končni uporabnik dostop do interneta, ki mu ga je ZZZS dodelil za izvajanje delovnih oziroma pogodbenih nalog, uporablja skladno z organizacijskim predpisom, s katerim se v ZZZS ureja uporabo storitev interneta in elektronske pošte ZZZS.

(2) Ne glede na prejšnji odstavek lahko končni uporabnik internet v omejenem obsegu in razumnih mejah uporablja tudi v zasebne namene. Internetne strani, ki se pregledujejo v zasebne namene, ne smejo biti z neprimerno vsebino.

(3) Generalna direktorica lahko z odredbo odredi blokado dostopa določenih končnih uporabnikov do določenih spletnih strani. Blokado dostopa v obsegu, določenem v odredbi, izvede PE IC.

(4) O blokadi se vse končne uporabnike, ki jih blokada zadeva, obvesti po elektronski pošti oziroma z objavo na intranetnih straneh ZZZS.

24. člen
(ukrepanje v primeru kršitve uporabe predala e-pošte in interneta)

(1) Če informacijski skrbnik sistema ZZZS e-pošte oziroma povezave z internetom ugotovi, da končni uporabnik predala e-pošte ali interneta ne uporablja v skladu s pravili uporabe e-pošte oziroma interneta, lahko končnemu uporabniku takoj blokira dostop do njegovega predala e-pošte oziroma do interneta ter zavaruje dokaze, ki kažejo na kršitev pravil uporabe. Umik blokade dostopa končnega uporabnika do predala e-pošte oziroma do interneta se izvede po zaključku postopka obravnave varnostnega dogodka suma nepravilne uporabe predala e-pošte oziroma interneta.

(2) Ob sumu, da kočni uporabnik preko službenega predala e-pošte ali priključka na internet izvršuje oziroma je izvršil kaznivo dejanje, je ZZZS dolžan to sporočiti pristojnim državnim organom.

25. člen
(zavarovanje dokazov)

Če ZZZS oceni, da mu je ali bi mu lahko zaradi kršitve uporabe predala e-pošte ali interneta s strani končnega uporabnika nastala škoda najmanj v višini majhne premoženjske škode po določbah Kazenskega zakonika, lahko zaradi zavarovanja dokazov onemogoči nadaljnjo uporabo službene računalniške opreme, vključno s službeno mobilno napravo, ki jo končni uporabnik uporablja za dostop do predala e-pošte oziroma interneta, jo zapečati in shrani. Pečatenje opravi komisija, ki jo imenuje generalna direktorica, pri čemer je eden od članov komisije predstavnik sindikata zaposlenih ZZZS. Zapečatena računalniška oprema se hrani dokler je to potrebno za potrebe uveljavljanja povračila škode. V tem času, razen pooblaščenih oseb ZZZS, ki sodelujejo pri uveljavljanju odškodninskega zahtevka ter razen pristojnih državnih organov, zapečatene računalniške opreme nihče ne sme vklopiti ali kako drugače posegati vanjo.

26. člen
(nadzor uporabe službenih telefonov)

(1) V prometne podatke mobilnih telefonskih priključkov, katerih lastnik je ZZZS in so zaposlenim v ZZZS dodeljeni za izvajanje delovnih nalog (v nadaljnjem besedilu: službeni telefon), lahko ZZZS vpogleda le takrat, kadar med ZZZS in zaposlenim pride do kakršnegakoli spora glede višine stroškov porabe konkretnega službenega telefona.

(2) ZZZS pri vpogledu v prometne podatke iz prejšnjega odstavka tega člena ne sme preverjati identitete oziroma lastništva klicanih ali kličočih številk, razvidnih iz prometnih podatkov.

