



Priloga 6. Varovanje osebnih podatkov

Kazalo

1	Varovanje osebnih podatkov.....	3
1.1	Splošno	3
1.2	Ključni elementi obdelave osebnih podatkov.....	5
1.2.1	Vrste osebnih podatkov	5
1.2.2	Predvideni nameni obdelave osebnih podatkov.....	6
1.2.3	Pravna podlaga za obdelavo osebnih podatkov	6
1.2.4	Opredelitev rokov hrambe.....	7
1.2.5	Predvidena dejanja obdelave osebnih podatkov	7
1.2.6	Opredelitev lokacije obdelave in hrambe podatkov.....	8
1.2.7	Kategorije uporabnikov	8
2	Skladnost z zakonodajo	10
2.1	Zakonodaja s področja varstva podatkov	10
2.2	Zakonodaja s področja delovne zakonodaje.....	11
3	Ukrepi	12
3.1	Zahteve ponudnika infrastrukture (NIJZ)	13
3.2	Zaupnost ter omejen dostop.....	14
3.3	Izobraževanje.....	14
3.4	Šifriranje podatkov	15
3.5	Sledljivost.....	16
3.6	Izhodni načrt / načrt prehoda	16
4	Obvladovanje tveganj.....	17
4.1	Metodološka izhodišča za oceno učinka v zvezi z varstvom podatkov	17
4.2	Minimalni nabor tveganj.....	19
4.3	Ocena učinka na temeljne pravice (FRIA)	22
5	Pravice posameznikov	24
6	Odzivanje na kršitve.....	25
7	Revizije in pregledi	26

1 Varovanje osebnih podatkov

1.1 Splošno

Namen rešitve IS ADRZ v ožjem smislu je zagotavljanje boljše organizacije dela v zdravstvenem sistemu (tj. enostavnejše, preglednejše in učinkovitejše načrtovanje urnikov v zdravstvenih ustanovah) in v širšem smislu doseganje učinkovitejšega in sodobnejšega zdravstvenega sistema (npr. izboljšanje delovne zakonodaje v zdravstvenem sistemu; izboljšanje komunikacije med deležniki, višja kakovost oskrbe pacientov).

V ožjem smislu IS ADRZ, skladno s terminologijo Splošne uredbe o varstvu podatkov¹, predstavlja **sredstvo obdelave osebnih podatkov** naslednjih kategorij posameznikov:

- delavci v delovnem razmerju,
 - delavci v drugem pogodbenem razmerju (izvajalci po delovršnih pogodbah, delavci na usposabljanju in specializaciji, študentje),
- za katere se v nadaljnjem besedilu poenoteno uporablja **izraz »zaposleni« ali tudi »posamezniki«**.

Namen rešitve v **ožjem smislu** v celoti sledi namenu obdelave osebnih podatkov v okviru kadrovskih procesov (tj. za potrebe izpolnjevanja zakonskih zahtev delodajalca oz. za potrebe uveljavljanja pravic in obveznosti zaposlenih iz delovnega ali drugega pogodbenega razmerja). V vlogi delodajalca nastopa javni zdravstven zavod, ki bo uporabnik IS ADRZ. Vsak javni zdravstveni zavod zase bo nastopal kot samostojni upravljavec osebnih podatkov svojih zaposlenih, kar je potrebno upoštevati pri zasnovi infrastrukture IS ADRZ (tj. ločene baze podatkov).

V **širšem smislu** namen IS ADRZ presega prvotni namen obdelave osebnih podatkov zaposlenih. Posledično se z ustreznimi ukrepi zagotovi obdelava osebnih podatkov na sekundarni ravni v popolnoma anonimizirani obliki (tj. analitični podatki). Dostop do slednjih se zagotovi resornemu ministrstvu za potrebe nadaljnjega oblikovanja strategij ter politik za izboljšanje učinkovitosti in dostopnosti zdravstvenega sistema.

¹ Uredba (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 (Splošna uredba o varstvu podatkov).

Tabela 1: Shema deležnikov*

Deležnik	Vloga z vidika obdelave OP	Vloga z vidika IS ADRZ	Naloge
Zaposleni / delavci	Posameznik, na katerega se osebni podatki nanašajo	Uporabnik IS ADRZ v ožjem smislu (zdravstveno osebje)	Uporaba IS ADRZ za izpolnjevanje delovnih obveznosti pri svojem delodajalcu (JZZ).
javni zdravstveni zavod (JZZ) / delodajalec	Upravljalac osebnih podatkov	Uporabnik IS ADRZ v ožjem smislu (načrtovalec delovnih razporedov, vodstvo zavoda, administrator na nivoju JZZ)	Uporaba IS ADRZ za izdelavo delovnih razporedov in razporejanje zaposlenih.
Ministrstvo za zdravje	Obdelovalec	Uporabnik IS ADRZ v širšem smislu (uporabnik anonimiziranih oz. analitičnih podatkov; administrator na nivoju rešitve)	Lastnik IS ADRZ (nosilec pogodbe s ponudnikom IS ADRZ; nosilec pogodbe z JZZ); podpora pri uporabi IS ADRZ; izobraževanja/usposabljanja
NIJZ	Pod-obdelovalec	Ponudnik infrastrukture	Zagotavljanje tehničnih ukrepov; podpora pri uporabi IS ADRZ; izobraževanja/usposabljanja
Ponudnik IS ADRZ	Pod-obdelovalec	Vzdrževanje, nadgradnje, podpora Razvija IS ADRZ Obdeluje podatke v imenu upravljavca.	Razvoj; vzdrževanje, podpora pri uporabi IS ADRZ

*OPOMBA: Zgoraj navedene vloge ter naloge so predvidene. Naročnik dopušča možnost, da se vloge posameznih deležnikov ter njihove naloge v fazi razvoja IS ADRZ ali v fazi oblikovanja pogodbenih odnosov določijo drugače glede na dejanske pravice in obveznosti posameznega deležnika.

Ponudnik IS ADRZ mora pri izvajanju storitev (razvoj, vzdrževanje in podpora) v največji možni meri upoštevati veljavne predpise, dobre prakse s področja varstva osebnih podatkov, mednarodno priznane standarde in varnostne usmeritve naročnika za ustrezno delovanje informacijsko-komunikacijskih tehnologij ter modernih tehnologij (npr. glede algoritmov, interneta, informacijske varnosti, umetne inteligence idr.) ter zaščito podatkov.

V tem dokumentu so določene zahteve, ki jih mora izpolnjevati ponudnik IS ADRZ in/ali rešitev IS ADRZ. V fazi razvoja IS ADRZ je potrebno v največji možni meri in s skrbnostjo dobrega strokovnjaka upoštevati načelo »vgrajenega in privzetega« varstva osebnih podatkov² ter slediti najnovejšemu tehnološkemu razvoju ob upoštevanju stroškovne učinkovitosti pri uporabi virov.

Naročnik si v fazi implementacije IS ADRZ pridržuje pravico, da v sodelovanju z izbranim ponudnikom IS ADRZ za namene izboljšanja (zasnove) rešitve IS ADRZ spremeni posamezne zahteve iz tega

² EDPB: Smernice št. 4/2019 o členu 25 Vgrajeno in privzeto varstvo podatkov, Različica 2.0, sprejete 20. oktobra 2020.

dokumenta ali slednje podrobneje opredeli. Vse morebitne dodatne zahteve po navodilih naročnika, naročnik in ponudnik IS ADRZ opredelita pisno (npr. dodatek k pogodbi o izvedbi javnega naročila).

V nobenem primeru opustitve posameznih ukrepov ali njihove spremembe niso dopustne, v kolikor bi lahko povzročile nižjo ali za posameznega upravljavca nesprejemljivo raven zaščite osebnih podatkov ali nižjo odpornost rešitve IS ADRZ ali bi lahko povzročile povečanje tveganja iz naslova učinkov obdelave osebnih podatkov na pravice posameznika.

1.2 Ključni elementi obdelave osebnih podatkov

V nadaljevanju so navedeni ključni elementi obdelave osebnih podatkov v okviru rešitve IS ADRZ, glede na predvideno zasnovo. Slednje je pomembno za pravilno razumevanje predvidenih obdelav osebnih podatkov in namena obdelave, ki mu mora ponudnik IS ADRZ v celoti slediti. Ponudnik IS ADRZ rešitve v nobenem primeru ne sme zasnovati na način, ki bi omogočal obdelavo osebnih podatkov tudi za druge namene ali na drugačen način ali s strani nepooblaščenih oseb.

