

Mitä tietoja suojataan?

Kuvaa järjestelmään tallentuva ja järjestelmän muutoin käyttämä tietosisältö.

Esim. henkilötietoja, arvosanoja, talouslukuja, säätietoja, lämpötiloja, jne. Hahmottele itsellesi käyttötapauksesi tiedon kulku (esim. verensokerimittauksen kulkeutuminen asiakkaalta hoitohenkilökunnalle). Muista integraatiot ja lokit.

Mihin tietoja käytetään?

Mikä on minkäkin tiedon käyttötarkoitus?

Huom. jos keräät henkilötietoja, pitää niillä lainsäädännön mukaan aina olla jokin käyttötarkoitus. Turhaa henkilötietoja ei saa kerätä.

Mihin tietoja tallennetaan?

Mihin ja miten tietoja on ajateltu tallennettavan.

Huom. erityisesti henkilötietojen käsittelyssä sijainti vaikuttaa sopimuksiin sekä suojausmekanismeihin.

Mikä on tiedon/järjestelmän elinkaari?

Miten kauan mitään tietoa säilytetään järjestelmässä, kuka on vastuussa tiedon elinkaaren hallinnoimisesta.

Usein pitkäaikaistallennus eriytetään eri järjestelmiin, esim. Metropoliassa tietovarastoon, joten muista dokumentoida tiedon elinkaari kaikissa järjestelmissä.

Ketkä tietoja käsittelevät?

Ketkä kaikki ja missä tilanteissa pääsevät tietoon käsiksi. Onko järjestelmässä roolit joilla on pääsy vain tiettyihin tietoihin.

Esim. yleensä opiskelijan kuuluu päästä vain tietoihin, joita hän tarvitsee työn suorittamiseksi.

Kuka vastaa mistäkin osasta tietojen käsittelyssä?

Onko palveluntarjoajan palveluiden osalta sovittu mikä kuuluu kenenkin vastuulle.

Palveluntarjoajaan kohdistuu tietoturvariskejä aivan kuten mihin tahansa muuhunkin yritykseen, joten sovi selkeä ja kattava sopimus tietoturvasta ja vastuista.