VI. DEL
VARSTVO OBDELAVE OSEBNIH PODATKOV

1. poglavje
Organizacijski ukrepi

27.člen
(vgrajeno in privzeto varstvo podatkov)

(1) ZZZS v okviru razvoja oziroma nabave programske in strojne opreme za rešitve in storitve obdelave osebnih podatkov dosledno sledi pravilu vgrajenega in privzetega varstva osebnih podatkov, ki obsega predvsem:
- obdelavo osebnih podatkov v najmanjšem obsegu za dosego namena obdelave;
- uporabo psevdonimizacije kot ukrepa varnosti obdelave in izraza načela najmanjšega obsega podatkov in anonimizacije osebnih podatkov, v primeru, ko je to možno;
- zagotavljanje revizijskih sledi oziroma vodenje dnevnika obdelav.

(2) Pri razvoju, oblikovanju, izboru in uporabi aplikacij, storitev in produktov, ki vključujejo obdelavo osebnih podatkov, mora ZZZS ali njegovi pogodbeni obdelovalci ob upoštevanju najnovejših tehnoloških možnosti, zagotoviti izpolnjevanje obveznosti varstva osebnih podatkov.

(3) Za izvajanje pravila vgrajenega in privzetega varstva osebnih podatkov so v ZZZS za izdelavo rešitev oziroma uvedbo produktov in storitev obdelave podatkov odgovorni pristojni vodje - direktorji področij, sektorjev oziroma drugih organizacijskih enot, katerih poslovanje bodo nove rešitve oziroma storitve podprle. Z namenom preverjanja zagotavljanja vgrajenega in privzetega varstva se ob spremembah obstoječih oziroma ob vpeljavi novih obdelav osebnih podatkov izpolni kontrolni vprašalnik iz Priloge 7, ki je sestavni del tega pravilnika, oziroma se smiselno izvede ocena učinka v zvezi z varstvom osebnih podatkov.

(4) Vsi dokumenti iz Priloge 8, ki je sestavni del tega pravilnika, in sestavljajo SUVI, ter v katerih so opredeljeni tehnični in organizacijski ukrepi, s katerimi ZZZS zagotavlja vgrajeno in privzeto varstvo, so ažurno objavljeni v e-gradivih.

(5) Svetovanje in nadzor nad upoštevanjem pravila vgrajenega in privzetega varstva osebnih podatkov v okviru obdelave osebnih podatkov izvaja DPO.

28. člen
(ustreznost osebnih podatkov)

Osebni podatki, ki jih obdeluje ZZZS, morajo biti točni, posodobljeni ter po obsegu primerni in ustrezni glede na namene, za katere se obdelujejo, za kar so dolžni poskrbeti skrbniki zbirk in končni uporabniki.

29. člen
(popis informacijskih sredstev)

(1) ZZZS pregled nad rešitvami, napravami, sistemi in drugo infrastrukturo, ki jih uporablja za obdelavo zbirk, vodi popis informacijskih sredstev. Pri tem upošteva politiko, s katero se v ZZZS ureja varovanje informacijskih virov.

(2) Iz popisa informacijskih sredstev mora biti, v povezavi z evidenco dejavnosti obdelave, razvidno, s katerim sredstvom se določena zbirka obdeluje in na katerem sredstvu se določena vrsta osebnih podatkov nahaja. Prikazi podatkov popisa informacijskih sredstev morajo biti prilagojeni tako zahtevam zaposlenih, odgovornih za obdelavo in zagotavljanje varnosti obdelave, kakor tudi reševanju zahtev za varstvo pravic posameznika v zvezi z obdelavo podatkov, ki se nanašajo nanj.

(3) Pristop k izdelavi popisa informacijskih sredstev, postopke in odgovornost za njegovo vzdrževanje in informacijsko podporo določa politika iz prvega odstavka tega člena. Izdelavo in vzdrževanje popisa informacijskih sredstev koordinira koordinator.

30. člen
(uporaba zasebnih naprav za obdelavo osebnih podatkov)

ZZZS v SUVI in posebnih navodilih določi pravila uporabe zasebnih naprav (računalnikov, tablic, pametnih telefonov) za obdelavo osebnih podatkov, s katerimi upravlja ali jih v okviru svojega poslovanja obravnava ZZZS. Politika in navodila morajo obsegati tudi postopke za zagotavljanje varnosti obdelave na zasebnih napravah in ukrepanje v primeru odtujitve ali pogrešitve take naprave.