Javni zdravstveni zavodi, ki bodo uporabniki IS ADRZ, bodo vsak zase nastopali kot upravljavec osebnih podatkov svojih zaposlenih. Vsak upravljavec zase vodi zadevne evidence dejavnosti obdelav osebnih podatkov s področja kadrovanja, in sam določa namene ter druge elemente obdelave osebnih podatkov. Samodejno povezovanje zbirk osebnih podatkov enega upravljavca s podatki drugega upravljavca ni dopustno. Ne glede na navedeno mora rešitev IS ADRZ omogočiti upravljavcu³ ali posamezniku možnost izvoza osebnih podatkov tega posameznika od enega k drugemu upravljavcu (npr. specializacije).

Glede na navedeno naročnik ne zagotavlja, da so vrste osebnih podatkov in drugi elementi obdelave, navedeni v tem poglavju izčrpni in točni. Rešitev AS ADRZ mora biti zasnovana dovolj fleksibilno, da posameznega upravljavca ne omejuje pri izvrševanju njegovih zakonskih obveznosti s področja varstva osebnih podatkov in ga ne usmerja v določeno ravnanje ali obdelave osebnih podatkov.

1.2.1 Vrste osebnih podatkov

Upravljavec bo v okviru IS ADRZ predvidoma zbiral in obdeloval naslednje vrste osebnih podatkov:

- enolična identifikacijska oznaka zdravstvenega delavca;
- številka delavca RIZDDZ;
- ime in priimek;
- spol;
- status zaposlitve;
- datum zaposlitve oz. začetka pogodbenega sodelovanja;
- datum prenehanja zaposlitve oz. pogodbenega sodelovanja;

³ Op. Pod pogojem, da upravljavec pri sebi zagotovi ustrezno pravno podlago.

- vrsta pogodbe (redna zaposlitev, podjemna pogodba, dopolnilno delo, pogodba, študentsko delo);
- oznaka organizacijske enote zdravstvenega delavca;
- podatki o omejitvah, ki lahko vključujejo posebne vrste osebnih podatkov (npr. zdravstveni podatki); podatki o soglasjih;
- datum in ura zadnje spremembe podatkov o zaposlenem;
- drugi nujno potrebni podatki (npr. podatki iz IS Kadrovska evidenca, podatki iz IS Registracija delovnega časa; .

Rešitev IS ADRZ mora biti zasnovana na način, ki omogoča enostaven dostop do zbirnega prikaza vseh osebnih podatkov o posamezniku vključno s podatki o datumu in času prvega vnosa ter (najmanj zadnjih) sprememb.

Poleg navedenih osebnih podatkov, se o ali v zvezi z dejanji posameznika lahko beležijo tudi naslednje vrste podatkov:

- tehnični podatki (tehnične informacije mobilne naprave ali računalnika);
- analitični podatki (IP naslov, ID naprave, vrsta operacijskega sistema);
- podatki, ki jih uporabnik samovoljno posreduje (tj. iz naslova dvosmerne komunikacije: sporočila, vprašanja ter s tem povezani metapodatki, idr.);
- podatki o nivoju uporabnika (obseg uporabniških pravic, npr. zdravstveno osebje, načrtovalec delovnih razporedov, vodstvo zavoda, administrator, blokirani);
- revizijska sled, npr. podatki o časovnih mejnikih (datum registracije, spremembe, preklica, pregleda itd.);
- drugi podatki, v kolikor bo to nujno potrebno in sorazmerno namenom obdelave.

1.2.2 Predvideni nameni obdelave osebnih podatkov

Predvideni namen obdelave osebnih podatkov posameznikov v IS ADRZ so:

- izpolnjevanje zakonskih obveznosti delodajalca iz delovnopravne zakonodaje (npr. vodenje evidence o izrabi delovnega časa; zdravstveno zavarovanje, itd.);
- izvajanje pravic in obveznosti iz delovnega ali drugega pogodbenega razmerja (npr. uveljavljanje pravice do odmora, počitka, odklopa).

1.2.3 Pravna podlaga za obdelavo osebnih podatkov

Posamezni upravljavec obdeluje osebne podatke o posameznikih za:

- izvajanje pogodbe, katere pogodbeni stranka je posameznik, na katerega se nanašajo osebni podatki, ali za izvajanje ukrepov na zahtevo takega posameznika pred sklenitvijo pogodbe (točka b) prvega odstavka 6. člena Splošne uredbe o varstvu podatkov);
- izpolnitev zakonske obveznosti, ki velja za upravljavca (točka c) prvega odstavka 6. člena Splošne uredbe o varstvu podatkov);

- namene preventivne medicine ali medicine dela, oceno delovne sposobnosti zaposlenega, zdravstveno diagnozo, zagotovitev zdravstvene ali socialne oskrbe ali zdravljenja ali upravljanje sistemov in storitev zdravstvenega ali socialnega varstva skladno z veljavnimi predpisi ali pogodbo z zdravstvenim delavcem (točka h) drugega odstavka 9. člena Splošne uredbe o varstvu podatkov).

Pravna podlaga za obdelavo osebnih podatkov skladno s prvo alinejo prejšnjega odstavka je pogodba o zaposlitvi, delovna ali druga pogodba, na podlagi katere za zaposleni (posameznik) vključen v delovni proces javnega zavoda.

Pravna podlaga za obdelavo osebnih podatkov skladno z drugo alinejo prejšnjega odstavka so zakonski predpisi, ki so navedeni v nadaljevanju tega dokumenta (poglavje 2 »Skladnost z zakonodajo«).

1.2.4 Opredelitev rokov hrambe

Upravljavec hrani osebne podatke v skladu zakonsko določenimi roki hrambe (npr. trajno, 10 let ali 5 let). Roki hrambe so določeni v zadevnih evidencah dejavnosti obdelav osebnih podatkov, ki jih vodijo upravljavci. Rešitev IS ADRZ mora biti zasnovana na način, ki posameznemu upravljavcu omogoča nastavitve ročnosti hrambe posameznih vrst osebnih podatkov z možnostjo izbire dejanj ob izteku rokov hrambe, najmanj izvoz podatkov na način, da se ohranijo relevantni metapodatki.

Rešitev IS ADRZ mora biti zasnovana na način, da se pred iztekom roka hrambe zagotovi samodejno obveščanje upravljavca o izteku roka hrambe za predvidene osebne podatke in se mu omogoči selektivno izbiro ali nabor podatkov za izvedbo akcije iz predhodnega odstavka.

Ne glede na navedeno mora biti rešitev IS ADRZ zasnovana na način, ki omogoča ustrezno zavarovanje osebnih podatkov, ki so predmet postopka, pred njihovim uničenjem (21. člen ZVOP-2).

1.2.5 Predvidena dejanja obdelave osebnih podatkov

Dejanja obdelave podatkov posameznikov so naslednja:

- zbiranje osebnih podatkov (osebni podatki se pridobivajo od posameznikov in iz evidenc delodajalcev s področja dela in socialne varnosti)
- obdelava osebnih podatkov
- posredovanje osebnih podatkov (izvajalcem zdravstvenega, pokojninskega in invalidskega zavarovanja, sodnim in upravnim organom)
- hramba (do poteka zakonskih rokov):
- anonimizacija podatkov (za potrebe analitične obdelave);
- izbris in uničenje (po izteku roka hrambe; ob anonimizaciji podatkov).

Upravljavec ne sprejema odločitev, ki bi temeljile na avtomatizirani obdelavi osebnih podatkov posameznikov in bi lahko imele pravne učinke ali posledice na pravice delavcev iz delovno pravnega razmerja. Upravljavec ne izvaja profiliranja posameznikov.

Upravljavec osebnih podatkov ne iznaša v tretje države.

