

Riskiarviointi suhteessa uusimpaan EU-tuomioon (Schrems II).

Päivitetty 09.10.2020

Schrems II -ratkaisun pohjalta olemme suorittaneet laajennetun riskiarvioinnin koskien henkilötietojen käsittelyämme tietojen käsittelijöillämme ja tietojen alikäsittelijöillämme USA:ssa.

Plandisc kunnioittaa kaikkia toiveita koskien verkossa luovutettujen henkilötietojen salassapitoa, ja huomioimme kaikkien saamiemme henkilötietojen asianmukaisen suojauksen ja vastuullisen käsittelemisen tarpeen.

Jaamme tiedot ensisijaisesti kolmeen luokkaan.

1. Sisältötieto (tiedot, jotka on syötetty vuosikelloon). Esim. vuosikelloon liitetyt liitetiedostot ja käyttäjän kuvauskenttiin kirjoittamat tiedot.
2. Plandiscin käyttäjän tiedot – tavalliset yhteystiedot. Esim. nimi, sähköpostiosoite ja puhelinnumero.
3. Verkkoselaimen selaushistoria Plandisc-työkalussa. Esim. värien muuttaminen, tulostukset ja muut vastaavat toiminnot.

Kohta 1:

Asiakas on rekisterinpitäjä koskien sisältötietoja, jotka syötetään Plandisciin – vuosikelloon, ja Plandisc on tietojen käsittelijä. Asiakkaan sisältötiedot säilytetään Microsoft Azuren palvelimella Irlannissa. Kaikki sisältötieto säilytetään näin ollen EU:n sisällä, ts. sisältötietoa ei säilytetä USA:ssa. Lisätietoja Microsoft Azuren turvallisuudesta löytyy linkistä [Microsoft Azure Security](#); sieltä löytyy lisätietoja myös tietojen salaamisesta eli [kryptauksesta](#). Microsoft Azuren säilyttämien tietojen varmuuskopiointista huolehtii [Amazon Webservices – Irland](#).

Kohdat 2 ja 3:

Plandisc on rekisterinpitäjä koskien kohtia 2 ja 3, ts. Plandiscin käyttäjäprofiiliin luovutettuja tietoja. Joitakin näistä tiedoista säilyttävät tietojen käsittelijämme USA:ssa. Näiden tietojen siirtäminen ja käsittely tapahtuu EU-komission hyväksymien vakiolausekkeiden (Standard Contractual Clauses, SCC) perusteella. Arvioimme, että henkilötiedot on riittävästi suojattu käyttämällä vakiolausekkeita (SCC) etenkin ottaen huomioon siirrettyjen henkilötietojen tyyppin. Tämän lisäksi Plandisc on varmistanut tiedot edelleen mm. pseudonymisoinnilla, lyhyellä säilytysajalla ja vastaanottamalla läpinäkyvyysraportit.