TIETOTURVASELVITYS

17.5.2018 - Julkinen

Janne Parri

Mysteeri Experience Oy

Sisältö

Johdanto **3**

Määritelmät **4**

Riskiarvio **5**
Henkilöstö *5*
Tietoturva-arkkitehtuuri *5*
Tietojen säilyttäminen ja käyttö *5*
Sovellukset ja ohjelma *6*
Käyttöympäristö (palvelimet, työasemat) *6*
Fyysinen ympäristö *6*
Ulkoisten palveluiden käyttö *6*

Henkilötiedot **7**
Henkilötietojen kerääminen *7*
Henkilötietojen säilyttäminen *7*
Rekisterit 8
Varmuuskopiot 9
Automaattinen poistaminen 9
Henkilötietojen käsitteleminen *10*
Henkilötietojen käsittelijät 10
Henkilötietojen käsittelypaikat ja -laitteet 10
Henkilötietojen päivittäminen 10
Henkilötietojen poistaminen pyydettäessä 11

Evästeet **12**
Verkkosivuston toiminnallisuus ja sisältö *12*
Verkkosivuston analysointi *13*

Tietoturvakäytänteet **14**
Käytänteet henkilötietojen käsittelyyn *14*
Laitteet *14*
Salasanakäytänteet *14*
Toimistokäytänteet *15*
Tietoturvatilinpäätös *15*

Tietoturvaloukkaukset **16**

Koulutukset **17**

Sopimukset **17**

Johdanto

Tämä on Mysteeri Experience Oy:n julkinen tietoturvaselvitys. Sen tarkoitus on valottaa, miten asiakkaiden henkilötietoja käsitellään ja kuinka tietoturva varmistetaan kyseisessä yrityksessä.

Määritelmät

Tässä asiakirjassa käsiteltävät termit ovat määritelty henkilötietolain (22.4.1999/523) mukaisesti.

1) *henkilötiedolla* kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi;

2) *henkilötietojen käsittelyllä* henkilötietojen keräämistä, tallettamista, järjestämistä, käyttöä, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista, tuhoamista sekä muita henkilötietoihin kohdistuvia toimenpiteitä;

3) *henkilörekisterillä* käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä muodostuvaa henkilötietoja sisältävää tietojoukkoa, jota käsitellään osin tai kokonaan automaattisen tietojenkäsittelyn avulla taikka joka on järjestetty kortistoksi, luetteloksi tai muulla näihin verrattavalla tavalla siten, että tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja kohtuuttomitta kustannuksitta;

4) *rekisterinpitäjällä* yhtä tai useampaa henkilöä, yhteisöä, laitosta tai säätiötä, jonka käyttöä varten henkilörekisteri perustetaan ja jolla on oikeus määrätä henkilörekisterin käytöstä tai jonka tehtäväksi rekisterinpito on lailla säädetty;

5) *rekisteröidyllä* henkilöä, jota henkilötieto koskee;

6) *sivullisella* muuta henkilöä, yhteisöä, laitosta tai säätiötä kuin rekisteröityä, rekisterinpitäjää, henkilötietojen käsittelijää tai henkilötietoja kahden viimeksi mainitun lukuun käsittelevää;

7) *suostumuksella* kaikenlaista vapaaehtoista, yksilöityä ja tietoista tahdon ilmaisua, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn.

Riskiarvio

Tietoturvariskejä arvioidaan potentiaalisten ongelmien analyysillä. Ongelmat ovat jaoteltu henkilöriskeihin, tietoturva-arkkitehtuuriin, tietojen säilyttämiseen ja käyttöön, sovelluksiin ja ohjelmiin, käyttöympäristöön (palvelimet, työasemat), fyysiseen ympäristöön, ulkoisten palveluiden käyttöön sekä hankintoihin.

