REPUBLIKA SLOVENIJA
MINISTRSTVO ZA DIGITALNO PREOBRAZBO
Davčna ulica 1, 1000 Ljubljana

T: 01 555 58 00
E: gp.mdp@gov.si
www.mdp.gov.si

Enotni kontaktni center državne uprave (EKC)

Splošni pogoji uporabe

Datum: 28. 04. 2025

VSEBINA

Verzija	Datum objave verzije	Bistvo dokumenta
Verzija: 0.1	28.04.2025	Splošni pogoji v celoti

1 Uvod

1.1 Namen dokumenta

Splošni pogoji uporabe storitve Enotnega kontaktnega centra državne uprave (v nadaljnjem besedilu: EKC) (v nadaljnjem besedilu: Splošni pogoji) urejajo razmerja med Ponudnikom storitve EKC in Uporabnikom storitve EKC. Urejajo jih tako glede same uporabe storitev kot tudi z vidika obdelave osebnih podatkov. V okviru tega se določijo dolžnosti Ponudnika storitve EKC in Uporabnika storitve EKC glede izpolnjevanja obveznosti pri upravljanju osebnih podatkov.

1.2 Izrazi

1. Vlada RS je za boljšo komunikacijo z državljani in drugimi strankami storitev organov državne uprave ter zaposlenimi pri organih državne uprave ustanovila EKC, ki deluje za namene izvrševanja nalog 24. člena Uredbe o upravnem poslovanju (Uradni list RS, št. 113/05 – uradno prečiščeno besedilo, 89/07 – odl. US, 126/07 – ZUP-E, 48/09, 8/10 – ZUP-G, 8/12 – ZVRS-F, 21/12, 47/13, 12/14, 90/14, 51/16, 36/21, 82/21, 189/21, 153/22 in 18/23). EKC je enotna vstopna točka za informacije s področja dela državne uprave ter pomoč strankam pri uporabi aplikacij in drugih elektronskih storitev organov državne uprave.
2. Ponudnik storitve EKC je Ministrstvo za digitalno preobrazbo (v nadaljnjem besedilu: Ponudnik storitve; sicer se storitev zagotavlja v okviru notranje organizacijske enote: Direktorat za podporo uporabnikom).
3. Stranke storitve EKC so javni uslužbenci, zaposleni v državni upravi (v nadaljnjem besedilu: javni uslužbenci), in ostale stranke, kot so državljani, tujci, poslovni subjekti (v nadaljnjem besedilu: ostale stranke).
4. Uporabniki storitve EKC so organi državne uprave, ki so vsebinski skrbniki storitev, za katere EKC nudi prvo raven podpore.
5. Skrbnik storitve, za katero EKC nudi prvo raven podpore, je oseba, ki skrbi za koordinacijo, komunikacijo in reševanje težav, ki so povezane z zagotavljanjem prve ravni podpore za dotično storitev.

1.3 Kontaktni podatki Ponudnika storitve EKC

Enotni kontaktni center
Ministrstvo za digitalno preobrazbo
Direktorat za podporo uporabnikom
Davčna ulica 1
1000 Ljubljana

Za javne uslužbence
01 478 87 78
Za klice iz tujine
01 478 85 90
ekc@gov.si
Za ostale stranke
0802002

2 Uporaba storitve EKC

2.1 Opis delovanja EKC

Enotni kontaktni center državne uprave (EKC) deluje v okviru Ministrstva za digitalno preobrazbo, Direktorata za podporo uporabnikom. EKC je namenjen vsebinski in tehnični pomoči na 1. ravni podpore pri uporabi elektronskih storitev, ki jih država zagotavlja prebivalcem, tujcem, poslovnim subjektom in zaposlenim v državni upravi (strankam).

Svetovalci EKC so strankam na voljo za splošna vsebinska vprašanja in tehnične težave, ki ih imajo pri uporabi elektronskih storitev organov državne uprave. EKC je razdeljen na podporo za težave javnih uslužbencev zaposlenih v državnih organih in podporo za ostale stranke. Delovni čas EKC je med delovniki od 8:00 do 22:00. Če vprašanja oziroma težave svetovalci EKC ne uspejo razrešiti sami, težavo posredujejo v reševanje na 2. raven podpore skrbnikom posamezne storitve.

2.2 Pravna podlaga za delovanje EKC

EKC deluje na podlagi 74.a člena Zakona o državni upravi (Uradni list RS, št. 113/05 – uradno prečiščeno besedilo, 89/07 – odl. US, 126/07 – ZUP-E, 48/09, 8/10 – ZUP-G, 8/12 – ZVRS-F, 21/12, 47/13, 12/14, 90/14, 51/16, 36/21, 82/21, 189/21, 153/22 in 18/23, v nadaljnjem besedilu ZDU-1), v skladu s katerih je Ministrstvo za digitalno preobrazbo pristojno za upravljanje informacijsko komunikacijske infrastrukture, razvoj skupnih informacijskih rešitev ter njihovo tehnološko, procesno in organizacijsko skladnost s centralnim informacijsko komunikacijskim sistemom, v povezavi s 24. členom Uredbe o upravnem poslovanju (Uradni list RS, št. 9/18, 14/20, 167/20, 172/21, 68/22, 89/22, 135/22, 77/23 in 24/24). Informacijska podpora storitvam, ki jih zagotavlja EKC, je informacijski sistem, ki ga skupaj sestavljata informacijski rešitvi Maximo aplikacija in platforma Omnichannel, kot sta opisani v 3.1 točki »Aplikaciji za spremljanje podpore« teh Splošnih pogojev.

2.3 Organizacijski pogoji

Ponudnik storitve EKC in posamezen Uporabnik storitve EKC skleneta Dogovor o sodelovanju (v nadaljnjem besedilu: Dogovor) za namene določitve medsebojnih obveznosti, postopkov medsebojnega obveščanja, dogovorjene stopnje razpoložljivosti in odzivnosti, predvsem pa določita, kateri podatki se izmenjujejo v postopkih reševanja težav strank.

Pričujoči Splošni pogoji so priloga Dogovora in kot takšni njegov sestavni del, razen če ni v Dogovoru navedeno, da v določenem delu Splošni pogoji ne veljajo ali če kakšen del stranki Dogovora dogovorita drugače.

Priloga Dogovora so tudi Tehnične specifikacije in skrbniki (v nadaljnjem besedilu: Tehnične specifikacije).

Posamezen Uporabnik storitve EKC in Ponudnik storitve EKC lahko skleneta dogovor o uporabi informacijske rešitve Platforme Omnichannel za zagotavljanje podpore storitve. V tem primeru Ponudnik storitve EKC v uporabo Uporabniku storitve EKC preda le platformo ne prevzema pa zagotavljanja podpore za njihovo storitev. V zvezi s tem se uporabijo posebni Splošni pogoji.

Ponudnik storitve EKC ima objavljene svoje Splošne pogoje na spletni strani Portala nacionalno interoperabilnostnega okvirja.

3 Tehnološki vidik

3.1 Aplikaciji, ki skupaj zagotavljata spremljanje podpore

Proces izmenjave zahtevkov in informacij poteka preko spletne aplikacije Maximo in platforme Omnichannel za komunikacijo s strankami preko novih komunikacijskih poti, kot so SMS, WhatsApp, Viber...

