UrakointiPlus Oy
29.9.2021

Tietoturvakuvaus

Puskee™-yhteistyösovellus

1 Johdanto

Tietoturva ja tietosuoja ovat UrakointiPlus Oy:lle (jäljempänä ”Toimittaja”) ensiarvoisen tärkeitä, ja ne on huomioitu yrityksemme kaikessa toiminnassa. Tässä asiakirjassa kuvataan, miten huolehdimme niistä Puskee™-yhteistyösovelluksessa (jäljempänä ”Sovellus”) sekä teknisesti että organisatorisesti kuten myöskin prosessien tasolla.

Kappaleessa 2 kuvataan tietoturvaa Sovelluksen ja siihen liittyvän palvelun näkökulmasta yleisesti, kattaen myös näihin liittyvät tietosuojanäkökulmat. Kappaleessa 3 esitellään vain henkilötietojen käsittelyyn liittyviä tietoturvaominaisuuksia.

2 Tietoturva

2.1 Tietoturva-arkkitehtuuri

UrakointiPlus Oy toimittaa Puskee™-sovelluksen SaaS-palveluna, joka on rakennettu luotettavalle ja nykyaikaiselle Microsoft Azure -pilvialustalle (jäljempänä Pilvialusta). Microsoft huolehtii osaltaan Pilvialustan tietoturvasta, ja tarjoaa Toimittajalle tietoa alustan turvalliseen käyttöön. Pilvialustan tietoturvaominaisuuksiin voit tutustua täällä: https://docs.microsoft.com/en-us/azure/security/fundamentals/overview

Toimittaja huolehtii ajantasaisesta tietoturvauhkien tunnistuksesta ja torjunnasta Sovelluksen käyttöliittymän ja liiketoimintalogiikan osalta, sekä vastaa siitä, että Sovellus käyttää Pilvialustaa kulloinkin suositeltujen parhaiden tietoturvakäytäntöjen mukaisesti.

Toimittaja vastaa myös siitä, että Sovellus ja Pilvialustan komponentit, joita Sovellus käyttää, on konfiguroitu siten, että ne keräävät oletusarvoisesti vain käyttötarkoituksen kannalta välttämättömiä tietoja, säilyttävät niitä vain tarkoituksenmukaisen ajan, ja noudattavat muiltakin osin tässä dokumentissa esitettyjä tietoturva- ja tietosuojaperiaatteita.

2.2 Pääsynhallinta

Sovelluksen pääsynhallinta toteutetaan henkilökohtaisten käyttäjätunnus-salasana-parien avulla. Kukin käyttäjä rekisteröi käyttäjätunnukseksi toimivan sähköpostiosoitteen, ja määrittää Sovelluksessa käytettävän salasanan. Asiakkaan siihen valtuuttama henkilö myöntää käyttäjilleen oikeuden Sovelluksessa hallitsemiinsa tietoihin, ja vastaa itse siitä, että hän ei myönnä oikeutta asiattomille henkilöille. Toimittaja myöntää vain Asiakkaan valitsemalle henkilölle tällaiset pääkäyttäjäoikeudet Asiakaskohtaisesti. Käyttäjätunnukseen liittyvä data lähetetään Sovelluksesta suojattuna siihen liittyvään rekisteröityyn sähköpostiosoitteeseen. Asiakas voi halutessaan parantaa pääsynhallinnan tietoturvan tasoa ottamalla käyttöön Toimittajan tarjoaman kaksivaiheisen tunnistautumisen.

Ylläpitoyhteydet on rajattu kulloinkin soveltuvin osin tarpeellisiin Sovelluksen tai Pilvialustan osiin, ja tarvittaessa suojattu lisäksi kaksivaiheisella tunnistautumisella. Pääsy Sovelluksen ohjelmakoodiin, konfiguraatioihin ja tietokantaan tarjotaan vain Toimittajan hyväksymien ja

hallinnassa olevien rajapintojen kautta. Tietoturvan kannalta kriittiset Sovelluksen konfiguraatiot, kuten tuotannossa käytettävät salausavaimet, säilytetään aina erillään Sovelluksen ohjelmakoodista, ja pääsy niihin rajataan erityisen perustellun tarpeen mukaisesti.

Sekä Toimittajan että asiakkaan käyttäjien käyttöoikeuksien osalta noudatetaan pienimmän oikeuden periaatetta. Tämän mukaisesti Sovelluksessa on oletusasetuksena, että käyttäjät voivat käsitellä vain itse syöttämiään tietoja, ja pääsevät käsittelemään laajemmin tietoja vain, jos asiakkaan pääkäyttäjä tai muu siihen oikeutettu henkilö on erikseen myöntänyt käyttäjälle laajemman käyttöoikeuden, tai nimenomaisesti jakanut tietyt tiedot hänen kanssaan.

