POLIISI

Eduskunnan hallintovaliokunta

HE 85/2026 vp

Poliisihallituksen kirjallinen asiantuntijalausunto hallituksen esitykseen eduskunnalle HE 85/2026 vp) viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain, tietoturvallisuuden arviointilaitoksista annetun lain sekä turvallisuusselvityslain 18 ja 48 §:n muuttamisesta

1 Asia

Hallituksen esityksessä (HE 85/2026 vp) ehdotetaan viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain, tietoturvallisuuden arviointilaitoksista annetun lain sekä turvallisuusselvityslain 18 ja 48 §:n muuttamista.

Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annettuun lakiin ehdotetuilla muutoksilla selkeytettäisiin viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen arviointimenettelyjä sekä parannettaisiin niiden saatavuutta mahdollistamalla nykyistä useammanlaisia arviointimenettelyjä. Myös muille luotettaviksi todetuille yrityksille kuin tietoturvallisuuden arviointilaitoksille säädettäisiin mahdollisuus tarjota tietoturvallisuuden ja varautumisen arviointipalveluja viranomaisille korkeintaan turvallisuusluokan IV tietojen käsittelyn arviointiin saakka. Lakiin lisättäisiin valtionhallinnon viranomaisille velvollisuus arvioida tietojärjestelmänsä ja tietoliikennejärjestelynsä vähintään itsearviointeina. Muidenkin kuin valtionhallinnon viranomaisten olisi mahdollista toteuttaa lain mukaisia arviointeja. Kaikkien viranomaisten tulisi kuitenkin pyytää arviointiviranomaisen arviointia turvallisuusluokan I ja II tietojen käsittelylle. Lisäksi kaikkien viranomaisten tulisi pyytää arviointiviranomaisen arviointia tai hankkia tietoturvallisuuden arviointilaitoksen arviointi turvallisuusluokan III tietojen käsittelylle, jollei viranomainen riskiarvioinnin perusteella päättäisi sen olevan tarpeetonta. Ehdotetuilla muutoksilla tehostettaisiin arviointeja korostamalla riskiarvion merkitystä arviointimenettelyn valinnassa ja painotettaisiin viranomaisten vastuuta omien tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuudesta ja varautumisesta sekä käyttöönottopäätöksistä.

Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista lakiin annettuun lakiin ehdotetuilla muutoksilla myös tarkennettaisiin Liikenne- ja viestintäviraston tehtäviä ja säädettäisiin turvallisuuskriittisten tuotteiden valmistajille oikeus hakea arviointia. Lisäksi lisättäisiin Puolustusvoimille arviointitehtävä, jolla vastattaisiin turvallisuusympäristön muutoksista johtuvaan arviointitarpeiden kasvuun. Ehdote-

tuilla muutoksilla tarkennettaisiin ja tehostettaisiin arviointiviranomaisten yhteistyötä, työjakoa ja tiedonsaantioikeuksia sekä mahdollistettaisiin arviointiviranomaista avustava tehtävä.

Tietoturvallisuuden arviointilaitoksista annettuun lakiin ehdotetuilla muutoksilla edistettäisiin tietoturvallisuuden arviointilaitosten elinkeinotoiminnan edellytyksiä yksinkertaistamalla ja tehostamalla tietoturvallisuuden arviointilaitosten luotettavuuden sääntelyä ja joustavoittamalla tietoturvallisuuden arviointilaitosten pätevyyksien hyväksyntää.

2 Lausunto

Poliisihallitus on aiemmin vastannut 23.1.2026 lausuntopyyntöön ehdotuksesta viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointia koskevan lainsäädännön muuttamisesta (Lausuntopyynnön diaarinumero: VN/36127/2023). Lausuntoon sisällytettyjä huomioita on viety nyt kyseessä olevaan hallituksen esitykseen (HE 85/2026 vp).

Hallituksen esitys (HE 85/2026 vp) on kannatettava. Poliisihallitus kiinnittää osana kirjallista lausuntoa huomion hallituksen esityksen ja lainsäädännön muutosten vaikutuksista virastoille.