Uporabnik ima v zvezi z obdelavo podatkov od upravljavca pravico zahtevati dostop do osebnih podatkov in popravek ali izbris osebnih podatkov ali omejitev obdelave v zvezi z njim ter pravico do ugovora obdelavi in pravico do prenosljivosti podatkov. Zahteva posameznika se obravnava skladno z določbami Splošne uredbe o varstvu podatkov. Rešitev IS ADRZ mora biti zasnovana na način, ki upravljavcu omogoča izpolnjevanje obveznosti pri obravnavi zahtevka posameznika in pri izvajanju nadzora s strani nadzornega organa (npr. inšpekcijski postopki), najmanj zagotovitev vseh informacij v zvezi z obdelavo osebnih podatkov posameznika v določenem obdobju.

1.2.6 Opredelitev lokacije obdelave in hrambe podatkov

Vsi procesi obdelave, vključno z hrambo podatkov v okviru informacijskega sistema bodo potekali na infrastrukturi, ki jo zagotavlja NIJZ, in sicer na območju mesta Ljubljana ter mesta Maribor.

Obdelava osebnih podatkov s strani ponudnika IS ADRZ (kot obdelovalca) se lahko izvaja na območju RS, na podlagi predhodnega obvestila upravljavcu tudi na območju znotraj EU. Brez predhodne pisne odobritve posameznega upravljavca, obdelava osebnih podatkov s strani ponudnika IS ADRZ ne sme potekati na drugih lokacijah (npr. v tretjih državah).

1.2.7 Kategorije uporabnikov

Kategorije uporabnikov:

- uporabniki na strani upravljavca (načrtovalci delovnih razporedov, zdravstveno osebje, vodstvo zavoda, administratorji na nivoju zavoda);
- obdelovalci (npr. ponudnik IS ADRZ, NIJZ).

Rešitev IS ADRZ mora biti zasnovana na način, da so zagotovljene funkcionalnosti, ki omogočajo kreiranje skrbniških in uporabniških pravic na več nivojih, s čimer je urejena pravica do obdelave OP s strani zaposlenih pri delodajalcu.

Poleg zaposlenih pri upravljavcu, se podatki posredujejo tudi izvajalcem zdravstvenega, pokojninskega in invalidskega zavarovanja, sodnim in upravnim organom. Rešitev IS ADRZ mora biti zasnovana na način, ki omogoča izvoz posameznih podatkov ali skupine podatkov uporabnikov z zadostnimi pravicami uporabe in sicer v preprosti in strojno berljivi obliki.

Rešitev IS ADRZ mora biti zasnovana na način, da je dostop do podatkov zagotovljen tudi obdelovalcem, ki jih določi (tj. odobri) upravljavec (npr. za namene reševanja morebitnih incidentov in preprečevanja resnih grožnje, za potrebe zagotavljanja tehnične podpore).

V sistem morajo biti vgrajeni mehanizmi, ki zagotavljajo revizijsko sled za vsa področja in procese, ki se izvajajo v okviru sistema, ne glede na kategorijo uporabnika ali nivo pravic, ki so posameznemu uporabniku zagotovljeni.

Rešitev IS ADRZ mora biti zasnovana na način, ki upravljavcu omogoča, da v primeru zlorabe ali suma zlorabe posameznemu uporabniku onemogoči uporabo ali dostop do rešitve IS ADRZ ali do posamezne funkcionalnosti ali do posamezne vrste ali skupne podatkov.

2 Skladnost z zakonodajo

2.1 Zakonodaja s področja varstva podatkov

Skladno z določbami Splošne uredbe o varstvu podatkov in ZVOP-2 je upravljavec odgovoren za zagotovitev zakonsko skladne obdelave osebnih podatkov. Upravljavec ohrani (tj. ves čas uporabe rešitve IS ADRZ) pravico in obveznost določitve namenov in sredstev obdelave osebnih podatkov, pri čemer lahko odločitev o uporabi posameznih sredstev poveri ponudniku IS ADRZ (npr. izbiro naprednih varnostnih sistemov). Morebitna pisna navodila in poveritev pravice določitve posameznih sredstev obdelave osebnih podatkov ponudniku IS ADRZ mora biti pisno dokumentirana in na voljo posameznemu upravljavcu.

Ponudnik IS ADRZ mora zagotoviti transparentnost pri zasnovi rešitve IS ADRZ ter slednjo dokumentirati na uporabniku razumljiv način. Vsakemu upravljavcu morajo biti v vsakem trenutku na voljo zadostne informacije glede zasnove in delovanja rešitve IS ADRZ.

V primeru, da ponudnik IS ADRZ (kot obdelovalec) meni, da pisna navodila naročnika (ali posameznega upravljavca) kršijo Splošno uredbo o varstvu podatkov ali ZVOP-2, mora o tem obvestil naročnika (ali posameznega upravljavca) brez nepotrebnega odlašanja.

IS ADRZ mora biti razvit na način, da je skladen z vsakokrat veljavnimi predpisi s področja varstva osebnih podatkov:

- Splošna uredba o varstvu podatkov;
- Zakon o varstvu osebnih podatkov (ZVOP-2; Uradni list RS, št. 163/22);

Ponudnik IS ADRZ je seznanjen, da so upravljavci osebnih podatkov kot izvajalci zdravstvenih storitev opredeljeni kot:

- kritična infrastruktura skladno z določbami Zakona o kritični infrastrukturi (ZKI-1; Uradni list RS, št. 102/24);
- visoko kritični sektorji (bistveni ali pomembni subjekti) skladno z določbami Zakona o informacijski varnosti (ZInfV-1; Uradni list RS, št. 40/25).

Naročnik si pridržuje pravico, da zaradi zagotavljanja neprekinjenosti poslovanja ponudnikov zdravstvenih storitev (tj. uporabnikov IS ADRZ) in zagotavljanja njihove digitalne operative odpornosti, v fazi razvoja rešitve IS ADRZ ali uporabe v produkcijskem okolju določi dodatne zahteve ali ukrepe za rešitev IS ADRZ ali/in za ponudnika storitev IS ADRZ v skladu in na podlagi v prejšnjem odstavku navedenih predpisov (ZKI-1; ZInfV-2).

V primeru, da ima posamezni upravljavec specifične in utemeljene zahteve za zagotavljanje varstva osebnih podatkov, ki izhajajo iz njegovih internih politik, na višji ravni, je ponudnik IS ADRZ dolžan

slednje upoštevati pri zasnovi IS ADRZ ali naknadno ob seznanitvi (npr. v okviru vzdrževanja ali nadgradenj IS ADRZ).

2.2 Zakonodaja s področja delovne zakonodaje

Sektorska zakonodaja, ki ureja pravice in obveznosti delodajalca in zaposlenega s področja izvajanja zdravstvene dejavnosti je naslednja:

- Zakon o delovnih razmerjih (ZDR-1; Uradni list RS, št. 21/13, 78/13 – popr., 47/15 – ZZSDT, 33/16 – PZ-F, 52/16, 15/17 – odl. US, 22/19 – ZPosS, 81/19, 203/20 – ZIUPOPĐVE, 119/21 – ZČmIS-A, 202/21 – odl. US, 15/22, 54/22 – ZUPŠ-1, 114/23 in 136/23 – ZIUZDS);
- Zakon o evidencah na področju dela in socialne varnosti (ZEPDSV; Uradni list RS, št. 40/06, 50/23 in 24/25);
- Zakon o javnih uslužbencih (ZJU-1; Uradni list RS, št. 32/25 – op. se uporablja od 1. 1. 2026 dalje);
- Zakon o sistemu plač v javnem sektorju (ZSPJS; Uradni list RS, št. 108/09 – uradno prečiščeno besedilo, 13/10, 59/10, 85/10, 107/10, 35/11 – ORZSPJS49a, 27/12 – odl. US, 40/12 – ZUJF, 46/13, 25/14 – ZFU, 50/14, 95/14 – ZUPPJS15, 82/15, 23/17 – ZDOdv, 67/17, 84/18, 204/21, 139/22, 38/24, 48/24 – odl. US in 95/24 – ZSTSPJS);
- Zakon o nalezljivih boleznih (ZNB – npr. za potrebe obveznega cepljenja; Uradni list RS, št. 33/06 – uradno prečiščeno besedilo, 49/20 – ZIUZEOP, 142/20, 175/20 – ZIUOPĐVE, 15/21 – ZDUOP, 82/21, 178/21 – odl. US in 125/22);
- Zakon o varnosti in zdravju pri delu (ZVZD-1; Uradni list RS, št. 43/11);
- Zakon o zdravstveni dejavnosti (ZZDej – zlasti za področja: usposabljanja, specializacija, pripravništva; Uradni list RS, št. 23/05 – uradno prečiščeno besedilo, 15/08 – ZPacP, 23/08, 58/08 – ZZdrS-E, 77/08 – ZDZdr, 40/12 – ZUJF, 14/13, 88/16 – ZdZPZD, 64/17, 1/19 – odl. US, 73/19, 82/20, 152/20 – ZZUOOP, 203/20 – ZIUPOPĐVE, 112/21 – ZNUPZ, 196/21 – ZDOsk, 100/22 – ZNUZSZS, 132/22 – odl. US, 141/22 – ZNUNBZ, 14/23 – odl. US, 84/23 – ZDOsk-1, 102/24 – ZZKZ in 32/25);
- Zakon o zdravniški službi (ZZdrS; Uradni list RS, št. 72/06 – uradno prečiščeno besedilo, 15/08 – ZPacP, 58/08, 107/10 – ZPPKZ, 40/12 – ZUJF, 88/16 – ZdZPZD, 40/17, 64/17 – ZZDej-K, 49/18, 66/19, 199/21, 136/23 – ZIUZDS, 35/24 in 32/25 – ZZDej-N).

