KoskiHoiva Oy Tietoturvasuunnitelma

31.8.2023
Versio 1
Päivitetty 27.10.2025

Laatija
Antti Kulmanen
LiteIT Oy
antti.kulmanen@liteit.fi

KoskiHoiva Oy tietosuojavastaava
Marko Kainulainen

Sisällysluettelo

Käyttötarkoitus

Tietoturvasuunnitelman käyttötarkoitus on auttaa yrityksen johtoa sekä henkilöstöä toimimaan oikein eri tilanteissa ja ottamaan huomioon näkökulma tietoturvan kannalta. Suunnitelma helpottaa myös nykytilanteen ymmärtämistä, riskiarvion luomista, ja tuo esille huomioitavat asiat ja käytännöt nykytilanteessa, mutta myös suuntaviivoja tulevaisuutta ajatellen.

Suunnitelma nojaa lakiin sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä. Lisäksi huomioon on otettu yrityksen omat tarpeet ja henkilöstön käytännöt muuhun dataan liittyen, kuin potilastietoihin.

Tietoturvasuunnitelmaa tulee päivittää säännöllisesti. Tietoturvasuunnitelman laadinnan ja noudattamisen vastuu on sosiaali- ja terveydenhuollon palvelunantajan vastaavalla johtajalla.

Suunnitelmissa ja toteutuksessa lähdetään liikkeelle kriittisimmistä kohteista tietoturvallisuuden omavalvonnan kohteen omassa toiminnassa tunnistettujen riskien ja tietoturvallisuuden tilan tarkastelun kannalta.

Suunnitelman päivityskäytännöt

Suunnitelmaa päivitetään tarpeen mukaan, kun lakiin, käytäntöihin tai tarpeisiin tulee muutoksia.

Yleiset tietoturvakäytännöt

KoskiHoiva Oy:ssä noudatetaan seuraavia yleisiä tietoturvakäytäntöjä, ja tehdään tietoturva-, tietosuoja-, asiakastietojen käsittelyn omavalvontatyötä sekä riskienhallintaa seuraavien dokumenttien mukaisesti:

- Verkkokaavio konttori & Villa Koski
- Etätyöohjeet konttori & Villa Koski
- Potilastietojärjestelmä Hilkka ohjeistus
- Potilastietojärjestelmä Hilkan toimittajan tietosuojaseloste
- Tietoturvakaavio
- Henkilöstön tietoturvaohjeet Intranetissä

Tietosuojasuunnitelman kohteet

Tämän tietosuojasuunnitelman piiriin kuuluvat:

- Nimi: KoskiHoiva Oy
- Y-tunnus: 2695507-5
- Osoite: Saapastie 2
  33950 Tampere

Toimipaikat:

- Pääkonttori Pirkkala (Pirkanmaa):
  - Vastuuhenkilö: Toimitusjohtaja Marko Kainulainen
  - Osoite: Saapastie 2, 33950 Pirkkala
- Espoo (Länsi-Uusimaa, Vantaa-Kerava & Helsinki)
  - Vastuuhenkilö: Emma Lehto
  - Osoite: Technopolis Tekniikantie 14, 02150 Espoo
- Forssa (Kanta-Häme)
  - Vastuuhenkilö: Emma Lehto
  - Osoite: Rajakatu 2, 30420 Forssa
- Tietosuojavastaava Marko Kainulainen

Menettelyt virhe- ja ongelmatilanteissa sekä jatkuvuuden hallinta

Poikkeustilanteisiin varautumisessa ja jatkuvuuden suunnittelussa noudatetaan seuraavia toimintatapoja:

- Internet-yhteyden katkeaminen
    - Odota hetki, jos yhteys palautuu
    - Jos ei palaudu, soita Elisan Vikapalveluun
    - Tarvittaessa jaa puhelimesta netti tietokoneelle, jolloin työ voi jatkua
- Tietokone ei käynnisty, tai koneessa muuta ongelmaa
    - Kone koitetaan käynnistää uudelleen pitämällä virtanappia pohjassa 20 sekuntia
    - Jos ei vieläkään toimi, soita IT-Tukeen Antti Kulmaselle
    - Tarvittaessa käytä vapaana olevaa varakonetta
- Tiedostojen varmuuskopiot
    - Tiedostot sijaitsevat Microsoft 365 pilvessä, jolloin työ voi jatkua toisella koneella pilvipalvelun turvin
    - Microsoft 365 pilvipalvelut ovat varmuuskopioituna suomalaiseen Nexetic M365 varmuuskopiopalveluun
        - Varmuuskopiot otetaan automaattisesti 2 krt päivässä
- Potilastietojärjestelmä Hilkka ei aukea
    - Tarkista, että internetyhteys on päällä ja toimii kokeilemalla jotain muuta verkkosivua
    - Soita Fastroin Hilkka-tukeen
- HaiPro ei aukea
    - Soita HaiPro tukeen

Käyttäjätunnuksia, henkilötunnuksia yms. ei saa säilyttää paperilla. Kaikki kriittistä dataa sisältävä paperit, tulosteet, tai sellaisiksi miellettävä pitää tuhota tietoturvallisesti käytön jälkeen.

Toimintatavat tietoturvan pettäessä tai vuodon sattuessa

KoskiHoivassa käsitellään GDPR ja potilastietolain alaista dataa, jolloin tietoturvan pettäessä vuodoista ilmoitetaan aina eteenpäin viranomaisille.

Virus tietokoneessa

Jos epäilet virusta, tai WithSecure ilmoittaa, että koneessa on virus. Sammuta kone ja ilmoita esimiehellesi. Odota lisäohjeita.

Tietojen vuotaminen ulkopuolisille

Vuoto voi ilmetä esimerkiksi näin:

- Sähköpostissa saapuneissa tai lähetetyissä kansioissa on outoja viestejä, tai viestejä katoaa
- Tiedostoja katoaa tai outoja tiedostoja ilmestyy koneelle
- Tiedostot on kryptattu, eikä niitä saada auki

Ilmoita aina esimiehellesi, joka ottaa yhteyttä tukeen asian selvittämiseksi.

Henkilöstön koulutus, osaaminen ja tietojärjestelmien turvallinen käyttö

Henkilöstölle pidetään perehdytyksiä säännöllisesti. Lisäksi Intranetissä ovat ohjeita käytännön asioihin.

Tietojärjestelmien ja laitteiden tietoturvakäytännöt

Kriittistä dataa sijaitsee potilastietojärjestelmä Hilkassa sekä Microsoft 365 pilvipalvelussa, sekä tietokoneilla.

Microsoft 365

- Toimiston, hallinnon ja Villa Kosken sähköpostin omaavilla on käytössä kaksivaiheinen kirjautuminen
    - Käyttäjätunnuksen ja salasanan lisäksi tarvitaan puhelimeen MS Authenticator appiin tuleva kertakäyttökoodi
- Muulla henkilökunnalla käytössä vain käyttäjätunnus ja salasana, jolla pääsee kirjautumaan Koskihoivan Microsoft-ympäristöön liitettyyn koneelle, mutta ei tiedostoihin
    - Lisäksi henkilökunnalla pääsy intranettiin, jossa ajankohtaisia ilmoituksia ja ohjeita työntekoon

Fastroi Hilkka

Liitteenä Fastroi Hilkka järjestelmäkuvaus.

Tietokoneet

- Koneissa käytössä Bitlocker-kryptaus
    - Koneen tiedostoihin ei pääse käsiksi ilman tunnuksia
- Tietokoneet liitetty KoskiHoivan Microsoft 365 ympäristöön
    - Koneet voidaan lukita ja tyhjentää etänä
- Koneissa on WithSecuren EPP Elements for computers premium tietoturvaohjelmisto
    - Valvoo koneen käyttäytymistä ja tietoturvapäivitysten asennuksia, sekä estää haittaohjelmia
- Kaikki tiedostot sijaitsevat pilvessä
    - Jos kone hajoaa tai katoaa, voidaan työtä jatkaa lennosta toisella koneella
- Näyttö lukitaan aina kun työpisteeltä poistutaan
    - Onnituu **CTRL + ALT + DEL** ja sieltä **LUKITSE NÄYTTÖ.**

Webpropol Whistleblowing-kanava

Liitteenä:

- Webpropol data security policy
- data security white paper
- privacy statement for users
- records of processing.

Tietojärjestelmien asennus, ylläpito ja päivitys

KoskiHoiva Oy käyttämät pääjärjestelmät ovat Microsoft 365 pilviympäristö, sekä Fastroi Hilkka potilastietojärjestelmä. Kummassakin tapauksessa toimittaja (Microsoft ja Fastroi) huolehtivat järjestelmien ja ohjelmien päivittämisestä. KoskiHoivalla ei ole omilla palvelimilla tietojärjestelmiä.

Tietokoneet ilmoittavat käyttäjälle, kun päivitys on saatavilla. Henkilöstöä ohjeistettu käynnistämään / asentamaan päivitykset ainakin kerran viikossa. Lisäksi koneita valvotaan Microsoft Defender portaalissa sekä WithSecuren portaalissa, josta voidaan pakottaa päivitykset asentumaan etänä koneille.

Käyttövaltuuksien hallinta ja tunnistautumiskäytännöt

Microsoft 365 ja tietokoneet

Windows-koneille ei pääse ilman käyttäjätunnusta, salasanaa tai pin-koodia. Lisäksi sähköpostin tai laajemman lisenssin omaavilta (lähinnä konttorin väki, villakoski hallinto) vaaditaan pilvipalveluihin kirjautuessa 2 vaiheinen tunnistautuminen:
käyttäjätunnuksen ja salasanan lisäksi puhelimen Authenticator-appiin tulee koodi, joka täytyy syöttää ennen sisään pääsyä.
Pilvipalveluiden yhteydet ovat SSL-salattuja.