Hallituksen esityksen tavoitteena on, että valtionhallinnon viranomaisille säädettäisiin velvollisuus toteuttaa tietojärjestelmien ja tietoliikennejärjestelyjen arviointi käyttäen arviointilaissa tarkoitettuja arviointimenettelyjä. Arviointimenettely valittaisiin riskiarvioinnin perusteella siten, että valtionhallinnon viranomainen toteuttaisi vähintään itsearvioinnin. Viranomaisten ja muiden valtionhallinnon toimijoiden tekemien arviointien vertailtavuus vaatimusten mukaisuuden todentamisessa on jatkossakin tärkeää. Viranomaiset ja muut valtionhallinnon toimijat tuottavat ja käyttävät tietojärjestelmiä ja tietoliikennejärjestelyjä ristiin. Hallituksen esityksessä esiin nostettuja itsearviointeja lähestytään käsitteenä ja toimintaprosessina hyvin eri lähtökohdista ja osaamistasolla.

Itsearviointien tulee olla määrämuotoisia ja vakiintuneita malleja, jotta riittävän laadukkaat ja vaatimustenmukaiset itsearvioinnit kyetään toteuttamaan läpinäkyvästi ja objektiivisesti. Valtionhallinnon yhteisten palveluympäristöjen ja viranomaisten tietojärjestelmien välillä on jo nykytilanteessa merkittävä määrä integraatioita. Itsearviointien määrämuotoisuus ja suorittajien osaamisen vaatimukset varmistavat osaltaan sen, että tietoa voidaan jatkossakin käsitellä sellaisissa tietojärjestelmissä, joihin on tehty toisen viranomaisen toimesta itsearviointi ja tietojärjestelmien tila tunnetaan. Itsearvioinnin ei tulisi olla itsetarkoituksellisesti kevyempi ja vähemmän vaativa prosessi vaan sille tulisi asettaa sellaiset vaatimukset, joilla pystytään varmistamaan ohjelmistojen ja tietojenkäsittely-ympäristöjen turvallisuus yhtä lailla kuin muissa arviointimenettelyissä.

Hallituksen esityksen mukaisesti turvallisuusluokkien I ja II osalta arviointiviranomainen toteuttaa arvioinnin. Turvallisuusluokan III osalta riskienarviointiin perustuva mahdollisuus on kannatettava, mikäli tämän menettelyn taustalla laaditaan määrämuotoinen menettely, joka koskee viranomaisia ja muita valtionhallinnon toimijoita. Turvallisuusluokan IV luokiteltujen tietoaineistojen osalta on huomattava, että palveluntarjoajille tulee olla

vastaavalla tavalla osaamisvaatimukset kuin muidenkin turvallisuusluokiteltujen tietoaineistojen osalta. Päämäärätietoisella työllä TLIV tietojen käsittelyyn tarkoitettujen tietojärjestelmien arvioinnin mahdollistamisella resursseja voitaisiin kohdentaa erityisesti tätä korkeampien turvallisuusluokiteltujen tietojen käsittelyyn tarkoitettujen tietojärjestelmien arviointiin. Kansallisten tietojärjestelmien arvioinneissa on huomioitava mahdollinen kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyyn tarkoitettuihin tietojärjestelmiin ja palveluympäristöihin liittäminen. Kansallisten tietojärjestelmien kehittämisen aikana päätetyt poikkeamat voivat muodostaa esteen liittämiselle kansainvälisiin tietojärjestelmiin.

Tietojärjestelmät ja niiden väliset integraatiot muodostavat toiminnallisia kokonaisuuksia. TLIV-tiedon käsittelyyn tarkoitettuja tietojärjestelmiä tuotetaan myös TLIII-tietojen käsittelyyn luokitelluista palveluympäristöistä, jotta tiedon saatavuus, eheys, luottamuksellisuus ja henkilötietojen suoja kyetään turvaamaan vaatimusten mukaisella tavalla. Valtionhallinnon palveluympäristöissä on palvelun saatavuuden ja tarvittavien integraatioiden näkökulmasta sijoitettu TLIV-luokiteltuja tietoja sisältäviä tietojärjestelmiä TLIII-luokiteltuun palveluympäristöön esimerkiksi Turvallisuusverkko Tuve:n. Tiedon luottamuksellisuuden luokittelu ei ole ainoa näkökulma määritettäessä tietojärjestelmän sijoittumista valtionhallinnon yhteisissä palveluympäristöissä, jolloin kyseisellä tietojärjestelmällä tulee arvioitavaksi myös palveluympäristöstä johtuen TLIV (luottamuksellisuus) kovempia kriteerejä (saatavuus ja/tai eheys).