Henkilöstö

Suurimmat riskit

- Työntekijä välittää henkilötietoja vahingossa väärille henkilöille.
- Henkilötietoihin murtaudutaan työntekijän laitteen kautta.
- Työntekijä välittää tarkoituksella henkilötietoja väärille henkilöille.

Toimenpiteet riskien välttämiseksi

- Työntekijällä on pääsy vain hänelle olennaisiin henkilötietoihin.
- Henkilötietojen käsittely rajoitetaan vain suojatuille laitteille.
- Henkilöstö koulutetaan tietoturvakäytänteistä.

Tietoturva-arkkitehtuuri

Suurimmat riskit

- Tietoturvaa ohjaava ohjeisto ja prosessit ovat vajaavaiset.
    - Työntekijät eivät saa tarpeellista koulutusta.
    - Käytänteitä ei noudateta.
    - Prosesseja ei tarkastella säännöllisesti.
- Tietoturvaa ei oteta vakavasti.

Toimenpiteet riskien välttämiseksi

- Tietoturvakäytänteet dokumentoidaan ja ne tarkastetaan säännöllisesti.
- Nimetään tietoturvavastaava, joka ei kuulu yrityksen johtoryhmään.
- Tietoturvakoulutus on osa työntekijän perehdytystä ja tietoturvaprosessia.

Tietojen säilyttäminen ja käyttö

Suurimmat riskit

- Henkilötiedot katoavat järjestelmävirheen vuoksi.
- Tietoa vuotaa, kun sitä siirretään järjestelmästä toiseen.
- Henkilötietoihin murtaudutaan niitä käytettäessä.
- Henkilötietoihin murtaudutaan järjestelmävirheen vuoksi.

Toimenpiteet riskien välttämiseksi

- Järjestelmät, joilla henkilötietoja käsitellään, päivitetään säännöllisesti.
- Henkilötietojen käyttö rajataan vain suojattuihin laitteisiin.
- Omat verkkosivut pidetään ajan tasalla ja suojattuna.
- Yhteistyökumppaneilta vaaditaan korkeat tietoturvastandardit.

Sovellukset ja ohjelma

Suurimmat riskit

- Ohjelmassa olevan tietoturvariskin takia, henkilötietoja vuotaa.
- Henkilötiedot katoavat ohjelmassa olevan virheen vuoksi.
- Tietoa vuotaa, kun sitä siirretään ohjelmasta toiseen.

Toimenpiteet riskien välttämiseksi

- Ohjelmistot pidetään ajan tasalla.
- Henkilötietojen käyttö rajataan vain suojattuihin laitteisiin.

Käyttöympäristö (palvelimet, työasemat)

Suurimmat riskit

- Henkilötietoja vuodetaan vanhentuneiden käyttöjärjestelmien takia.
- Henkilötietoja vuodetaan palvelimelta.
- Henkilötietoja vuodetaan mobiililaitteista.
- Henkilötietoja vuodetaan Wlan-verkon kautta.

Toimenpiteet riskien välttämiseksi

- Järjestelmät, joilla henkilötietoja käsitellään, päivitetään säännöllisesti.
- Henkilötietojen käyttö rajataan vain suojattuihin laitteisiin.
- Yhteistyökumppaneilta vaaditaan korkeat tietoturvastandardit.
- Wlan-verkot piilotetaan ja niiden suojauksesta huolehditaan.

Fyysinen ympäristö

Suurimmat riskit

- Sähkölukkoihin päästään käsiksi tietokoneiden kautta.
- Henkilötietoihin päästään käsiksi murtautumalla toimitiloihin.
- Asiakastietoja löytyy työntekijöiden muistiinpanoista.

Toimenpiteet riskien välttämiseksi

- Sähkölukot eivät ole yhdistettyinä tietokoneisiin tai internettiin.
- Tietokoneet suojataan salasanoilla, jotka eivät ole nähtävillä toimistoympäristössä.
- Jokaiselle toimipisteellä on silppuri asiakastietoja sisältäviä muistiinpanoja varten.