Rešitev IS ADRZ mora biti razvita na način, ki je skladen z navedeno sektorsko zakonodajo. Ponudnik IS ADRZ mora upoštevati navodila naročnika in posameznega upravljavca, ki izhajajo iz sektorske zakonodaje. V primeru, da se pred ali po implementaciji rešitve v produkcijsko okolje ugotovijo neskladnosti ali zasnova posamezne funkcionalnosti ni razvita na opisani način, ponudnik IS ADRZ v sodelovanju z naročnikom pripravi predlog spremembe funkcionalnosti oz. prilagoditve rešitve za zagotovitev skladnosti. V fazi razvoja rešitve IS ADRZ se zagotavlja doseganje skladnosti s sektorsko zakonodajo na način, da se posamezne enote, sheme, strukture in funkcionalnosti razvijajo etapno z vmesnem preverjanjem in potrjevanjem s strani naročnika.

3 Ukrepi

Ponudnik IS ADRZ si prizadeva pri razvoju rešitve upoštevati najnovejše in najvišje standarde kakovosti informacijske varnosti ter s tem zagotoviti potrebno razpoložljivosti, avtentičnosti, celovitosti in zaupnosti v zvezi z varstvom podatkov, vključno z osebnimi podatki.

V ta namen ponudnik v fazi razvoja IS ADRZ ravna skladno z načelom »vgrajeno in privzeto« sprejme ali uvede ustrezne postopke in metode za odkrivanje, preprečevanje, prepoznavo, ocenjevanje in odpravljanje vseh ranljivosti, zlonamerne kode in drugih motenj v zvezi z delovanjem rešitve IS ADRZ.

Ponudnik mora **v fazi zasnove in razvoja rešitve IS ADRZ** zagotoviti najmanj naslednje:

- zagotavljanje skladnosti rešitve z GDPR in ZVOP-2;
- ukrepe za zadostno zaščito osebnih podatkov pred nepooblaščenim dostopom, izgubo, uničenjem ali spreminjanjem;
- ukrepe za zagotavljanje omejenega dostopa (avtorizacije, avtentikacije uporabnikov, omejitve dostopov; večnajemniški model – ločene zbirke podatkov; validacije podatkov);
- šifriranje podatkov pri prenosu in posredovanju podatkov;
- ukrepe za zagotavljanje sledljivosti dejanjem obdelave (dnevniški zapisi, revizijske sledi);
- ukrepe za hitro odkrivanje in obvladovanje incidentov ter odzivanje na kršitve.

Ponudnik IS ADRZ bo **po izvedbi implementacije IS ADRZ v produkcijsko okolje** s (posameznim) upravljavcem na njegovo zahtevo sklenil uravnoteženo pogodbo o obdelavi osebnih podatkov ter prevzeti najmanj naslednje obveznosti:

- obdelava osebne podatke na podlagi dokumentiranih navodil upravljavca;
- vodenje evidence vseh vrst dejavnosti obdelave, ki jih bo izvajal v imenu in za račun upravljavca;
- sprejel in izvajal politiko varstva podatkov skladno z najboljšimi praksami, ki zagotavlja spoštovanje načel razpoložljivosti, pristnosti, celovitosti in zaupnosti osebnih podatkov upravljavca;
- izvajal ustrezne tehnične in organizacijske ukrepe za zagotavljanje ustrezne ravni varnosti glede na s strani upravljavca identificirana tveganja

Ponudnik IS ADRZ je **po prenehanju pogodbe o izvedbi javnega naročila** dolžan naročniku vrniti vse podatke, ne glede na obliko zapisa, ki jih je v povezavi s pogodbo prejel od naročnika. Elektronski dokumenti, informacije ali sredstva dostopa se uničijo, izbrišejo ali prepišejo na način, da jih ni več mogoče obnoviti. Na zahtevo naročnika ter v dogovorjenem obsegu ponudnik IS ADRZ zagotavlja naročniku in/ali posameznemu upravljavcu tudi podporo in pomoč pri prehodu na novega izvajalca ali prevzemu v upravljanje z lastnimi kapacitetami.

Ponudnik IS ADRZ je seznanjen, da se določila pogodbe o izvedbi javnega naročila in njenih prilog, v delu, ki ureja obveznost varovanja zaupnosti osebnih podatkov ter odgovornosti za škodo, nastalo iz razlogov na strani ponudnika IS ADRZ v času veljavnosti pogodbe o izvedbi javnega naročila, uporabljajo tudi po prenehanju obdelave osebnih podatkov.

Zahteve za posamezne skupine ukrepov so v nadaljevanju podrobneje opredeljene.

3.1 Zahteve ponudnika infrastrukture (NIJZ)

Minimalni nabor zahtev, ki vključujejo organizacijske ter tehnične ukrepe in jih mora izpolnjevati ponudnik IS ADRZ za dostop do infrastrukture, ki jo zagotavlja NIJZ, je naveden v nadaljevanju:

- izvajanje rednega izobraževanja zaposlenih, zlasti novo-zaposlenih, na področju skrbne uporabe IS ADRZ in pomembnosti zakonite obdelave osebnih podatkov (s poudarkom na resnosti tveganj, potencialne posledice in odgovornosti zaposlenih) v prvem kvartalu zaposlitve kot del uvajanja v delovni proces in redno (obdobno) izvajanje izobraževanj ter ozaveščanje zaposlenih o pomembnosti varstva osebnih podatkov;
- izvajanje periodičnih internih revizij postopkov obdelave osebnih podatkov (najmanj 1x letno);
- posodobitev ustreznih obvestil o zasebnosti, ki vsebujejo informacije iz člena 13 in 14 GDPR, prek katerega bodo vsi relevantni posamezniki ustrezno informirani o osebnih podatkih, ki se obdelujejo v okviru IS ADRZ;
- priprava internih aktov v katerih se opredeli nabor odgovornih oseb in postopkov za uveljavljanje pravic posameznikov skladno z GDPR, in zagotovi vsaj postopek obravnave zahtevkov;
- redno spremljanje in preverjanje integracije z drugimi sistemi;
- vzpostavitev ustreznega komunikacijskega kanala za uveljavljanje pravic posameznikov;
- vzpostavitev primerne tehnične podpore rednega in intervencijskega vzdrževanja (npr. vzpostavitev službe za prijavo napak in zahtev in zagotavljanje primerne tehnično ekipo, ki bo skrbela za obravnavo zahtev, delovanje rešitve in odpravo napak, usposabljanje pooblaščenih uporabnikov, priprava navodil in politik, ipd.);
- vodenje ustrezne evidence dejavnosti obdelav (kot obdelovalec) v okviru, ki ga zahteva GDPR,
- sklenitev ustrezne pogodbe o obdelavi osebnih podatkov s posameznim upravljavcem na njegovo zahtevo;
- zagotavljanje revizijske sledi za obdobje 2 let od zaključka koledarskega leta, v katerem so bila zabeležena dejanja obdelave;
- redno spremljanje in posodabljanje varnostnih tehničnih rešitev IS ADRZ ob upoštevanju tehnološkega razvoja;
- izvedba penetracijskega testa pred prehodom v produkcijsko okolje in nato redno periodično izvajanje penetracijskih testov.