Puhelimet

Puhelimissa on käytössä 6 numeroinen pin-koodi. Lisäksi android-puhelimet tullaan liittämään KoskiHoiva Oy:n Microsoft järjestelmään. Tällöin saadaan täysi hallittavuus puhelimiin. Puhelimet ovat nyt kiinni Google-tilissä, jotta ne voidaan etänä tyhjentää.

Fastroi Hilkka

Hilkka sijaitsee pilvessä ja sitä käytetään nettiselaimella. Yhteys on SSL-salattu. Järjestelmään kirjaudutaan käyttäjätunnuksella ja salasanalla. Liitteenä Hilkan järjestelmäkuvaus.

Etätyöt ja niiden mahdollistaminen

Konttorin väellä sekä Villa Kosken hallinnolla ovat henkilökohtaiset tietokoneet. Tarvittaessa he voivat tehdä töitä etänä.

Koneissa tietoturvaohjelmisto, joka suojaa konetta haittaohjelmilta. Lisäksi koneissa ib VPN-yhteys. VPN yhteydellä turvataan työskentely ja data myös niissä paikoissa, missä KoskiHoiva ei voi taata nettiyhteyden turvallisuutta. Henkilöstöä on ohjeistettu käyttämään VPN-yhteyttä kaikkialla muualla, kuin Villa Koskessa tai pääkonttorilla.

Tietokoneisiin hankitaan etätöitä varten tietosuojakalvot uteliaiden katselijoiden varalle.

Fyysinen turvallisuus osana yrityksen tietoturvaa

Fyysinen turvallisuus sisältää seuraavat:

- Ovien lukitseminen
- hälytysjärjestelmät
- Painetun tiedon tietoturvallinen tuhoaminen
- tietokoneiden näyttöjen lukitseminen
- näyttöjen sijoittelu niin, etteivät ulkopuoliset vahingossa lue tietoja
- laitteiden, kuten tulostimen sijoittelu niin, etteivät ulkopuoliset pääse hakemaan papereita
- arkistointitoimenpiteet
- kulunvalvonta

Etähoidon tietoturvasuunnitelma

1. Tietoturvasuunnitelman käyttötarkoitus

Tämä dokumentti on KoskiHoiva Oyn etäkotihoidon tietoturvasuunnitelma. Tämä dokumentti täydentää organisaation yleistä tietoturvasuunnitelmaa. Tämän tietoturvasuunnitelman käyttötarkoitus on täyttää asiakastietolain[1] 703/2023 77 §:n 1 ja 2 momentin ja THL:n määräyksen 3/2024 mukaiset velvoitteet.

2. Tietoturvasuunnitelman kohde ja päivityskäytännöt

Tämän tietoturvasuunnitelman piiriin kuuluvat:
Etäkotihoidon tietojärjestelmä _____ (yrityksen nimi)

Toimintayksiköt _____
Y-tunnus _____
Vastuuhenkilöt _____
Toimipaikat/palveluyksiköt _____
Suunnitelman piiriin kuuluvat alihankkijat ja sopimuskumppanit: Digihappy Oy tietojärjestelmä- ja palvelutoimittaja

Suunnitelman toteuttamisessa ja päivittämisessä noudatetaan seuraavia käytäntöjä:

- Suunnitelman ja sen päivittämisen vastuuhenkilö: _____
- Suunnitelman toteuttamisen vastuuhenkilöt: _____
- Katselmointi- ja päivityskäytännöt: Suunnitelma otetaan aktiiviseen käyttöön etäkotihoivan perehdytyksessä ja se on käytössä etäkotihoivan palvelutuotannossa. Suunnitelmaa katselmoidaan ja päivitetään vähintään kerran vuodessa ja aina, jos ilmenee tarve, esimerkiksi oleellisen tietoteknisen muutoksen tai poikkeamatilanteen seurauksena
- Suunnitelman seuranta ja seurannan dokumentointi: Suunnitelman toteuttamisen seuranta liitetään osaksi johtoryhmän työskentelyä, jossa toteuttamisen vastuuhenkilö raportoi ja dokumentoidaan toteutuminen vähintään kerran vuodessa.
- Suunnitelman käyttö tietojärjestelmien hankinnoissa ja päivityksissä: Suunnitelmissa kuvatut toimenpiteet huomioideaan hankittaessa tai päivitettäessä tietojärjestelmää.
- Päätös suunnitelman hyväksymisestä ja käyttöönotosta: Suunnitelman ja sen uusien versioiden käyttöönotosta päättää suunnitelman vastuuhenkilö. Päätös kirjataan johtoryhmän kokousmuistioon.

3. Yleiset tietoturvakäytännöt

[1] Asiakastietolaki 703/2023

Tietoturvallisuustyötä etäkotihoidossa tehdään organisaation yleisten tietoturvadokumenttien mukaisesti, jotka ovat Tietoturvapolitiikka, Tietosuojapolitiikka, Riskienhallintapolitiikka ja riskienhallintaan liittyvät ylläpito- ja kehittämissuunnitelmat, Selosteet henkilötietojen käsittelytoimista, Lista tietoturvasuunnitelmaan kuuluvista tietojenkäsittelyyn ja tietoturvallisuuteen liittyvistä sopimuskumppaneista alihankkijoineen, Tietojärjestelmäpalvelun tuottajien tietoturvallisuusohjeet, Omat tietoturvallisuusohjeet, Etä- ja hybridityöohjeistukset tietoturvallisuuden osalta. Tietosuojavastaava etäkotihoidossa on organisaation tietosuojavastaava.

Organisaation dokumentteihin lisätätään Etäkotihoivan tietoturva, joka sisältää etäkotihoidon tietoturvan yksityiskohdat.

4. Menettelyt virhe- ja ongelmatilanteissa sekä jatkuvuudenhallinta

Virhe- ja ongelmatilanteiden ehkäisy, hallinta, toipuminen ja jatkuvuudenhallinta on dokumentoitu ja toteutetaan seuraavasti:

VIrhe- ja ongelmatilanteita ehkäistään seuraavasti

- Palvelutuottaja
  - käyttää vain korkealuokkaisia laitteita ja lisäosia
  - ohjelmistot ovat kehitetty modernilla, luotettavalla teknologialla ja kehityksessä ja hallinnassa korkeimmalla prioriteetilla on palvelun jatkuvuus ja turvallisuus
  - Järjestelmiä päivitetään ja hallitaan aktiivisesti
  - Poikkeamien syyt selvitetään aktiivisesti
- Organisaatio
  - Kouluttaa ja perehdyttää Digihappyn tuella henkilöstön huolellisesti
  - Dokumentaatio on luotettavaa ja ajantasaista
  - Loppukäyttäjät on selkeästi informoitu järjestelmästä
  - Raportoi poikkeamista palvelutuottajalle aktiivisesti

Videopuheluyhteysongelman asiakastilanteen hallinta, toipuminen ja jatkuvuudenhallinta

- Jos videoviestintäyhteyttä asiakkaaseen ei saada suunnitellusti tai yhteys katkeaa ei suunnitellusti, toimitaan seuraavasti
  - työntekijä arvioi tilanteen kriittisyyden asiakkaan välittömän terveyden kannalta
    - Luokka 1 , asiakas tarvitsee heti apua
    - Luokka 2, asiakas tarvitsee yhteyden kahden kuluessa
    - Luokka 3, asiakas tarvitsee yhteyden neljän tunnin kuluessa
- Luokka 1
  - On kyseessä, jos on odottamaton hätätilanne ja videoyhteys asiakkaaseen katkeaa, ja jossa asiakkaan henki on välittämästi uhattuna, esimerkiksi vaikea sairaskohtaus videopuhelun aikana ja yhteys katkeaa. Työntekijä hälyttää 112.
- Luokka 2 ja 3
  - Työntekijä ottaa asiakkaaseen uudestaan yhteyttä vähintään kolme kertaa.
  - Työntekijä käyttää yhteydenottoon videoviestialustaa, ja lisäksi soittaa asiakkaan puhelinnumeroon. Työntekijällä on aina saatavissa tieto myös asiakkaan puhelinnumerosta.
  - Työntekijä ilmoittaa it-palvelutuottajan it-tukeen yhteysongelmasta.

  - Työntekijä infornoi esimiestään ja kokonaisarvion pohjalta, he suunnittelevat asiakkaan hoidon jatkuvuuden, korvaten videokäyntejä puhelinkäynnillä tai/ja lähikäynnillä.

