

Na podlagi 1. odstavka 35. člena Splošne uredbe o varstvu podatkov (EU) 2016/679 je organizacija izvedla oceno učinka dejanj obdelave na varstvo osebnih podatkov.

OCENA UČINKA NA VARSTVO OSEBNIH PODATKOV

Projekt	Ocene učinkov na varstvo osebnih podatkov (DPIA)
Pogodbeni obdelovalec	FAKULTETA ZA DRUŽBENE VEDE KARDELJEVA PLOŠČAD 5, 1000 LJUBLJANA MATIČNA ŠTEVILKA: 1626957
Upravljavec podatkov	Uporabniki portala 1ka, ki kreirajo anketo
Verzija	1.0.
Datum	Julij 2019
Namen dokumenta	Identifikacija skladnostnih tveganj in njihova omejitev z ustreznimi ukrepi za zmanjševanje tveganj
Pripravil	Inštitut za ekonomijo, pravo in informatiko Dunajska cesta 106 1000 Ljubljana
Odobril	

Vsebina

I.	Uvod	3
II.	Izrazi	4
III.	Postopki obdelave, ki so predmet ocene učinka.....	5
IV.	Postopek izvedbe DPIA.....	7
V.	Ocena učinka obdelave osebnih podatkov v okviru obdelave podatkov iz portala 1KA	9
	1. RAZLOGI ZA IZVEDBO DPIA IN PRIČAKOVAN VPLIV NA ZASEBNOST POSAMEZNIKOV	
	2. OPIS OBDELAVE OSEBNIH PODATKOV	
	3. ANALIZA TVEGANJ IN UKREPI ZA OBVLADOVANJE TVEGANJ	
	4. DPIA POROČILO	

Uvod

35. člen Splošne uredbe o varstvu podatkov uvaja koncept **Ocene učinka v zvezi z varstvom osebnih podatkov**. **DPIA** je proces, ki je namenjen **opisovanju obdelave, oceni nujnosti in sorazmernosti obdelave** ter pomaga pri **obvladovanju tveganj** za pravice in svoboščine fizičnih oseb, ki izhajajo iz obdelave osebnih podatkov (z njihovo oceno in določanjem ukrepov za njihovo obravnavo). **DPIA** je pomembno orodje za vzpostavitev odgovornosti, saj pomaga upravljavcem, da ne le izpolnjujejo zahteve **GDPR** in področne zakonodaje v zvezi z varstvom osebnih podatkov, ampak tudi dokažejo, da so bili sprejeti ustrezni ukrepi za zagotovitev skladnosti z **GDPR**.

Organizacija Fakulteta za družbene vede (v nadaljevanju organizacija) v zadevnem procesu obdelave podatkov sicer sodeluje kot pogodbeni obdelovalec osebnih podatkov, saj upravljavcem omogoča uporabo portala za izvajanje anket. Ker gre za množično obdelavo podatkov se je organizacija odločila za izvajanje **DPIA** tudi v imenu upravljavcev, saj ocenjuje, da bi obdelava osebnih podatkov iz določenih zbirk lahko povzročila veliko tveganje za pravice in svoboščine posameznikov. Organizacija je izvedla **DPIA** v sodelovanju z **zunanjim strokovnjakom s področja osebnih podatkov**.

V dokumentirani analizi **DPIA** je organizacija upoštevala minimalne zahteve **Splošne uredbe o varstvu podatkov** (člen 35 (7) ter uvodne izjave 84 in 90 GDPR) in smernice Informacijskega pooblaščenca »Ocene učinkov na varstvo podatkov«.

V **DPIA** je na posameznih kritičnih področjih podrobneje opredeljen(a):

- (a) sistematičen opis predvidenih dejanj obdelave in namenov obdelave,
 - (b) ocena potrebnosti in sorazmernosti dejanj obdelave glede na njihov namen,
 - (c) ocena tveganj za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, ter
 - (d) izvajanje ukrepov za obravnavanje tveganj in za dokazovanje skladnosti z določbami zakonodaje.
-

Izrazi

V Oceni učinka v zvezi z varstvom osebnih podatkov so uporabljeni naslednji izrazi:

- (1) **DPIA:** pomeni Ocena učinka v zvezi z varstvom osebnih podatkov (»Data Protection Impact Assessment«).
- (2) **DPO:** pomeni pooblaščenca oseba za varstvo osebnih podatkov (»Data Protection Officer«).
- (3) **GDPR:** pomeni Splošna uredba o varstvu podatkov (»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«).
- (4) **Upravljevec osebnih podatkov:** upravljevec pomeni fizično ali pravno osebo, ki sama ali skupaj z drugimi določa namene in sredstva obdelave osebnih podatkov.
- (5) **Pogodbeni obdelovalec:** pomeni fizično ali pravno osebo, ki obdeluje osebne podatke v imenu upravljavca.
- (6) **Osební podatek:** osebni podatek pomeni katero koli informacijo v zvezi z določenim ali določljivim posameznikom (v nadaljnjem besedilu tudi: posameznik, na katerega se nanašajo osebni podatki); določljiv posameznik je tisti, ki ga je mogoče neposredno ali posredno določiti, zlasti z navedbo identifikatorja, kot je ime, identifikacijska številka, podatki o lokaciji, spletni identifikator, ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika.
- (7) **Obdelava osebnih podatkov:** obdelava pomeni vsako dejanje ali niz dejanj, ki se izvaja v zvezi z osebnimi podatki ali nizi osebnih podatkov z avtomatiziranimi sredstvi ali brez njih, kot je zbiranje, beleženje, urejanje, strukturiranje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, prilagajanje ali kombiniranje, omejevanje, izbris ali uničenje.
- (8) **Zbirka podatkov:** zbirka pomeni vsak strukturiran niz osebnih podatkov, ki so dostopni v skladu s posebnimi merili, niz pa je lahko centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi.
- (9) **Privolitev posameznika:** privolitev posameznika, na katerega se nanašajo osebni podatki pomeni vsako prostovoljno, izrecno, informirano in nedvoumno izjavo volje posameznika, na katerega se nanašajo osebni podatki, s katero z izjavo ali jasnimi pritrdilnimi dejanjem izrazi soglasje za obdelavo osebnih podatkov, ki se nanašajo nanj.

