Tuomioistuinvirasto
Domstolsverket

Lausunto
3.9.2026
TIV/1134/2026
Ei vielä julkinen

Eduskunnan hallintovaliokunta
HaV@eduskunta.fi

HE 85/2026 vp

Tietojärjestelmien tietoturvallisuuden ja varautumisen arviointi

Hallituksen esityksen tavoitteena on luoda ja kirjata lakiin menettely tietojärjestelmien tietoturvallisuuden ja varautumisen arvioimiseksi. Arviointimenettelyn kohdentamisessa tulisi kuitenkin erottaa selkeästi tietoturvallisuus, turvallisuusluokittelu sekä organisaation varautuminen ja toiminnan jatkuvuus. Esityksessä nämä on kytketty toisiinsa epätarkoituksenmukaisella tavalla.

Tietoturvallisuus muodostuu tiedon ja tietojärjestelmien luottamuksellisuudesta, eheydestä ja saatavuudesta. Turvallisuusluokittelu kohdistuu näistä lähtökohtaisesti vain luottamuksellisuuteen ja siihen oletettuun haittaan, jonka tiedon oikeudeton paljastuminen voisi aiheuttaa. Tämän vuoksi turvallisuusluokkaa ei tulisi käyttää ainoana kriteerinä sen ratkaisemiseen, tulisiko tietojärjestelmään kohdistaa erityinen tietoturvallisuuden arviointi tai millaisia arviointimenettelyjä siinä tulisi käyttää.

Turvallisuusluokka ei kuvaa järjestelmän merkitystä organisaation toiminnalle, järjestelmän kriittisyyttä, tiedon eheys- tai saatavuusvaatimuksia eikä järjestelmän merkitystä häiriötilanteesta selviytymiselle. Sillä ei siten ole suoranaista yhteyttä myöskään varautumisen tarpeeseen tai tasoon. Varautumisen lähtökohtana on organisaation kyky ylläpitää tehtäviään, toimintaedellytyksiään ja toimintakykyään häiriötilanteissa. Toiminnan kannalta erittäin kriittinen järjestelmä voi käsitellä kokonaan turvallisuusluokittelematonta tietoa, kun taas turvallisuusluokiteltua tietoa käsittelevä järjestelmä ei välttämättä ole toiminnan jatkuvuuden kannalta kriittinen.

Ajatus turvallisuusluokan käyttämisestä arviointimenettelyn perusteena on ongelmallinen myös sen vuoksi, että luokittelu perustuu tiedon laatijan tai omistajan tekemään subjektiiviseen arvioon tiedon paljastumisesta aiheutuvasta haitasta. Vaikka arvioinnille on säädetty perusteet, yksittäiseen tietoon liitettävä luokitus sisältää väistämättä tapauskohtaista harkintaa eikä sellaisenaan muodosta objektiivista mittaria tietojärjestelmän kokonaisriskistä tai kriittisyydestä. Tällaisen luokituksen käyttäminen ratkaisevana perusteena järjestelmään kohdistettaville tarkastus- tai arviointimenettelyille voi johtaa arviointien kohdentumiseen tavalla, joka ei vastaa organisaation tosiasiallisia riskejä. Tarkastus- ja arviointimenettelyt sekä tietojärjestelmien suojaustoimet aiheuttavat myös kustannuksia, joten niiden väärä kohdentuminen johtaa myös rajallisten resurssien hukkakäyttöön.

Monissa organisaatioissa, kuten tuomioistuimissa, toiminnan jatkuvuuden kannalta tiedon eheys ja saatavuus voivat olla vähintään yhtä keskeisiä kuin luottamuksellisuus. Olennaista on esimerkiksi, voidaanko tietoon ja sen avulla tehtyihin päätöksiin luottaa, ovatko liittymien kautta toisista järjestelmistä päivitetyt tiedot ajan tasalla, ovatko

esitetyt tiedot oikeassa muodossa sekä ovatko tieto ja tietojärjestelmät käytettävissä silloin, kun lainsääteinen tehtävä ja toiminnalliset prosessit sitä edellyttävät.

Tietoturvallisuuden ja varautumisen arvioinnin ensisijaisena lähtökohtana tulisi tämän vuoksi olla organisaation toiminta ja riskienhallinta. Toimenpiteiden kohdentamisen ja käytettävien hallintakeinojen tulee olla johdettavissa organisaation tehtävistä, sen toimintaympäristöstä, käytössä olevan järjestelmän kriittisyydestä tukea lakisääteistä tehtävää sekä tunnistetuista riskeistä. Yleiset arviointikriteeristöt voivat tukea tietojärjestelmän riskien hallintakeinojen valintaa, mutta niitä ei tulisi soveltaa kaavamaisina tarkastuslistoina. Turvallisuuden kannalta olennaista on hallintakeinojen muodostaman kokonaisuuden toimivuus suhteessa tunnistettuihin riskeihin, eivät yksittäiset hallintakeinot. Henkilötietoja käsittelevien tietojärjestelmien osalta tulee organisaatioriskien lisäksi arvioida myös käsittelyn henkilötietoriskit ja niiden hallinta.