2. poglavje
Ocena učinka v zvezi z varstvom osebnih podatkov

31. člen
(obveznost izdelave ocene učinka)

(1) ZZZS osebne podatke in njihovo obdelavo varuje s tehničnimi in organizacijskimi ukrepi, ki temeljijo na oceni tveganj za pravice in svoboščine posameznika, zlasti zaradi namernega ali nezakonitega uničenja, izgube, spremembe, nepooblaščenega razkritja ali dostopa do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani.

(2) Ocena učinka v zvezi z varstvom osebnih podatkov (v nadaljnjem besedilu: DPIA) je obvezna za vsako novo obdelavo osebnih podatkov v ZZZS, če je na seznamu vrst dejanj obdelave, za katere je DPIA obvezna (npr. za nove tehnologije, oblikovanje profilov ter sprejemanje odločitev, ki imajo pravne učinke na posameznika, obsežno spremljanje javno dostopnega območja, obsežna obdelava posebnih vrst osebnih podatkov).

(3) DPIA se pripravi tudi, kadar ZZZS oceni, da bi lahko določena obdelava osebnih podatkov, četudi ni na seznamu obvezne izdelave DPIA, povzročila veliko tveganje za pravice in svoboščine posameznikov. V eni oceni je lahko obravnavan niz podobnih dejanj obdelave, ki predstavljajo podobna velika tveganja.

(4) Nosilec izdelave DPIA je lastnik oziroma vsebinski skrbnik zbirke oziroma procesa, v okviru katerih se bodo obdelovali podatki, katerih obdelava bi lahko vplivala na pravice in svoboščine zadevnih posameznikov, v sodelovanju z informacijskim skrbnikom. Za mnenje k DPIA vedno zaprosi DPO.

(5) Presoja potrebnosti izvedbe DPIA in izdelava DPIA se izvaja na način, kot je določeno v Prilogi 9, ki je sestavni del tega pravilnika.

32. člen
(vsebina DPIA)

(1) DPIA zajema vsaj:
- sistematičen opis predvidenih dejanj obdelave in namenov obdelave, kadar je ustrezno pa tudi zakonitih interesov, za katere si prizadeva ZZZS;

- oceno potrebnosti in sorazmernosti dejanj obdelave glede na njihov namen;
- oceno tveganj za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki;
- ukrepe za obravnavanje tveganj, vključno z zaščitnimi ukrepi, varnostne ukrepe ter mehanizme za zagotavljanje varstva osebnih podatkov in za dokazovanje skladnosti z GDPR in ZVOP-2, ob upoštevanju pravic in zakonitih interesov posameznikov, na katere se nanašajo osebni podatki, ter drugih oseb, ki jih to zadeva.

(2) Po potrebi ZZZS glede ocenjevane obdelave zaprosi za mnenje posameznike, na katere bi se nanašali obdelovani podatki, ali njihove predstavnike (npr. združenja, zbornice).

(3) Ugotovitve DPIA se dokumentirajo v poročilu, ki mora obsegati oceno:
- ali je predlagani način obdelave skladen s predpisanimi zahtevami;
- ali bo za zagotovitev skladnosti treba izvesti dodatne ukrepe;
- ali je treba v zvezi z ocenjevano obdelavo izvesti predhodno posvetovanje z Informacijskim pooblaščencem;
- ali pa so ugotovljena tveganja tako visoka, da ocenjevane obdelave ni mogoče izvesti v skladu s predpisanimi zahtevami.

(4) Poročilo o DPIA postane sestavni del dokumentacije projekta nove obdelave osebnih podatkov in podlaga za izvedbo tehničnih in organizacijskih ukrepov vgrajenega in privzetega varstva osebnih podatkov v sredstva obdelave, skladnih z GDPR, ZVOP-2 in drugimi relevantnimi predpisi.