Ulkoisten palveluiden käyttö

Suurimmat riskit

- Ulkoiset palveluntarjoajat joutuvat tietoturvahyökkäyksen kohteeksi.

Toimenpiteet riskien välttämiseksi

- Yhteistyökumppaneilta vaaditaan korkeat tietoturvastandardit.

Henkilötiedot

Henkilötietojen käsittelyä uudistetaan 25.5. mennessä siten, että se vastaa kaikkia voimassaolevia lakeja ja asetuksia. Käytännössä tämä merkitsee ylimääräisten rekisterien poistamista, markkinointilupien varmistamista ja tietoturvakäytänteiden uudistamista.

Henkilötietojen kerääminen

Henkilötietoja kerätään neljällä tapaa.

- Varausjärjestelmä (Asiakas jättää varauksen Slottiin)
- Verkkosivujen lomakkeet
  (Asiakas jättää yhteydenottopyynnön tai tilaa uutiskirjeen)
- Kysymällä henkilökohtaisesti asiakkaalta (Työntekijä kysyy, haluaako asiakkaat liittyä kanta-asiakaskerhoon)
- Verkkokauppa (Asiakas ostaa tuotteen verkkokaupasta)

Henkilötietoja kerättäessä henkilöllä on oltava ymmärrys, mitä varten hänen tietoja kerättään ja miten Mysteeri Experience Oy tulee säilyttämään ja käsittelemään näitä tietoja.

Verkossa tehtävän varauksen yhteydessä asiakas hyväksyy asiakastietojen säilyttämisen ja käsittelyn rekisteriselosteen mukaisella tavalla.

Verkkosivujen lomakkeet osoittavat tiedonkeruun tarkoituksen selkeästi. Joissain tapauksissa asiakkaalle lähetetään vahvistusviesti, johon hänen on reagoitava, jotta tiedot säilytetään ja viestintää jatketaan (esimerkiksi uutiskirjeen tilaus).

Henkilökunta koulutetaan keräämään henkilötiedot, siten että asiakkaalla on ymmärrys siitä, mihin heidän tietoja käytetään. Tämän jälkeen työntekijä itse syöttää nämä tiedot järjestelmiin, joista lähetehään vahvistusviesti asiakkaille.

Henkilötietojen säilyttäminen

Henkilötietorekisterin tiedot säilytetään seuraavalla tavalla.

1. Ensisijainen säilytyspaikka on varausjärjestelmän Slotti (Teones Oy)
2. ActiveCampaign on ensisijaisesti sähköpostien lähettämistä varten.
   (Siellä ei säilytetä henkilötietoja, ellei asiakas ole esimerkiksi tilannut uutiskirjettä tai muita aiheita sähköpostiinsa.)
3. Varmuuskopiot tehdään säännöllisesti Dropbox-palveluun
4. Kanta-asiakasrekisteri tallennetaan ActiveCampaigniin ja sen varmuuskopio on Google Sheets palvelussa.