Za delovanje Platforme Omnichannel in aplikacije Maximo je bila pripravljena ocena učinkov na varstvo podatkov, v kateri sta oba sistema bolj podrobno opisana in obravnavana z vidika določil o varstvu osebnih podatkov.

Za spremembo namena obdelave osebnih podatkov v platformi Omnichannel se morata pisno strinjati obe odgovorni osebi za izvajanje storitve.

3.1.1 Platforma Omnichannel

Platforma Omnichannel je celostna platforma, namenjena komunikaciji med stranko in EKC. V praksi to pomeni, da stranke z EKC lahko najprej komunicirajo preko enega kanala, kasneje pa preko drugega. Agent lahko vsakokrat preveri zgodovino interakcij ne glede na komunikacijski kanal, kar mu omogoča, da s stranko komunicira efektivno, dolgoročno, predvsem pa personalizirano. Če stranka nadaljuje prejšnji pogovor preko drugega kanala, lahko agent enostavno združi ta pogovora v enega. Trenutno so podprti naslednji komunikacijski kanali:

- Klic
- E-mail
- Viber
- WhatsApp
- SMS
- LiveChat (Chat Bot).

OPOMBA:

Posamezni komunikacijski kanali se uporabljajo v skladu s pravili posameznega ponudnika komunikacijskega kanala, pri čemer lahko posameznik kadarkoli zamenja komunikacijski kanal.

3.1.2 Aplikacija Maximo

Javni uslužbenci za prijavo svojih težav lahko uporabljajo Center za samopomoč znotraj aplikacije Maximo ter nato spremljajo njihovo reševanje Tako ima ta kanal poseben status, saj je na voljo le zaposlenim v državnih organih.

Prav tako je Maximo namenjena komunikaciji med EKC in drugimi ravnmi podpore. To pomeni, da zahtevke, ki jih svetovalci sami na prvi ravni podpore ne uspejo rešiti, posredujejo preko aplikacije Maximo v reševanje na drugo raven podpore.

4 Obravnava incidentov in tehničnih težav storitve

Če pride do napak pri delovanju storitve, za katero EKC nudi prvo raven podpore, vodja notranje organizacijske enote, v okviru katere deluje EKC, ali operativni vodja EKC in skrbnik storitve izmenjujejo in usklajujejo ravnanje vseh vpletenih preko telefona ali elektronske pošte, navedene v Tehničnih specifikacijah. Operativni vodja EKC oceni nujnost reševanja in prične z obveščanjem glede na nujnost oziroma vse potrebno, da se reševanje prične.

Če skrbnik storitve zazna incidente in tehnične težave, mora s tem seznaniti vse skrbnike, ki so s konkretnim incidentom ali tehničnimi težavami povezani vključno z operativnim vodjem EKC.

Če pride do napak pri delovanju EKC operativni vodja EKC oziroma vodja notranje organizacijske enote, v okviru katere deluje EKC, izmenjujeta in usklajujeta ravnanje vseh vpletenih preko telefona ali elektronske pošte, ki je dogovorjena s skrbniki aplikacije Maximo in platforme Omnichannel.

5 Razpoložljivost storitve EKC

Storitve EKC se za stranke zagotavljajo vsak delovni dan od 8:00 do 22:00 ure.

5.1 Višja sila

Ponudnik storitve EKC in skrbniki storitev niso odgovorni za zagotavljanje podpore pri uporabi storitev v primeru nastopa višje sile ali drugih razlogov, na katere nimajo vpliva ter jih niso mogli predvideti ali preprečiti. V teh primerih so se dolžni takoj medsebojno obvestiti.

6 Poslovni vidik

Stroški zagotavljanja storitve EKC se krijejo iz sredstev Ministrstva za digitalno preobrazbo.

7 Obdelava osebnih podatkov

7.1 Splošno

Ponudnik storitve EKC in Uporabnik storitve EKC sta zavezana k spoštovanju predpisov o varstvu osebnih podatkov in to tako Zakona o varstvu osebnih podatkih (Uradni list RS, št. 163/22, v nadaljnjem besedilu: ZVOP-2), kot tudi Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (v nadaljnjem besedilu: Splošna uredba o varstvu podatkov). S pričujočimi Splošnimi pogoji so določena razmerja med njima in odgovornosti, katerih posebnosti izhajajo iz procesa podpore, prav tako pa so določene tudi dolžnosti Ponudnika storitve EKC in Uporabnika storitve EKC z namenom izpolnjevanja obveznosti in odgovornosti, katerih posebnosti izhajajo iz obdelave osebnih podatkov pri zagotavljanju in uporabi storitve podpore EKC. Ponudnik storitve EKC in Uporabnik storitve EKC neodvisno od teh Splošnih pogojev lahko v Dogovoru ali Tehničnih specifikacijah tudi drugače dogovorita svoja razmerja in odgovornosti, v tem primeru velja posebni dogovor.

Obdelava osebnih podatkov, kot je opredeljena v tem dokumentu, je zapisana splošno za vso obdelavo osebnih podatkov v okviru zagotavljanja storitve EKC, razen če ni drugačna obdelava posebej opredeljena, za katero od tehničnih rešitev.

7.2 Pravna podlaga

Pravna podlaga za obdelavo osebnih podatkov strank pri nudenju in uporabi storitve EKC:

- za obdelavo podatkov javnih uslužbencev, zaposlenih v državni upravi: (b) alineja prvega odstavka 6. člena Splošne uredbe o varstvu podatkov, in sicer za namene zagotavljanja storitve EKC pri opravljanju nalog, ki izhajajo iz delovnega razmerja z organom državne uprave – Uporabnikom storitve EKC.

Zaposleni, ki sklene delovno razmerje pri organu državne uprave, ki je tudi Uporabnik storitve EKC, mora za svoje delo pridobiti določena sredstva in kasneje ta sredstva tudi uporabljati. Za namene določitve in dodelitve teh delovnih sredstev se v okviru storitve EKC obdelujejo podatki, ki se nanašajo na zaposlenega, prav tako pa se v okviru storitve EKC obdelujejo podatki, ki so potrebni za zagotovitev podpore delu tega zaposlenega. Zaposleni nima možnosti izbire subjekta, ki bi zagotovil tako delovna sredstva, kot pomoč pri njihovi uporabi, saj je s svojo pogodbo o zaposlitvi vezan na storitve, za katere se je dogovoril njegov delodajalec. Vrsta in obseg teh podatkov je odvisna od posamezne storitve in jo določita Ponudnik storitve EKC in Uporabnik storitve EKC v okviru Dogovora ali Tehničnih specifikacij;

- za obdelavo podatkov ostalih strank: (a) alineja prvega odstavka 6. člena Splošne uredbe o varstvu podatkov, v povezavi s tretjim odstavkom 6. člena ZVOP-2, torej privolitev posameznika za obdelavo osebnih podatkov. Privolitev ni določena v zakonu, saj pri obdelavi podatkov v konkretnem primeru ne gre za izvrševanje zakonskih pristojnosti – oblastvenih dejanj. Privolitev poda: stranka – s posredovanjem podatkov, za katere meni, da so potrebni za pridobitev pomoči, za katero zaprosi, oziroma s posredovanjem podatkov, za katere mu zaposleni na EKC sporočijo, da jih rabijo za zagotovitev zahtevane pomoči. Vrsta in obseg teh podatkov je odvisna od posamezne storitve EKC in jo določita Ponudnik storitve EKC in Uporabnik storitve v okviru Dogovora ali Tehničnih specifikacij;

7.3 Vloga Ponudnika storitve EKC in Uporabnikov storitve EKC z vidika Splošne uredbe o varstvu podatkov

Ponudnik storitve EKC in Uporabnik storitve EKC sta v okviru obdelave podatkov pri zagotavljanju podpore skupna upravljavca, kot slednje določa 26. člen Splošne uredbe o varstvu podatkov (v

nadaljnjem besedilu: skupna upravljavca), saj Ponudnik storitve EKC določa sredstva obdelave osebnih podatkov, ker zagotavlja delovanje podpore EKC, Uporabnik storitve EKC pa določa sredstva obdelave v delu, ko se odloči, da bo za zagotavljanje podpore strankam uporabil storitve EKC, ter namene obdelave teh podatkov.