Postopki obdelave, ki so predmet ocene učinka

Ocena učinka je obvezna takrat, ko je možno, da bi vrsta obdelave, zlasti z uporabo novih tehnologij, ob upoštevanju narave, obsega, okoliščin in namenov obdelave lahko povzročila *veliko tveganje za pravice in svoboščine posameznikov*.

Ocena učinka se zahteva zlasti v primeru (3. odstavek 35. člena GDPR):

- (a) sistematičnega in obsežnega vrednotenja osebnih vidikov v zvezi s posamezniki, ki temelji na avtomatizirani obdelavi, vključno z oblikovanjem profilov, in je osnova za odločitve, ki imajo pravne učinke v zvezi s posameznikom ali nanj na podoben način znatno vplivajo;
- (b) obsežne obdelave posebnih vrst podatkov iz člena 9(1) ali osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški iz člena 10, ali
- (c) obsežnega sistematičnega spremljanja javno dostopnega območja.

Za lažje ugotavljanje, kdaj je DPIA v praksi obvezna, je Informacijski pooblaščenec objavil seznam kriterijev, ki naj bi pomenili visoko tveganje za pravice in svoboščine posameznikov. Samo dejstvo, da konkretna obdelava ne izpolnjuje nobenega od kriterijev za izvedbo ocene učinka, ne zmanjšuje splošne obveznosti upravljavca, da sprejme ustrezne ukrepe za ustrezno obvladovanje tveganj za pravice in svoboščine posameznikov. To v praksi pomeni, da mora družba nenehno ocenjevati tveganja, da bi ugotovila, kdaj bo neka vrsta obdelave »verjetno povzročila veliko tveganje za pravice in svoboščine posameznikov«.

Kriteriji, ki naj bi se upoštevali pri odločitvi, ali DPIA izvesti ali ne, so naslednji:

1. Obsežno vrednotenje in profiliranje posameznikov
2. Avtomatizirano odločanje s pravnim ali podobnim učinkom
3. Sistematičen nadzor nad posameznikom brez njegovega zavedanja
4. Obdelava posebnih vrst osebnih podatkov
5. Množičnost obdelave osebnih podatkov
6. Primerjanje in kombiniranje različnih zbirk podatkov (npr. pridobljenih skozi različne aktivnosti upravljavca) in analitika na osnovi masovnih podatkov
7. Nesorazmerje moči
8. Inovativna uporaba obstoječih in novih tehnologij
9. Omejitev dostopa do storitve/pogodbe
10. Neposredno tveganje za zdravje in varnost posameznikov

Seznam ni končen, saj lahko tveganja povzročijo tudi druge vrste obdelave. Informacijski pooblaščenec meni, da več kriterijev kot je izpolnjenih, večja je verjetnost, da o bo DPIA obvezna.

Zaradi narave obdelave podatkov organizacija v imenu upravljavcev obdeluje veliko količino osebnih podatkov, med katerimi so tudi posebne vrste osebni podatki, obdelava katerih lahko v določenih primerih povzroči visoko tveganje za pravice in svoboščine posameznikov.

Skladno z uredbo, smernicami in kriteriji, ki jih je podal Informacijski pooblaščenec se je organizacija odločila, da izvede oceno učinka za naslednje procese obdelave osebnih podatkov:

Proces obdelave	Kriteriji
Obdelava osebnih podatkov iz portala 1KA	- množičnost obdelave osebnih podatkov - obdelava posebnih vrst osebnih podatkov

Postopek izvedbe DPIA

Pri izdelavi ocene učinkov na obdelavo osebnih podatkov se je organizacija posvetovala z zunanjim strokovnjakom s področja varstva osebnih podatkov (v nadaljevanju strokovnjak).

Ker metodologija za izvedbo DPIA ni predpisana, sta se organizacija in strokovnjak odločila za izvedbo ocene učinka v okviru pravne in informacijske analize. Podrobneje je bila izvedena analiza tveganj s strani upravljavcev in organizacije, ki bi lahko vplivala na pravice in svoboščine posameznikov, katerih osebni podatki se obdelujejo. V prvi fazi smo opredelili razloge oziroma kriterije, na podlagi katerih smo se odločili za izvedbo DPIA ter opisali splošen postopek obdelave osebnih podatkov.

V drugem delu smo na podlagi temeljnih načel varstva osebnih podatkov analizirali pravna in informacijska tveganja, ki jo ima obdelava osebnih podatkov na pravice in svoboščine posameznika ter upravljavce in organizacijo ter opredelili ukrepe, ki se izvajajo za zagotavljanje skladnosti. Pri tem smo se osredotočili na naslednja načela:

Pravna analiza:

- Načelo zakonitosti, poštenosti in preglednosti
- Načelo omejitve namena
- Načelo najmanjšega obsega podatkov
- Načelo točnosti
- Načelo omejitve shranjevanja
- Načelo odgovornosti

Informacijska analiza:

- Načelo celovitosti
- Načelo zaupnosti
- Načelo dostopnosti
- Načelo sledljivosti.

Raven tveganja je bila določena kot zmnožek **verjetnosti**, da se bo tveganje uresničilo in **resnosti**, ki jih ima uresničitev tveganja. Stopnje verjetnosti in resnosti smo opredelili v razmerju 1 – 3, kjer 1 predstavlja nizko stopnjo tveganja, 2 srednjo in 3 visoko stopnjo tveganja.

Oceno verjetnosti, da bi se tveganje uresničilo smo ocenili na podlagi naslednjih kriterijev:

1 (nizka): Verjetnost, da bi se tveganje uresničilo je ocenjeno na 0 – 10%.

2 (srednja): Verjetnost, da bi se tveganje uresničilo je ocenjeno na 10 – 50%.