Videopuheluyhteysongelman tekninen hallinta, toipuminen ja jatkuvuudenhallinta

- Käyttöön liittyvä ongelma, mikä voidaan ratkaista laite- ja etähallintajärjestelmällä
  - Digihappylla on laite- ja etähallinta laitteisiin, mikä mahdollistaa useiden ongelmien ratkaisemisen hallintajärjestelmän kautta suoraan. Tällöin Digihappy säätää laitteen asetuksia tai esimerkiksi uudelleen käynnistää laitteen.
- Käyttöön liittyvä ongelma, mitä tarvitsee toimenpiteitä laitteella, kuten esimerkiksi laitteen laittaminen lataukseen, jos akku on loppunut
  - Työntekijä saa ohjeet palvelutuottajalta ongelman ratkaisemiseksi
  - Työntekijä toimii ohjeiden mukaisesti lähikäynnillä ja saa tukea tarvittaessa palvelutuottajan it-tuesta. Jos asiakas pystyy itse koskemaan laitteeseen, myös asiakasta voidaan neuvoa yksinkertaisen ongelman ratkaisussa.
- Kyseessä on laiterikko
  - Digihappy toimittaa valmiiksi asennetun uuden laitteen tai palvelukokonaisuuden osan, kuten esimerkiksi sim-kortin. Laite on käyttövalmiiksi asennettu ja toimitusvalmis arkipäivisin 24 tunnin kuluessa laitevian toteamisesta. *Organisaatiolla on varalaite mahdollisen laiterikon varalle.*

Pitkittyneen ja laajan yhteysongelman tai poikkeustilanteen hallinta, toipuminen ja jatkuvuudenhallinta

- Jos kysessä on laaja ja pitkäkestoinen ongelma tai poikkeustila, organisaatio siirtyy noudattamaan ennalta laadittua väliaikaista hoidon toimintasuunnitelmaa
- Palvelutuottaja ratkaisee tietoteknistä ongelmaa korkealla prioriteetilla kaikilla käytettävissä olevilla keinoilla. Jos kyseessä on force majeure tilanne, esimerkiksi sota tai tietoliikennehäirintä, palvelutuottaja ratkaisee ongelmaa välittömästi kun force majeure tilanne on ratkennut korkealla prioriteetilla kaikilla käytettävisssä olevilla keinoilla.

Koulutus ja varautuminen
Organisaatio varautuu virhe-ja poikkeamatilanteisiin ennalta

- Toimintatavat on dokumentoitu työntekijöiden sisäisiin ohjeisiin
- Toimintatavat on käyty läpi etäkotihoivan perehdytyskoulutuksessa
- Toimintatavat on sisällytetty uuden työntekijän perehdytykseen

Toimenpiteet tietosuojapoikkeamissa
Etäkotihoivan tietosuojapoikkeamissa toimintatavat on samat kuin muissa tietosuojapoikkeamissa.

5. Henkilökunnan koulutus ja osaaminen sekä tietojärjestelmien käyttöohjeet ja tietoturvallinen käyttäminen

Etäkotihoivan tietojärjestelmä koulutus, osaamisen ylläpito ja kehittäminen toteutetaan kuten organisaation muiden tietojärjestelmien koulutus. Koulutus, ylläpito ja kehittäminen koskee niitä henkilöitä, jotka käyttävät järjestelmää tai ovat varalla, esimerkiksi sairastapauksen yhteydessä.

Etäkotihoivan tietojärjestelmä koulutuksessa, ylläpidossa ja kehittämisessä huomioidaan erityisesti seuraavat asiat yleisten toimintatapojen lisäksi.

- Kirjautuminen järjestelmiin
- Asiakkaan informoiminen etäkotihoivasta, videopuheluista sekä laitteista
- Asiakkaan tai/ja edunvalvojan kanssa kirjallisesti sopiminen toimintatavoista
    - Milloin soitot tapahtuvat ja missä tilanteissa
    - Halutaanko videopuhelujen avautuvan automaattisesti vai ei
- Virhe-ja poikkeamatilanteissa toimiminen

Koulutus tapahtuu monimuotokoulutuksena, joka sisältää interaktiiviset etävideokokouskoulutukset ja laajan koulutusmateriaalin, joka jää organisaation käyttöön. Materiaaleja Digihappy päivittää säännöllisesti, vähintään kerran vuodessa. Digihappy tuottaa palvelun aloituksessa laajan videokoulutuksen työntekijoille ja tuottaa havainnollisen koulutusmateriaalin. Uusien, myöhemmin rekrytoitavien työntekijöiden perehdytys on organisaation vastuulla tai organisaatio sopii Digihappyn kanssa lisäkoulutuspalveluista. Organisaatio kirjaa koulutukseen osallistumisen vastaavasti kuten muuhun tietojärjestelmäkoulutuksiin osallistumisen. Koulutus tuotetaan suomeksi ja tarvittaessa ruotsiksi tai englanniksi.

Tietojärjestelmien käyttöohjeet ja ohjeiden mukainen käyttö

Etäkotihoivan teknisen koulutusmateriaalin tuottaa Digihappy ja Digihappy päivittää niitä säännöllisesti, vähintään kerran vuodessa. Organisaation informoi työntekijöitä ohjeista ja niiden saatavuudesta organisaation järjestelmissä.

6. Tietojärjestelmän tietoturvakäytännöt

Etäkotihoivan tietojärjestelmän tietoturvakäytännöt noudattavat organisaation yleisiä tietoturvakäyntöjä kaikin soveluvin osin. Tässä dokumentissa on edellä kuvattu etäkotihoidon tietojärjestelmän erityispiirteitä organisaatiossa.

Digihappy Oy:lla on erillinen tietoturvadokumentti, joka perustuu lain ja asetusten noudattamiseen kaikissa tietoturvakäytännöissä. Digihappyn tietoturvasuunnitelman periaatteet ovat, että tietoja saavat käyttää vain ne, joilla on siihen hänen tehtäväänsä tarvittavat oikeudet, tiedot ovat oikeita ja ajantasaisia sekä tiedot ja järjestelmät ovat käytettävissä ja tiedon käyttö on todennettavissa silloin, kun niitä tarvitaan.

Digihappy tietosuoja noudattaa Suomen ja EU:n asetuksia ja EU:n yleisen tietosuoja-asetuksen (GDPR) mukainen rekisteri- ja tietosuojaseloste on aina saatavilla https://digihappy.fi. Digihappy kerää asiakkaista vain minimimäärän tietoa, Digihappy ei esimerkiksi kerää henkilötunnuksia ja videopuheluita ei tallenneta. Kaikki data on EU-alueella.

Digihappy etäkotihoivan tietojärjestelmä on muu tietojärjestelmä

Digihappy tietojärjestelmä ei ole potilastietojärjestelmä tai asiakastietojärjestelmä, eikä sitä koske niitä koskeva lainsäädäntö.

Digihappy tietojärjestelmä on Valviran päätöksen mukaisesti video- äänipalvelu- ja viestintäalusta. Digihappy tietojärjestelmä ei ole asiakastietojärjetelmä. Alla on Valviran päätöksen keskeiset kohdat: ”Sosiaali- ja terveysalan lupa ja valvontavirasto (Valvira) on vastaanottanut 12.4.2023 Digihappy Oy:n valmistaman Digihappy-tietojärjestelmän rekisteri-ilmoituksen. Ilmoituksen mukaan tietojärjestelmän käyttötarkoitus on seuraava: ‘ Mobiilipohjainen video- ja äänipalvelu- ja viestintäalusta kotisairaanhoitoon, palveluasuntoihin ja hoivakoteihin. Järjestelmän asiakkaita ovat siihen liitetyt, palvelutuottajan olemassa olevat, tunnistetut asiakkaat. Järjestelmä ei tallenna potilas- tai sosiaalihuollon tietoja ja järjestelmä ei ole yhteydessä sairas- tai sosiaalihuollonkertomusjärjestelmiin tai Kanta- tai Sosiaalihuollon arkistoon. ‘ Digihappy-tietojärjestelmän nykyinen käyttötarkoitus ei vastaa asiakastietolain 3 §:n 6 kohdassa olevaa tietojärjestelmän määritelmää. Näin ollen Digihappytietojärjestelmää ei koske asiakastietolain 30 §:n mukainen rekisteröintivelvoite, eikä Valvira rekisteröi kyseistä tietojärjestelmää asiakastietolain mukaiseen tietojärjestelmärekisteriin. “

Etäkotihoidossa käytetään asiakastietojen kirjaamiseen erillistä, varsinaista asiakastietojärjestelmää eli samoja asiakastietojärjestelmiä kuin lähikotihoidossa. Etäkotihoidossa käytetään Digihappy Oy tuottamaa viestintävideoalustatietojärjestelmää. Digihappyn tietojärjestelmään ei tallenneta asiakastietoja ja se ei ole yhteydessä Kanta-arkistoon. Videopuheluita ei tallenneta. Järjestelmän käyttäjiä ovat siihen liitetyt, palvelutuottajan olemassa olevat, tunnistetut asiakkaat.

HILKKA JÄRJESTELMÄKUVAUS

JÄRJESTELMÄKUVAUS TIETOTURVASUUNNITELMAN LIITTEEKSI

23.8.2022

Y | Länsikatu 15, FI-80110 Joensuu | www.fastroi.com | sales@fastroi.com

23.8.2022

Luottamuksellinen

SISÄLLYSLUETTELO

23.8.2022

Luottamuksellinen

1 Johdanto

1.1 Liitteen käyttö tietoturvasuunnitelmassa

Tässä dokumentissa esitetään Hilkka-järjestelmän (myöhemmin järjestelmä) osalta ne tiedot, jotka palveluntuottaja tarvitsee oman tietoturvasuunnitelmansa laatimiseksi ja dokumentti on tarkoitettu tämän tietoturvasuunnitelman liitteeksi. Sosiaali- ja terveydenhuollon palvelunantaja voi viitata tähän dokumenttiin omassa tietoturvasuunnitelmassaan kuvaten oman organisaationsa menettelytavat Hilkka-järjestelmän käytön osalta, kuten käyttäjien koulutus ja virhetilanteet.