3. poglavje
Spremembe načina obdelave osebnih podatkov

33. člen
(upravljanje sprememb načina obdelave osebnih podatkov)

(1) Upravljanje sprememb načina obdelave osebnih podatkov se izvaja skladno s politiko, s katero se v ZZZS upravlja pobude in spremembe informacijskega sistema ZZZS.

(2) Razvojno, testno in produkcijsko okolje informacijskih rešitev, s katerimi se izvaja obdelava osebnih podatkov, morajo biti popolnoma ločena.

(3) Vsaka sprememba informacijskih rešitev, ki vpliva na varstvo osebnih podatkov, se najprej preizkusi izključno v razvojnem okolju in izključno z imaginarnimi podatki ali javno dostopnimi digitalnimi vsebinami. Vsaka sprememba informacijske rešitve se mora ustrezno dokumentirati, in sicer tako, da se označi nova različica, opisno opredelijo vzroki spremembe in bistvene dopolnitve ter določi mesto hrambe nove in prejšnje različice. Vedno se varno hranijo vse različice informacijske rešitve in dokumentacije za nazaj.

(4) Realni podatki ne smejo nikoli zapustiti produkcijskega okolja in se ne smejo prenašati v nobeno drugo okolje ali posredovati drugim osebam brez izrecne podlage v veljavnem zakonu ali brez

izrecnega soglasja vseh pogodbenih strank, na katero se podatki nanašajo, ter po vnaprejšnji presoji, ali je takšno ravnanje v skladu z vsemi veljavnimi predpisi.

(5) Pred vsakokratno namestitvijo nove različice informacijske rešitve se:
- predvidi način in morebitne težave namestitve in delovanja v sistemu;
- uspešno preizkusi nova različica v testnem okolju, kar se ustrezno dokumentira;
- skladno s spremembami dopolni oziroma drugače popravi relevantna dokumentacija.

(6) Novih različic informacijskih rešitev, ki vplivajo na varstvo osebnih podatkov, ni dopustno nameščati, preden se uspešno in pravilno ne izvedejo vsa opravila po prejšnjem odstavku.

(7) Pred namestitvijo nove informacijske rešitve oziroma aplikativne podpore za storitve, ki vplivajo na varstvo osebnih podatkov, oziroma namestitvijo spremembe že obstoječe informacijske rešitve, vsebinski skrbnik določi potrebne aktivnosti za usposabljanje oziroma informiranje vseh uporabnikov.

(8) Nadzor nad spoštovanjem pravil upravljanja sprememb načina obdelave osebnih podatkov izvajata koordinator in DPO.

4. poglavje
Posredovanje osebnih podatkov osebam javnega sektorja ali drugim osebam

34. člen
(postopek posredovanja osebnih podatkov)

(1) Posredovanje osebnih podatkov osebam javnega sektorja ali drugim fizičnim ali pravnim osebam se izvaja v skladu z navodilom, s katerim se v ZZZS določa postopek posredovanja osebnih in drugih podatkov.

(2) Zahteva za posredovanje osebnih podatkov, ki mora vsebovati podatke, določene v 41. členu ZVOP-2, se lahko poda tudi obrazcu iz Priloge 10, ki je sestavni del tega pravilnika.

(3) Posredovanje osebnih podatkov iz zbirk lahko poteka tudi avtomatizirano, preko neposrednega dostopa pooblaščenega uporabnika do informacijskega sistema ZZZS. Način tovrstnega posredovanja se uredi s pogodbo oziroma dogovorom med ZZZS in uporabnikom.

35. člen
(evidentiranje posredovanja osebnih podatkov)

(1) Vsako posredovanje osebnih podatkov se zaznamuje z navedbo kateri, kdaj in komu so bili osebni podatki posredovani, na kateri pravni podlagi in s kakšnim namenom oziroma iz katerih razlogov oziroma za potrebe katerega postopka.

