

Rakennetun ympäristön tietojärjestelmän tietoturvaehdot, luovutusrajapinnat

Tietoturva ja tietosuoja

Hakijan/Luvan saajan saajan on noudatettava lakia rakennetun ympäristön tietojärjestelmästä (431/2023), lakia viranomaisen toiminnan julkisuudesta (621/1999), lakia julkisen hallinnon tiedon hallinnasta (906/2019) sekä muita soveltuvia lakeja käsitellessään rakennetun ympäristön tietojärjestelmän tietoja. Näissä tietoturvaehdoissa nostettu esiin keskeisempiä tietoturvaan ja tietosuojaan liittyviä ehtoja.

Hakijalla/Luvan saajalla tulee olla kuvattuna tietojen käsittely, ja siitä pitää selvittää tietojen käsittelyyn liittyvät asiat, prosessit ja käsittelijät Hakijan/Luvan saajan ympäristössä. Kuvauksen tulee sisältää kuvaus myös lokitietojen käsittelystä, käsittelyoikeuksista ja säilyttämisestä säilytysaikoihin. Hakijan/Luvan saajan tulee pyynnöstä toimittaa tai esittää kuvaus Suomen ympäristökeskukselle.

Mikäli haetaan lupaa henkilötietojen käsittelyyn, Hakijan/Luvan saajan tulee laatia luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 (jäljempänä ”EU:n yleinen tietosuoja-asetus”) 30 artiklassa tarkoitettu seloste käsittelytoimista, jonka piirissä tiedot ovat. Hakijan/Luvan saajan tulee pyynnöstä toimittaa tai esittää seloste Suomen ympäristökeskukselle.

Suomen ympäristökeskus voi luovuttaa Hakijalle/Luvan saajalle Rakennetun ympäristön tietojärjestelmän henkilötietoja Euroopan unionin alueen ja Euroopan talousalueen ulkopuolelle vain, jos EU:n yleisen tietosuoja-asetuksen V luvussa henkilötietojen siirtämiselle asetetut edellytykset täyttyvät. Siirtämisellä tarkoitetaan myös pääsyn mahdollistamista henkilötietoihin esimerkiksi hallinta- ja valvontayhteyden välityksellä. Lupa henkilötietojen luovuttamiseen Euroopan unionin alueen ja Euroopan talousalueen ulkopuolelle on haettava erikseen. Mikäli Hakijan/Luvan saajan tarkoituksena on käsitellä Tietoja Euroopan unionin alueen ja Euroopan talousalueen ulkopuolella, Hakija/Luvan saajan tulee antaa erillinen selvitys tietojen luovuttamisesta Euroopan unionin alueen ja Euroopan talousalueen ulkopuolelle sekä henkilötietojen käsittelystä EU:n tietosuoja-asetusten mukaisesti.

Lisäksi Hakijan/Luvan saajan tulee huolehtia tietojen asianmukaisesta suojaamisesta laittoman tai tapaturmaisen häviämisen tai hävittämisen varalta. Edellä olevan lisäksi, tämän tulee käsitellä tietoja vain siten, kuinka Hakija/Luvan saaja on ilmoittanut luvan liitteenä olevan hakemuksen kohdassa 4 sekä mahdollisesti kyseisen kohdan perusteella hakemukseen liittämässään selvityksessä.

Hakija/Luvan saaja sitoutuu käsittelemään salassa pidettäviä ja turvakiellollisten henkilöiden tietoja säännösten mukaisesti. Turvaluokiteltua tietoa saavat käsitellä vain henkilöt, joilla on voimassa oleva turvallisuusselvitys.



Tietoaaineiston käsittely

Hakijan/Luvan saajan tulee antaa pääsy tietoihin vain sellaisille käsittelijöille, jotka tarvitsevat kyseistä tietoa työtehtävissään, ja huolehtia siitä, että kyseiset käsittelijät tietävät, miten tietoa koskevasta tietoturvasta huolehditaan. Hakijan/Luvan saajan tulee huolehtia erityisesti, että turvakiellolistien henkilöiden tietoja käsittelevät vain henkilöt, joilla on oikeus niiden käsittelyyn ja joiden tehtäviin kyseisten tietojen käsittely välittömästi liittyy. Hävitettäväksi tai poistettaviksi tarkoitetut tiedot tulee tuhota niin, että niiden luottamuksellisuus ja tietosuojat on varmistettu.