3.2 Zaupnost ter omejen dostop

Ponudnik IS ADRZ mora zagotavljati izvajanje vseh ukrepov, opredeljenih v Prilogi 5 Arhitektura, integracije in infrastruktura.

Vsi podatki, ki jih zagotovi naročnik, kot so dokumenti, podatki, informacije, nosilci podatkov, dostop do sistemov, strojne opreme ali drugih objektov, so zaupne narave in se uporabljajo izključno za izvajanje javnega naročila.

Pooblastila za dostop, zlasti do informacijskih in drugih sistemov, ki jih ponudniku IS ADRZ zagotovi naročnik ali posamezni upravljavec, in pooblastilo za uporabo infrastrukture, računalnikov ali licenc preneha ob izpolnitvi oz. prenehanju pogodbe o izvedbi javnega naročila.

Ponudnik IS ADRZ mora zagotoviti najmanj:

- da imajo zaradi ohranjanja celovitosti podatkov dostop do posameznih podatkov ali skupin podatkov samo pooblaščen osebe (pooblaščen osebe na strani ponudnika IS ADRZ morajo biti zavezane k zaupnosti podatkov, kot npr. NDA, sporazumi o sprejemljivi uporabi, pravila vedenja, sporazumi o navzkrižju interesov);
- da je implementiran sistem nadzora dostopa za vse uporabnike, ki dostopajo do informacijskega sistema. Rešitev omogoča ustvarjanje, odobravanje, pregledovanje in brisanje uporabniških računov;
- da je vzpostavljen mehanizem preverjanja pristnosti uporabnika. Zahtevana je dvofaktorska avtentikacija uporabnika;
- v primeru uporabe gesel, morajo le-ta upoštevati določeno (nastavljivo) stopnjo kompleksnosti (politika mora vsebovati vsaj dolžino gesla, zapletenost, obdobje veljavnosti, ter tudi število sprejemljivih neuspešnih poskusov prijavi), pri čemer sistem nadzora dostopa sam zazna in prepreči uporabo gesel, ki ne upoštevajo določene (nastavljive) stopnje kompleksnosti.

Ponudnik IS ADRZ mora tudi za svoje osebje zagotoviti, da je seznam oseb, ki delujejo na strani obdelovalca in katerim je omogočen dostop do osebnih podatkov upravljavcev, redno pregledovan. Na podlagi rednih pregledov bo dostop do osebnih podatkov ukinjen, če ni več potreben, s čimer osebni podatki zadevnim osebam ne bodo več dostopni. Na zahtevo upravljavca bo obdelovalec izkazal, da imajo zadevne osebe pod nadzorom obdelovalca dostop do podatkov samo ob obstoju potrebe po dostopu do osebnih podatkov.

3.3 Izobraževanje

Ponudnik mora zagotoviti, da njegovo osebje, ki v imenu obdelovalca izvaja dejanja obdelave, zagotavlja, da:

- osebje razume grožnje in pomisleke glede varstva podatkov;

- so vzpostavljeni strukturirani in redni programi usposabljanja za osebje, vključno s posebnimi programi za uvajanje (v zadeve varstva podatkov) novincev, pri čemer se načrt usposabljanja z jasno opredeljenimi cilji redno pripravlja, izvaja in pregleduje in obsega najmanj: formalni program usposabljanja za ozaveščanje o informacijski varnosti; ciljno usmerjen program usposabljanja za ozaveščanje o potrebnih tehničnih znanjih; obdobjni testi ali simulacije z ocenami ozaveščenosti zaposlenih;
- vsi zaposleni so ustrezno obveščeni o varnostnih kontrolah rešitve IS ADRZ, ki se nanašajo na njihovo vsakdanje delo.

3.4 Šifriranje podatkov

Ponudnik IS ADRZ mora zagotavljati izvajanje zahtev oz. ukrepov, ki so opredeljene v dokumentu Priloga 5. Arhitektura, integracije in infrastruktura (npr. razpoložljivost, zanesljivost, šifriranje podatkov, psevdonimizacija ter anonimizacija podatkov).

Ponudnik IS ADRZ bo vse podatke (vključno z neosebnimi podatki), ki se obdelujejo v okviru IS ADRZ ali v zvezi z njimi, upravljal skladno z najboljšimi standardnimi praksami. Pri tem bo zagotovil najmanj:

- vsi ključi in gesla morajo biti enostavno zamenljivi in so del natančno opredeljenega postopka za ponovno šifriranje občutljivih podatkov;
- uporabniki ne morejo de aktivirati ali zaobiti varnostnih nastavitev;
- uporabniki nimajo pravic za namestitve ali de aktivacijo nepooblaščenih programskih aplikacij;
- ima rešitev časovne omejitve seje, ko uporabnik določeno obdobje ni aktiven;
- so kritične varnostne posodobitve redno nameščene;
- se protivirusne aplikacije in podpisi za zaznavanje konfigurirajo vsak dan.

Za potrebe dostopa preko mobilne / prenosne naprave, morajo biti zagotovljeni primerni ukrepi za zagotavljanje varstva osebnih podatkov, vsebovanih v IS ADRZ, najmanj:

- mobilne naprave, ki omogočajo dostop do IS ADRZ, morajo biti vnaprej registrirane in predhodno avtorizirane;
- zagotovljena je možnost oddaljenega upravljanja (npr. blokade) mobilnih naprav z dostopom do IS ADRZ v primeru suma zlorabe mobilne naprave;
- za mobilne naprave veljajo enake ravni postopkov nadzora dostopa (do sistema za obdelavo podatkov) kot za drugo opremo;
- samodejno beleženje podatkov o napravi, iz katere se dostopa do IS ADRZ (npr. revizijske sledi);
- vloge in odgovornosti v zvezi z upravljanjem mobilnih in prenosnih naprav so jasno opredeljene.

3.5 Sledljivost

Ponudnik IS ADRZ mora zagotavljati izvajanje zahtev oz. ukrepov, ki so opredeljene v dokumentu Priloga 5 Arhitektura, integracije in infrastruktura (npr. razširljivost, zmogljivost, interoperabilnost, vzdržljivost).

Skladno z določbami ZVOP-2 (22. člen ZVOP-2) je v danem primeru (vsak) upravljavec dolžan voditi dnevnik obdelave za potrebe izkazovanje zakonitosti obdelave osebnih podatkov, za izvajanje nadzora, za potrebe zagotavljanja celovitosti in varnosti OP, odpravljanja napak v delovanju IS ADRZ ali pri obdelavi podatkov.

Dnevnik obdelave mora obsegati najmanj naslednje vsebine:

- vrsta dejanja obdelave,
- datum in čas obdelave,
- identifikacija osebe, ki je izvedla dejanje obdelave ter
- identifikacijo uporabnika OP.

3.6 Izhodni načrt / načrt prehoda

Ponudnik IS ADRZ kot obdelovalec bo dolžan ob prekinitvi zagotavljanja storitev obdelave osebnih podatkov vrniti vse osebne podatke naročniku / upravljavcu in izbrisati morebitne obstoječe kopije osebnih podatkov, razen če nadaljnjo hrambo osebnih podatkov od njega zahtevajo veljavni predpisi.

Za potrebe nemotenega delovanja sistemov naročnika / upravljavca, bo ponudnik IS ADRZ dolžan pomagati naročniku / upravljavcu pri prevzemu storitev ali prehodu na novega ponudnika IS ADRZ za čas prehodnega obdobja, ki ne sme biti krajše od 3 mesecev. Za potrebe slednjega naročnik in ponudnik AS ADRZ najpozneje v (6) mesecih od prehoda v produkcijsko okolje, pripravita načrt prehoda, ki določa najmanj naslednje vsebine/obveznosti: ključne in odgovorne osebe ali službe; potrebne procesne aktivnosti za prehod ter roke za izvedbo posameznih aktivnosti, popis podatkov (vrste, obliko zapisa, posebnosti ali omejitve prenosa) ter morebitne finančne učinke, vključno z viri financiranja.