3 (visoka): Verjetnost, da bi se tveganje uresničilo je ocenjeno na 50 – 100%.

Resnost, ki bi jo imelo uresničenje tveganja smo določili na podlagi naslednjih kriterijev:

1 (nizka): Kadar uresničeno tveganje nima posledic za organizacijo ali posameznike.

2 (srednja): Kadar bi uresničeno tveganje pomenilo, da je organizacija neskladna z zakonodajo to pa bi lahko vplivalo tudi na manjše število zadevnih posameznikov.

3 (visoka): Kadar bi uresničeno tveganje pomenilo, da je organizacija neskladna z zakonodajo to pa bi lahko vplivalo tudi na večje število zadevnih posameznikov.

Raven tveganja je določena kot **zmnožek stopnje verjetnosti in stopnje resnosti**.

RAVEN TVEGANJA	PREDVIDENI UKREPI
1 do 3	Nizka raven tveganja: Posvetovanje z Informacijskim pooblaščencom in dodatki ukrepi niso potrebni.
4 do 8	Srednja raven tveganja: Organizacija mora izvesti dodatne ukrepe, s katerimi zmanjša ali odpravi tveganja. Posvetovanje z Informacijskim pooblaščencom ni potrebno.
9	Visoka raven tveganja: Potrebno je posvetovanje z informacijskim pooblaščencom.

Glede na zmnožek, ki ga raven tveganja predstavlja, smo ugotovili, v katerih primerih mora organizacija izvesti ustrezne ukrepe, da se tveganje zmanjša/odpravi.

Ker je v primerih, ko je raven tveganja 1, 2 ali 3, resnost ali verjetnost vedno ocenjena z nizko, menimo, da je tveganje v teh primerih že obvladano, zato dodatni ukrepi niso potrebni.

V primeru, ko je raven tveganja 4 ali 6, so potrebni dodatni ukrepi, s katerimi bo organizacija zmanjšala ali tveganje odpravila. Da bi organizacija ukrepe odpravila čimbolj učinkovito, smo določili rok za izvedbo ukrepa, ter odgovorno osebo.

V primeru, da sta verjetnost in resnost tveganja visoka, je potrebno **posvetovanje z Informacijskim pooblaščencom**.

Ocena učinka obdelave osebnih podatkov v okviru obdelave podatkov iz portala 1KA

1. RAZLOGI ZA IZVEDBO DPIA IN PRIČAKOVAN VPLIV NA ZASEBNOST POSAMEZNIKOV

Organizacija je ponudnik odprtokodne aplikacije, ki omogoča storitev spletnega anketiranja, v okviru katere lahko uporabniki izdelajo spletni vprašalnik, izvedejo spletno anketo ter urejajo in analizirajo podatke, pridobljene preko spletne ankete. V okviru spletnih anket se lahko obdelujejo tudi osebni podatki, zaradi česar je potrebno pri obdelavi podatkov upoštevati določbe GDPR. Organizacija nastopa kot pogodbeni obdelovalec podatkov, ki se obdelujejo znotraj aplikacije. Ker se v aplikaciji obdeluje velika količina osebnih podatkov, med katerimi so lahko tudi posebne vrste osebni podatki in ker bi kršitev varstva podatkov lahko vplivalo na pravice in svoboščine posameznikov, se je organizacija odločila, da izdela oceno učinka na varstvo osebnih podatkov.

Izrazi, ki bodo v dokumentu uporabljeni so naslednji:

Upravljavec osebnih podatkov – registrirani uporabniki aplikacije, ki izdelajo in izvedejo spletno anketo. Ker uporabniki podatke obdelujejo v svojem imenu so upravljavci osebnih podatkov.

Organizacija – organizacija FDV, ki v razmerju z upravljavci nastopa kot pogodbeni obdelovalec. Ta upravljavcem omogoča uporabo portala 1ka ter shranjuje podatke na strežnikih.

Respondent – posamezniki, ki rešujejo anketo, ki jo je pripravil in izdelal upravljavec osebnih podatkov.

2. OPIS OBDELAVE OSEBNIH PODATKOV

Uporabnik spletne aplikacije je lahko vsakdo, ki se registrira na portal in sprejme splošne pogoje uporabe z namenom izdelave spletne ankete. Uporabnik je skladno z GDPR upravljavec podatkov, ki podatke obdeluje v okviru izvajanja spletne ankete, za svoje lastne namene. Reševanja spletne ankete se lahko udeležijo vsi, ki jih uporabnik povabi k reševanju ankete.

V svojem uporabniškem profilu ima vsak upravljavec dostop do podatkov iz rešenih anket, ki jih je kreiral preko svojega profila. Do teh podatkov ima lahko dostop tudi morebitni drugi registrirani uporabnik portala, kateremu upravljavec podeli pravice. Uporabniški računi se skupaj z upravljavčevimi anketami hranijo trajno, na strežniku v Sloveniji.

Organizacija nastopa kot pogodbeni obdelovalec in podatkov reševalcev anket, zbranih s pomočjo aplikacije 1KA ne uporablja za svoje lastne namene. Za upravljavce organizacija podatke hrani na strežnikih zunanjega izvajalca in jim nudi orodje za izvedbo anket.

Organizacija je aplikacijo posodobila na način, ki zagotavlja, da se podatki obdelujejo skladno z določbami GDPR. Pri tem je upoštevala naravo, obseg, okoliščine in namene obdelave ter tudi tveganja za pravice in svobodo posameznikov, ki so povezana z obdelavo podatkov.

Kategorije posameznikov, na katere se nanašajo osebni podatki

Podatki, ki se v okviru aplikacije obdelujejo, se nanašajo na respondente, tj. osebe, ki preko spleta rešijo anketo, izdelano s strani upravljavca.