Tietoturvasuunnitelman laatimisvelvoite koskee kaikkia sosiaali- ja terveydenhuollon palvelunantajia. Tietoturvasuunnitelman laatimisvelvoitteesta säädetään asiakastietolain (748/2021) 27 §:ssä ja sen laatimisessa on noudatettava THL:n määräyksen 3/2021 velvoitteita. Tietoturvasuunnitelman ylläpitovastuu on myös sosiaali- ja terveydenhuollon palvelunantajalla.

2 Järjestelmän perustiedot

Järjestelmä	Fastroi Hilkka
Luokka	A3
Toimittaja	Fastroi Oy
Käyttötarkoitus	Fastroi Hilkka on selainkäyttöinen lääkemääräyksiä käsittelevä hoiva-alan toiminnanohjausjärjestelmä, jota käytetään päivittäisen hoivatyön kirjausten tekemiseen. Järjestelmän avulla kirjataan asiakkaiden hoitomerkinnät ja tiedot työntekijöiden työsuorituksista.
Käyttökontekstit ja käyttäjät	• julkiset terveydenhuollon palvelut • julkiset sosiaalihuollon palvelut • yksityiset terveydenhuollon palvelut • yksityiset sosiaalihuollon palvelut Sosiaali- ja terveydenhuollon asumis- ja avopalveluissa sekä näiden tukitoiminnoissa, kuten toimistopalvelut ja IT-tuki, työskentelevät henkilöt.
Järjestelmäprofiilit	• Lääkemääräyksiä käsittelevä potilastietojärjestelmä (PTJ) • Kanta-arkistointipalveluun toimitettavia tietoja tuottava sovellus • Potilaskertomusjärjestelmä (perusvaatimukset) • Asiakas- tai potilastietojen käsittelyyn tarkoitettu järjestelmä

2.1 Rekisterinpitäjyys

Palvelunjärjestäjä on rekisterinpitäjä. Järjestelmää käyttävä palveluntuottaja toimii henkilötietojen käsittelijänä järjestelmässä käsiteltävien tietojen osalta.

Fastroi Oy toimii henkilötietojen käsittelijänä ja käsittelee henkilötietoja osapuolten sopimuksen perusteella palveluidensa tarjoamiseksi, esimerkiksi tilanteissa, joissa Hilkka-järjestelmään liittyvien tukipyyntöjen käsittely edellyttää henkilötietojen käsittelyä.

3 Järjestelmän kuvaus

3.1 Tietoturvakäytännöt

Fastroi Oy:llä on ISO 9001-laadunhallintajärjestelmän, ISO 27001 tietoturvallisuuden hallintajärjestelmän, sekä ISO 14001-ympäristöhallintajärjestelmän sertifioinnit, jotka auditoidaan säännöllisesti akkreditoidun toimijan toimesta.

3.1.1 Tietoturvan auditointi

Järjestelmä auditoidaan tietoturvan osalta säännöllisesti akkreditoidun toimijan toimesta.

Kanta-palveluihin liitettyjen järjestelmien ja Kanta-välityspalveluiden viranomaisten vaatimuksena on tietoturvallisuuden sertifiointi ja tähän liittyvä tietoturva-auditointi on suoritettu Hilkka-järjestelmän osalta viimeksi 17.6.2021.

Tietoturvavaatimusten kategorioita ovat :

- sähköinen allekirjoitus
- tunnistaminen (sulkulistat ja ammattioikeuden rajoitukset)
- käyttövaltuushallinta
- valvonta ja lokitus
- tietojen käsittely ja ohjeistus
- muut pakolliset vaatimukset
- sovellusturvallisuus
- järjestelmän käyttöympäristö

3.1.2 Järjestelmän tietoturvallinen ohjelmistokehitys, operointi ja valvonta

Järjestelmän kehittämisen korkea laatu ja turvallisuus varmistetaan hyvillä ohjelmiston kehitysmenetelmillä. Järjestelmän toteutuksessa hyödynnetään versionhallintaa, jolloin muutosten jäljitettävyys on mahdollista. Laadunhallintaan kuuluu sääntö, että versionhallinnan kehityshaaraan menevälle koodille tehdään aina koodikatselmointi jonkun toisen kehittäjän toimesta. Lisäksi jokaisen muutoksen jälkeen koodi ajetaan koodianalysaatorin läpi. Tämän lisäksi laadunvarmistukseen käytetään automaattisia yksikkötestejä, jotka ajetaan aina koodin muuttuessa. Testausprosessiin kuuluvat jokaisen muutoksen manuaaliset testaukset ja isompien versioiden julkaisujen yhteydessä tehtävät regressiotestit.

Tuotantoympäristö on rakennettu turvalliseksi viranomaismääräysten mukaisesti. Tuotantoympäristö on turvallisessa konesaliympäristössä, jonka yhteydet ja kriittinen infrastruktuuri on kahdennettu. Tuotannossa käytettävät palvelimet on kovennettu hyvien käytäntöjen (”best practices”) ja viranomaisvaatimusten mukaisesti. Järjestelmän käyttö vaatii vahvasti salattujen tietoliikenneyhteyksien käyttöä. Vastaavasti järjestelmä ottamat yhteydet kriittisiin kolmannen osapuolen palveluihin (esim. Kelan Kanta-palvelu) ovat vahvasti salattuja.

Hallintayhteydet alustapalvelimiin luodaan salatun VPN-yhteyden läpi käyttäen salattua etäyhteysmenettelyä. Hallintayhteydet järjestelmään luodaan salatun yhteyden kautta. Järjestelmän käytöstä kerätään asianmukaista lokia. Kaikki hallintayhteydet vaativat monivaiheisen todennuksen (MFA). Järjestelmää valvotaan konesalitoimittajan ja Fastroin toimesta. Valvonnan tavoitteena on tunnistaa palvelun tuottavan ympäristön ongelmat (laitteiston ongelmat, verkkoyhteydet jne) ja seurata palvelun kuormitusta, saatavuutta sekä häiriötilanteita.

3.1.3 Tietoturvan vastuiden rajaus

Hilkkaa koskevat sertifiointitodistukset ovat voimassa vain Hilkka-järjestelmän osalta. Mikäli Hilkka-järjestelmästä on toteuttu integraatio toiseen järjestelmään, on tämän järjestelmän toimittaja vastuussa ko. järjestelmän tietoturvasta. Integroidut järjestelmät tulee tarvittaessa auditoida erikseen.

Sosiaali- ja terveydenhuollon palvelunantaja vastaa itse oman organisaationsa tietoturvallisuudesta, kuten tietoliikenteen ja työasemien päivityksistä.

3.2 Tukipalvelu

Fastroin helpdesk palvelee asiakkaitamme ohjelmiston käytössä ja ongelmatilanteissa. Tukipyynnöt voi lähettä täyttämällä tukipyyntölomakkeen Fastroin kotisivuilla www.fastroi.com , sähköpostilla: helpdesk@fastroi.com tai soittamalla numeroon 010-327 8000. Helpdesk palvelee arkisin klo 8-16 tai laajennettu tekninen tuki päivystää eri sopimuksella sopimuksen mukaisena aikana.

3.3 Asennus ja käyttöönotto

Järjestelmä tarjotaan SaaS-palveluna, johon kirjaudutaan selaimen kautta.

Kanta-palveluja käytettäessä, käyttäjällä tulee olla voimassa oleva toimikortti ja kortinlukijalaite, sekä ladattuna työasemalle kortinlukijaohjelmisto (eRA SmartCard arkistoja käytettäessä ja mPollux Digisign client sähköistä lääkemääräystä käytettäessä). Kortinlukijaohjelmistojen päivitys on käyttäjäorganisaation vastuulla.

3.4 Tunnistautuminen järjestelmään ja järjestelmän lukittuminen

Tiedon salauksen lisäksi luottamuksellisuus ja eheys varmistetaan käyttäjien henkilökohtaisilla käyttäjätunnus-salasana -pareilla, kun järjestelmään kirjaudutaan. Organisaatio voi määritellä järjestelmässä salasanan turvatason, vaihtovälin sekä sen montako epäonnistunutta kirjautumisyritystä sallitaan ennen kuin tunnus lukitaan.

Järjestelmässä on automaattinen aikakatkaisu, mikäli järjestelmää ei käytetä päätelaitteelta tietyn ajan kuluessa. Organisaatio voi itse määritellä ajan automaattiselle aikakatkaisulle, määritellyn ajan jälkeen käyttäjä kirjataan automaattisesti ulos ellei järjestelmää käytetä.

Kanta-palveluiden käytössä edellytetään lisäksi sähköisen varmennekortin käyttöä.

3.5 Menettely virhe- ja ongelmatilanteissa

3.5.1 Toiminta virhe- ja ongelmatilanteissa

Käyttäjän havaitessa ongelma- tai virhetilanteen on hän yhteydessä oman organisaationsa pääkäyttäjään. Mikäli ongelmatilanne on sellainen, että se estää tai haittaa järjestelmän käyttöä, on käyttäjä/organisaation yhteyshenkilö yhteydessä järjestelmätoimittajan tukeen.

Tukipyyntö etenee Fastroin tukiprosessin mukaisesti olennaisille tahoille ja käyttäjäorganisaatiota tiedotetaan tehtävistä toimenpiteistä.

3.5.2 Vastuut virhe- ja poikkeustilanteissa

Vastuukysymykset ja palvelulupaukset on käsitelty sopimuksessa tai erillisessä SLA-dokumentaatiossa.

1.

3.6 Käyttäjien roolit ja oikeudet

Käyttövaltuushallinta on roolipohjainen ja käyttäjäorganisaatio valitsee itse käyttäjilleen sopivat roolit kuhunkin käytettävään yksikköön.