4 Obvladovanje tveganj

Naročnik / Upravljavec bo pred prehodom v produkcijsko okolje ocenil tveganja za pravice in svoboščine posameznikov, ki jih povzroča obdelava osebnih podatkov v okviru IS ADRZ. Ponudnik IS ADRZ je dolžan aktivno sodelovati pri izdelavi ocene učinkov v zvezi z varstvom osebnih podatkov obdelovanih v okviru rešitve IS ADRZ (DPIA), mu zagotovil vse potrebne informacije za identifikacijo in oceno tveganj ter, po potrebi, izvedel potrebne ukrepe za ublažitev nesprejemljivih tveganj.

4.1 Metodološka izhodišča za oceno učinka v zvezi z varstvom podatkov

Ocena tveganja predstavlja na eni strani sistematično prepoznavanje tveganj in na drugi strani razvrščanje le-teh po prioriteti. Rezultati tako pridobljene ocene tveganj morajo določiti ustrezne ukrepe za uspešno upravljanje s tveganji oz. zniževanje stopnje verjetnosti za uresničevanje. V nadaljevanju so grafično ponazorjene stopnje ravni tveganj, ki bodo uporabljene pri izdelavi DPIA.

Tabela 2: Stopnje tveganj:

2 in 3	Zanemarljivo tveganje
4	Majhno tveganje
5 in 6	Srednje tveganje
7 in 8	Veliko (znatno) tveganje*

* Potrebno predhodno posvetovanje pri IP RS.

Ocena ali raven tveganja je seštevek verjetnosti uresničitve (tj. kakšna je verjetnost, da bi se kršitev oz. neskladnost obdelave osebnih podatkov zgodila) in teže posledic (tj. kakšen je vpliv na pravice in obveznosti posameznika). Kombinacija verjetnosti uresničitve in teže posledic je izhodišče za odločitev, ali je potrebno posamezno tveganje obravnavati.

Tabela 3: Formula za izračun ocene ali ravni tveganja

$$\text{Raven/Ocena tveganja} = \text{Verjetnost} + \text{Teža posledic}$$

V nadaljevanju je prikazana raven ali ocena tveganja v zvezi z varstvom osebnih podatkov, izračunana po zgoraj navedeni formuli.

Tabela 4: Raven (ocena) tveganja:

		Verjetnost			
Teža posledic		1	2	3	4
	1	2	3	4	5
	2	3	4	5	6
	3	4	5	6	7
	4	5	6	7	8

Verjetnost uresničitve kategoriziramo v štiri ravni v odvisnosti od tega, kakšna je verjetnost, da bi pri obdelavi osebnih podatkov prišlo do kršitve Splošne uredbe o varstvu podatkov oziroma nacionalnih predpisov s področja varstva podatkov.

V spodnji tabeli so označene stopnje verjetnosti nastopa kršitve pravic in svoboščin posameznika zaradi neskladnosti obdelave osebnih podatkov ter opis posamezne stopnje.

Tabela 5: Stopnje verjetnosti nastanka kršitve (verjetnost tveganja)

1	Zelo redko se zgodi (zanemarljiva možnost, da bi se kršitev oz. neskladnost zgodila).
2	Redko se zgodi (nizka verjetnost, da bi se kršitev oz. neskladnost zgodila).
3	Obstaja verjetnost, da se bo zgodil (možno, da se bo kršitev oz. neskladnost zgodila).
4	Verjetno se bo zgodil (velika verjetnost, da se bo kršitev oz. neskladnost zgodila).

V nadaljevanju so podane stopnje negativnega vpliva načina obdelave osebnih podatkov posameznika in načina uveljavljanja njegovih pravic ter opis posamezne stopnje ali ravni negativnega vpliva, tj. teže posledic.

Tabela 6: Stopnje teže posledic (vpliv tveganja ali teža posledic)

1	Zanemarljiva - način obdelave je povsem skladen z relevantnimi predpisi; način uveljavljanja njegovih pravic je določen, skladen s predpisi in posamezniku enostavno dostopen.
2	Majhna - način obdelave lahko oteži zagotavljanje skladnosti in/ali povzroči krajšo prekinitev dela poslovnega procesa, vezanega na dotično obdelavo; način uveljavljanja pravic posameznika v zvezi z obdelavo je

	določen, vendar informacije o tem posamezniku niso enostavno dostopne oz. jasno sporočene.
3	Srednja - način obdelave ni povsem v skladu z zakonom, kar ima lahko za posledico prekinitve poslovnega procesa, vezanega na dotično obdelavo, manjšo finančno škodo, negativni vpliv na dobro ime organizacije ter možno globo in druge predpisane ukrepe nadzornega organa (npr. iz člena 58(2) Splošne uredbe); način uveljavljanja pravic posameznika v zvezi z obdelavo ni formalno notranje pravno določen, informacije o načinu uveljavljanja pravic posamezniku niso enostavno dostopne oz. jasno sporočene, vendar se zahtevki posameznika obravnavajo.
4	Velika - način obdelave pomeni kršitev zakona, zaradi česar lahko pride do prekinitve kritičnega poslovnega procesa, vezanega na dotično obdelavo, velike finančne škode, izgube dobrega imena organizacije, izrečene globe in izvedbe drugih ukrepov nadzornega organa (npr. iz člena 58(2) Splošne uredbe); postopki uveljavljanja pravic posameznika v zvezi z obdelavo niso določeni in se ne izvajajo.

4.2 Minimalni nabor tveganj

Pri izdelavi DPIA je potrebno identificirati tveganja, ki izhajajo iz spoštovanja vseh temeljnih načel obdelave osebnih podatkov, kot jih določa Splošna uredba o varstvu podatkov.

Načelo zakonitosti se nanaša na obstoj zadostne in ustrezne pravne podlage za obdelavo osebnih podatkov. **Načelo poštenosti** od upravljavca osebnih podatkov zahteva preglednost obdelave oziroma ne zavajajoče ravnanje pri obdelavi osebnih podatkov (npr. ustrezno informiranje o obdelavi; jasnost in točnost informacij v zvezi z obdelavo osebnih podatkov; obdelava ne sme biti tajna in prikrita ipd.). **Načelo preglednosti**, ki je pravzaprav eden od elementov poštene obdelave osebnih podatkov, pa od upravljavca zahteva, da posameznike, čigar osebne podatke obdeluje, obvešča o tem, kako in za kakšen namen se osebni podatki obdelujejo. Vsa tri navedena načela se nanašajo na razmerje med upravljavcem in posameznikom.

Minimalni nabor tveganj iz naslova kršitve načela zakonitosti, poštenosti ter preglednosti, ki morajo biti ovrednotena in podrobno obravnavana v okviru DPIA so navedena v nadaljevanju:

- 1) Pravna podlaga za obdelavo OP je določena vnaprej, jasna in znana.
- 1) Pravna podlaga za obdelavo OP je ustrezna.
- 2) Vir pridobivanja OP.
- 3) Postopek in način informiranja posameznika, na katerega se nanašajo osebni podatki je v skladu s členi 12 - 14 GDPR.
- 4) Posameznik ne pričakuje profiliranja ali sprejemanja odločitev, ki bi ime zanj pravne posledice.

- 5) Posameznik je seznanjen s pravicami v zvezi z varovanjem osebnih podatkov ter z načinom uveljavljanja pravic.

Načelo omejitve namena obdelave zahteva, da se osebni podatki obdelujejo izključno za namene, s katerimi je posameznik vnaprej na jasn in razumljiv način seznanjen oz. za katere upravičeno pričakuje, da so namen obdelave osebnih podatkov. To pomeni, da mora biti namen obdelave določen in izkazan pred začetkom obdelave podatkov. Obdelava za namene, ki niso združljivi s prvotnim namenom obdelave, ni dopustna. Prav tako ni dopustna obdelava za namene, ki niso določeni. Vsak namen obdelave osebnih podatkov mora imeti svojo samostojno pravno podlago. Posameznikom je potrebno omogočiti, da samovoljno odločijo, za katere namene dopuščajo obdelavo osebnih podatkov. Slednje posameznikov ne bi smelo neupravičeno omejevati pri uporabi storitev, ki jih upravljavec ponuja.