Upravljanje s privoljenji posameznika za obdelovanje osebnih podatkov

Obdelava podatkov iz aplikacije 1KA se lahko izvaja le na podlagi predhodnega soglasja respondenta. Organizacija je aplikacijo zasnovala na način, da mora respondent v primeru, ko se v anketi obdelujejo kakršnikoli osebni podatki, za obdelavo predhodno podati soglasje. V primeru, da respondent soglasja ne poda, izpolnjevanje ankete ni mogoče. Pred podajo soglasja, je respondent seznanjen z informacijami o tem kdo je upravljavec osebnih podatkov, za katere namene se obdelujejo osebni podatki, kdo so morebitni uporabniki podatkov, ali se podatki iznašajo v tretje države, koliko časa se podatki hranijo ter katere pravice ima v zvezi z obdelavo osebnih podatkov.

Hramba osebnih podatkov

Podatki se hranijo trajno, na strežniku zunanjega izvajalca. V primeru, da bi se podatki po nesreči zbrisali, se lahko izvede restavriranje, saj se podatki hkrati shranjujejo tudi na sekundarni strežnik, ki je na drugi lokaciji. Dnevno se na zunanje enote izdelujejo tudi varnostne kopije.

Vrste osebnih podatkov

Med osebnimi podatki, ki se obdelujejo v okviru spletne aplikacije, so različne vrste osebni podatki, med katerimi so lahko tudi posebne vrste osebni podatki. Vrsta osebnih podatkov, ki se obdeluje, je odvisna od vsakega upravitelja posebej, saj je on tisti, ki določa, katere vrste osebnih podatkov potrebuje za izvedbo posamezne ankete.

Od upravitelja osebnih podatkov je prav tako odvisen obseg osebnih podatkov, ki se obdelujejo. Organizacija ne more omejiti količine osebnih podatkov, ki se v okviru anket zbirajo, saj le ta ne določa namena obdelave.

Na točnost in ažurnost podatkov organizacija in upravitelj nimata vpliva, je pa znotraj aplikacije podana možnost, da se podatki na zahtevo respondenta spremenijo oziroma popravijo.

Namen obdelave podatkov

Aplikacija je namenjena izdelavi in izvedbi spletnega vprašalnika. V splošnih pogojih je upravitelj seznanjen z namenom aplikacije in pravilno uporabo le te.

Postopek uveljavljanja pravic iz GDPR

Za uveljavljanje pravic, ki jih posameznikom daje GDPR so znotraj aplikacije predvideni obrazci, ki jih lahko izpolnijo respondenti. Obrazci so oblikovani na način, da posameznik, ki želi uveljavljati katero izmed pravic, v obrazec vpiše ime ankete, elektronski naslov in URL ankete ter katero izmed pravic želi uveljavljati. Zahtevek se nato samodejno pošlje na elektronski naslov avtorja ankete (upravitelja) ter organizacije. Po poteku 30 dni organizacija preveri, ali je upravitelj zahtevku ugodil ter ga v primeru, da tega ni storil, ponovno pozove k izpolnitvi zahteve. V primeru, da upravitelj na zahtevo ne odgovori, si organizacija pridržuje pravico, da izbriše anketo, v zvezi s katero je bila poslana zahteva.

Informacijska analiza

Aplikacija se nadgrajuje s strani zunanjih izvajalcev pri katerem se shranjujejo tudi podatki.

Zunanji izvajalec za organizacijo izvaja naslednje aktivnosti:

- hramba podatkov iz aplikacije na lastnih strežnikih (vključno z virtualnim strežnikom in MySQL strežniško podatkovno bazo),
- izdelava, šifriranje in hramba šifriranih kopij virtualnega strežnika,
- restavriranje virtualnih strežnikov iz šifriranih varnostnih kopij na zahtevo organizacije, pri čemer izvajalec zagotavlja popolno sledenje vsem dnevnikom na lastnih strežnikih, vključno z dokumentiranjem vseh sprememb in posegov.

Zunanji izvajalec zagotavlja 99,9% razpoložljivost sistema in omrežja, ki je uporabnikom aplikacije na voljo 24 ur dnevno in 7 dni v tednu, razen med vzdrževalnimi posegi, ki so predhodno najavljeni. Uporabljajo se orodja za merjenje dostopnosti strežnikov, kar pomeni, da so vzdrževalci takoj obveščeni, če strežnik ne bi bil dostopen ali pa bi bilo njegovo delovanje kakorkoli upočasnjeno.

Z zunanjim izvajalcem je sklenjen aneks k pogodbi o gostovanju in vzdrževanju strežniške infrastrukture, v katerem je opredeljena tudi vsebina obdelave osebnih podatkov.

Razvojno, produkcijsko in testno okolje je ločeno. Razvojno in produkcijsko okolje je na strežniku zunanjega izvajalca, testno pa na strežniku organizacije, s čimer se zagotavlja, da morebitne napake v testnem okolju ne vplivajo na zaupnost, celovitost ali dostopnost podatkov v produkcijskem okolju.

Avtentikacija uporabnikov in politika gesel

Dostop do podatkov iz aplikacije s strani organizacije je mogoč z uporabo uporabniškega imena in gesla. Za vstop v domeno se uporablja eno uporabniško ime in geslo, za vstop v aplikacijo pa drugo. Gesla niso predpisana, prav tako ni predvideno redno menjavanje gesel.

Postopek dodelitve uporabniških pravic formalno ni predpisan, velja pa, da uporabniške pravice dodeli administrator na zahtevo vodje projekta. V primeru, da oseba, ki dela na projektu odide ne bo več sodelovala pri projektu, se ji uporabniške pravice ukinejo.

Upravljalci do podatkov iz anket, ki jih kreirajo dostopajo preko svojega uporabniškega profila z uporabo uporabniškega imena in gesla. Do teh podatkov lahko dostopajo tudi drugi uporabniki, če jim upravljaivec dodeli ustrezne pravice.

Upravljanje varnostnih dogodkov (incidentov), ki imajo vpliv na raven zavarovanja osebnih podatkov

Zunanji izvajalec je morebitne varnostne dogodke po pogodbi dolžan sporočiti organizaciji, o čemer ta obvesti upravljalce podatkov.