Sovellukseen kirjautumisista kerätään lokia, joka sisältää onnistuneet ja epäonnistuneet kirjautumiset. Lokitiedot kerätään siten, että Sovelluksen käyttö voidaan yhdistää yksittäiseen käyttäjään. Sovelluksen ajanlähteet on synkronoitu luotettavaan ajanlähteeseen siten, että lokitapahtumien kellonajat ovat totuudenmukaisia. Lokitiedot on suojattu valtuuttamattomilta muutoksilta.

Toimittaja huolehtii, että tietojen muutoksista tallentuu historiatietoa, ja sitä voi selata käyttöliittymällä. Toimittaja kerää tietojen katselulokia, joka voidaan asiakkaan pyynnöstä toimittaa asiakkaalle. Tietojen perusteella voidaan esimerkiksi tarvittaessa yksilöidä käyttäjä, joka on tiettynä ajankohtana käsitellyt tiettyä rekisterin tietuetta.

2.3 Sovelluskehityksen tietoturva

Toimittaja vastaa, että tietoturva otetaan huomioon kaikissa sovelluskehityksen vaiheissa. Sovelluksen uudet ominaisuudet määritellään ja suunnitellaan alusta pitäen tietoturvallisiksi. Tärkeissä tietoturva-arkkitehtuurikysymyksissä ja kriittisten toimintojen katselmoinneissa ja tietoturvatestauksessa konsultoidaan tietoturva-alan asiantuntijoita.

Sovelluksen ohjelmakoodia säilytetään suojatussa versionhallintajärjestelmässä, johon on rajattu pääsy vain Sovelluksen kehittäjillä. Kaikista ohjelmakoodin muutoksista jää pysyvä merkintä versionhallintaan. Muutoksia katselmoidaan säännöllisesti mahdollisten teknisten tietoturva-aukkojen tunnistamiseksi ja korjaamiseksi jo ennen kuin ne päätyvät tuotantoon. Kehityksen aikana Sovelluksen uusia ominaisuuksia testataan manuaalisesti ja olemassa olevia ominaisuuksia myös automaattitestein. Testit suoritetaan automaattisesti joka kerta, kun sovelluksen ohjelmakoodia on muutettu.

Sovelluksen testiympäristöt on eristetty tuotantoympäristöistä siten, että Asiakkaan tiedot ja testauksessa käytettävät tiedot eivät pääse sekoittumaan, eivätkä testauksessa mahdollisesti syntyvät kuormituspiikit alenna Asiakkaan kokemaa Sovelluksen suorituskykyä.

Pilvialusta- ja Sovellustason tietoturvapäivitykset asennetaan säännöllisesti. Kriittiset päivitykset asennetaan tarvittaessa ylimääräisessä huoltokatkossa.

2.4 Jatkuvuuden hallinta, valvonta ja seuranta

Jatkuva saatavuus on huomioitu Sovelluksen arkkitehtuurissa muun muassa siten, että kaikki asiakkaan työkuormien suorittamiseen liittyvät komponentit mukautuvat automaattisesti

kuorman vaatimaan resurssitarpeeseen. Teknisiä riippuvuuksia komponenttien välillä vältetään, jolloin yhden komponentin vikaantuminen tai huolto ei estä Sovelluksen muihin komponentteihin liittyvien ominaisuuksien käyttöä. Saatavuuden parantamiseksi Sovelluksen komponentit ja tietokanta voidaan myös Toimittajan harkinnan mukaan siirtää tai hajauttaa fyysisesti eri paikoissa sijaitseviin Pilvialustan konesaleihin esimerkiksi käyttäjämäärien kasvaessa tietyllä maantieteellisellä alueella tai alueellisten häiriöiden takia.

Toimittaja huolehtii siitä, että Sovelluksen toipuminen, huolto ja Sovelluksen käyttämisen varakeinot on ratkaistu siten, että Sovellusta voidaan käyttää sen tarkoitusta vastaavalla tavalla mahdollisimman tehokkaasti myös häiriötilanteissa. Toimittaja pyrkii tekemään Sovelluksen ylläpidon ja huollon toimenpiteet muina aikoina kuin silloin, kun Sovelluksen käyttö on aktiivista. Tietojen tahattoman poistamisen tai häviämisen riski minimoidaan varmuuskopioimalla kaikki tiedot vähintään kerran vuorokaudessa. Toimittajalla on myös dokumentoitu prosessi varmuuskopioinnin ja tietojen palauttamiskyvyn tarkistamiseksi säännöllisesti.