Auditoinnissa palveluntarjoaja saa laajan näkyvyyden viranomaisen tietojärjestelmien arkkitehtuuriin, verkkoratkaisuihin, käyttöoikeuksiin, suojausmenetelmiin, konfiguraatioihin, havaittuihin puutteisiin ja haavoittuvuuksiin. Tällaisen tiedon keskittyminen ulkopuolisille toimijoille kasvattaa muun muassa valtiollisen vaikuttamisen, tiedustelun ja toimitusketjuihin kohdistuvan vaikuttamisen riskiä. Riskiä voivat lisätä esimerkiksi palveluntarjoajan omistus- ja määräysvaltasuhteet, ulkomaiset sidonnaisuudet, alihankintaketjut sekä se, mistä maista auditointiin osallistuvilla henkilöillä tai palveluntarjoajan käyttämillä tietojärjestelmillä on pääsy auditointiaineistoon.

Hallituksen esityksessä kuvatulla tavalla tietoturvallisuudella voidaan katsoa tarkoitettavan yleisesti tiedon luottamuksellisuuden, eheyden ja saatavuuden turvaamista. Tietoturvallisuuden ja varautumisen arvioinnilla selvitetään säädettyjen ja riskiarvioinnin perusteella valittujen vaatimusten täyttymistä tietojärjestelmissä, tietoliikennejärjestelyissä ja turvallisuuskriittisissä tuotteissa. Arviointi keskittyy nykyisin vahvasti tiedon luottamukselliseen arviointiin. Tiedon luottamuksellisuuden ja eheyden rinnalla tiedon saatavuuden merkitys korostuu erityisesti virastojen valmius-, varautumis- ja jatkuvuussuunnittelussa. Virastojen lakisääteiset tehtävät, toiminnalliset vaatimukset ja tiedon käsittelytarpeet nostavat saatavuuden merkitystä kaikissa olosuhteissa: normaalioloissa, normaaliolojen häiriötilanteissa ja poikkeusoloissa. Arvioinnissa ja sen merkityksellisyydessä tulee kiinnittää huomioita salassa pidettävän ja salassa pidettävän turvallisuusluokitellun lisäksi aiempaa enemmän tiedon saatavuuden ja eheyden turvaamiseen.

Salassa pidettävän turvallisuusluokitellun tiedon osalta arviointimenettelyt ja käytettävät arviointikriteeristöt vaativat tarkennusta. HE-luonnokseen on keskeisesti sidoksissa

myös muu tieto- ja kyberturvallisuuden arviointimenettelyihin liittyvä kehitystyö. Arviointikriteeristöjen (Katakri, Julkri, Pitukri) osalta on esitetty yhtenäistämisen ja karsimisen tarvetta, mutta viimeisten tietojen perusteella kriteeristöjä kootaan yhteiselle alustalle, mutta varsinaiseen yhtenäistämiseen tai karsimiseen ei toistaiseksi päästä. Tämä asettaa myös eri arviointimenettelyille tunnistettuja tarpeita, koska Suomessa on ollut vain rajallisesti kriteeristöt tuntevien palveluntuottajien palveluita saatavilla ja toisaalta eri kriteeristöjen käytöstä vaatimusten mukaisuuden todentamisessa on ollut erilaisia tulkintoja.

Hallituksen esityksessä ei esitetä henkilöstöresurssien lisäystä viranomaisille. Tavoitteiden osalta riittävän teknisen osaamistason ja kyvykkyyden kasvattaminen tiedonhallintayksikössä arvioidaan kestävän vuosia ja resurssit on kohdennettava sisäisesti uudelleen. Itsearvioinnit edellyttävät osaamista ja kyvykkyyttä, joka rakennetaan ajan myötä työssä oppien sekä määrämuotoisen osaamispolun ja koulutusten toteuttamista itsenäisesti, tiedonhallintayksiköiden yhteistyönä, palveluostoina tai näiden yhdistelmänä. Toiminnan objektiivisuuden ja läpinäkyvyyden vuoksi toiminta tulisi erottaa omaksi kokonaisuudekseen ja resursoida niin, että tiedonhallintayksiköllä on tosiasiallinen mahdollisuus toteuttaa vaatimusten mukainen arviointimenettely.

Tuomas Kokkomäki, Tietoturvapäällikkö

Asiakirja on sähköisesti allekirjoitettu asianhallintajärjestelmässä. Poliisi 04.09.2026 klo 15:08. Allekirjoituksen oikeellisuuden voi todentaa kirjaamosta.

Liitteet

-

Jakelu

Eduskunnan hallintovaliokunta, HaV@eduskunta.fi

Tiedoksi

Poliisihallitus, Esikunta

Poliisihallitus
Opastinsilta 12 B, PL 1000, 00521 Helsinki
kirjaamo.poliisihallitus@poliisi.fi
Puhelin +358 295 480 181, Faksi +358 295 411 780, poliisi.fi