(2) Kadar osebje pooblaščenega uporabnika do podatkov v zbirkah ZZZS dostopa neposredno, na podlagi pogodbe oziroma dogovora, se posredovanje evidentira z zabeležbo posameznega dostopa v revizijski sledi oziroma dnevniku obdelave ZZZS informacijskega sistema.

36. člen
(prenos osebnih podatkov v tretje države in mednarodne organizacije)

Zahteve za posredovanje oziroma prenos osebnih podatkov v tretje države ali mednarodne organizacije se obravnavajo in izvajajo na način, kot je določeno v Prilogi 11, ki je sestavni del tega pravilnika.

5. poglavje
Varovanja in sledenje obdelavam osebnih podatkov

37. člen
(nadzor dostopa do obdelovanih osebnih podatkov)

(1) Dostop končnih uporabnikov do osebnih podatkov mora biti kontroliran s sistemom gesel oziroma drugih avtentikacijskih sredstev, povezanih s sistemom za upravljanje pravic posameznika za uporabo določenih informacijskih rešitev oziroma sistemov in določenih vrst oziroma zbirk osebnih podatkov.

(2) Končnemu uporabniku se obseg dostopnih pravic za obdelavo osebnih podatkov oziroma uporabo informacijskega sistema, ki je nujno potreben za izvajanje njegovih delovnih nalog, določi skladno s shemo pooblastil oziroma navodilom za dodeljevanje pooblastil v ZZZS.

VII. DEL
KRŠITEV VARNOSTI OSEBNIH PODATKOV

38. člen
(varnostni dogodki in incidenti)

(1) ZZZS v SUVI določi postopke obravnavanja kršitev pravil varnosti, določenih v tem pravilniku in drugih notranjih aktih, ki bi lahko povzročile ali povzročijo uničenje, izgubo, spremembo, nepooblaščeno razkritje ali dostop do osebnih podatkov, ki so poslani shranjeni ali kako drugače obdelani, ali katastrofalen izpad oziroma uničenje opreme za izvajanje obdelave.

(2) O obravnavanih kršitvah varstva osebnih podatkov DPO najmanj enkrat letno poroča strateški skupini.

39. člen
(obveznost obveščanja o kršitvah varnosti osebnih podatkov)

(1) Končni uporabniki so dolžni o aktivnostih, ki so povezane z odkrivanjem ali nepooblaščenim uničenjem osebnih podatkov, zlonamerni ali nepooblaščeni uporabi, prilaščanju, spreminjanju ali poškodovanju osebnih podatkov oziroma o pojavu računalniškega virusa ali druge škodljive programske kode oziroma v primeru kateregakoli drugega varnostnega dogodka ali incidenta takoj obvestiti službo za podporo uporabnikom PE IC, sami pa ukreniti vse, kar je v njihovi moči, da takšna dejavnost preneha oziroma se njeno nadaljnje izvajanje prepreči.

(2) Končni uporabniki morajo v zvezi s kršitvijo varnosti osebnih podatkov, ki lahko povzroči premoženjsko ali nepremoženjsko škodo, kot je izguba nadzora nad osebnimi podatki ali omejitev njihovih pravic, diskriminacija, kraja ali zloraba identitete, finančna izguba, neodobrena reverzija psevdonimizacije, okrnitev ugleda, izguba zaupnosti osebnih podatkov, zaščitenih s poklicno skrivnostjo, ukrepati v skladu z organizacijskim navodilom, s katerim se v ZZZS ureja upravljanje varnostnih dogodkov in incidentov.

(3) Kadar obdelavo osebnih podatkov izvaja obdelovalec, je treba zahteve iz prejšnjega odstavka vključiti v pogodbo o obdelavi osebnih podatkov in k njihovemu izvajanju zavezati tudi osebje obdelovalca.