Sovelluksen käytettävyyttä ja Pilvialustan toimivuutta valvotaan ja seurataan valvontaohjelmistoilla 24/7, ja hälytykset eskaloidaan Sovelluksen toiminnasta vastaaville teknisille ylläpitäjille. Jos pääsy tietoihin on teknisen vian takia estynyt, tekniset ylläpitäjät selvittävät vian juurisyyn, ja korjaavat tai kiertävät sen mahdollisimman pian palvelutasovaatimusten mukaisessa määräajassa.

Laajoja poikkeustilanteita varten on dokumentoitu toipumissuunnitelma.

2.5 Henkilöstöturvallisuus

Toimittaja huolehtii, että sen oma ja alihankkijoiden henkilöstö on sitoutunut tietoturvaperiaatteisiin ja toimintatapoihin kouluttamalla, ohjeistamalla sekä salassapitosopimuksilla työtehtävien mukaisesti. Toimittaja edellyttää työntekijöiltään sekä kaikilta alihankkijoiltaan, joille annetaan pääsy Toimittajan tiloihin tai Sovellukseen (esimerkiksi siivoustoimi, huoltohenkilöstö, tallentajat) vaitiolositoumusta. Pilvialustan toimittajan kanssa nämä asiat on sovittu Pilvialustan toimittajan sopimuksen mukaisesti.

Toimittaja huolehtii, että pääsy Sovellukseen, Pilvialustaan tai niiden osiin on vain henkilökohtaisilla tunnuksilla ja tarvittavilla työntekijöillä sekä rajatuilla alihankkijoilla, jotka toimenkuvansa puolesta oikeuksia tarvitsevat. Työ voidaan suorittaa sellaisessa ympäristössä, missä se on työntekijän, työnantajan ja tehtävän työn kannalta tehokkainta ja tarkoituksenmukaisinta. Näin ollen työ voidaan suorittaa myös etätyönä. Tällöinkin kaikkien sekä teknisten että henkilöstöturvallisuuteen liittyvien edellytysten tulee täyttyä. Työt tulee ensisijaisesti suorittaa Toimittajan tarjoamalla laitteella, tai toissijaisesti muutoin varmistaa, että käytetty laite täyttää vastaavat Toimittajan asettamat tietoturvavaatimukset.

Toimittaja huolehtii, että työntekijän työsuhteen päättyessä henkilön käyttöoikeudet ja käyttäjätunnukset poistetaan Sovelluksesta ja Pilvialustasta sekä muut henkilön hallussa olevat Toimittajan omistamat materiaalit otetaan Toimittajan haltuun.

2.6 Toimittajan tilat ja fyysinen turvallisuus

Toimittaja huolehtii, että kiinteistössä, jossa Toimittaja toimii, on asianmukainen kulunvalvonta, hälytys-, lukitus- ja palohälytysjärjestelmät sekä vartiointi. Vierailijat saavat liikkua vain yleisissä tiloissa eikä heitä päästetä työtiloihin. Vierailijat ovat kutsujan valvonnassa. Toimittaja edellyttää olennaisilta osin vastaavia tai muuten riskiä vastaavan turvallisuustason huomioiden asianmukaisia järjestelyitä myös alihankkijan tiloissa.

Muiden tilojen osalta Toimittaja edellyttää, että soveltuvin osin kunkin sen oman tai alihankkijan työntekijän tulee kiinnittää erityistä huomiota laitteen lukitsemiseen, salasanaturvallisuuteen ja siihen, ettei asiattomilla henkilöillä ole näköyhteyttä laitteen näppäimistöön tai näytöllä mahdollisesti näkyviin henkilötietoihin.

2.7 Tietoaineistoturvallisuus

Sovellus säilyttää Asiakkaan tietoja ja henkilötietoja sisältävät asiakirjat digitaalisessa muodossa, asianmukaisesti suojattuna, siten että niihin on pääsy vain henkilöillä, joiden työnkuva sitä edellyttää. Toimittaja huolehtii, että Sovellus ja sen tietokanta sekä sinne tallennetut henkilötiedot ja muut tiedot ovat fyysisesti EU-alueella sijaitsevassa konesalissa ja tietokanta on suojattu. Tiedot tallennetaan salattuna. Kaikki julkisen internetin läpi kulkeva ja Pilvialustan sisäinen tietoliikenne on salattu Sovelluksen käyttämien tietoliikenneprotokollien mukaisesti.

2.8 Toimittajan IT- ja Tietoturvahallinto sekä johto

Toimittajalla on nimetty tietoturvasta vastaava henkilö, jonka tehtävänä on päivittäinen tietoturvatoiminta. Normaalit hallinnolliset päätökset ja yleisen tietoisuuden ylläpitäminen tapahtuu tietoturvavastaavan toimesta ja johdolla. Merkittävät hallinnolliset päätökset käsitellään Toimittajan ylimmän johdon nimeämässä tietoturvaryhmässä.