7.4 Namen in način

Namen obdelave osebnih podatkov v okviru zagotavljanja podpore EKC je:

- pomoč in reševanje težav strank ter morebitno posredovanje le-teh na druge ravni podpore.

7.5 Način pridobitve podatkov

Podatki se pridobivajo preko različnih komunikacijskih kanalov, ki so na razpolago strankam za uporabo storitve EKC s strani posameznega končnega uporabnika ali osebe, ki je zahtevala pomoč ali rešitev težave za zaposlenega v organu državne uprave.

Pred začetkom zagotavljanja storitve EKC Ponudnik storitve EKC in Uporabnik storitve EKC poleg vrste in obsega osebnih podatkov določita tudi način pridobitve osebnih podatkov, katerih obdelava je potrebna za zagotavljanje določene storitve EKC.

7.6 Obseg

V okviru zagotavljanja storitve EKC se obdelujejo podatki strank. Obseg določita Ponudnik storitve EKC in Uporabnik storitve EKC v Tehničnih specifikacijah za posamezno storitev EKC.

7.7 Vrste osebnih podatkov, ki so lahko predmet obdelave

Pred začetkom zagotavljanja vsake od storitev EKC Ponudnik storitev EKC in Uporabnik storitev EKC natančno določita vrste osebnih podatkov, katerih obdelava je potrebna za zagotavljanje določene storitve EKC, se pa v okviru uporabe platforme Omnichannel lahko obdelujejo naslednji podatki ostalih strank:

- Elektronski naslov stranke
- Telefonska številka stranke
- Drugi osebni podatki, ki se določijo v tehničnih specifikacijah za vsako storitev posebej.

Prav tako pa se obdelujejo tudi osebni podatki javnih uslužbencev, zaposlenih v državni upravi:

- Ime in priimek stranke
- Elektronski naslov stranke
- Telefonska številka stranke
- Delodajalec stranke
- Drugi osebni podatki, ki se določijo v tehničnih specifikacijah za vsako storitev posebej.

V okviru uporabe aplikacije Maximo pa se lahko v okviru drugih osebnih podatkov obdelujejo tudi naslednji podatki javnih uslužbencev, zaposlenih v državni upravi:

- Ime in priimek stranke
- Naslov bivališča stranke
- Elektronski naslov stranke
- Telefonska številka stranke

- Davčna številka stranke
- EMŠO stranke
- Delodajalec stranke

Ob tem je treba poudariti, da lahko »Drugi osebni podatki, ki se določijo v tehničnih specifikacijah za vsako storitev posebej« vsebujejo tudi druge podatke strank, ki jih slednje navedejo brez predhodnega dogovora med Ponudnikom storitve EKC in Uporabnikom storitve EKC. Na ta nabor Upravljavec storitve EKC nima vpliva.

Revizijska sled za določeno poizvedbo pri zagotavljanju delovanja platforme Omnichannel vključuje naslednje podatke:

1. za namene identifikacije uporabnika – uporabniško ime in ID uporabnika, ki je izvedel dejanje.
2. Časovni žig – datum in čas izvedbe dejanja.
3. Vrsta dejanja – specifično dejanje: dostop, sprememba ali brisanje podatkov.
4. Dostopani podatek – navedba podatka, ki je bil dostopan, če je bilo to pomembno za izvedbo dejanja.
5. Izvorni IP naslov – IP naslov EKC svetovalca/nadzornika.
6. Status uspešnosti – informacija o tem, ali je bilo dejanje uspešno ali neuspešno.

Beleženje uporabniških aktivnosti v revizijskih sledeh vključuje:

• Uspešne in neuspešne poskuse prijave.

• Spremembe podatkov, vključno s posodobitvami in brisanjem.

• Administrativna dejanja nadzornikov.

• Druge pomembne interakcije nadzornikov s sistemom, ki bi lahko vplivale na celovitost ali varnost podatkov.

Revizijska sled za določeno poizvedbo pri zagotavljanju delovanja Maximo vključuje naslednje podatke:

- Sprememba statusov

- Sprememba lastništva

- Spremljanje dodajanje zapisov v delovnem in komunikacijskem dnevniku

- Zgodovina delovnega toka

- Sledenje prijave

- Sprememba statusa uporabnika (aktiven/neaktiven)

7.8 Rok hrambe osebnih podatkov in anonimizacija

7.8.1 Roki hrambe podatkov

Roki hrambe podatkov so določeni:

- če se podatki nanašajo na zaposlenega v državni upravi, je rok hrambe 5 let po prenehanju delovnega razmerja v organu državne uprave, pri čemer se rok 5 let preverja večkrat mesečno,
- če se podatki nanašajo na stranko, je rok hrambe 5 let po oddaji posameznega zahtevka s strani stranke, pri čemer se rok 5 let preverja večkrat mesečno.

Tehnično se rok hrambe zagotavlja z izvedbo anonimizacije podatkov po naslednjih kriterijih:

1. Če se podatki nanašajo na javnega uslužbenca, se v Maximo aplikaciji večkrat mesečno preveri, ali je stranka v statusu »INACTIVE« več kot 5 let ali ne.
    a. Če stranka NI v statusu »INACTIVE« več kot 5 let, se proces zaključi brez anonimizacije.
    b. Če JE stranka v statusu »INACTIVE« več kot 5 let, se sproži anonimizacija in proces se zaključi.
2. Če se podatki nanašajo na ostale stranke, se preveri, ali je prvi datum zahtevka v Maximo aplikaciji »REPORTDATE«, na katerega se navezujejo osebni podatki, starejši od 5 let.
    a. Če zahtevki NISO starejši od 5 let, se proces zaključi brez anonimizacije.
    b. Če SO zahtevki starejši od 5 let, se sproži anonimizacija in proces se zaključi.

Osebni podatki v Omnichannel se shranjujejo eno leto.

Osebni podatki v revizijskih sledeh se za Omnichannel shranjujejo eno leto.
Dnevnik revizijskih sledi prijav in odjav uporabnikov v sistemu Maximo se hrani do 6 mesecev.

7.8.2 Anonimizacija

Anonimizacija v aplikaciji Maximo se izvede na način, da se anonimizira podatke, ki bi lahko razkrili posameznika, obdrži pa se tehnične podatke o zapisih, ki so potrebni za upravljanje EKC in sicer: številka zapisa, čas zapisa, čas zaključka zapisa, število vseh zapisov, stroški dela.