Človeški viri

Zaposleni, ki delajo na projektu 1KA so se udeležili izobraževanj na področju varstva osebnih podatkov, prav tako pa so vsi zaposleni v organizaciji ob zaposlitvi podpisali izjavo o varovanju osebnih podatkov.

Politika čistega zaslona je vzpostavljena, čas zaklepanja zaslona pa je prilagojena dinamiki dela zaposlenih.

Varovanje podatkov

Komunikacija med uporabniki in spletnim mestom 1ka poteka prek standarda standarda Transport Layer Security (TLS), ki s pomočjo šifriranja zagotavlja, da do podatkov ne morejo dostopati tretje osebe.

Podatki iz aplikacije 1KA se hranijo na strežniku pogodbenega obdelovalca organizacije (Akson d.o.o.), v Sloveniji. Akson d.o.o. ima svojo strojno opremo nameščeno v podatkovnih centrih Pošte Slovenije. Podatkovni center je zavarovan na način, ki zagotavlja visok nivo zaščite podatkov pred požarom, potresom, elektromagnetnimi vplivi, plini, tekočinami, prahom, vlomi in drugimi morebitnimi okoljskimi vplivi. Prostori podatkovnega centra so fizično varovani. Dostop do podatkovnega centra je omejen z magnetno zaporo ter sistemom za identifikacijo, izvaja pa se tudi videonadzor. Vsak skrbnik se mora ob vstopu identificirati z magnetno kartico in šifro, dostopi pa se zabeležijo v nadzornem centru.

Commented [ZK1]: Od aprila 2020 strežniki niso več na Aksonu temveč na Telemach d.o.o.

Za zagotavljanje dostopnosti oziroma razpoložljivosti podatkov se vsi podatki varnostno kopirajo in replicirajo na rezervni strežnik na dveh različnih lokacijah. Obe lokaciji imata enako stopnjo fizične zaščite strežnikov in ostale opreme. Za zaščito pred nepooblaščenim dostopom skrbijo zaposleni pogodbenega obdelovalca, med drugim tudi z večstopenjskimi požarnimi pregradami, ki se redno posodablajo.

Sledljivost obdelave

Uporabniški ter administratorski dostopi in spremembe se beležijo, zaradi česar je omogočena sledljivost dostopov in sprememb podatkov.

3. ANALIZA TVEGANJ IN UKREPI ZA OBVLADOVANJE TVEGANJ

Vrste tveganja, ki smo jih identificirali so prikazana v spodnji tabeli:

TVEGANJE	VPLIV TVEGANJA		
	Tveganje za posameznike	Tveganje neusklajenosti	Poslovno tveganje
Nezakonita obdelava s strani upravljavcev	x	x	x
Nezakonita obdelava s strani organizacije	x	x	x
Neveljavna privolitev	x	x	x
Nepoštena in nepregledna obdelava osebnih podatkov	x	x	x
Posameznik nima možnosti uveljavljati svojih pravic	x	x	x
Podatki se obdelujejo za namene, za katere niso bili pridobljeni	x	x	x
Prekomerna obdelava osebnih podatkov	x	x	x
Podatki so netočni/neažurni		x	x
Podatki se hranijo preko ustreznega roka hrambe	x	x	x
Pogodbe o obdelavi osebnih podatkov niso sklenjene s pogodbenimi obdelovalci	x	x	x
Organizacija ne izvaja nadzora pogodbenih obdelovalcev	x	x	x
Organizacija nima izdelane evidence dejavnosti obdelave podatkov, ki jih obdeluje v imenu upravljavcev		x	x
Neozaveščenost oseb na področju varstva osebnih podatkov	x	x	x
Izguba podatkov zaradi naravnih pojavov (poplava, požar...)			x
Izguba podatkov zaradi zlonamernih napadov (vlomi, vandalizem...)	x		x
Nedelovanje sistema			x
Do podatkov dostopajo nepooblaščen osebe	x	x	x
Zloraba dostopnih pravic	x		x
Zunanji vdori v bazo podatkov	x		x
Sledljivost obdelave osebnih podatkov se ne zagotavlja		x	x

NAČELO		TVEGANJE	VERJETNOST/RESNOST	RAVEN TVEGANJA	UKREPI ZA ZMANJŠEVANJE TVEGANJ
PRAVNA ANALIZA	Načelo zakonitosti, poštenosti in preglednosti	1.1 Nezakonita obdelava s strani upravljavcev	2/2	4	Opozorilo upravljavcem osebnih podatkov o morebitnih posledicah nezakonite obdelave osebnih podatkov.
		1.1 Nezakonita obdelava s strani organizacije	2/2	4	Vključitev določb pogodbene obdelave podatkov v splošne pogoje uporabe portala za uporabnike.
		2. Neveljavna privolitev	1/2	2	-
		3. Nepoštena in nepregledna obdelava osebnih podatkov	2/2	4	Dodatno opozorilo upravljavcem podatkov o obveznostih, ki jih imajo do respondentov, če od njih pridobivajo osebne podatke.
		4. Posameznik nima možnosti uveljavljati svojih pravic	1/2	2	-
	Načelo omejitve namena	5. Podatki se obdelujejo za namene, za katere niso bili pridobljeni	2/2	4	Opozorilo upravljavcem podatkov o morebitnih posledicah, če aplikacijo in podatke, ki jih zberejo z uporabo aplikacije uporabijo za druge namene.
		6. Prekomerna obdelava osebnih podatkov	2/2	4	Opozorilo upravljavcem osebnih podatkov, da se v okviru spletne ankete obdelujejo le tisti osebni podatki, ki so nujno