Käyttäjäroolit voidaan määritellä järjestelmään yksikkökohtaisesti ja/tai asiakasryhmittäin. Käyttöoikeuksilla määritellään kullekin käyttäjätasolle luonti-/muokkaus-/poisto-oikeudet järjestelmän eri osioihin ja lisäksi rooleihin voidaan asettaa rajoituksia sosiaalihuollon asiakkuuksien/-palveluprosessien ja/tai asiakirjatyyppien mukaisesti.

3.6.1 Käyttöoikeuksien myöntäminen

Käyttäjäorganisaatio määrittelee itse käyttöoikeuksien myöntämisen. Organisaatio voi itse määritellä roolit eli käyttäjätasot ja niiden oikeudet. Järjestelmässä on valmiina neljä oletus käyttäjätasoa, joiden oikeuksia ei voi muokata. Kullakin käyttäjällä on oltava vähintään yksi rooli kussakin käytettävässä yksikössä.

3.7 Käyttäjien koulutus

3.7.1 Käyttöönottoon liittyvät koulutukset

Ennen järjestelmän tuotantokäyttöönottoa järjestetään yleensä käyttäjäorganisaation nimetyille pääkäyttäjille käyttökoulutus. Lisäkoulutusta on käyttäjille tarjolla myös erillisellä sopimuksella.

3.7.2 Käyttöohjeiden ylläpito ja jakelu

Järjestelmän käyttöohjeet löytyvät järjestelmästä sähköisessä muodossa. Käyttöohjeiden päivitys kuuluu ohjelmistokehityksen päivitysprosessiin ja muutokset ohjeisiin ovat kaikkien järjestelmän käyttäjien saavutettavissa.

3.8 Lokit

Järjestelmässä on teknisten virhe- ja tiedonsiirtolokien lisäksi käyttö- ja muutosloki. Lokien käsittely edellyttää erillistä käyttöoikeutta, jonka pääkäyttäjä voi määritellä halutuille käyttäjille.

Asiakas- ja potilastietojen käsittelystä tallennetaan lokeihin merkinnät, joista nähdään kuka on katsellut tai muokannut tietoja, sekä se milloin tämä on tapahtunut. Järjestelmän lokien lisäksi Kanta-palveluissa potilastiedon arkiston osalta on käytettävissä myös Atostek eRA-järjestelmän lokit.

3.9 Palvelun käytön lopettaminen

Hilkka-järjestelmä on käytettävissä palvelun tuottamisen ajan, jonka jälkeen palvelua ei voi enää käyttää. Palvelun käytön lopettamisen yhteydessä sosiaali- ja terveydenhuollon palvelunantajan on säilytettävä lokitietoja voimassa olevan lainsäädännön mukaisesti.

3.10 Palvelun tuotannossa käytettävät alihankkijat

Käytetyt konesalitoimittajat ovat ISO 27001 -sertifioituja ja vastaavat osaltaan tietosuojan sekä tietoturvan toteutumisesta. Konesalit sijaitsevat Suomessa.

4 Muutostenhallinta

4.1 Hilkka

Tarkempi kuvaus ja mahdollinen palvelulupaus on sopimuksessa tai erillisessä SLA-dokumentissa.

4.1.1 Valmistautuminen

Järjestelmä testataan sekä automaatti- että manuaalitestauksia käyttäen aina kun järjestelmään tehdään muutoksia. Ennen uuden version julkaisua järjestelmässä suoritetaan myös regressiotestaus, joka sisältää kaikkien järjestelmän olennaisten osien testaamisen ja näiden raportoinnin.

Järjestelmä asennetaan Fastroin toimesta tarvittaessa asiakkaan testiympäristöön ennakkotestattavaksi, mikäli asiakasorganisaatiolla on testiympäristö käytössä.

4.1.2 Tiedottaminen

Järjestelmästä julkaistaan vuosittain 4-6 pääversiota, sekä useita pienempiä hotfix-versioita, jotka sisältävät virheiden korjauksia, teknisiä päivityksiä jne.

Päivitykset asennetaan huoltokatkojen tai erillisesti sovittujen aikataulujen mukaan, ja niistä tiedotetaan järjestelmän sisäänkirjautumissivulla ja sopimuksen mukaisella tavalla.

Asiakasorganisaation vastuulla on toimittaa Fastroille yhteyshenkilön tiedot.

4.1.3 Päivittäminen

Huoltokatkot, joiden aikana päivitykset asennetaan, sijoittuvat pääsääntöisesti varhaiseen aamuun ja järjestelmä on käytettävissä heti huoltokatkon päätyttyä. Asennuksen yhteydessä julkaistaan tarvittaessa uusi versio käyttöohjeista, vaatimuksenmukaisuustodistuksesta ja tästä dokumentista.

Tietoturvakuvaus Webropol-kyselypalvelut

Tämä dokumentti sisältää yleiskuvauksen Webropol Survey & Reporting kysely-, raportointi- ja analyysityökalun tietoturvasta sekä tietosuojasta. Dokumentissa kuvataan yleisimpien tietoturvaan, tietosuojaan ja järjestelmien tekniseen tietoturvaan liittyvien kysymysten ratkaisut.

Helmikuu 2023

Sisällysluettelo

Webropolista

Vuonna 2002 perustettu Webropol Oy on Webropol Survey&Reporting kysely- ja raportointisovelluksen kehittäjä. Palvelukokonaisuuten sisältyy kyselytyökalun lisäksi laaja valikoima lisämoduuleja sekä integraatioratkaisuja. Tarjoamme myös palveluita kuten koulutusta, konsultointia ja projektinhallintaa parhaan lopputuloksen saavuttamiseksi ratkaisujemme avulla. Tällä hetkellä meillä on toimipisteet Iso-Britanniassa, Saksassa, Ruotsissa ja Suomessa. Itsenäinen Webropol- jälleenmyyjä toimii Belgiassa. Webropol on kasvanut 20 vuoden aikana selvästi kansainväliseksi yritykseksi. Webropol-tytäryritykset ja - jälleenmyyjät ovat laajentaneet asiakaspohjamme jo 30 maahan.

Joka vuosi yli 20 miljoonaa ihmistä vastaa kyselytutkimuksiin, joita laatii kaikkiaan 70 000 Webropol-käyttäjää. Me pyrimme antamaan asiakkaillemme mahdollisimman täydellisen käyttäjä- ja asiakaskokemuksen. Kehitämme tuotetta jatkuvasti, jotta se pysyy helppokäyttöisenä ja erittäin tietoturvallisena. Haluamme tarjota asiakkaillemme vain parasta. Me uskomme kustannustehokkaaseen järjestelmään, jonka laadusta ja tietoturvasta ei tingitä.

Tietoturvan merkitys kyselypalvelua valittaessa

Verkkokyselyillä voit helposti ja nopeasti kerätä tietoa erilaisiin liiketoimintatarpeisiin. Vaikka tiedonkeruu onkin nykyään todella helppoa, on silti tärkeää muistaa tietoturvan ja tietosuojan merkitys. Kerätessäsi tietoa, erityisesti jos se sisältää henkilötietoja tai luottamuksellista liiketoimintaa koskevaa tietoa, on varmistuttava siitä, että sitä käsitellään asiankuuluvalla luottamuksellisuudella. Lisäksi on huomioitava tietoturvaa ja tietosuojaa koskeva lainsäädäntö ja muu mahdollinen säätely. Tämä koskee sekä kyselypalvelun käyttäjää että palveluntarjoajaa. Me Webropolilla otamme tietoturvaa ja tietosuojaa koskevat asiat erittäin vakavasti.

Tietoturva

Webropol on sitoutunut käyttämään alan parhaita teknisiä käytänteitä turvatakseen tietosi Webropol-palvelussa. Näillä menetelmillä ja prosesseilla varmistamme, että tietosi luottamuksellisuus on turvattu eikä luvaton käyttö ole mahdollista.

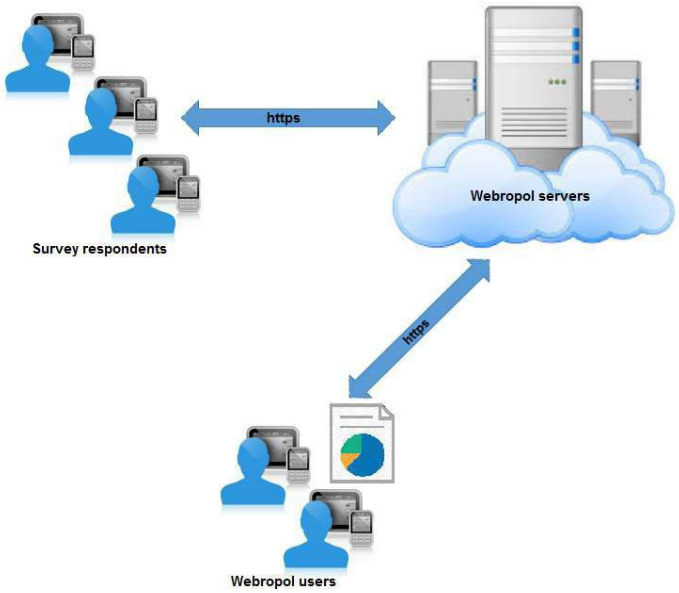
Webropol arvioi ja kehittää jatkuvasti loogista, organisaatiollista ja fyysistä tietoturvaansa. Tällä hetkellä teemme töitä saadaksemme käyttöön uusia ohjeistuksia ja käytäntöjä koskien niin teknisiä, fyysisiä ja organisaatiollista tietoturvaa. Tavoitteemme on saada toimistollemme ISO 27001 sertifiointi. Alihankkijamme, joka vastaa palveliemme ylläpidosta, on sertifioitu ISO 27001 standardin mukaan.