V aplikaciji Maximo se podatki anonimizirajo tako, da se posamezen podatek nadomesti s splošnim izrazom, ki je enak vsem istim vrstam podatka, in sicer:

a) s splošnim izrazom se nadomestijo podatki o prijavitelju, in sicer:

- ime, priimek
- naslov elektronske pošte
- telefon
- podrobnosti

b) s splošnim izrazom se v modulu Storitveni zahtevki nadomestijo podatki, in sicer:

- ime, priimek obravnavane osebe
- naslov elektronske pošte obravnavane osebe
- telefon obravnavane osebe
- Komunikacijskega dnevnika: Ustvaril, Za

c) s splošnim izrazom se v modulih Spremembe, Incidenti, Delovni nalogi in Aktivnosti nadomestijo podatki , in sicer:

- ime, priimek obravnavane osebe
- naslov elektronske pošte obravnavane osebe
- telefon obravnavane osebe
- komunikacijskega dnevnika: Ustvaril, Za
- dejavnosti: Delavec.

7.9 Uporabnik storitve EKC

Osebni podatki, ki se obdelujejo v okviru storitve podpore EKC, se lahko posredujejo na druge ravni podpore, in sicer kot to določita Ponudnik storitve EKC in Uporabnik storitve EKC v Dogovoru ali Tehničnih specifikacijah.

Edini uporabniki podatkov, zbranih v procesu podpore strankam, so osebe, ki konkretno zagotavljajo izvajanje podpore strankam in podatke uporabljajo izključno za namen reševanja težav strank.

Vpogled v revizijske sledi Omnichannel in Maximo ima samo administrator sistema, uporabniki revizijskih sledi so le osebe, ki so do njih upravičene v skladu z veljavnimi predpisi.

7.10 Prenos osebnih podatkov v tretje države ali mednarodne organizacije

Podatki se ne prenašajo v tretje države ali mednarodne organizacije.

7.11 Uveljavljanje in izvrševanje pravic posameznikov iz členov 15 do 22 Splošne uredbe

Pravice posamezniki lahko uveljavljajo neposredno pri Upravljavcu EKC ali pri Uporabniku EKC.

7.11.1 Način izvrševanja pravic

Ko Upravljavec EKC ali Uporabnik EKC prejmeta zahtevo posameznika za uveljavitev katere od pravic, prejemnik zahteve ugotovi, če se zahteva nanaša na podatke, ki so v skupnem upravljanju, kot je to opisano v 7.11.2 podpoglavju, in:

1. če ugotovi, da se zahteva ne nanaša na podatke, ki sodijo v skupno upravljanje (npr. zahteva se nanaša na podatke, ki so pri eni od strank Dogovora), prejemnik o tem obvesti posameznika in v skladu z ZUP posreduje zahtevo pristojnemu upravljavcu;
2. če ugotovi, da podatki sodijo v skupno upravljanje in je prejemnik pristojen za izvršitev zahteve posameznika, je prejemnik odgovoren za pripravo takojšnjega odziva v skladu z veljavnimi predpisi v obsegu iz 7.12.2 poglavja;
3. če ugotovi, da podatki sodijo v skupno upravljanje in ugotovi, da ima pristojnost za izvršitev zahteve posameznika glede na obseg iz 7.12.2 poglavja drugi skupni upravljavec, zahtevo nemudoma odstopi v skladu z ZUP drugemu pristojnemu skupnemu upravljavcu. O razlogih za odstop in o tem, komu je zahtevo odstopil, pa obvesti posameznika;

- skupni upravljavec, ki mu je bila zahteva odstopljena, mora nemudoma preveriti, če se z odstopom strinja in o tem obvestiti tako prvega prejemnika zahteve, kot tudi posameznika, ki zahteva uveljavitev pravice. Če se z odstopom ne strinja, pa mora nemudoma sklicati sestanek obeh skupnih upravljavcev, katerega namen je ugotoviti način rešitve zahteve za uveljavitev pravic posameznika, ali zagotoviti kakšen drugačen način rešitve spora o pristojnosti;
- če ugotovi, da podatki sodijo v skupno upravljanje in ne more ugotoviti, kdo ima pristojnost za izvršitev zahteve posameznika glede na obseg iz 7.12.2 poglavja ali ima kakršnekoli druge težave, o tem nemudoma obvesti drugega skupnega upravljavca in skupaj pristopita k rešitvi zahteve;
- končni odgovor stranki pripravi skupni upravljavec, ki je pristojen za izvršitev zahteve, če se stranki ne dogovorita drugače.

Skupna upravljavca si nudita vso potrebno pomoč za obravnavo zahtevkov za uveljavljanje pravic, če kateri od skupnih upravljavcev prosi za to.

Končni odgovor mora biti posamezniku posredovan brez nepotrebnega odlašanja, najkasneje pa v roku enega meseca po prejemu zahteve s strani posameznika.

7.11.2 Obseg uveljavljanja pravic

a. pravica do informiranja o obdelavi osebnih podatkov – pravica do informiranja o obdelavi osebnih podatkov se zagotavlja na način, da je končni uporabnik seznanjen z obdelavo podatkov pred oddajo zahtevka. Pravico v celoti zagotavlja Upravljavec EKC z odzivom na posamezno zahtevo končnega uporabnika;
b. pravica dostopa posameznika, na katerega se nanašajo osebni podatki – avtomatiziran dostop do podatkov se zagotavlja končnim uporabnikom v obsegu, v katerem končni uporabnik uporablja komunikacijske kanale, do katerih dostopa, sicer pa se avtomatiziran dostop do podatkov ne zagotavlja. Pravico v celoti zagotavlja Upravljavec EKC z odzivom na posamezno zahtevo končnega posameznika;
c. pravica do popravka – pravico se zagotavlja s preklicem posameznega zahtevka in ponovno oddajo zahtevka. Pravico v celoti zagotavlja Upravljavec EKC z odzivom na posamezno zahtevo končnega posameznika;
d. pravica do izbrisa (“pravica do pozabe”) – pravico se zagotavlja z anonimizacijo zahtevka. Pravico v celoti zagotavlja Upravljavec EKC z odzivom na posamezno zahtevo končnega posameznika;
e. pravica do omejitve obdelave – za uveljavljanje pravice je pristojen Upravljavec EKC, in sicer z odzivom na posamezno zahtevo posameznika;
f. obveznost obveščanja v zvezi s popravkom ali izbrisom osebnih podatkov ali omejitvijo obdelave – za uveljavljanje pravice je pristojen tisti skupni upravljavec, ki je pravico zagotovil z odzivom na posamezno zahtevo posameznika;
g. pravica do ugovora – za uveljavljanje pravice je pristojen Upravljavec EKC, in sicer z odzivom na posamezno zahtevo posameznika;
h. pravica, da za posameznika, na katerega se nanašajo osebni podatki, ne velja odločitev, ki temelji zgolj na avtomatizirani obdelavi, vključno z oblikovanjem profilov – v okviru EKC se ne sprejema odločitev, ki temeljijo na avtomatizirani obdelavi podatkov, za uveljavljanje pravice pa je pristojen Upravljavec EKC.