NAČELO		TVEGANJE	VERJETNOST/RESNOST	RAVEN TVEGANJA	UKREPI ZA ZMANJŠEVANJE TVEGANJ
					potrebni za izvedbo ankete.
	Načelo točnosti	7. Podatki so netočni/neažurni	1/1	1	-
	Načelo omejitve shranjevanja	8. Podatki se hranijo preko ustreznega roka hrambe	2/2	4	Preveriti, ali obstaja učinkovita informacijska rešitev, da bi se vse ankete samodejno brisale po poteku določenega časa (npr. 5 let), pred tem pa bi upravljavci dobili obvestilo o brisanju, pri čemer bi imeli možnost, da se brisanje še ne izvede.
	Načelo odgovornosti	9. Pogodbe o obdelavi osebnih podatkov niso sklenjene s pogodbenimi obdelovalci	2/2	4	V aneksu je potrebno natančno opredeliti kakšne ukrepe izvaja pogodbeni obdelovalec za zagotavljanje varnosti, integritete ter dostopnosti oz. razpoložljivosti podatkov, kateri podatki se obdelujejo idr. Določbe, ki jih mora pogodba o obdelavi vsebovati, da je skladna z GDPR.
		10. Organizacija ne izvaja nadzora pogodbenih obdelovalcev	3/2	6	Je predviden v pogodbi o obdelavi podatkov –

NAČELO		TVEGANJE	VERJETNOST/RESNOST	RAVEN TVEGANJA	UKREPI ZA ZMANJŠEVANJE TVEGANJ
INFORMACIJSKA ANALIZA					upravitelji lahko izvedejo revizijo pri pog. obdelovalcu.
		11. Ni vzpostavljene evidence dejavnosti obdelave osebnih podatkov	1/2	2	-
		12. Organizacija nima izdelane evidence dejavnosti obdelave podatkov, ki jih obdeluje v imenu upraviteljev	2/2	4	Izdelati dokument evidenc obdelave podatkov, ki jih za upravitelja obdeluje obdelovalec.
		13. Neozaveščenost oseb na področju varstva osebnih podatkov	1/2	2	-
	Načelo celovitosti, zaupnosti, dostopnosti in sledljivosti	14. Izguba podatkov zaradi naravnih pojavov	1/1	1	-
		15. Izguba podatkov zaradi zlonamernih napadov (vlomi, vandalizem...)	1/3	3	-
		16. Nedelovanje sistema	1/2	2	-
		17. Do podatkov dostopajo nepooblaščen osebe	2/1	2	Opozorilo upraviteljem na posledice nepooblaščenega dostopa do podatkov.
		18. Zloraba dostopnih pravic	1/2	2	-
		19. Zunanji vdor v sistem	1/3	3	-
		20. Sledljivost obdelave osebnih podatkov se ne zagotavlja	1/2	2	-

1. Nezakonita obdelava podatkov:

1.1. Nezakonita obdelava s strani upravljavcev: Znotraj aplikacije je vzpostavljena možnost, da posameznik poda soglasje za obdelavo podatkov, če se v okviru ankete obdelujejo osebni podatki. Upravitelji osebnih podatkov, ki izdelajo anketo, morajo namreč označiti, ali se v anketi zbirajo kakšni osebni podatki. V primeru, da gre za obdelavo osebnih podatkov, je aplikacija programirana na način, da mora respondent pred izpolnjevanjem ankete in posredovanjem osebnih podatkov podati soglasje za obdelavo. Če soglasja ne poda, izpolnjevanje ankete ni mogoče. Ali se bo pred izpolnjevanjem ankete zahtevalo soglasje respondentov pa je odvisno od upravljavcev samih. Upravitelj je v primeru, da se obdelujejo osebni podatki, dolžan to v aplikaciji tudi označiti. Ker je aplikacija nastavljena na način, da je soglasje potrebno samo v primeru, ko upravitelj označi, da bo šlo za obdelavo osebnih podatkov, bi lahko zaradi morebitnega nepoznavanja oziroma nerazumevanja definicije osebnih podatkov ali nepozornosti upravljavcev pri izdelavi anket obstajala verjetnost, da bi se podatki respondentov obdelovali brez ustrezne pravne podlage, zaradi česar bi bili upravljavci osebnih podatkov neskladni z zakonodajo.

Ukrep: Opozorilo upravljavcem osebnih podatkov o morebitnih posledicah nezakonite obdelave osebnih podatkov.

1.2. Nezakonita obdelava s strani organizacije: Organizacija v tem primeru nastopa kot pogodbeni obdelovalec, zaradi česar mora imeti z vsakim upravljavcem (tj. vsakim, ki kreira anketo, v kateri se zbirajo osebni podatki) sklenjeno pogodbo o obdelavi podatkov. Če določbe pogodbe o obdelavi podatkov ne bodo del splošnih pogojev, ki jih mora sprejeti vsak uporabnik, se lahko zgodi, da bi se pogodbeni obdelava za določene uporabnike izvajala brez ustrezne pravne podlage.

Ukrep: Vključitev določb pogodbene obdelave podatkov v splošne pogoje uporabe portala za uporabnike.

2. Neveljavna privolitev: V zahtevku za podajo privolitve v obdelavo podatkov je respondent napoten na povezavo, na kateri so informacije v zvezi z obdelavo osebnih podatkov. Privolitev je podana z izkazljivim aktivnim dejanjem respondenta ter oblikovana na način, da zagotavlja resnično izbiro in nadzor, ne prinaša škodljivih posledic za posameznika, če je ne poda, je dokazljiva in podana za konkretno opredeljen namen, jasno pove kdo je upravitelj, za kakšen namen se bodo podatki obdelovali, o morebitnem prenosu v tretje države in kakšne pravice ima posameznik v zvezi z obdelavo podatkov.

3. Nepoštena in nepregledna obdelava osebnih podatkov: Znotraj aplikacije so respondentom na voljo vse informacije (13. člen GDPR), ki mu morajo biti predložene, preden se od njega pridobivajo osebni podatki. Ker obstaja možnost, da upravitelj podatkov izključi opcijo

posredovanja teh podatkov respondentom, obstaja verjetnost, da bi bili podatki respondentov obdelovani na nepošten način.

Ukrep: Dodatno opozorilo upravljavcem podatkov o obveznostih, ki jih imajo do respondentov, če od njih pridobivajo osebne podatke.