Rekisterit

Mysteeri Experience Oy:n asiakasrekisteri

- Rekisterin pitäjä: Mysteeri Experience Oy
- Reksiterin nimi: Mysteeri Experience Oy:n asiakastietorekisteri
- Rekisteriseloste
- Sisältö:
    - nimi,
    - sähköposti,
    - puhelinnumero,
    - varatut palvelut ja niiden tiedot,
    - yritys,
    - laskutustiedot,
    - verkkokaupasta ostetut tuotteet,
    - vapaaehtoinen lisätietokenttä
- Käyttötarkoitus:
    - Varausvahvistusten ja muistutuksien lähettäminen,
    - asiakassuhteen hoitaminen ja kehittäminen,
    - palvelun toteuttaminen,
    - asiakastapahtumien varmentaminen ja niistä muistuttaminen,
    - analysointi ja tilastointi,
    - mielipide- ja markkinatutkimukset,
    - markkinointi
    - muut vastaavat käyttötarkoitukset.
- Sijainti
    - Slotti-varausjärjestelmä (Teonos Oy)
        - Ensisijainen käyttötarkoitus: Varausten vastaanotto ja hallinnointi
        - Sopimus asiakastietojen hallinnasta on luotu
        - Suojaus: salasanoilla ja suojatulla yhteydellä
        - Teonos Oy:n oma rekisteriseloste
    - Mysteeri.com-verkkosivut (Wordpress)
        - Ensisijainen käyttötarkoitus: Verkkokauppa tilauste vastaanotto ja hallinnointi
        - Suojaus: salasanoilla ja suojatulla yhteydellä
        - Suomen Hostingpalvelu Oy:n oma rekisteriseloste
    - ActiveCampaign
        - Ensisijainen käyttötarkoitus: Uutiskirjeen lähettäminen,
        - Suojaus: salasanoilla ja suojatulla yhteydellä
    - Paytrail kauppiaspaneeli
        - Ensisijainen käyttötarkoitus: Verkkokaupan maksuliikenteen toteuttaminen,
        - Suojaus: salasanoilla ja suojatulla yhteydellä

Mysteeri-illallinen asiakasrekisteri

- Rekisterin pitäjä: Mysteeri Experience Oy
- Reksiterin nimi: Mysteeri-illallisten asiakastietorekisteri
- Sisältö: nimi, sähköposti, puhelinnumero, osoite, verkkokaupasta ostetut tuotteet, vapaaehtoinen lisätietokenttä
- Suojaus: Salasanoilla ja suojatulla yhteydellä
- Käyttötarkoitus:
    - asiakassuhteen hoitaminen ja kehittäminen,
    - palvelun toteuttaminen,
    - asiakastapahtumien varmentaminen ja niistä muistuttaminen,
    - markkinointi,
    - analysointi ja tilastointi,
    - mielipide- ja markkinatutkimukset sekä
    - muut vastaavat käyttötarkoitukset.
- Sijainti
    - Mysteeri.com-verkkosivut (Wordpress)
        - Ensisijainen käyttötarkoitus: Varausten vastaanotto ja hallinnointi
        - Suojaus: salasanoilla ja suojatulla yhteydellä
        - Suomen Hostingpalvelu Oy:n oma rekisteriseloste
    - ActiveCampaign
        - Ensisijainen käyttötarkoitus: Uutiskirjeen lähettäminen,
        - Suojaus: salasanoilla ja suojatulla yhteydellä

Varmuuskopiot

Dropbox

- Rekisterin pitäjä: Mysteeri Experience Oy
- Reksiterin nimi: Mysteeri Experience Oy:n asiakastietorekisterien varmuuskopio
- Sisältö: nimi, sähköposti, puhelinnumero, osoite, varatut ajat, verkkokaupasta ostetut tuotteet, vapaaehtoisten lisätietokenttien sisällöt
- Suojaus: Salasanoilla ja suojatulla yhteydellä (tietoturvaseloste)
- Käyttötarkoitus:
    - asiakastietojen säilyttäminen ja organisointi,
    - palvelun toteuttaminen,
    - asiakastapahtumien varmentaminen,
    - analysointi ja tilastointi,

Automaattinen poistaminen

Mikäli henkilö on ollut passiivisena 26 kuukautta, hänen tietonsa poistetaan tai anonymisoidaan. Toisin sanoen varaus- ja maksutapahtumat säilyvät, mutta niihin yhdistettävät henkilötiedot poistetaan.

Henkilötietojen käsitteleminen

Henkilötietojen käsittelijät

Mysteerin työntekijöistä kaikki käsittelevät henkilötietoja. Tämä siksi, että jokainen vastaa asiakaspalvelusta ja kaikilla on näin oltava mahdollisuus lisätä tai päivittää henkilötietoja. Mysteeri pitää huolen siitä, että kaikki työntekijät ovat koulutettu noudattamaan tietoturvakäytänteitä.