Za uveljavljanje vseh pravic posameznika, ki se nanašajo na revizijske sledi, je v obsegu, v katerem posameznik lahko uveljavlja svoje pravice, odgovoren Upravljavec EKC, pri čemer gre za obseg:

a. pravica do informiranja o obdelavi osebnih podatkov (ne glede na način pridobitve podatkov) – v celoti;
b. pravica dostopa posameznika, na katerega se nanašajo osebni podatki – v celoti, avtomatiziran dostop do podatkov se ne zagotavlja;
c. pravica do popravka – popravek podatkov v revizijskih sledeh ni mogoč zaradi namena obstoja revizijske sledi;
d. pravico do izbrisa (“pravico do pozabe”) – izbris podatkov v revizijskih sledeh ni mogoč zaradi namena obstoja revizijske sledi;
e. pravico do omejitve obdelave – v celoti;
f. obveznost obveščanja v zvezi s popravkom ali izbrisom osebnih podatkov ali omejitvijo obdelave – v celoti;

g. pravica do ugovora – v celoti, pri čemer se poudari, da posameznika ni mogoče prisiliti, da bi predal svoje podatke v obdelavo;

Ponudnik storitve EKC vse pravice, ki se nanašajo na revizijske sledi, zagotavlja z odzivom na posamezno zahtevo končnega posameznika.

7.11.3 Način uveljavljanja zahtev posameznikov glede zagotavljanja izvrševanja pravic posameznikov

Posameznik lahko zahtevo za uveljavitev njegovih pravic posameznikov, kot posameznike določa Splošna uredba o varstvu podatkov (od 15. do 22. člena Splošne uredbe o varstvu podatkov), vloži osebno na zapisnik ali posreduje v fizični ali elektronski obliki, in sicer na naslova:

1. Ponudnika storitve EKC, MDP: gp.mdp@gov.si in
2. Uporabnika storitve EKC, pri čemer je naslov Uporabnika storitve EKC razviden iz vsakokratnih Dogovorih ali Tehničnih specifikacij.

Pravice se izvršijo na način in v obsegu, ki je določen v prejšnjem poglavju.

Ponudnik storitve EKC in Uporabniki storitve EKC pritožbe posameznika obravnavajo v skladu z ZUP. Pristojni organ za odločanje o pritožbi je:

Informacijski pooblaščenec, Dunajska cesta 22, 1000 Ljubljana

e-pošta: gp.ip@ip-rs.si

Ponudnik storitve EKC in Uporabniki storitve EKC imajo določeno vsak svojo pooblaščeno osebo za varstvo podatkov. Kontaktni podatki pooblaščenih oseb so navedeni v Tehničnih specifikacijah.

7.12 Način seznanjanja posameznikov z informacijami glede obdelave podatkov

Ponudnik in Uporabniki storitve EKC na svojih spletnih straneh objavijo obvestila posameznikom o obdelavi osebnih podatkov v skladu s 13. in 14. (v delu, v katerem se nanaša na podatke v revizijskih sledeh) členom Splošne uredbe o varstvu podatkov, lahko tudi v okviru Splošnih pogojev uporabe storitve EKC.

Če Ponudnik storitve EKC ali Uporabniki storitve EKC ocenijo, da bi se moralo katero od obvestil posameznikom dopolniti, o tem obvestijo drug drugega.

7.13 Varnost osebnih podatkov (tehnični in organizacijski ukrepi)

7.13.1 SPLOŠNO – odgovornost

EKC kot Ponudnik storitve EKC zagotavlja tehnične in organizacijske ukrepe za varstvo osebnih podatkov v informacijskem sistemu.

7.13.2 UKREPI ZA ANOMINIZIRANJE OSEBNIH PODATKOV

Podatki se v apilkaciji Maximo anonimizirajo v skladu z določili poglavja 7.8.2. Anonimizacija.

V aplikaciji Omnichannel se anonimizacija ne uporablja, ker se vsi podatki brišejo po preteku enega leta.

7.13.3 UKREPI ZA ZAGOTAVLJANJE STALNE ZAUPNOSTI, CELOVITOSTI, RAZPOLOŽLJIVOSTI IN ODPORNOSTI SISTEMOV IN STORITEV ZA OBDELAVO

Do podatkov iz zapisov v aplikaciji za spremljanje podpore strankam IBM Control Desk – Maximo lahko dostopajo samo aktivni uporabniki Maximo aplikacije, ki so jim dodane pravice dostopa, pri čemer je dostop varovan s avtentikacijo preko Active Directory (AD) in dostop do podatkov zunaj HKOMa še s avtentikacijo preko VPN protokola.

Sistemska podpora izvaja nadzor nad spremembami v podatkovnih bazah z Oracle DataVault tehniko in hrani aplikativne loge za potrebe morebitnih revizijskih postopkov.

Dostop do aplikacije Omnichannel je omejen na svetovalce EKC, pri čemer je dostop varovan z dvostopenjsko avtentikacijo (uporabniškim imenom in geslom ter sms sporočilom).

Ukrepi za zagotavljanje stalne zaupnosti, celovitosti, razpoložljivosti in odpornosti sistemov in storitev za obdelavo za Omnichannel vključuje naslednje vidike:

1. **Fizična in okoljska varnost**: Uporabljeni so postopki in kontrole za preprečevanje nepooblaščenega fizičnega dostopa in za zmanjšanje tveganja za poškodbe ali motnje informacijskih sistemov. Informacijsko procesna središča so zavarovana s fizičnimi pregradami, nadzor dostopa pa je urejen z uporabo varnostnih oseb, ključavnic in video nadzora.
2. **Kriptografska zaščita**: Za varovanje zaupnosti, celovitosti in pristnosti osebnih podatkov in drugih občutljivih informacij so uporabljeni sodobni kriptografski algoritmi. Ti vključujejo šifriranje prenosa podatkov (HTTPS, VPN) in šifriranje podatkov v mirovanju z algoritmom AES-256.
3. **Varovanje dostopa**: Pristop temelji na načelih najmanjših potrebnih pravic in potrebe po poznavanju. Dostop je omejen in se upravlja s postopki odobritve. Dostop do informacijskih sistemov je zaščiten z dvofaktorsko avtentikacijo (2FA).
4. **Upravljanje operativne varnosti**: Procesi za spremembe, varnostne kontrole in testiranja zagotavljajo zaščito produkcijskega okolja. Ločevanje razvojnega, testnega in produkcijskega okolja zmanjšuje tveganje nepooblaščenih dostopov ali sprememb produkcijskega okolja.
5. **Nenehno spremljanje in beleženje**: Sistem beleženja in spremljanja omogoča evidentiranje uporabniških dejavnosti, dogodkov in varnostnih izjem. Beleženje je zaščiteno pred nedovoljenimi posegi in omogoča sledljivost vseh interakcij v informacijskih sistemih.
6. **Obnovitveni načrti in odpornost**: Načrti za obnovo in neprekinjeno poslovanje zagotavljajo, da so sistemi in podatki zaščiteni tudi v primeru motenj ali izrednih razmer. Periodična testiranja in pregledi zagotavljajo veljavnost teh načrtov.

Ti ukrepi omogočajo, da se vzdržuje visoko raven varnosti in odpornosti sistemov za obdelavo podatkov, kar zagotavlja stalno zaščito in dostopnost informacij.