4. Posameznik nima možnosti uveljavljati svojih pravic: Respondenti lahko pravice, ki jim gredo po GDPR uveljavljajo preko obrazcev, ki so jim dostopni v aplikaciji. Zahtevek se samodejno pošlje na elektronski naslov upravljavca in organizacije. Če upravljavec v 30 dneh ne odgovori na zahtevek, ga na to ponovno opomne organizacija. Če tudi po opominu organizacije upravljavec zahtevku ne ugotovi oziroma na zahtevek ne odgovori, si organizacija pridržuje pravico, da izbriše anketo, v zvezi s katero je bila poslana zahteva.

5. Podatki se obdelujejo za namene, za katere niso bili pridobljeni: Aplikacija 1KA je namenjena izdelavi in izvajanju anket, o čemer je upravljavec seznanjen s splošnimi pogoji uporabe, ki jih mora sprejeti ob registraciji. Organizacija ne more vplivati na to, da podatki ne bi bili uporabljeni še za druge namene, obstaja pa verjetnost, da bi upravljavci podatkov, podatke, ki so jih pridobili v okviru anketnih vprašalnikov uporabili še za druge namene, kar je neskladno z zakonodajo.

Ukrep: Opozorilo upravljavcem podatkov o morebitnih posledicah, če aplikacijo in podatke, ki jih zberejo z uporabo aplikacije uporabijo za druge namene.

6. Prekomerna obdelava osebnih podatkov: Obseg osebnih podatkov, ki se obdelujejo v okviru aplikacije s strani organizacije ni omejen, saj obseg podatkov, ki so potrebni za izpolnitev določenega namena obdelave določa upravljavec sam. Če upravljavec osebnih podatkov ni seznanjen z načeli varovanja osebnih podatkov obstaja verjetnost, da bi se zbirali osebni podatki, ki jih upravljavec ne potrebuje za dosego namena, zaradi katerega se obdelujejo.

Ukrep: Opozorilo upravljavcem osebnih podatkov, da se v okviru spletne ankete obdelujejo le tisti osebni podatki, ki so nujno potrebni za izvedbo ankete.

7. Podatki so netočni/neažurni: Zaradi namena in narave zbranih podatkov, točnost in ažurnost podatkov nista relevantna, in ne vpliva na pravice in svoboščine respondentov.

8. Podatki se hranijo preko ustreznega roka hrambe: Organizacija zaradi kvalitetnega zagotavljanja storitev (uporabe portala 1ka) ne more samodejno določati roka hrambe podatkov, saj bi s tem lahko prekomerno posegla v interese upravljavca, če bi se ankete zbrisale po določenem času, upravljavec pa bi podatke še vedno potreboval za izpolnitev svojega namena. Rok hrambe je zato trenutno neomejen. Ker v večini primerov upravljavci anket po izpolnitvi namena ne zbršejo, se le te hranijo trajno, kar pomeni prekomerno hrambo podatkov.

Ukrep: Preveriti, ali obstaja učinkovita informacijska rešitev, da bi se vse ankete samodejno brisale po poteku določenega časa (npr. 5 let), pred tem pa bi upravitelji dobili obvestilo o brisanju, pri čemer bi imeli možnost, da se brisanje še ne izvede.

9. Pogodbe o obdelavi osebnih podatkov niso sklenjene s pogodbenimi obdelovalci: Za ustrezno delovanje aplikacije organizacija sodeluje s ponudnikom gostovanja in vzdrževanja spletnega strežnika aplikacije 1KA (Akson d.o.o.). Organizacija je s ponudnikom sicer sklenila aneks k pogodbi, v katerem so zapisane določbe glede obdelave podatkov, ne vsebuje pa vseh določb, ki predstavljajo obvezno sestavino pogodbe o obdelavi podatkov.

Ukrep: V aneksu je potrebno natančno opredeliti kakšne ukrepe izvaja pogodbeni obdelovalec za zagotavljanje varnosti, integritete ter dostopnosti oz. razpoložljivosti podatkov, kateri podatki se obdelujejo idr. obvezne sestavine.

10. Organizacija ne izvaja nadzora pogodbenih obdelovalcev: Organizacija zaenkrat ne izvaja pregledov in ne presoja ali se storitve izvajajo skladno s pogodbo o obdelavi podatkov.

Ukrep: Predlagamo vam, da enkrat letno izvajate preglede in presojo izvajanja storitev, v okviru katerih se obdelujejo osebni podatki.

11. Ni vzpostavljene evidence dejavnosti obdelave osebnih podatkov: Znotraj aplikacije je za upravitelje podatkov kreirana evidenca dejavnosti obdelave podatkov.

12. Organizacija nima izdelane evidence dejavnosti obdelave podatkov, ki jih obdeluje v imenu upraviteljev: Organizacija nima izdelanega dokumenta evidence dejavnosti obdelave podatkov v imenu upravitelja.

Ukrep: Izdelati dokument evidenc obdelave podatkov, ki jih za upravitelja obdeluje obdelovalec.

13. Neozaveščenost oseb na področju varstva osebnih podatkov: Zaposleni, ki delajo na projektu 1KA so se udeležili izobraževanj na področju varstva osebnih podatkov, prav tako pa so vsi zaposleni v organizaciji ob zaposlitvi podpisali izjavo o varovanju osebnih podatkov.

14. Izguba podatkov zaradi naravnih pojavov (poplava, požar...): Strežniki, na katerih se hranijo podatki so nameščeni v podatkovnih centrih, ki so zavarovani na način, ki zagotavlja visok nivo zaščite podatkov pred požarom, potresom, elektromagnetnimi vplivi, plini, tekočinami, prahom in drugimi morebitnimi okoljskimi vplivi. Verjetnost, da bi zaradi naravnih pojavov prišlo do izgube podatkov je majhna, majhne pa bi bile tudi posledice, saj se podatki varnostno kopirajo in replicirajo na rezervni strežnik na drugi lokaciji.