Minimalni nabor tveganj iz naslova kršitve načela omejitve namena obdelave, ki morajo biti ovrednotena in podrobno obravnavana v okviru DPIA so navedena v nadaljevanju:

- 1) Nameni obdelave so določeni vnaprej, natančno in jasno.
- 2) Možnost razširitve namena obdelave že zbranih OP v obsegu, ki je združljiv s prvotno določenim namenom, je podana in ustrezno protokolirana.
- 3) Možnost obdelave OP za namene, ki prvotno niso bili določeni, je protokolirana. Ustrezno je obravnavan način in postopek za zakonito obdelavo OP.
- 4) Možnost obdelave OP s strani upravičenih oseb (npr. pooblaščen osebe; obdelovalci) za namene, ki niso predvideni, niso dopustni.

Načelo najmanjšega obsega podatkov upravljavca zavezuje, da v okvir pridobivanja oz. zbiranja osebnih podatkov zbere izključno tiste, ki so nujno potrebni za doseg namena obdelave.

Minimalni nabor tveganj iz naslova kršitve načela najmanjšega obsega obdelave, ki morajo biti ovrednotena in podrobno obravnavana v okviru DPIA so navedena v nadaljevanju:

- 1) Nabor oz. obseg OP, zajetih v predvideno obdelavo OP, je skladen z zakonsko dopustnim.
- 2) Nabor oz. obseg OP, zajetih v predvideno obdelavo OP, je nujno potreben za doseganje ciljev upravljavca.
- 3) Obdelava posebnih vrst OP je nujna in sorazmerna za doseganje ciljev upravljavca.

Načelo točnosti in ažurnosti od upravljavca zahteva, da obdeluje zgolj točne in pravilne osebne podatke ter slednje sproti osvežuje in pregleduje. V okvir navedenega spada tudi redno pregledovanje obstoječih evidenc dejavnosti obdelav osebnih podatkov. Od upravljavca se pričakuje in zahteva, da bo pri vnosu, hrambi in obdelavi osebnih podatkov skrben (npr. programska oprema je zasnovana na način, ki preprečuje napake ali spremembe osebnih podatkov) in obenem, da bo ob vsakokratnem prejemu obvestila o spremembi osebnih podatkov te tudi upošteval oz. se odzval na zahteve posameznika.

Minimalni nabor tveganj iz naslova kršitve načela točnosti in ažurnosti, ki morajo biti ovrednotena in podrobno obravnavana v okviru DPIA so navedena v nadaljevanju:

- 1) Predmet obdelave so osebni podatki, ki so pravilni in popolni.
- 2) Predmet obdelave so osebni podatki, ki so ažurirani in posodobljeni.
- 3) Identifikacija posameznika je zagotovljena.
- 4) Preveritev OP se opravi v uradnih evidencah. Preveritve se protokolirajo (revizijska sled).

Načelo omejitve shranjevanja vелеva upravljavcem, da smejo osebne podatke posameznikov obdelovati le toliko časa, kolikor je potrebno za doseganje in uresničevanje namenov, za katere se osebni podatki obdelujejo. Hramba za daljše časovno obdobje ni dopustna, razen v izjemnih primerih (npr. dolgoročna hramba skladno z določbami ZVDAGA; predpisi s področja računovodstva, hramba za potrebe zavarovanj npr. v primeru odškodninskih tožb). Trajnejša hramba je dopustna v obliki anonimiziranih podatkov.

Minimalni nabor tveganj iz naslova kršitve načela omejitve shranjevanja, ki morajo biti ovrednotena in podrobno obravnavana v okviru DPIA so navedena v nadaljevanju:

- 1) Roki hrambe obdelovanih podatkov so določeni vnaprej in jasno.
- 2) Roki hrambe obdelovanih podatkov so določeni sorazmerno.
- 3) Postopek obravnave podatkov po poteku roka hrambe je določen.
- 4) Postopek hrambe podatkov po poteku roka hrambe za namene arhiviranja v javnem interesu, za znanstveno raziskovalne ali statistične namene je določen.
- 5) Postopek uničenja OP je določen.
- 6) Po izpolnitvi namena obdelave OP je dostop do OP omejen oz. blokiran.

Načelo celovitosti in zaupnosti osebnih podatkov oziroma njihove integritete izvirata iz varnosti obdelave osebnih podatkov. Upravljavec mora zagotoviti, da so osebni podatki ves čas pod njegovim nadzorom in dostopni. V okvir navedenih načel spada tudi informacijska varnost in ukrepi za zmanjšanje tveganj varnostnih incidentov.

Minimalni nabor tveganj iz naslova kršitve načela celovitosti in zaupnosti, ki morajo biti ovrednotena in podrobno obravnavana v okviru DPIA so navedena v nadaljevanju:

- 1) Vse lokacije hrambe podatkov so znane.
- 2) Zagotovljene so varnostne kopije OP.
- 3) Lokacije hrambe podatkov so znane. Zagotovljeno je varovanje lokacije hrambe in prostorov. Sprejeti so primerni organizacijski in tehnični ukrepi za zavarovanje strojne in programske opreme.
- 4) Povezave z zunanjim okoljem so ustrezno varovane.
- 5) Sprejeti so ukrepi za zmanjšanje tveganj, ki izvirajo iz sfere posameznika/uporabnika.
- 6) Osebe/zaposleni, ki opravljajo obdelavo OP, so usposobljeni za ravnanje z OP. Kadrovske kapacitete so zadostne. Finančni resursi so zadostni.
- 7) Varnostne politike so sprejete in se v praksi izvajajo.

- 8) Zloraba OP s strani zaposlenih je ustrezno protokolirana in sankcionirana.
- 9) OP se ob prenosu šifrira.
- 10) Vzpostavljeni so mehanizmi za zavarovanje OP pred namernimi in nenamernimi dejanji.
- 11) Vzpostavljeni so mehanizmi, ki onemogočajo uporabo nepodprte programske opreme; uporaba ne licenciranih rešitev; nerednih posodobitev programske opreme.
- 12) Ustrezno zavarovani komunikacijski kanali med komponentami rešitve.
- 13) Zagotovljena je anonimizacija podatkov, psevdonimizacija podatkov.
- 14) Ukrepi in postopki za obravnavanje in poročanje o kršitvi varnosti obdelave osebnih podatkov pri upravljavcu so določeni v skladu z določbami člena 33 GDPR.
- 15) Tehnični in organizacijski ukrepi za obnovo/okrevanje sistema v primeru fizičnega ali tehničnega incidenta so določeni/vzdrževani/preverjeni in dokumentirani
- 16) Naročnik je obveščen o dejanskih incidentih, o načinih odkrivanja in rokovanja z incidenti (tudi pri obdelovalcih).

Načelo odgovornosti je zadnje od temeljnih načel in je krovno, t.i. »overall« načelo. Skladno s slednjim je upravitelj sposoben vsak trenutek izkazati, da osebne podatke obdeluje skladno z veljavnimi predpisi. Glede na vse navedeno je mogoče zaključiti, da je ob ustrezni izvedbi vseh ukrepov mogoče zagotoviti spoštovanje načela odgovornosti s strani upravitelja.

Minimalni nabor tveganj iz naslova kršitve odgovornosti, ki morajo biti ovrednotena in podrobno obravnavana v okviru DPIA so navedena v nadaljevanju:

- 1) Vodenje dnevnika obdelave (22. člen ZVOP-2).
- 2) Zavarovanje osebnih podatkov, ki so predmet postopka (21. člen ZVOP-2).
- 3) Sklenjene so ustrezne pogodbe o obdelavi OP (člen 28 GDPR).
- 4) Zagotovljen je nadzor nad vsemi obdelovalci in obsegom njihovih pooblastil.
- 5) OP niso predmet iznosa v tretje države.
- 6) Evidenca dejavnosti obdelave OP je vzpostavljena v skladu s členom 30 GDPR.
- 7) Evidenca dejavnosti obdelave OP je vodena v skladu s členom 30 GDPR.
- 8) Vodenje evidence in hramba zadevnih informacij poteka z uporabo učinkovitega sistema za upravljanje evidence.
- 9) Evidence se hranijo in varujejo tako dolgo, dokler se potrebujejo za revizijo in preiskovanje kršitev varnosti ter hrambo podatkov, nato se evidence po vnaprej določenem protokol varno uničijo.