7.13.4 UKREPI ZA ZAGOTAVLJANJE ZMOŽNOSTI ZA PRAVOČASNO POVRNITEV RAZPOLOŽLJIVOSTI IN DOSTOP DO OSEBNIH PODATKOV V PRIMERU FIZIČNEGA ALI TEHNIČNEGA INCIDENTA

Maximo aplikacija je nameščena na večjem številu instanc. Če se pojavijo težave na eni instanci, se promet preusmeri na druge, delujoče.

V primeru izpada delovanja na primarni lokaciji sistem Maximo aplikacije vzpostavi delujoče stanje na rezervni lokaciji.

Ob morebitnem izpadu sistema se za namene varstva osebnih podatkov zagotavlja delovanje Maximo na rezervnih lokacijah. Za Omnichannel pa je vzpostavljen obnovitveni načrt, kot je opisano v 6. točki podpoglavja 7.13.3.

Informacijski sistem deluje na primarni lokaciji ter dodatno na disaster-recovery lokaciji NIC Maribor, kjer je druga veja baze podatkov – Maximo torej zagotavlja asinhrono replikacijo. Realen zamik asinhronega osveževanja je tipično nekaj sekund. Rezervna lokacija je predmet vsakoletnega preklopa in enodnevnega delovanja iz rezervne lokacije.

Ukrepi, ki se jih uporablja za zagotovitev pravočasne povrnitve razpoložljivosti in dostopa do osebnih podatkov v primeru fizičnega ali tehničnega incidenta, za storitev Omnichannel vključujejo naslednje:

1. **Strategija varnostnega kopiranja in obnavljanja**: redno izvajanje varnostnega kopiranja podatkov, programske opreme in sistemskih slik. Varnostne kopije so zaščitene z ustreznimi kontrolnimi mehanizmi, kot so nadzor dostopa in kriptografska zaščita. Testiranje obnovitve se izvaja vsaj enkrat letno, da se preveri integriteta varnostnih kopij in trajanje procesa obnove.
2. **Visoka razpoložljivost in redundanca**: implementirane so tehnike redundance in visoke razpoložljivosti informacijskih procesnih središč, ki zagotavljajo dostopnost storitev tudi v primeru motenj.
3. **Načrti za neprekinjeno poslovanje**: Za zagotavljanje varnosti podatkov v času nepredvidenih dogodkov ali kriz so vzpostavljeni in redno testirani načrti za neprekinjeno poslovanje. Ti načrti omogočajo vzdrževanje ključnih funkcionalnosti ter hitro obnovitev sistemov in podatkov po incidentih.

   V primeru izpada platforme Omnichannel se na telefonu EKC vklopi odzivnik, s katerim se stranke obvesti o nedelovanju storitve. V primeru internetnega izpada (HKOM) se vzpostavi povezava do platforme preko zunanjega interneta ali telefona.

Zgoraj navedeni ukrepi omogočajo, da se v primeru incidenta hitro povrne dostopnost do podatkov in zagotovi nemoteno nadaljevanje storitev.

7.13.5 UKREPI ZA POSTOPKE REDNEGA TESTIRANJA, OCENJEVANJA IN VREDNOTENJA UČINKOVITOSTI TEHNIČNIH IN ORGANIZACIJSKIH UKREPOV ZA ZAGOTAVLJANJE VARNOSTI OBDELAVE

Maximo je razvit na najsodobnejši IBMovi infrastrukturi, kot so IBM WebSphere (aplikacijski in spletni strežnik), IBM DB2 (podatkovni strežnik). S tem so zagotovljeni najsodobnejši varnostni mehanizmi. IBM redno na tedenskem nivoju obvešča o potencialno varnostnih problemih in jih vključuje v posodobitve.

Delovanje Maximo je nadzorovano preko nadzornega sistema Icinga, ki omogoča spremljanje delovanja same aplikacije, kakor tudi povezave z drugimi sistemi.

Za Omnichannel se izvaja postopke rednega testiranja, ocenjevanja in vrednotenja učinkovitosti tehničnih in organizacijskih ukrepov za zagotavljanje varnosti obdelave podatkov prek naslednjih pristopov:

1. **Redna testiranja varnostnih kontrol**: izvaja se redna varnostna testiranja sistemov, vključno s penetracijskimi testi in avtomatiziranimi pregledi ranljivosti. To pomaga identificirati in odpraviti morebitne varnostne ranljivosti, še preden postanejo tveganje za obdelavo podatkov.
2. **Nadzor in spremljanje**: uporablja se sisteme za nadzor in spremljanje, ki omogočajo neprekinjeno opazovanje varnostnih dogodkov in odzivanje na morebitne incidente. S tem se zagotavlja, da varnostni ukrepi delujejo pravilno in da so tveganja obvladovana sproti.
3. **Periodična ocena učinkovitosti**: Tehnični in organizacijski ukrepi so predmet rednega vrednotenja in prilagajanja, da ostajajo skladni z najnovejšimi varnostnimi standardi in praksami.

To vključuje tudi presoje, s katerimi se ocenjuje učinkovitost obstoječih varnostnih kontrol in postopkov.

4. **Revizije in samoocenjevanja**: redno se izvaja notranje in zunanje revizije, ki omogočajo neodvisno preverjanje skladnosti varnostnih praks. Poleg tega izvajajo samoocenjevanja, da se preveri skladnost s predpisi in učinkovitost tehničnih ter organizacijskih varnostnih ukrepov.

Navedeni ukrepi zagotavljajo, da so tehnični in organizacijski ukrepi za varnost obdelave podatkov učinkoviti in skladni z regulativnimi zahtevami ter najboljšimi praksami v industriji.

7.13.6 UKREPI ZA PREPREČEVANJE NEPOOBLAŠČENEGA DOSTOPA DO OSEBNIH PODATKOV

Vzpostavljeni so vsi mehanizmi za avtentikacijo preko AD sistema, uporablja se protokol zaščiten s SSL, spletna povezava je možna samo preko https protokola. Povezave so šifrirane.

Za preprečevanje nepooblaščenega dostopa do osebnih podatkov za Omnichannel se uporablja večslojni pristop varnostnih ukrepov:

1. **Nadzor dostopa**: Dostop do informacijskih sistemov temelji na načelu najmanjših potrebnih pravic in potrebi po poznavanju. Vsi uporabniki imajo samo dostop, ki je posebej odobren glede na njihove vloge in odgovornosti. Za zagotavljanje dodatne varnosti se uporablja dvostopenjska avtentikacija (2FA), ki vključuje dodatne faktorske avtentikacije za dostop do občutljivih sistemov.
2. **Avtentikacija in šifriranje**: Sistem zahteva varne prijavne postopke, ki vključujejo močne geselske zahteve, skladne z najboljšimi praksami, kot jih določa NIST (National Institute of Standards and Technology). Dostop do sistemov je zaščiten s šifriranimi povezavami prek protokolov, kot so HTTPS in VPN .
3. **Ločevanje okolij**: Razvojno, testno in produkcijsko okolje so ločena, kar zmanjšuje tveganje za nepooblaščen dostop do operativnih sistemov in občutljivih podatkov.
4. **Revizijske sledi in spremljanje**: izvaja se redno spremljanje in beleženje vseh dostopov do sistemov, vključno z revizijskimi sledmi, da se zagotovi sledljivost vseh interakcij s podatki. Te revizijske sledi so zaščitene pred posegi in so redno pregledovane za odkrivanje morebitnih varnostnih incidentov.