Toimittajalla on prosessi, jonka mukaisesti se testaa, tutkii ja arvioi säännöllisesti Sovelluksen tietoturvaan ja saatavuuteen vaikuttavia teknisiä, liiketaloudellisia ja organisatorisia riskejä, ja vastaa, että niihin reagoidaan sopimusten ja kulloinkin voimassa olevan lainsäädännön mukaisesti. Niiltä osin kuin Sovelluksen toiminta on riippuvaista kolmannen osapuolen tarjoamista palveluista, Toimittaja varmistaa, että myös kolmas osapuoli sitoutuu vähintään yhtä tiukkoihin tietoturva- ja palvelutasovaatimuksiin kuin Sovelluksen sopimuksessa on esitetty.

Toimittajalla on suunnitelma säännöllisten sisäisten tietoturvatarkastusten tekemisestä sekä dokumentoidut tulokset tehdyistä tarkastuksista ja niiden aiheuttamista toimenpiteistä. Mikäli havaitaan tietoturvapoikkeama, toimittaja varmistaa kyvyn tukea sen kattavaa teknistä tutkintaa.

Toimittajan tietoturvadokumentaatio on soveltuvin osin Toimittajan henkilöstön ja tarvittavien yhteistyökumppanien saatavilla ja tiedossa.

3 Tietosuoja

3.1 Käyttötarkoitussidonnaisuus ja tietojen minimointi

Asiakas vastaa siitä, että Sovellukseen syötetään vain käyttötarkoituksen kannalta välttämättömiä henkilötietoja. Sovellus tukee tätä minimoimalla oletusarvoisesti henkilötietokenttien näyttämistä käyttöliittymässä, ja mahdollistamalla Asiakkaalle lomakkeiden räätälöinnin kattamaan vain Asiakkaan käyttötarkoituksen kannalta oleelliset tiedot. Jos jokin Sovelluksen ominaisuus vaatii tiettyjen henkilötietojen keräämistä, Sovellus ilmaisee tietojen käyttötarkoituksen selkeästi Asiakkaalle ja käyttäjälle suunnatuissa ohjeistuksissa.

3.2 Tietojen täsmällisyys

Jotta Sovelluksessa olevat tiedot ovat täsmällisiä ja laadukkaita ja Asiakas voi hyödyntää Sovellukseen syötettyä tietoa tarkoituksenmukaisesti, on Asiakkaan vastuulla ohjeistaa käyttäjät syöttämään tiedot riittävän kattavasti, sekä laadullisesti ja asiasisällöltään oikeina, kuten myöskin päivittämään näitä tietoja, ml. että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä.

3.3 Tietojen elinkaari ja siirrettävyys

Asiakas vastaa siitä, että määrittää tietojen säilytysajat ja anonymisoi tai poistaa elinkaarensa päähän tulleet tiedot. Lisäksi asiakas voi tarvittaessa anonymisoida tai poistaa tiettyyn yksittäiseen henkilöön liittyvät tiedot erikseen. Asiakas voi hyödyntää näihin toimenpiteisiin tarjolla olevia Sovelluksen ominaisuuksia.

Asiakas voi Sovelluksen ominaisuuksia hyödyntäen siirtää Sovellukseen syötetyt henkilötiedot (tai valitsemansa osan niistä) yleisesti käytetyssä ja koneellisesti luettavassa muodossa itselleen, rekisteröidylle tai toiselle rekisterinpitäjälle. Mikäli Sovelluksen ominaisuudet eivät ole riittävät Asiakkaan nimenomaisiin tarkoituksiin, tai Asiakas muuten pyytää, Toimittaja kokoaa Sovellukseen syötetyt henkilötiedot Asiakkaan pyynnöstä siirrettävään, yleisesti käytettyyn koneellisesti luettavaan muotoon, ja toimittaa ne Asiakkaalle. Toimittaja voi veloittaa tästä työstä sopimuksen ja/tai hinnastonsa mukaisesti.

3.4 Tietojen pseudonymisointi

Vain käyttäjä, jolle on myönnetty oikeus tietyn henkilön tietoihin, näkee ne asiayhteydessään. Sen jälkeen, kun tietyn henkilön tiedot on muuten poistettu Sovelluksesta, niiden paikalla näytetään henkilön pseudonyymi.

3.5 Osoitusvelvollisuuden noudattaminen

Toimittaja vastaa siitä, että se voi osoittaa noudattavansa tietosuoja-asetuksen mukaisia henkilötietojen käsittelyä koskevia periaatteita (”osoitusvelvollisuus”) valvovalle viranomaiselle ja Asiakkaalle sopimuksen niin edellyttäessä.