15. Izguba podatkov zaradi zlonamernih napadov (vlomi, vandalizem...): Prostori podatkovnega centra so tehnično in fizično varovani na način, ki onemogoča dostop nepooblaščenim osebam. Dostop do podatkovnega centra je omejen z magnetno zaporo ter sistemom za identifikacijo, izvaja pa se tudi videonadzor. Vsak skrbnik se mora ob vstopu identificirati z magnetno kartico in šifro, dostopi pa se zabeležijo v nadzornem centru. Verjetnost izgube podatkov zaradi zlonamernih napadov je majhna, posledice pa bi, zaradi morebitnega shranjevanja posebnih vrst osebnih podatkov, lahko bile velike, saj bi se s podatki lahko seznanile nepooblaščene osebe, ki bi lahko podatke tudi zlorabile.

16. Nedelovanje sistema: Za delovanje sistema je zadolžen pogodbeni obdelovalec organizacije, ki zagotavlja 99.9% razpoložljivost sistema in omrežja, ki je uporabnikom na voljo 24 ur dnevno in 7 dni v tednu, razen med vzdrževalnimi posegi, ki bodo predhodno najavljeni. Izvajalec v času trajanja pogodbe zagotavlja tudi varnostne kopije podatkov, kar omogoča povrnitev podatkov, ki so izpadli iz produkcije.

17. Do podatkov dostopajo nepooblaščene osebe: Dostop do podatkov iz aplikacije je mogoč z uporabo uporabniškega imena in gesla. Vsak upravljavec podatkov je odgovoren za vse aktivnosti, opravljene z uporabo njegovega uporabniškega računa. Upravitelji so zaenkrat zgolj obveščeni, da mora biti geslo, ki si ga določijo kompleksno ter shranjeno na varni lokaciji, sam program pa tega zaenkrat samodejno še ne zahteva. Če upravitelji teh zahtev ne bodo upoštevali, obstaja verjetnost, da do podatkov dostopajo nepooblaščene osebe, predvsem če storitve uporabljajo na javnih računalnikih oz. računalnikih, ki so dostopni več osebam. Če se v anketah obdelujejo tudi posebne vrste osebni podatki, je lahko resnost dostopa do podatkov s strani nepooblaščenih oseb visoka.

Ukrep: Opozorilo upravljavcem na posledice nepooblaščenega dostopa do podatkov in ureditev aplikacije na način, da zahteva ustrezno kreirano geslo.

18. Zloraba dostopnih pravic: Postopki dodelitve in odvzema dostopnih pravic niso vnaprej predpisani, ker pa gre za projekt, na katerem sodeluje majhna skupina oseb, je postopek dodelitve in odvzema dostopnih pravic jasn, zato ni verjetno, da bi dostopne pravice imela oseba, ki do podatkov ne sme dostopati. Dostopne pravice dodeli administrator na zahtevo vodje projekta. V primeru, da oseba, ki dela na projektu odide ne bo več sodelovala pri projektu, se ji uporabniške pravice ukinejo.

19. Zunanji vdor v bazo podatkov: Za preprečevanje vdora v bazo podatkov skrbi pogodbeni obdelovalec z večstopenjskimi požarnimi pregradami, ki se redno posodablja. Verjetnost zunanjega vdora v bazo je majhna, posledice pa bi lahko bile velike, saj se shranjuje velika količina podatkov, med katerimi so lahko tudi posebne vrste osebni podatki.

20. Sledljivost obdelave osebnih podatkov se ne zagotavlja: Uporabniški ter administratorski dostopi in spremembe se beležijo, zaradi česar je omogočena sledljivost dostopov in sprememb podatkov.

4. DPIA POROČILO

Na podlagi izvedene ocene učinka procesov obdelave osebnih podatkov so bile identificirane nekatere pomanjkljivosti, ki pa niso tako velike, da bi lahko pomenile visoko tveganje za pravice in svoboščine oseb, katerih osebni podatki se obdelujejo. Za odpravo pomanjkljivosti mora organizacija izvesti naslednje ukrepe:

Ukrep	Rok za izvedbo ukrepa	Odgovorna oseba
Opozorilo upravljavcem osebnih podatkov o morebitnih posledicah nezakonite obdelave osebnih podatkov.	Konec oktobra 2019	Katja
Vključitev določb pogodbene obdelave podatkov v splošne pogoje uporabe portala za uporabnike.	Konec oktobra 2019	Katja
Dodatno opozorilo upravljavcem podatkov o obveznostih, ki jih imajo do respondentov, če od njih pridobivajo osebne podatke.	Konec oktobra 2019	Katja, Peter
Opozorilo upravljavcem podatkov o morebitnih posledicah, če aplikacijo in podatke, ki jih zberejo z uporabo aplikacije uporabijo za druge namene.	Konec oktobra 2019	Katja, Peter
Opozorilo upravljavcem osebnih podatkov, da se v okviru spletne ankete obdelujejo le tisti osebni podatki, ki so nujno potrebni za izvedbo ankete.	Konec oktobra 2019	Katja, Peter
Preveriti, ali obstaja učinkovita informacijska rešitev, da bi se vse ankete samodejno brisale po poteku določenega časa (npr. 5 let), pred tem pa bi upravljavci dobili obvestilo o brisanju, pri čemer bi imeli možnost, da se brisanje še ne izvede.	Konec decembra 2019	Peter
V aneksu je potrebno natančno opredeliti kakšne ukrepe izvaja pogodbeni obdelovalec za zagotavljanje varnosti, integritete ter dostopnosti oz. razpoložljivosti podatkov, kateri podatki se obdelujejo idr. obvezne sestavine.	/	/
Predlagamo vam, da enkrat letno izvajate preglede in presojo izvajanja storitev, v okviru katerih se obdelujejo osebni podatki.	Enkrat letno	Vasja
Izdelati dokument evidenc obdelave podatkov, ki jih za upravljavca obdeluje obdelovalec.	Konec oktobra 2019	Katja
Opozorilo upravljavcem na posledice nepooblaščenega dostopa do podatkov.	Konec oktobra 2019	Katja

Z izvedbo vseh navedenih ukrepov, bodo tveganja obvladana, zato v tem trenutku ni potrebe po predhodnem posvetovanju z Informacijskim pooblaščencom.