Webropol on tehnyt jatkuvaa, kuukausittaista yhteistyötä toistakymmentä vuotta tietoturva-alan huippuasiantuntijayritysten kanssa. Tällä hetkellä yhteistyökumppanimme on KPMG Cyber Security Services. Yhteistyöhön kuuluu lähdekoodin arviointi sekä palvelumme penetraatiotestit ja auditoinnit. Webropol käyttää Cyber Security Services -konsultteja ohjelman tietoturvan testaamiseen. Testeistä saadun tiedon pohjalta voimme kehittää ympäristömme tietoturvaa ja hallita mahdollisia riskejä.

Miten Webropol toimii?

Webropol-palvelu tarjotaan asiakkaillemme SaaS- palveluna (Software as a Service). Palvelut koostuvat useista erillisistä web-sovelluksista sekä niitä tukevista taustapalveluista. Kaikki Webropolin käyttäjät ovat samassa SaaS -ympäristössä, mutta kaikki asiakasdata on rajattu erillisiin, loogisiin asiakasympäristöihin.

Webropolin käyttäjät luovat kyselyitä Webropol-alustalla osoitteessa: https://new.webropolsurveys.com. Verkkokyselyitä voi lähettää esimerkiksi sähköpostitse tai SMS-kutsuin, tai julkaisemalla linkin esimerkiksi kotisivuilla. Kun tietoa on kerätty, voivat käyttäjät luoda monipuolisen raportointi- ja analyysityökalun avulla visuaalisia raportteja, jakaa niitä tai tallentaa aineiston jossakin useista tuetuista tiedostomuodoista. Lisäksi kerättyä tietoa voi analysoida monipuolisilla analysointityökaluilla, kuten Webropol Text Mining -tekstianalyysityökalulla tehtävät avointen vastausten ryhmittelyt tai Webropol Insights -työkalulla tehtävät ennusteanalyysit ja simulaatiot.



Kaikki palvelinten ja käyttäjien selaimen välinen liikenne on salattua,käyttäen TLS 1.2 ja TLS 1.3 salausalgoritmejä. Estettyjä versioita: TLS 1.0,TLS 1.1 sekä SSL 3.0.

Tietokannan kryptaus

Tietokanta on krypattu Microsoftin TDE-salauksella.

Kerätty tieto

Vaikka onkin tärkeää ymmärtää, miten Webropol toteuttaa kerätyn tiedon turvallisen käsittelyn, on myös yhtä lailla tärkeää tiedostaa, että kyselyn kysymysten laatiminen ja päätökset siitä, mitä tietoa kerätään, ovat aina Webropolia käyttävän asiakkaan vastuulla. Palvelulla kerätyn tiedon omistaa asiakas, ja asiakkaan on ymmärrettävä, että tiedosta voi muodostua asiakkaan vastuulla oleva henkilörekisteri. Jos kyselyaineisto sisältää henkilötietoja, on asiakkaan huomioitava henkilötietoja koskeva lainsäädäntö.

Palveluun kerättyä tietoa säilytetään oletusarvoisesti 1 kuukausi siitä hetkestä, kun käyttäjä käyttöliittymän kautta poistaa tiedon itse. Tarvittaessa vahingossa poistettu tieto voidaan palauttaa. Kaikki asiakkaan tiedot poistetaan 1 kuukauden kuluttua asiakkaan palvelusopimuksen päättymisestä.

Edellä kuvatun kyselytiedon lisäksi Webropol kerää ainoastaan eräitä käyttäjiin, ja teknisiin logeihin liittyviä tietoja. Lisätietoja kerättävistä tiedoista löytyy käyttöstatistiikkaan Tietosuojalain (5.12.2018/1050) mukaisesta rekisteriselosteesta.

Webropol on tehnyt tietoturvavaltuutetulle toimintailmoituksen: Dnro 1343/428/11.

Pääkäyttäjä voi luoda Webropoliin rajattoman määrän käyttäjätunnuksia yhteen asiakasympäristöön. Käyttäjätunnuksia on kahdentasoisia: Pääkäyttäjä ja Perustaso. Pääkäyttäjät voivat luoda uusia käyttäjätunnuksia asiakasympäristöön ja he hallinnoivat asiakkaan ympäristöä. Pääkäyttäjillä on pääsy kaikkiin kyselyihin ja raportteihin asiakkaan ympäristössä. Perustasoiset käyttäjät pääsevät niihin kyselyihin, jotka he ovat itse luoneet tai joihin heille on annettu pääsy, mutta eivät voi luoda muita käyttäjiä tai muuttaa käyttöympäristön yleisiä asetuksia. Pääsyoikeuksia voi antaa kolmella tasolla: **Lukuoikeus:** pääsee näkemään kyselyt ja raportit, mutta ei voi tehdä muutoksia **Kirjoitusoikeus:** pääsee näkemään ja muokkaamaan kyselyitä ja raportteja. Ei voi muokata kyselyn pääsyoikeuksia eikä poistaa kyselyä. **Hallintaoikeus:** voi tehdä kaikkia toimenpiteitä kyselylle. Vastaa kyselyn luojan oikeuksia.

Käyttäjätunnuksiin on liitetty sähköpostiosoite ja ne on suojattu käyttäjän itse valitsemalla salasanalla. Käyttäjien salasanat on tallennettu alan standardien mukaisesti SHA1- tiivisteinä (salted hash format). Webropolissa on mahdollista käyttää SAML 2.0/ADFS - pohjaista kertakirjautumisratkaisua (Single Sign-On, SSO). Webropolissa on suojaus ns. Brute Force -hyökkäystä vastaan: käyttäjätunnus lukkiutuu viiden epäonnistuneen kirjautumisyrityksen jälkeen.

Webropol suosittelee rajaamaan pääkäyttäjätasoiset oikeudet pienelle määrälle organisaation luotettuja käyttäjiä noudattaaksenne pääsynhallinnan prosessejanne. Suositeltavaa on kuitenkin nimetä vähintään kaksi pääkäyttäjää, jotta käytössä on myös varahenkilö varsinaisen pääkäyttäjän ollessa tavoittamattomissa.

Nimetyillä Webropolin asiakastuen henkilöillä on - asiakkaan kirjallisella luvalla - pääsy asiakkaan kyselyihin asiakastuen ja käytönneuvonnan antamiseksi. Webropolilla on tiukat politiikat ja kontrollit sen varmistamiseksi, ettei asiakasdataan päästä luvattomasti.

Lokitiedot ja kirjausketjut

Webropol-palvelut keräävät kattavasti lokitietoja ja kirjausketjuja (Audit Trail Log). Lokiin kirjataan tiedot esimerkiksi epäonnistuneista ja onnistuneista sisään- ja uloskirjautumisista, kyselytiedon lukemisesta, raportin tallentamisesta ulkoiseen tiedostomuotoon sekä käyttäjätunnusten ja pääsyoikeuksien luomisesta ja muokkaamisesta. Webropol Survey&Reporting -palvelussa lokien läpinäkyvyyttä on parannettu entisestään, muun muassa niin, että yksittäisten kyselyiden laatijat näkevät suoraan kyselyn tiedoista siihen kohdistuvat lokimerkinnät, esimerkiksi nähdäkseen onko joku muu käyttäjä katsonut raporttia.

Käyttäjien sisäänkirjautumistietoja säilytetään 10 vuotta. Tähän tietoon ei ole pääsyä muilla kuin Webropolin teknisellä tiimillä, emmekä luovuta tietoja eteenpäin kenellekään, edes kyselyn laatijalle.

Turvallinen tuotekehitys

Tietoturva on varmistettu tuotekehityksessä, käyttämällä tietoturva-alan parhaita käytänteitä sekä turvallisen tuotekehityksen standardeja. Webropol on tehnyt tuotekehityksen osalta jatkuvaa, kuukausittaista yhteistyötä toistakymmentä vuotta tietoturva-alan huippuasiantuntijayritysten kanssa. Tällä hetkellä yhteistyökumppanina on KPMG Cyber Security Services. Yhteistyöhon kuuluu lähdekoodin arviointi sekä palvelumme penetraatiotestit ja auditoinnit. Webropol käyttää Cyber Security Services -konsultteja ohjelman tietoturvan testaamiseen. Testeistä saadun tiedon pohjalta voimme kehittää ympäristömme tietoturvaa ja hallita mahdollisia riskejä.

Ote penetraatio- ja auditointilausunnosta

Information Security Statement

During a six (6) week period 2021 F-Secure Cyber Security Services conducted a full verification test of Webropol's web and mobile applications and their underlying platforms. The assessment focused on attempting to hijack users' surveys and the result of the surveys, viewing users' personal information and bypassing authorization, and gain access to accounts with regular and high privileges. It was also assessed that sufficient security controls are in place top revent vulnerabilities listed in OWASP Top 10.

This assessment concluded that the recommended technical changes for Webropol's web applications and platforms had been implemented and no open issues remain therein, leading to tangible advancements in securing the environment. In addition, it's planned to continue monthly assessments of every sprint to verify fixes and assist Webropol into further strengthening its security posture.

The extent of the time period and the number of projects carried out clearly indicate that Webropol is fully committed to the security of their product and pays attention to the security risk mitigation involved in delivering excellent services to their customers.