4.3 Ocena učinka na temeljne pravice (FRIA)

V primeru, da bo delovanje IS ADRZ podprto z uporabo sistemov umetne inteligence, bo ponudnik IS ADRZ dolžan med razvojem sistema (tj. pred implementacijo v produkcijsko okolje) izdelati celovito oceno učinka uporabe takšnih sistemov na temeljne pravice v skladu s 27. členom Akta o

umetni inteligenci⁴ (v nadaljevanju: FRIA) z namenom prepoznav rezultatov, ki bi bili lahko škodljivi za temeljne pravice posameznika. Ocena učinka oz. njena novelacije se redno izvaja tudi po prehodu v produkcijsko okolje z namenom rednega beleženja informacij o uporabi in rezultatih sistema ter ob priložnosti rednih mejnikov (npr. spremembe katerega od pomembnih dejavnikov).

Kot izhodišče pri izdelavi FRIA ponudnik IS ADRZ upošteva najmanj naslednja izhodišča:

- tveganja zakonite obdelave osebnih podatkov;
- tveganja enakega obravnavanja, zlasti diskriminacije zaščitenih skupin;
- tveganja za kršitve pravičnih in poštenih delovnih pogojev;
- tveganja transparentnosti (priporočljive prakse dobrega obveščanja), vključno z zagotavljanjem enostavnih poti za pritožbe zoper podane rezultate oz. odločitve.

Ponudnik IS ADRZ mora v izdelavo FRIA vključiti tudi predstavnike naročnika (najmanj skrbnike sistema, ključne uporabnike, DPO) ter predstavnike zaposlenih.

Glede na ugotovljena tveganja mora ponudnik IS ADRZ določiti ukrepe, ki jih je treba sprejeti v primeru uresničitve teh tveganj, vključno z ureditvami za notranje upravljanje in pritožbene mehanizme, za zmanjšanje tveganj za temeljne pravice v konkretnih primerih uporabe ter z naročnikom uskladiti časovno dinamiko izvedbe primernih ukrepov.

⁴ UREDBA (EU) 2024/1689 EVROPSKEGA PARLAMENTA IN SVETA z dne 13. junija 2024 o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (Akt o umetni inteligenci).

5 Pravice posameznikov

Ponudnik IS ADRZ bo pomagal upravljavcu pri zagotavljanju skladnosti z dolžnostmi upravljavca po členu 32 Splošne uredbe o varstvu podatkov, med drugim z zagotavljanjem informacij, ki zadevajo tehnične in organizacijske ukrepe, ter zagotovil vse ostale informacije, ki so potrebne, da lahko upravljavec zagotovi skladnost z določbami člena 32 Splošne uredbe o varstvu podatkov.

Navedeno pomeni, da bo obdelovalec, kolikor je to mogoče, pomagal upravljavcu pri izpolnjevanju obveznosti upravljavca, ki se nanašajo na pravice posameznikov, in sicer:

- 1) pravico do informiranja o obdelavi osebnih podatkov, kadar se osebni podatki pridobijo od posameznika, na katerega se nanašajo osebni podatki;
- 2) pravico do informiranja o obdelavi osebnih podatkov, kadar osebni podatki niso bili pridobljeni od posameznika, na katerega se nanašajo osebni podatki;
- 3) pravico dostopa posameznika, na katerega se nanašajo osebni podatki;
- 4) pravico do popravka;
- 5) pravico do izbrisa ("pravico do pozabe");
- 6) pravico do omejitve obdelave;
- 7) obveznost obveščanja v zvezi s popravkom ali izbrisom osebnih podatkov ali omejitvijo obdelave;
- 8) pravico do prenosljivosti podatkov;
- 9) pravico do ugovora;
- 10) pravico, da za posameznika, na katerega se nanašajo osebni podatki, ne velja odločitev, ki temelji zgolj na avtomatizirani obdelavi, vključno z oblikovanjem profilov.

Ponudnik IS ADRZ je seznanjen, da bodo obveznosti iz naslova zagotavljanja informacij, pomoči in podpore pri uresničevanju pravic posameznikov določene v pogodbi o obdelavi osebnih podatkov, ki bo zavezovala ponudnika IS ADRZ kot pod-obdelovalca.

6 Odzivanje na kršitve

Ponudnik IS ADRZ mora zagotavljati izvajanje zahtev oz. ukrepov, ki so opredeljene v dokumentu Priloga 5 Arhitektura, integracije in infrastruktura (npr. razširljivost, zmogljivost, interoperabilnost, vzdržljivost).

Ponudnik IS ADRZ je dolžan za potrebe takojšnje prepoznave, reševanja ter odprave posledic varnostnega incidenta ali druge kršitve skladnosti obdelave osebnih podatkov ves čas trajanja pogodbe o izvedbi javnega naročila zagotavljati:

- redne interne revizije ter samoocenitve;
- redno usposabljanje odgovornih oseb;
- politike SUVI – sistem za upravljanje varovanja informacij;
- politike SUNP – sistem za upravljanje neprekinjenega poslovanja;
- Politike upravljanja incidentov.

Ponudnik IS ADRZ je dolžan spremljati in evidentirati vsak informacijski varnostni dogodek (incident), ki ima ali bi lahko imel v razmerju do naročnika / upravljavca za posledico:

- nerazpoložljivost rešitve ali njegovega dela oziroma storitev;
- razkritje zaupnih podatkov ali izgubo oz. nezaželeno spremembo podatkov;
- poškodovanje ali izgubo opreme in sredstev, ali
- drugo dejanje, ki krši varnostne postopke ali usmeritve naročnika.

Ponudnik IS ADRZ zagotavlja, da se pooblaščen in strokovno usposobljeni zaposleni odzovejo na vsak informacijski varnostni dogodek ter izvedejo vse potrebne ukrepe za preprečevanje posledic dogodka in za preprečevanje bodočih takšnih dogodkov.

Ponudnik IS ADRZ je seznanjen z roki za poročanje o varnostnem incidentu nadzornemu organu in posameznikom ter drugimi zakonskimi zahtevami za poročanje o incidentih. Ponudnik IS ADRZ bo zagotovil pomoč in podporo naročniku / upravljavcu v primeru dejanskega incidenta IKT. V ta namen je dolžan pridobiti in upravljavcu posredovati spodaj naštete informacije:

- naravo kršitve varnosti osebnih podatkov, po možnosti tudi kategorije in približno število zadevnih posameznikov, na katere se nanašajo osebni podatki, ter vrste in približno število zadevnih evidenc osebnih podatkov;
- verjetne posledice kršitve varnosti osebnih podatkov;
- ukrepe, ki naj jih upravljavec sprejme ali katerih sprejetje predlaga upravljavcu za obravnavanje kršitve varnosti osebnih podatkov, pa tudi, kjer ustrezno, ukrepe za ublažitev morebitnih škodljivih učinkov kršitve.

7 Revizije in pregledi

Ponudnik IS ADRZ bo naročniku / upravljavcu dal na voljo vse informacije, potrebne za dokazovanje izpolnjevanja obveznosti iz člena 28 Splošne uredbe o varstvu podatkov, ter mu (ali zunanjemu neodvisnemu revizorju) omogočil izvajanje revizij, vključno s pregledi, ter pri njih sodeloval. O izvedeni reviziji se pripravi poročilo, ki mu ponudnik IS ADRZ kot obdelovalec lahko oporeka ter zahteva novo revizijo. Na podlagi rezultatov revizije lahko naročnik / upravljavec zahteva nadaljnje ukrepe, ki so potrebni za zagotovitev skladnosti s Splošno uredbo o varstvu podatkov ter ZVOP-2.

Ponudnik IS ADRZ se zavezuje tudi, da bo omogočal nadzornim organom, ki imajo skladno z relevantno zakonodajo dostop do prostorov in sredstev obdelave upravljavca oz. pravico ali dolžnost nadzora nad upravljavcem, v delu, ki ga zagotavlja ponudnik IS ADRZ omogočil dostop do svojih prostorov in sredstev obdelave ter mu dal na voljo zahtevane informacije in dokumentacijo.

Naročnik ima pravico od ponudnika IS ADRZ zahtevati tudi aktivno sodelovanje in vključenost pri penetracijskem testu na podlagi groženj, v kolikor bo naročnik slednje ocenil kot potrebno.