Prosessikuvaukset ja työntekijöiden koulutus käsitellään myöhemmin.

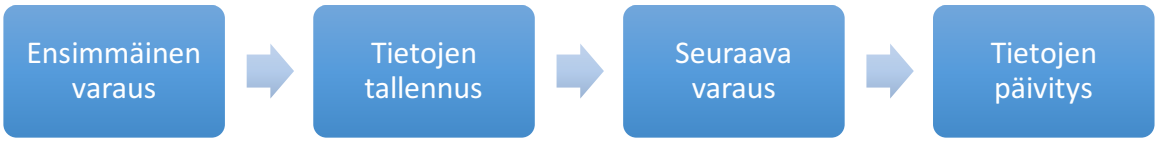
Henkilötietojen käsittelypaikat ja -laitteet

Henkilötietoja ei voi käsitellä koneella tai laitteella, joissa ei ole tietoturvakäytänteiden mukaisia ohjelmia ja tehtyjä toimenpiteitä. Tietoturvavastaava tarkistaa työpaikkojen koneet ja antaa tai evää luvan käsitellä henkilötietoja henkilökohtaisilla laitteilla.

Lähtökohtaisesti vain täysipäiväisillä työntekijöillä on oikeus tarkastella henkilötietorekistereitä heidän omilla laitteillaan. Muut työntekijät voivat tarkastella varauksia kalenterien kautta, mutta siten, että niistä on poistettu henkilötiedot.

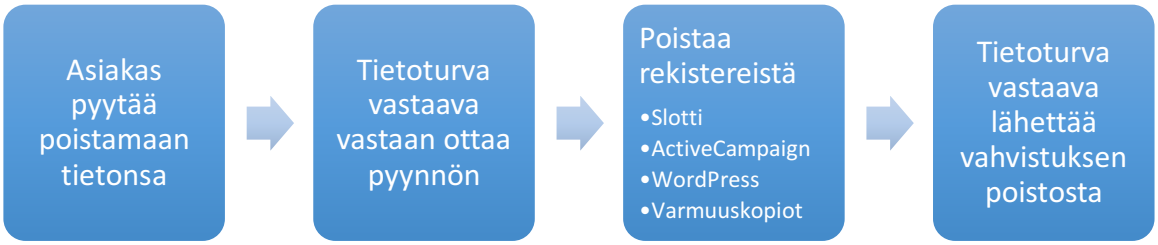
Henkilötietojen päivittäminen

Henkilötiedot päivitetään uuden varauksen tai yhteydenoton yhteydessä sekä asiakkaan sitä pyytäessä. Tiedot päivitetään ensisijaisesti Slotti- ja ActiveCampaign-järjestelmiin. Varmuuskopioihin ne päivittyvät kuukauden sisällä.



Henkilötietojen poistaminen pyydettäessä

Mikäli asiakas pyytää poistamaan hänen tietonsa, tehdään se manuaalisesti kaikista henkilötietorekistereistä tietoturvavastaavan toimesta. Tietoturvavastaava pyytää myös varauksen käsittellyttä henkilöä tarkistamaan oman sähköpostinsa ja muistiinpanonsa.

