

Kuinka Sharebook suojaa tietosi

Uusi Tietosuoja-asetus GDPR

EU:n uusi tietosuoja-asetus astuu voimaan 25. toukokuuta 2018. EU:n koordinoitussa ja harmonisoidussa lainsäädäntöä henkilötietosuojaan liittyen, tulee yksittäisille henkilöille EU:ssa helpommaksi tietää ja tunnistaa omat oikeutensa. Sama lainsäädäntö koskee henkilötietojen käsittelyä kaikissa maissa, joissa käsitellään EU-kansalaisten henkilötietoja.

Sharebook ohjelma on mukautettu näihin uudistuksiin täyttääkseen tietosuojavaatimukset ja prosessit asetuksen edellyttämällä tavalla.

Mitä sinun tulee tietää Sharebookin käyttäjänä?

Sinä ja organisaatiosi toimitte rekisterinpitäjinä kerätessänne ja käsitellessänne tietoja (fyysisistä) henkilöistä. Sharebook on tekninen alusta, joka auttaa teitä käsittelemään tietoja tarkoituksenne mukaisesti.

Täten teidän tulee tehdä selväksi rekisteröidyillenne miksi te haluatte kerätä henkilötietoja, ja mihin tarkoitukseen niitä käytetään.

Tämän toteutate laatimalla rekisterikuvauksen (lisätietoja osoitteesta www.tietosuoja.fi), jossa ilmoitatte esimerkiksi kuka vastaa tietojen keräämisestä, sekä miksi ja miten tietoja kerätään ja käsitellään. Rekisterikuvauksen tulee olla saatavilla rekisteröityjen tarkasteltavaksi. Helpoiten mahdollistatte tämän julkaisemalla rekisterikuvauksen verkkosivuillette tai lähettämällä sen rekisteröidyillenne.

Teidän tulee esimerkiksi ilmoittaa, mikäli jostain syystä luovutate keräämiänne henkilötietoja jollekin toiselle osapuolelle markkinointi- tai jossain muussa tarkoituksessa. Teidän tulee myös kertoa, kuinka kauan säilytätte tietoja, ja kuinka rekisteröity voi tarkastella ja mahdollisesti muuttaa tietojään.

Vastaatte toisin sanoen siitä, että:

1. Teillä on oikeus kerätä kyseisiä tietoja ja että oikeus on perusteltu (esim. sopimuksen mukaista laskutusta varten).
2. Keräätte sellaisia tietoja, jotka ovat tarpeen. Ei sitä enemmän, eikä vähemmän.
3. Teillä on korrekrit tiedot rekisteröidystä ja poistatte sellaiset henkilötiedot, jotka eivät enää ole tarpeen.
4. Voitte todistaa rekisteröidylle oikeutenne säilyttää henkilötietoja, sekä esittää mitä tietoja henkilöstä teillä on rekisterissä.
5. Käsittelette henkilötietoja asianmukaisesti ja suojatusti.

Rekisterinpitäjänä olette vastuussa uuden tietosuoja-asetuksen ja sen sisällön tuntemisesta. Asetuksen koskiessa kaikkia EU-maita ja niiden kansalaisia, löytyy netistä valtava määrä tietoa sekä suomen-, ruotsin-, että englanninkielellä. Kannattaa siis pitää itsensä ajan tasalla.

Säännöt ja suositukset voivat osittain riippua edustamastanne toimialasta. Suosittelemme olemaan yhteydessä lakimieheenne tai toimialaliittoonne saadaksenne tarkempaa ohjausta juuri teidän tilanteeseenne. Joidenkin organisaatioiden tulee suorittaa riskiarviointeja ja nimittää henkilötietoasiamies (DPO), mikäli tietojen kerääminen on laaja-alaista tai koskee tiettyjä alueita, joiden arvioidaan olevan arkaluontoisia (esim. terveys- ja sairaanhoito).

Tässä helppo muistilista päästäksesi eteenpäin



Mitä muita ohjelmia ja palveluja käytätte?

On myös tärkeää, että organisaatiosi dokumentoi mitä eri tyyppisiä järjestelmiä, ohjelmia ja prosesseja käytätte henkilötietojen keräämiseen ja käsittelemiseen.

Sharebookin yleisistä käyttöehdoista voit lukea vastuun jakautumisesta koskien henkilötietojen käsittelyä, kun käytätte Sharebookin palveluita.

Käyttäessänne muita ohjelmistotoimittajia henkilötietojen käsittelemiseen tai tallentamiseen, tulee teidän laatia **tietojenkäsittelysopimus** heidän kanssaan varmistaaksenne, että toimittaja noudattaa tietosuojasetusta ja teidän ohjeistustanne.