Fyysinen tietoturva

Webropolin palvelimet sijaitsevat Telia Inmics-Nebula Oy:n korkean tietoturvatason palvelinkeskuksissa Helsingissä. Palvelinkeskuksissa on kahdennetut varavirtalähteet, palosammutusjärjestelmä, tallentava kulunvalvonta ja anti-masking videovalvonta sekä 24/7/365 miehitetty valvonta.

Kaikki kriittiset komponentit (palvelimet, verkko, tallennusjärjestelmät) on kahdennettu erillisiin konesaleihin jatkuvan saatavuuden varmistamiseksi myös tilanteissa, jolloin verkossa tai muussa fyysisessä infrastruktuurissa on häiriötilanteita (Tier 3). Palvelinten hosting-palvelu sekä palvelinkeskukset auditoidaan säännöllisesti ja ne täyttävät esimerkiksi PCIDSS sekä Cloud Security Alliance v3 -vaatimukset.

IPS-ominaisuus Webropolin palomuurissa

IPS (Intruson prevention system) on palomuurin lisäominaisuus josta käytetään myös termiä murron estämisjärjestelmä. Järjestelmä pyrkii ottamaan kiinni vääränkaltaista liikennettä.
IPS:n avulla on mahdollista tunnistaa hyökkäyksiä, ja antaa ennalta määriteltyjä toimintoja näihin. Hyökkäys voi olla esimerkiksi sellainen, jossa yritetään järjestelmällisesti kokeilemalla löytää oikea salasana.
Tällä tavalla voidaan saada kiinni mm. ns. brute force ja 0-päivä hyökkäyksiä.

Tietokanta

Tietokanta on Webropolin omalla palvelimella Telia-Inmics Nebulan korkean tietoturvatason palvelinkeskuksessa.

Kehittyneiden tietoturvauhkien havaitseminen

Webropolilla on käytössä Telia Inmics-Nebulan palvelu**: Managed Detection and Response** (MDR). MDR:n tarkoituksena on havaita kehittyneitä tietoturvauhkia ja kohdistettuja hyökkäyksiä. Webropolin palvelimiin asennetun **Endpoint Detection and Respondent** (EDR) avulla arvioidaan palvelun hallintakäyttöliittymän tietojen perusteella havaitut tietoturvauhkat, analysoidaan ja tehdään tarvittavat toimenpiteet.

Palvelinalustan haavoittuvuusskannaukset ajetaan joka kuukausi Webropol-palvelussa käytettäviin palvelimiin.

Häiriötilanteista palautuminen ja tiedon varmistus

Webropol-palveluiden sisältämät tiedot varmuuskopioidaan päivittäin erilliseen, ammattilaistason varmistusjärjestelmään. Varmuuskopioita ei tehdä siirrettäville medioille tietoturvasyistä. Varmuuskopioita säilytetään 14 päivää. Webropolilla on erillinen jatkuvuus- ja häiriötilannesuunnitelma, jota testataan vuosittain.

IP-osoitteiden säilyminen

Kyselyn vastaajien IP-osoitteet säilyvät web-palvelimen lokissa kaksi (2) viikkoa. Tähän tietoon ei ole pääsyä muilla kuin Webropolin teknisellä tiimillä, emmekä luovuta tietoja eteenpäin kenellekään, edes kyselyn laatijalle.

VPN-yhteys

Webropolin tietoliikenne eri toimipisteiden ja palvelun tuottamiseen osallistuvien työntekijöiden etätyölaitteistoiden VPN-yhteys täyttää tietoturvaluokka TL III -tason vaatimukset.

Euroopan Unionin säätely ja GDPR

Webropol noudattaa toiminnassaan Suomen lainsäädäntöä. Euroopan Unionin jäsenmaana, EU-säädökset on huomioitu. Kaikki palvelun sisältämä tieto on tallennettu EU:n sisällä, eikä sitä missään tilanteessa luovuteta tai käsitellä EU:n ulkopuolella.

Euroopan Unionin yleisen tietosuoja-asetuksen (General Data Protection Regulation, GDPR) soveltaminen alkaa 28.5.2018, mikä yhtenäistää henkilötietojen käsittelyn koko Unionin alueella. Webropol on sitoutunut varmistamaan, että palveluidemme käyttö on asetuksen mukaista ja on kehittänyt palveluun toimintoja, jotka edesauttavat asiakkaidemme toimintaa asetuksen vaatimusten mukaisesti.

Webropol Oy Huovitie 3, 00400 Helsinki, Finland, www.webropol.fi

Lopuksi

Webropol käyttää alan parhaita teknologioita ja käytänteitä suojaamaan asiakkaidemme tietoa luvattomalta käytöltä. Nämä suojaavat toimenpiteet mahdollistavat asiakkaidemme käyttää Webropol-palvelua turvallisella tavalla, taaten kerätyn tiedon saatavuuden, eheyden ja luottamuksellisuuden.

Lisätietoja

Mikäli sinulla on kysymyksiä tai haluat lisää tietoa, ole hyvä ja ota yhteyttä sähköpostitse: servicedesk@webropol.com tai soittamalla paikalliseen Webropol -toimistoon:

Suomi: +358 20 155 2150
Ruotsi: +46 13 470 72 00
UK: +44 1788 833 881
Belgia: +32 2 808 04 30
Saksa: +49 202 94658630

Webropol Oy, Huovitie 3, 00400 Helsinki, Finland www.webropol.fi

Liite 1, OWASP-kuvaus

Tämä on kuvaus siitä, miten vältetään vähintään OWASP Top 10 -julkaisussa (https://owasp.org/www-project-top-ten/) kuvatut tietoturvaongelmat. Lisätietoa löytyy kunkin otsikon takaa löytyvästä linkistä. Vastaavat otsikot löytyvät myös OWASP Top 10 -julkaisun etusivulta.

Tämä kuvaus on liitetty Webropol tietoturvakuvauksen liitteeksi.

Sisällys

1 A01:2021-Broken Access Control

Pääsynhallinta toteutettu Microsoftin .NET frameworkin parhaiden käytäntöjen mukaan. Sovelluksesta lähtee hälytyksiä järjestelmänvalvojille toistuvista virheistä ja haitallisista toiminnoista. Sovelluspalvelimen juuressa ei ole tietoa liittyen git, varmuuskopioihin tai muuhun metadataan. Käyttäjähallinnassa voidaan määrittää käyttäjien pääsy vain tiettyihin resursseihin. Muutoksia voidaan seurata päivämäärä-, kellonaika- ja käyttäjätasolla, jolloin toimintojen jäljittäminen on mahdollista.

Lisätietoa: https://learn.microsoft.com/en-us/aspnet/mvc/overview/security/

2 A02:2021-Cryptographic Failures

Sovellus ei käytä TLS 1.2 vanhempia protokollia ja heikoksi tunnettuja salausmenetelmiä. Sovellus ei ole haavoittuvainen tunnetuille haavoittuvuuksille, kuten: Heartbleed, CCS, Ticketbleed, ROBOT, Secure Renegotiation, Secure-Client-Initiated Renegotiation, CRIME, BREACH, POODLE, TLS_FALLBACK_SCSV, SWEET32, FREAK, DROWN, LOGJAM, BEAST, LUCKY13, Winshock tai RC4.

Webropol käyttää avainten välityksessä Forward Secrecyä (FS). Sovellus tarjoaa seuraavia salausmenetelmiä:

TLSv1.2	0xc030	ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLSv1.2	0xc02f	ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLSv1.2	0x009f	DHE_RSA_WITH_AES_256_GCM_SHA384
TLSv1.2	0x009e	DHE_RSA_WITH_AES_128_GCM_SHA256
TLSv1.3	0x1302	TLS_AES_256_GCM_SHA384
TLSv1.3	0x1303	TLS_CHACHA20_POLY1305_SHA256
TLSv1.3	0x1301	TLS_AES_128_GCM_SHA256
TLSv1.3	0x1304	TLS_AES_128_CCM_SHA256

Sovelluksen käyttämät elliptiset käyrät ovat *prime256v1, secp384r1, secp521r1, X25519 ja X448*, käytössä oleva Diffie Hellman ryhmä on Group 14 (2048-bit) RSA avaimen pituus on 2048 bittiä. Tietokanta on salattu Microsoftin omalla salauksella, joka on Transparent data encryption (TDE). Tietokannan ja sovelluspalvelimen välinen liikenne on salattu.

Lisätietoa: https://learn.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption?view=sql-server-ver16

3 A03:2021-Injection

Käytössä on .NET frameworkin oma input validointikirjasto https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-input-validation

Lisäksi kaikki käyttäjien syötteet ja käyttäjälle palautuva tieto sanitoidaan (sisällön tarkastus). SQL-kyselyissä hyödynnetään valmisteltuja SQL-käskyjä ja kyselyt ovat parametrisoituja.

Lisätietoa: https://en.wikipedia.org/wiki/Prepared_statement

4 A04:2021-Insecure Design

Webropol on suunniteltu Microsoftin .net framework parhaiden käytäntöjen mukaan. Järjestelmä on testattu F-Securen toimesta 2021. Kehitys-, QA- ja tuotantoympäristöt on määritetty samalla tavalla ja tietoturvatestaamista tehdään QA-ympäristössä, jolloin haavoittuvuudet voidaan replikoida ja korjata muissa ympäristöissä. Sovelluksen arkkitehtuuri on segmentoitu käyttäen palomuureja ja kuormantasaajaa. Sovelluksessa on käytössä tietoturvaotsakkeet (security-headers).