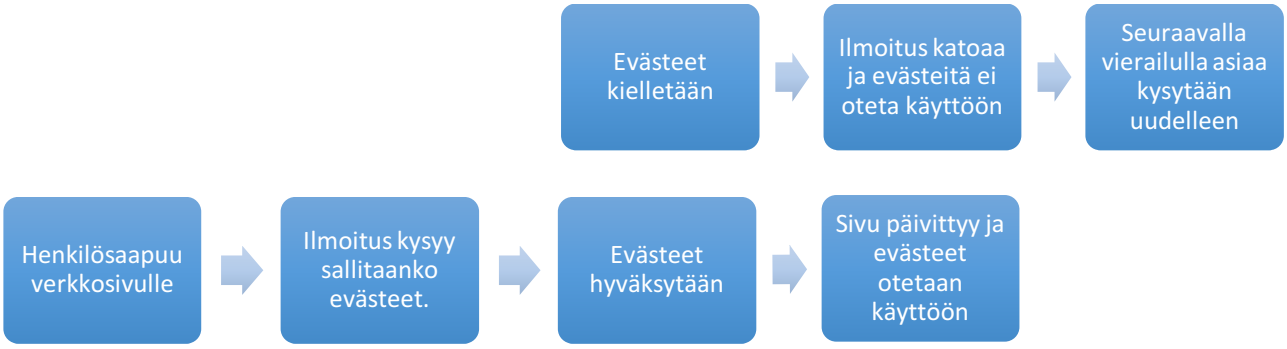


Evästeet

Käytämme evästeitä verkkosivuillamme pyytämiesi palveluiden tarjoamiseen. Näihin palveluihin kuuluvat käyttäjän sisäänkirjautuminen, ostoskorin sisällön hallinta, kieliasetusten asettaminen ja suojaukset, jotka ovat olennaisen tärkeitä sivuston käyttämisessä. Seuraamme myös eri lomakkeiden lähetyksiä ja sivukohtaista skrollausta.

Käyttäjälle tarjotaan mahdollisuus ei välttämättömien evästeiden hylkäämiseen hänen tullessa verkkosivuille. Näitä ei välttämättömiä evästeitä ovat:

- Google Tag Manager (evästeiden hallinta)
- Google Analytics (liikenteen analysointi & markkinointi)
- Google Optimize (konversio-optimointi)
- Facebook Pixel (liikenteen analysointi & markkinointi)
- ActiveCampaign (sähköpostiautomaatio)



Verkkosivuston toiminnallisuus ja sisältö

Jakamistoiminnolla vierailijat voivat suositella verkkosivustojamme ja sisältöämme sosiaalisissa verkoissa, kuten Facebookissa ja Twitterissä. Evästeet tallentavat tietoa vierailijoiden jakamistoiminnon käytöstä – ei kuitenkaan käyttäjäkohtaisesti – verkkosivuston parantamiseksi. Jos et salli evästeitä, mitään tietoja ei tallenneta.

Käytämme kolmannen osapuolen toimittajia joissakin verkkosivustomme toiminnoissa, esimerkiksi silloin, kun vierailet sivustolla, jossa on YouTube-sivuston videoita tai linkkejä niihin. Kyseiset videot tai linkit (ja muu kolmansien osapuolien sisältö) voivat sisältää kolmannen osapuolen evästeitä ja niiden käytöstä saa lisätietoa kolmannen osapuolen verkkosivuston evästekäytännöstä.

Verkkosivuston analysointi

Tämä verkkosivusto käyttää Google Analytics ja Facebook analytics -ohjelmia, joka käyttää evästeitä. Evästeet tallentavat tietoa yhteen kerätyssä muodossa verkkosivuston käyttäjien toiminnoista, näihin tietoihin kuuluvat avattujen sivujen määrä, mistä vierailija tulee verkkosivustolle sekä vierailujen määrä.

Kyseisten evästeiden kautta saamme tietoomme myös sivulla käyneiden henkilöiden ikään, sukupuoleen ja kiinnostuksen kohteiseen liittyviä tietoja. Kaikkia edellä mainittuja tietoja käytetään verkkosivuston parantamiseen, hyvän käyttäjäkokemuksen takaamiseen ja mainosyleisöjen luomiseen. Jos et salli evästeitä, mitään tietoja ei tallenneta.