Sharebook ja tietosuoja

Me Sharebookin kanssa työskentelevät painotamme kaikessa toiminnassamme tietoturvaa, yksilöiden yksityisyyden suojaa sekä käyttäjäturvallisuutta. Kaikki työntekijämme ovat hyväksyneet salassapitosopimuksen, ja noudattavat yrityksemme sisäisiä tietosuoja- ja laatulinjauksia sekä ohjesääntöjä.

Alla luemme lyhyesti ne toimenpiteet ja käytännöt, joita seuraamme dataympäristömme tietoturvan ja jatkuvuuden varmistamiseksi.

Fyysinen ympäristö

Alusta on asennettu kahteen, maantieteellisesti toisistaan erilliseen palvelinsaliin. Salit on yhdistetty kuituliittymällä toisiinsa ja Gpbs kaistanleveydellä Internetiin.

Sähkönjakelu on viimeistelty keskeytymättömällä virransyötöllä (UPS), sekä dieselgeneraattorilla jatkuvuuden varmistamiseksi.

Kaikki palvelimet sisältyvät yrityksen ylläpitojärjestelmään, jossa päivitysrutiinit, tietoturvatarkastukset, tietosuojavalvonta ja muut turvallisuusrutiinit ovat huomioituina.

Tavanomaiset päivitykset hoituvat juoksevasti aikataulun mukaan ja kattava ratkaisumme huolehtii siitä, että suurin osa näistä voidaan asentaa ilman käyttökatkoja.

Varmuuskopiot

Koko ympäristö varmuuskopioidaan päivittäin kahteen erilliseen palvelinsaliin siten, että koko ympäristö ja kaikki siihen sisältyvä data löytyy varmuuskopioituna kummastakin hallista.

Kuukausittaiset varmuuskopiot säilötään 3-2-1 strategian mukaisesti. Tällä tarkoitetaan sitä, että varmuuskopiosta on kolme jäljennöstä, joista kaksi löytyy paikallisesti palvelinsaleista, ja kolmas tallenne säilötään palvelinsalien ulkopuolella.

Varmuuskopioista viedään vuosittain kopiot pankin tallelokeroon, jossa niitä säilötään 10 vuotta.

Kuorivalvonta

Kuorivalvontaan sisältyy murto- ja palohälytys, sekä lämpötilan valvonta. Vain asianmukaisella henkilökunnalla on pääsy saleihin. Saleihin pääsy edellyttää sähköistä kulkulupaa/avainkoodia.

Tieturva ja ylläpito

Palvelinympäristö on turvattu ylimääräisin IPS-suojatuin (Intrusion Prevention System) palomuurein, jotka tunnistavat eri tyyppiset hyökkäykset ja tunkeutumisyrietykset. Ympäristö on myös suojattu paikallisin palomuurein jokaisella palvelimella.

Ympäristöä valvontaan vuorokauden ympäri saatavuuden varmistamiseksi ja mahdollisten turvallisuusriskien tunnistamiseksi. Myös palvelimilla on reaaliaikainen valvonta, joka tunnistaa hyökkäysyritysten merkit tai järjestelmien sopimattoman käytön.

Elintärkeät, aukottoman kirjausketjun (audit trail) perustana olevat lokit tallennetaan erilliselle lokipalvelimelle niiden koskemattomuuden varmistamiseksi.

Käytössämme on myös järjestelmä yrityksemme tietoturvakäytännön noudattamiseksi, jolla taataan korkein mahdollinen suoja palvelintasolla. Poikkeamat tästä käytännöstä raportoidaan automaattisesti vastuuhenkilöille. Kaikki palvelimemme läpikäyvät myös antivirus- ja rootkit-skannauksia päivittäisellä tasolla.

Palvelimet on konfiguroitu audit-lokikirjauksin ja pääsy palvelimille, ja täten järjestelmiin, on rajattu ainoastaan asianmukaiselle henkilökunnalle.

Tietojen luovuttaminen kolmannelle osapuolelle tai EU:n ulkopuolelle

Kaikki tietojen tallentaminen ja käsittely toteutetaan Suomen rajojen sisällä. Sharebook ei koskaan luovuta tietoja kolmannelle osapuolelle, tai hyödynnä alihankkijoita ilman asiakkaan yksiselitteistä toimeksiantoa tai hyväksyntää. Sellainen tietojen luovuttaminen voi koskea esimerkiksi kirjeitä tai viestejä, joiden lähetyksen asiakas itse on käynnistänyt, tai asiakkaan pyynnöstä toteutettavaa viranomaisraportointia.

Sopimus tietojenkäsittelystä

Sharebookin Käyttöehdoissa on kuvattu vastuiden jakautuminen teidän (asiakas) ja meidän (Sharebook) välillämme. Ehdoista käy ilmi teidän velvollisuutenne ja meidän vastuamme.

Sharebookin kanssa allekirjoitettavan sopimuksen yhteydessä osapuolet hyväksyvät myös Käyttöehdot, joissa tietojenkäsittelijän vastuusta säädetään.