Ti ukrepi omogočajo, da je dostop do osebnih podatkov omejen in zaščiten, kar zmanjšuje tveganje nepooblaščenih dostopov in zagotavlja varnost občutljivih informacij.

7.13.7 UKREPI ZA VARSTVO PODATKOV MED PRENOSOM

Uporabljajo se mehanizmi za šifriranje podatkov med prenosom iz podatkovnega strežnika k aplikacijskem strežniku in do spletnega strežnika. Povezava od aplikacijskega strežnika in klienta poteka preko HTTPS protokola. Povezava od spletnega strežnika do aplikacijskih strežnikov je zaščitena s TLS/SSL protokolom enako kakor povezava med aplikacijskim strežnikom in Oracle bazo, ki uporablja še svojo dodatno avtentikacijo.

Za Omnichannel se uporablja naslednje ukrepe za varstvo podatkov med prenosom, da se zagotovi njihovo varnost in zaupnost:

1. **Šifriranje prenosa podatkov**: Prenos podatkov poteka prek varnih komunikacijskih protokolov, kot so HTTPS za spletne vmesnike, IPSec VPN za vzpostavitev varnih tunelov in SFTP za varen prenos datotek. Ti protokoli zagotavljajo šifriranje podatkov med prenosom, kar preprečuje nepooblaščeno prestrezanje.

2. **Varnostni protokoli SSL/TLS**: Za zaščito prenosa podatkov na različnih ravneh omrežja se uporabljajo protokoli SSL/TLS. Na primer, protokol SMPP (Short Message Peer-to-Peer) za prenos sporočil je zavarovan s SSL/TLS, kar omogoča varno komunikacijo.

3. **Avtentikacija in nadzor dostopa**: Vsaka povezava, prek katere se prenašajo podatki, zahteva preverjanje pristnosti uporabnikov in nadzor dostopa. S tem se zagotavlja, da do podatkov dostopajo le pooblaščeni uporabniki in sistemi, kar dodatno varuje podatke pred morebitnimi nepooblaščenimi dostopi.

Skupaj ti ukrepi zagotavljajo, da so podatki med prenosom ustrezno zaščiteni in varovani pred nepooblaščenimi dostopi ali prestrezanjem.

7.13.8 UKREPI ZA VARNOST PROGRAMSKE OPREME, KI SE UPORABLJA ZA OBDELAVO OSEBNIH PODATKOV

Pred vsako namestitvijo nove verzije programske opreme se izvede varnostni pregled kode. Nova verzija kode se namesti v produkcijo šele, ko so odpravljene morebitne pomanjkljivosti. Testi se izvedejo avtomatsko po odložitvi nove verzije v SVN repozitorij.

Programska oprema, na kateri se izvaja uporaba Maximo aplikacije, je varovana v skladu s prakso, ki je uveljavljena za strežnike, ki strežejo prometu znotraj HKOM omrežja, in je zaščitena s sistemom virtualizacije, dostop pa je varovan na mrežnem nivoju.

Programska oprema in podatki se dnevno varnostno kopirajo.

Omnichannel platforma je nameščena na oblaku na območju Evropske unije.

Za zagotavljanje varnosti programske opreme, ki se uporablja za obdelavo osebnih podatkov se izvajajo naslednje ukrepe:

1. **Pregled kode**: Pred namestitvijo nove različice programske opreme se izvede varnostni pregled kode, s čimer se odkrijejo in odpravijo morebitne ranljivosti. Programska oprema se namesti v produkcijsko okolje šele, ko so vse ugotovljene napake odpravljene.
2. **Samodejno testiranje**: Po odložitvi nove kode v repozitorij SVN se izvedejo avtomatski testi, ki preverijo varnostne in funkcionalne vidike programske opreme. Ta postopek zagotavlja, da nova programska oprema ne uvaja novih ranljivosti ali napak v produkcijsko okolje.
3. **Ločitev razvojnega in produkcijskega okolja**: Razvoj in integracija potekata v ločenem in zaščitenem okolju, kar zmanjšuje tveganje za nepooblaščene spremembe produkcijskih sistemov. Ta ločitev pomaga tudi pri zmanjševanju varnostnih tveganj med razvojem in uvajanjem novih funkcionalnosti.
4. **Varnostne posodobitve in popravki**: sistemsko programsko opremo se redno posodablja s potrebnimi varnostnimi popravki, kar zagotavlja zaščito pred znanimi ranljivostmi. Ti popravki vključujejo posodobitve operacijskih sistemov, podatkovnih baz in aplikacijskih strežnikov.

Vse navedeno zagotavlja, da je programska oprema za obdelavo osebnih podatkov zanesljiva, varna in zaščitena pred morebitnimi grožnjami ali ranljivostmi.

7.13.9 UKREPI ZA VARNOST PODATKOV V ČASU HRAMBE

Vsi podatki so shranjeni na Oracle bazi, ki skrbi za varnost podatkov.

Razpored hrambe podatkov za storitve Omnichannel se nanaša na podatke, ki se shranjujejo in obdelujejo v imenu MDP času zagotavljanja storitev (podatki stranke). Ukrepi zagotavljajo, da so podatki stranke v času hrambe ustrezno zaščiteni in da se po zaključku obdobja hrambe varno odstranijo, kar zmanjšuje tveganje za nepooblaščen dostop ali uhajanje informacij.

7.13.10 UKREPI ZA VARNOST PROSTOROV, OPREME IN SISTEMSKE PROGRAMSKE OPREME ZA OBDELAVO OSEBNIH PODATKOV

Strežniška oprema, na kateri se nahaja baza podatkov, je nameščena v sistemskih prostorih, do katerih je dostop fizično varovan. Sistemska programska oprema je na mrežnem nivoju zaščitena proti nepooblaščenim dostopom. Sistemska programska oprema se dnevno arhivira.

Sistemska podpora Maximo aplikacije redno izvaja aktivnosti nalaganja varnostnih popravkov na sistemsko programsko opremo (operacijski sistemi, podatkovne baze, aplikacijski strežniki).

Za Omnichannel se za varnost prostorov, opreme in sistemske programske opreme, ki so namenjeni obdelavi osebnih podatkov uporablja naslednje ukrepe:

1. **Fizična in okoljska varnost**: Informacijsko-procesna središča in drugi prostori, ki vsebujejo informacijsko-komunikacijsko tehnologijo (IKT), so zaščiteni s fizičnimi pregradami, kot so varnostne ograje, ključavnice in nadzorovane točke dostopa. Dodatno zaščito zagotavljajo varnostno osebje in video nadzor, ki preprečujeta nepooblaščen fizični dostop.
2. **Dostopne točke**: Točke, kot so območja za dostavo in nakladanje, ki bi lahko omogočile dostop nepooblaščenim osebam, so pod strogim nadzorom ali so fizično ločene od prostorov za obdelavo informacij, da se prepreči nepooblaščen dostop.
3. **Politika čiste mize in zaslona**: Organizacija uporablja politiko čiste mize za fizične dokumente in odstranljive medije ter politiko čistega zaslona za računalniško opremo, s čimer se zmanjša tveganje za nepooblaščeno pridobivanje ali ogled občutljivih informacij.
4. **Redne posodobitve in varnostni popravki**: Sistemska programska oprema se redno posodablja in vzdržuje, vključno z namestitvijo varnostnih popravkov za operacijske sisteme, podatkovne baze in strežniško programsko opremo. Ti popravki zagotavljajo zaščito pred znanimi ranljivostmi in ohranjajo varnost infrastrukture.