Lisätietoa: https://securityheaders.com/?q=https%3A%2F%2Fnew.webropolsurveys.com

Lisätietoa: https://learn.microsoft.com/en-us/aspnet/mvc/

5 A05:2021-Security Misconfiguration

Verkkoliikenne on sallittu vain porttiin 443. Koko ympäristö on kovennettu vuonna 2021 F-securen auditoinnin yhteydessä. Kovennukset tarkistetaan seuraavassa tietoturva-auditoinnissa. Sovellusta testataan kuukausittain mahdollisilta konfiguraatiovirheiltä tai muutoksilta. Sovelluksessa on käytössä tietoturvaotsakkeet (security-headers).

Lisätietoa: https://securityheaders.com/?q=https%3A%2F%2Fnew.webropolsurveys.com

6 A06:2021-Vulnerable and Outdated Components

Palvelinalustan komponentit skannataan ylläpitäjän (3-osapuoli) toimesta. Ylläpitäjä ilmoittaa palvelinalustaan kohdistuvista haavoittuvuuksista ja päivittää alustakomponentit. Sovelluksen komponentit skannataan 4 kertaa vuodessa, komponentit, joissa havaitaan haavoittuvuuksia, päivitetään heti kun mahdollista.

7 A07:2021-Identification and Authentication Failures

Sovellus lukitsee käyttäjätunnukset viiden (5) väärinkirjautumisen jälkeen. Lukitus voidaan poistaa organisaation pääkäyttäjän toimesta. Sovellukseen voidaan myös ottaa 2-vaiheinen tunnistautuminen käyttöön, salasanapolitiikkaa voidaan määrittää asiakasorganisaation haluamalle tasolle.

API-kutsuissa on käytössä myös ”Bearer token”, jolla palvelimelta kysytään resursseja.
https://blog.restcase.com/4-most-used-rest-api-authentication-methods/ .

Sovellukseen voidaan myös kirjautua käyttäen SSO:ta HAKA federoinnilla, jolloin pääsynhallinta on organisaation käsissä.

8 A08:2021-Software and Data Integrity Failures

Sovelluskehityksessä on otettu huomioon OWASP-suositukset. Kirjastojen säilytyspaikat ovat ensisijaisesti luotettuja. Webropol käyttää NuGet (https://www.nuget.org/) .NET kirjastojen asentamiseen. CI/CD puoli on konfiguroitu parhaiden käytänteiden mukaan. Ohjelmistokoodi tarkistetaan staattisesti useamman henkilön toimesta, millä varmistetaan koodin laadun ylläpitäminen. http://www.rharbridge.com/wp-content/uploads/2010/08/Code-Review-Checklist.docx, https://medium.com/c-sharp-progarmming/c-best-practices-and-code-review-checklist-25880d9606, https://security-code-scan.github.io/

Ohjelmistokoodia säilytetään omassa versionhallintajärjestelmässä ja koodistoon on järjestetty pääsynhallinta, mistä Webropol vastaa. Versionhallinnasta voidaan seurata koodistoon tehtyjä muutoksia. Kehitysympäristöt on erotettu tuotantoympäristöstä. Kehitysympäristössä, integraatio- ja hyväksymistestaus on eriytetty.

9 A09:2021-Security Logging and Monitoring Failures

Sovelluksesta lokitetaan kaikki http-kutsut. Sovelluksessa on käytössä audit ja virhelokitus. Palvelinalustassa kerätään myös audit ja IIS -lokit. Virheistä ja haitalliseksi havaituista toiminnoista muodostuu hälytyksiä, johon voidaan reagoida.

10 A10:2021-Server-Side Request Forgery

Sovelluksessa sanitoidaan kaikki käyttäjän kirjaamat syötteet. Sovelluksesta on poistettu käytöstä http-uudelleenohjaukset ja verkkoliikenne on sallittu porttiin 443 (https). Käyttämättömät URL schemat poistetaan käytöstä. Sisäisten palveluiden pääsyrajoitukset on määritetty asianmukaisesti

Webropol Oy:n asiakas- ja käyttäjärekisterin tietosuojaseloste

Tässä tietosuojaselosteessa kerrotaan EU:n tietosuoja-asetuksen ja muun henkilötietolainsäädännön edellyttämiä tietoja henkilötietojen käsittelystä. Tämä seloste koskee kaikkia Webropol-ohjelmiston käyttäjiä sekä prospektirekisteriin tallennettuja henkilöitä.

Rekisterinpitäjä

Webropol Oy
y-tunnus: 1773960-2
Huovitie 3, 00400 Helsinki
0201 552 150 | servicedesk@webropol.fi

Yhteydenotot tietosuoja-asioissa osoitteeseen

Webropol Oy
Tietosuojavastaava
Huovitie 3, 00400 Helsinki
tietosuojavastaava@webropol.com

Rekisterin nimi

Webropol Oy:n asiakas- ja käyttäjärekisteri.

Henkilötietojen käsittelyn tarkoitus

Henkilötietojen käsittelyn perusteena on Webropolin ja asiakkaan välinen asiakassuhde tai asiakkaan antama suostumus henkilötietojen käsittelyyn.

Kerättäviä henkilötietoja käytetään palvelumme käyttäjien asiakassuhteiden ylläpitoon ja hoitoon sekä palvelun edellyttämien yhteydenottojen mahdollistamiseen. Tietoja voidaan käyttää myös Webropolin markkinoinnin toteuttamiseen kuten esimerkiksi yhteydenottoihin puhelimitse ja sähköpostilla.

Rekisterin tietosisältö

- Etu- ja sukunimi
- Puhelinnumero
- Sähköpostiosoite
- yrityksen/yhteisön osoite (vain pääkäyttäjiltä)
- yrityksen/yhteisön Y-tunnus (vain pääkäyttäjiltä)
- osaston nimi
- ostotapahtuma- ja laskutustiedot
- Asiakassuhteen alkamispäivä
- Asiakassuhteen hoidon aikana merkityt tiedot
- Palvelutapahtumat

Säännönmukaiset tietolähteet

Tiedot hankitaan Webropol-ohjelmiston käyttäjiltä heidän suostumuksellaan tai asiakasorganisaation Webropol-pääkäyttäjiltä. Annettuja yhteystietoja ei luovuteta muille osapuolille. Henkilötietoja voidaan päivittää henkilötietoja koskevia palveluja tarjoavilta viranomaisilta ja yrityksiltä.

Tietoryhmien poistamisen määräajat

Asiakassuhteen päättymisen jälkeen varmuuskopioita kaikesta asiakkaan käyttöympäristön sisältämästä tiedosta (ml. käyttäjien henkilötiedot) säilytetään 1 kuukauden ajan. Tämän jälkeen tiedot poistetaan. Asiakkaan poistaessa yksittäisen käyttäjän tai kyselyn järjestelmästä, säilyvät tiedot varmuuskopiossa 1 kuukauden ajan.

Webropol toteuttaa henkilötietojen välittömän poistamisen kohtuullisessa ajassa aina asiakkaan sitä pyytäessä, mikäli poistaminen on vain teknisesti mahdollista.

Tietojen siirto kolmanteen maahan

Webropol ei missään tilanteessa siirrä tai käsittele henkilötietoja EU:n tai ETA:n ulkopuolella.

Kuvaus teknisistä ja organisatorisista turvatoimista

Sähköisessä muodossa olevat henkilötiedot on suojattu toimialalla yleisesti hyväksyttävin ja kohtuullisin teknisin keinoin kuten palomuurein ja salasanoin. Muut kuin sähköisessä muodossa olevat rekisterin henkilötietoja sisältävät aineistot sijaitsevat lukituissa tiloissa, joihin asiattomilta on pääsy estetty.

Nimetyillä Webropolin asiakastuen, teknisen henkilöstön ja tutkimuspalveluiden henkilöillä on pääsy henkilötietoihin. Kullakin määrätyllä käyttäjällä on voimassaoleva ja sitova salassapitosopimus sekä oma henkilökohtainen käyttäjätunnus ja salasana. Jokainen käyttäjä on saamistaan tiedoista vaitiolovelvollinen salassapitosopimuksen nojalla.

Webropolin lisäksi rekisterinpitäjän lukuun käsittelytoimia voivat suorittaa Webropolin erikseen määrätyt alihankkijat. Alihankkijat noudattavat käsittelytoimissa samoja vaatimuksia kuin Webropol. Ajantasaiseen listaukseen alihankkijoista pääset tästä.

Tarkastusoikeus, oikeus oikaista virheellinen tieto ja oikeus tulla unohdetuksi

Rekisteröidyllä on Euroopan parlamentin ja neuvoston yleisen tietosuoja-asetuksen (GDPR) artiklan 15 mukaisesti oikeus tarkastaa, mitä häntä koskevia tietoja henkilörekisteriin on talletettu sekä artiklan17 mukaisesti vaatia häntä koskevien virheellisten tietojen korjaamista ja / tai tietojen poistamista rekisteristä. Rekisteröity voi milloin tahansa kieltää henkilötietojensa käsittelyn markkinointitarkoituksiin. Kun rekisteröity ei halua, että hänen tietojaan enää käsitellään, hänellä on oikeus vaatia kaikkien tietojen poistamista.

Lisätietoa >>

Tietopyynnöt tulee lähettää kirjallisesti sähköpostilla tai paperipostilla Webropol Oy:lle:
Webropol Oy, Huovitie 3, 00400 Helsinki. Sähköposti: servicedesk@webropol.fi