Varautumisen tarpeet, toimintamallit ja ratkaisut määräytyvät puolestaan organisaation tehtävistä, sen toiminnan prioriteeteista, riippuvuuksista ja käytettävissä olevista vaihtoehtoisista toimintatavoista. Näitä ei voida tarkoituksenmukaisesti johtaa turvallisuusluokituksesta eikä geneerisistä tietojärjestelmien arviointikriteeristöstä tai hallintakeinolistoista. Tietojärjestelmät eivät edes välttämättä ole käytössä kaikissa tilanteissa, joihin varaudutaan. Ulkopuolinen arvioija voi arvioida varautumisen järjestelyjä ja systemaattisuutta, mutta varautumisen sisällön ja toiminnallisten prioriteettien tulee perustua organisaation omaan riskienhallintaan.

Varautumiskyvyn toimivuutta voidaan parhaiten koestaa harjoituksilla, simulaatioilla ja muilla käytännön testeillä. Pelkkä teknisiin hallintakeinoihin tai dokumentaatioon perustuva arviointi antaa organisaation todellisesta toimintakyvystä vain rajallisen kuvan. Arviointimenettelyn laajentaminen varautumiseen voi siten lisätä kustannuksia ja pidentää tietojärjestelmien käyttöönottoa ilman että saavutetaan vaikutusta organisaation tosiasialliseen varautumiskykyyn.

Hallituksen esitykseen sisältyvää arvioijan oikeus (6§) tehdä toimenpiteitä arvioitavissa tietojärjestelmissä tulee rajata tarkasti. Tuomioistuinlaitoksen tietojärjestelmiin kohdistuvien toimenpiteiden kohdalla on vielä erikseen huomioitava tuomioistuimien perustuslaillinen asema. Tuomioistuimet eivät ole hallintoviranomaisia, vaan itsenäisiä ja riippumattomia tuomiovallan käyttäjiä.

Kriittisiin järjestelmien toimintaympäristöön, myös arviointimielessä, tehtävät muutokset sekä toteutettavat tekniset toimenpiteet tulee aina perustua suunniteltuun muutoshallintaan, ennakolta arvioituihin vaikutuksiin ja asianmukaiseen ennakkotestaukseen. Arvioijan suorittamat (tarkastus)ohjelmisto asennukset, ajettavat komennot tai muut järjestelmäympäristöön vaikuttavat toimenpiteet eivät saa vaarantaa järjestelmän eheyttä, saatavuutta tai häiriötöntä toimintaa. Sääntelyssä tulee myös määritellä arvioijan vastuu mahdollisesti aiheutuvista vahingoista.

Turvallisuusluokitusta ei tulisi käyttää tietojärjestelmien arviointimenettelyn ensisijaisena kohdentamisperusteena. Arvioinnin tulee perustua järjestelmän todelliseen merkitykseen organisaation toiminnalle sekä siihen liittyviin luottamuksellisuus-, eheys-, saatavuus- ja jatkuvuusriskeihin. Varautuminen puolestaan tulee nähdä organisaation toimintakykyä koskevana kokonaisuutena, jota tiedon turvallisuusluokka ei sellaisenaan kuvaa.

3.9.2026
TIV/1134/2026

Ylijohtaja	Pasi Kumpula
Riskienhallintapäällikkö	Kimmo Helaskoski

Käyntiosoite: Silkkitehtaantie 5 C, Vantaa • Postiosoite: PL 100, 00085 Tuomioistuinvirasto • Vaihde: 029 56 50500 Besöksadress: Silkesfabriksvägen 5 C, Vanda • Postadress: PB 100, 00085 Domstolsverket • Växel: 029 56 50440 tuomioistuinvirasto@oikeus.fi • www.tuomioistuinvirasto.fi

Digitaalinen PDF-allekirjoitus / Digital PDF-signatur
Kimmo Helaskoski
Erityisasiantuntija
Tuomioistuinvirasto
kimmo.helaskoski@oikeus.fi
Asian tunnus / Ärende-ID: TIV/1134/2026
Asiakirjan tunnus / Dokument-ID: TIV-AK-2026-10566
07.09.2026 09:25:23

Digitaalinen PDF-allekirjoitus / Digital PDF-signatur
Pasi Kumpula
Ylijohtaja
Tuomioistuinvirasto
pasi.kumpula@oikeus.fi
Asian tunnus / Ärende-ID: TIV/1134/2026
Asiakirjan tunnus / Dokument-ID: TIV-AK-2026-10566
07.09.2026 09:52:21