Ti ukrepi zagotavljajo, da so prostori, oprema in sistemska programska oprema ustrezno zaščiteni, kar zmanjšuje tveganje za nepooblaščene dostope in fizične varnostne incidente.

7.13.11 UKREPI ZA UPORABO ODDALJENEGA DOSTOPA/DELA OD DOMA

Upravljavec in Uporabnik aplikacije za spremljanje podpore Maximo ima uporabo oddaljenega dostopa urejeno z Navodilom o upravljanju z dostopi do informacijskih storitev Ministrstva za digitalno preobrazbo.

Za oddaljeni dostop za potrebe dela od doma se uporablja službena oprema. Za administracijo sistemov se vzpostavi varovana VPN komunikacijska povezava ali ISL dostop do službenih osebnih računalnikov.

7.13.12 UKREPI ZA SLEDLJIVOST OBDELAVE

Revizijske sledi na Maximo aplikaciji se izvajajo za spremembe na zapisih, kot so (SR,INCIDENT, Varnostne skupine, Uporabniki), na katerih bi se lahko nahajali osebni podatki strank. Revizijske sledi se nahajajo v Maximo aplikaciji.

Revizijske sledi prijav strank v Maximo aplikaciji se nahajajo v logih in se hranijo do 6 mesecev, saj obdelava v okviru storitve EKC ni takšne vrste, d bi jo bilo mogoče šteti med obdelave v skladu s prvim odstavkom 22. člena ZVOP-2. Do njih lahko dostopa samo skrbnik aplikacije.

Za zagotavljanje sledljivosti obdelave podatkov se za Omnichannel uporablja naslednje ukrepe:

1. **Revizijske sledi**: Vsi dostopi in aktivnosti uporabnikov v sistemih, ki obdelujejo osebne podatke, so beleženi v revizijskih sledeh. To vključuje beleženje dejavnosti, kot so dostopi, spremembe podatkov, sistemski dogodki in varnostni incidenti. Revizijske sledi so zaščitene pred posegi in nedovoljenimi spremembami.
2. **Dostop samo za pooblaščeno osebje**: Dostop do revizijskih sledi je omogočen le pooblaščenim administratorjem in operaterjem.
3. **Centralizirano usklajevanje časa**: Ure vseh relevantnih sistemov za obdelavo informacij so sinhronizirane na centralni referenčni vir časa, kar omogoča natančno časovno sledljivost in preglednost vseh dogodkov, povezanih z obdelavo podatkov.
4. **Prilagodljive nastavitve hrambe**: Hramba zapisov o dejavnosti in prometnih logih je prilagojena poslovnim in regulatornim zahtevam.

Ti ukrepi omogočajo natančno sledljivost vseh postopkov obdelave podatkov, kar povečuje preglednost in zagotavlja varnost ter skladnost z zahtevami glede varstva osebnih podatkov.

7.14 Dolžnosti, postopek in način poročanja v primerih kršitev varnosti osebnih podatkov

Če Ponudnik storitve EKC ali Uporabnik storitve EKC na kakršenkoli način ugotovita, da je pri celotnem postopku izvajanja storitve prišlo do kršitve varnosti osebnih podatkov, bo tisti, ki je kršitev ugotovil ali je bil z njo seznanjen, brez nepotrebnega odlašanja obvestil drugega (razen, če je bil s kršitvijo seznanjen s strani drugega).

Ponudnik storitve EKC in Uporabnik storitve EKC vsak sam izpolnita obveznosti skladno z določbami 33. člena Splošne uredbe o varstvu podatkov, in sicer v delu, v katerem se kršitev nanaša na njun del zagotavljanja nalog, in o kršitvi uradno obvestita Informacijskega pooblaščenca brez nepotrebnega odlašanja, najpozneje pa v 72 urah po seznanitvi s kršitvijo. Če se Ponudnik storitve EKC in Uporabnik storitve EKC ne moreta v kratkem času dogovoriti, v katerem delu je prišlo do kršitev, sta skupaj dolžna izpolniti obveznost obveščanja. Če to ni mogoče, je vsak sam dolžan izpolniti obveznost obveščanja, in to ne glede na to, od koga je izvedel za kršitev.

Obvestilo pristojnemu nadzornemu organu o kršitvi varnosti osebnih podatkov mora skladno z določbami 33. člena Splošne uredbe o varstvu podatkov vsebovati:

a. 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;
b. verjetne posledice kršitve varnosti osebnih podatkov;
c. ukrepe, ki naj jih posamezen skupni upravljavec sprejme ali katerih sprejetje predlaga drugemu skupnemu upravljavcu za obravnavanje kršitve varnosti osebnih podatkov, pa tudi, kjer ustrezno, ukrepe za ublažitev morebitnih škodljivih učinkov kršitve.

Smiselno enako velja tudi za obvestilo posamezniku v skladu s 34. členom Splošne uredbe o varstvu podatkov.

7.15 Pristojni nadzorni organ in način komuniciranja z njim

Nadzorni organ je določen v skladu z ZVOP-2 in Zakonom o Informacijskem pooblaščencu (Uradni list RS, št. 113/05 in 51/07 – ZUstS-A), in sicer kot Informacijski pooblaščenec.

Pristojni nadzorni organ za obveščanje:

Informacijski pooblaščenec, Dunajska cesta 22, 1000 Ljubljana

e-pošta: gp.ip@ip-rs.si

Ponudnik storitve EKC in Uporabnik storitve se bosta pred komuniciranjem s pristojnim nadzornim organom obvestila o namenu in času komunikacije s pristojnim nadzornim organom.

7.16 Pooblaščene osebe za varstvo osebnih podatkov in njihovi kontakti

Pooblaščene osebe za varstvo osebnih podatkov Ponudnik storitve EKC in Uporabnik storitve EKC določita v Dogovoru ali Tehničnih specifikacijah.

7.17 Izbris podatkov

Čas in način brisanja je opredeljen v poglavju 7.8. rok hrambe osebnih podatkov in anonimizacija.

8 Način reševanja sporov v zvezi z uporabo storitve EKC

Ponudnik storitve EKC in Uporabnik storitve se vzdržita vsakršnih dejanj, ki nasprotujejo dobrim poslovnim običajem, morebitne spore pa rešujeta sporazumno z medsebojnim dogovarjanjem, sicer je za reševanje sporov pristojno stvarno sodišče v Ljubljani.

9 Skrbniki Dogovora

Skrbnike Dogovora Ponudnik storitve EKC in Uporabnik storitve EKC določita v Dogovoru.

Skrbnika Dogovora se medsebojno redno in pravočasno obveščata o vseh okoliščinah, ki bi lahko vplivale na izvajanje dogovora.

Skrbnika storitve EKC na strani Ponudnika storitve EKC in Uporabnika storitve EKC lahko sama dogovorita morebitne spremembe Tehničnih specifikacij. Spremembe morata potrditi pisno.

10 Veljavnost Splošnih pogojev uporabe storitve EKC

Splošni pogoji začnejo veljati tretji dan po podpisu predstojnika Ministrstva za digitalno preobrazbo.