Voit lukea evästepolitiikkamme myös täältä:
https://www.mysteeri.com/keksipolitiikka/

Tietoturvakäytänteet

Käytänteet henkilötietojen käsittelyyn

Henkilötietoja käsitellään niille tarkoitetuilla laitteilla. Yksilöiviä tietojen sisällyttämistä rekisterin ulkopuolisiin järjestelmiin vältetään. Näitä järjetelmiä ovat mm.:

- Sähköposti
- Workplace chat
- Evernote
- Google Sheets
- Excel

Laitteet

Henkilötietoja käsittelevän henkilön on käytettävä tietoturvavaltuutetun hyväksymää laitetta, jossa on ajantasainen virustorjunta ja palomuuri. Myös käyttöjärjestelmät tulee päivittää mahdollisimman nopeasti uusimpiin versioihin.

Salasanakäytänteet

Salasanat muodostavat Mysteerille kenties suurimman tietoturvariskin. Tämän takia rekisterit suojataan usealla tasolla.

1. Laitteen salasana tai pääsykoodi/kuvio (henkilö- ja laitekohtainen)
2. Salasanan hallintaohjelman salasana (henkilökohtainen)
3. Järjestelmän salasana (henkilökohtainen tai jaettu salasananhallintaohjelmassa)
4. Kaksinkertainen kirjautuminen (tietyt järjestelmät ja ylimmän tason tunnukset)

Kaksivaiheista kirjautumista käytetään mahdollisuuksien mukaan eri alustoilla. Näistä tärkeimmät ovat Google ja Dropbox.

Jaetut salasanat uusitaan kahden kuukauden välein ja henkilökohtaiset salasanat neljän kuukauden välein.

Henkilötietoja sisältävien rekisterien salasanoja ei tallenneta selainten muistiin ikinä. Niitä voi kuitenkin säilyttää salasananhallintaohjelmassa halutessaan.

Tarkistukset toteutetaan tietoturvavastaavan toimesta pistotarkistuksina, mutta vähintään puolivuosittain.

Toimistokäytänteet

Toimistolla huolehditaan tietoturvasta lukitsemalla huone (mikäli mahdollista), jossa asiakastietoja käsitellään. Lisäksi jokaisella toimipisteellä on silppuri ja fyysisiä muistiinpanoja ei säilytetä pidempää kuin on tarpeen.

Tietoturvatilinpäätös

Tietoturvavastaava laatii tietoturvatilinpäätöksen neljännesvuosittain. Se sisältää mm. seuraavat asiat.

- mitä tietovarantoja organisaation hallussa on?
- mikä on organisaation tietoarkkitehtuuri?
- mikä on organisaation hallussa olevien tietojen laatu ja käytettävyys?
- mitä menettelytapoja ja periaatteita tietojen käsittelyssä noudatetaan?
- miten tiedot on suojattu?
- miten tietojen käyttöä valvotaan?
- miten rekisteröityjen oikeudet tietojen käsittelyssä toteutetaan?

Tietoturvaloukkaukset

Erilaisista tietoturvaloukkauksista ilmoitetaan mahdollisimman nopeasti asianosaisille. Ehdoton takaraja ilmoitukselle on 72 tuntia sen toteutumisesta. Tämä tarkoittaa, että henkilötietojen käsittelijän on viipymättä ilmoitettava rekisterin ylläpitäjälle ja tietoturvavastaavalle mahdollisista loukkauksista. Ilmoitus tehdään ensisijaisesti sähköpostilla, mutta mikäli se koskee pienempiä ryhmiä, voidaan käyttää myös muita keinoja.

Koulutukset

Uudet työntekijät koulutetaan tietoturvavastaavan toimesta noudattamaan tietoturvakäytänteitä ja tunnistamaan riskitekijöitä.

Sopimukset

Mysteeri Experience Oy on solminut sopimukset henkilötietoja käsittelevien yhteistyötahojen kanssa. Näillä sopimuksilla varmistetaan, että yhteistyötahot säilyttävät ja käsittelevät henkilötietoja turvallisesti ja vain silloin kuin siihen on todellinen tarve.

Henkilötietoja käsittelevät tahot

- Teneos Oy
- Paytrail Oyj
- ActiveCampaign
- Suomen Hostingpalvelu Oy