40. člen
(obveščanje posameznikov in Informacijskega pooblaščenca o kršitvah varnosti osebnih podatkov)

(1) V primeru kršitve varnosti osebnih podatkov, zaradi katere bi lahko bile ogrožene pravice in svoboščine posameznikov, mora DPO pripraviti in najpozneje v 72 urah po seznanitvi s kršitvijo, Informacijskemu pooblaščencu, z izpolnitvijo obrazca iz Priloge 12, ki je sestavni del tega pravilnika, poslati uradno obvestilo o kršitvi varnosti osebnih podatkov. S tem obvestilom mora DPO seznaniti tudi generalno direktorico.

(2) Kadar je verjetno, da kršitev varnosti osebnih podatkov povzroči veliko tveganje za pravice in svoboščine posameznikov, mora ZZZS brez nepotrebnega odlašanja o tem obvestiti posameznike, katerih osebni podatki so bili kršeni ali je verjetno, da so bili kršeni, razen kadar obveščanje skladno z GDPR in ZVOP-2 ni potrebno.

(3) Presoja, ali je o določeni kršitvi varnosti osebnih podatkov potrebno obveščati Informacijskega pooblaščenca oziroma zadevne posameznike, se izvede v skladu s protokolom iz Priloge 13, ki je sestavni del tega pravilnika.

VIII. DEL
ODGOVORNOST ZA IZVAJANJE POSTOPKOV IN UKREPOV ZA ZAVAROVANJE OSEBNIH PODATKOV

41. člen
(izvajanje postopkov in ukrepov varstva osebnih podatkov)

(1) Končni uporabniki so dolžni izvajati ukrepe za varstvo osebnih podatkov, skladno s SUVI ter varovati zaupnost osebnih podatkov, s katerimi so se seznanili pri opravljanju svojega dela. Obveznost varovanja podatkov ne preneha s prenehanjem delovnega razmerja oziroma drugega pogodbenega razmerja.

(2) Kadar obdelavo izvaja obdelovalec, je treba zahteve iz prejšnjega odstavka vključiti v pogodbo o obdelavi osebnih podatkov in k njihovemu izvajanju zavezati tudi osebje obdelovalca.

(3) Ob zaključku dela na ZZZS, vsi zaposleni in vsi tisti zunanji sodelavci ZZZS, ki so pri svojem delu obdelovali osebne podatke ZZZS in so v zvezi s tem prejeli v uporabo opremo za dostop do informacijskega sistema ZZZS, podpišejo izjavo na obrazcu iz Priloge 14, ki je sestavni del tega pravilnika.

42. člen
(dolžnost varovanja osebnih podatkov v pogodbi o zaposlitvi)

Pogodba o zaposlitvi v ZZZS mora obsegati obvestilo o obveznostih zaposlenega glede varovanja osebnih podatkov.

43. člen
(odgovornost za kršitev varnosti osebnih podatkov)

Kršitev določil tega pravilnika glede varnosti osebnih podatkov s strani končnih uporabnikov pomeni kršitev obveznosti iz delovnega oziroma pogodbenega razmerja.

44. člen
(izvajanje notranjega nadzora nad varstvom osebnih podatkov)

(1) Nadzor nad izvajanjem postopkov in ukrepov varstva osebnih podatkov in varnosti obdelave, določenih s tem pravilnikom, relevantnimi predpisi in veljavnimi pogodbami, izvajata DPO in koordinator.

(2) O ugotovitvah izvedenega nadzora o stanju varstva osebnih podatkov najmanj enkrat letno DPO in koordinator poroča strateški skupini.

IX. DEL
KONČNI DOLOČBI

45. člen
(prenehanje veljavnosti)

Z dnem uveljavitve tega pravilnika preneha veljati Pravilnik o varstvu osebnih podatkov Zavoda za zdravstveno zavarovanje Slovenije, št. 0071-4/2007-DI/2, z dne 6. 3. 2020.

46. člen
(začetek veljavnosti)

Ta pravilnik začne veljati petnajsti dan po objavi na spletni strani ZZZS.

Številka: 0071-1/2023-IC/30
Ljubljana, 23. 8. 2023

doc. dr. Tatjana Mlakar
generalna direktorica