Mikäli tietoja tulostetaan, Hakijan/Luvan saajan tulee huolehtia tulosteiden asianmukaisesta käsittelystä. Salassa pidettävien tietojen tulostamista tulee välttää ja Hakijan/Luvan saajan tulee varmistaa, että tulosteet eivät päädy sellaisten henkilöiden haltuun, joilla ei ole tietoihin käyttöoikeutta. Tulosteet tulee hävittää asianmukaisesti.

Lokitus ja lokien hallinta

Lokit tulee laatia niin, että niihin kirjautuu rajapintapalvelusta suoritettujen tietojen haun ajankohta, käsittelijän henkilöllisyyden selvittävä tunnistamistieto sekä rajapintapalvelusta haettujen tietojen hakuehdot. Mikäli tietoja käsitellään Hakijan/Luvan saajan omassa ympäristössä, käsittelystä tulee laatia vastaavat lokitiedot. Pääsy Hakijan/Luvan saajan järjestelmän lokitietoihin tulee olla rajattu vain lokitietojen käsittelystä vastaaville, nimetyille henkilöille, jotka ovat sitoutuneet lokitietojen salassapitoon ja asianmukaiseen käsittelyyn.

Hakijan/Luvan saajan tulee määrärajoin varmistaa lokien muodostuminen sekä seurata ja valvoa säännöllisesti lokitietojen käsittelyä organisaatiossaan. Lokitiedot tulee hävittää tietoturvallisesti. Hakijan/Luvan saajan tulee varmistaa, että lokitietoja ei pysty ennen aikaisesti hävittämään tai että niitä ei pysty jälkikäteen muuttamaan.

Käyttöoikeuksien ja pääsyn hallinta

Hakijalla/Luvan saajalla tulee olla kuvaus käsittelijän käyttöoikeuksien ja -valtuuksien hallintaprosessistaan. Kuvauksen tulee sisältää tieto siitä, kuinka käsittelijän käyttöoikeuksien hallinta (käyttöoikeuksien myöntäminen, muuttaminen, tarkistaminen, poistaminen ja hyväksyminen) hoidetaan. Kuvauksen tulee koskea kaikkia niitä, joilla on pääsy tietoihin.

Hakijalla/Luvan saajalla tulee olla myös kuvaus, missä rooleissa Hakijan/Luvan saajan palveluksessa olevalla tai Hakijan/Luvan saajan lukuun toimivalla tietojen käsittelevällä luonnollisella henkilöllä on mahdollisuus käsitellä tietoja. Jokaisella käsittelijällä pitää olla henkilökohtaiset käyttäjätunnukset. Tiedon käsittelijä ja tämän käyttöoikeuden voimassaoloaika tulee voida selvittää aukottomasti myös jälkikäteen. Hakijan/Luvan saajan tulee varmistua siitä, että käsittelijöiden käyttöoikeudet ovat jatkuvasti ajan tasalla. Käsittelijän käyttöoikeus pitää poistaa välittömästi, jos käyttöoikeuden voimassaolon edellytykset eivät enää täyty.

Mikäli Suomen ympäristökeskus lakkauttaa Hakijan/Luvan saajan luvan, Hakija/Luvan saaja vastaa siitä, että kaikkien käsittelijöiden käyttöoikeudet poistetaan välittömästi tai viimeistään seuraavana arkipäivänä siitä, kun Suomen ympäristökeskus on ilmoittanut luvan lakkauttamisesta. Käsittelijöiden käyttöoikeuksien voimassaolon edellytykset tulee tarkastaa säännöllisesti sekä tarvittaessa poistaa käyttöoikeudet ainakin henkilövaihdosten, vanhempainvapaiden tai vastaavien pitempiaikaisten poissaolojen yhteydessä, työtehtävien muuttuessa tai virka- tai työsuhteen päättyessä.



Käyttö-, laitteisto-, ohjelmisto- ja tietoliikenneturvallisuus

Hakijalla/Luvan saajalla tulee olla nimetty henkilö tai nimetyt henkilöt, jotka vastaavat organisaation käyttö- ja laitteisto-, ohjelmisto- ja tietoliikenneturvallisuudesta. Käyttö-, laitteisto- ohjelmisto- ja tietoliikenneturvallisuudesta tulee huolehtia asianmukaisesti, esimerkiksi, kun suoritetaan käyttöönottoasennus sellaisille laitteille ja tietojärjestelmille, joissa käsitellään tietoja. Tiedot pitää hävittää tietoturvallisesti, kun tällaiset laitteet ja tietojärjestelmät poistetaan käytöstä. Tietojen käsittelyssä käytettävien laitteiden ja tietojärjestelmien päivitys- ja muutostarpeen seuranta, päivityspäätösten teko ja päivitysten asennukset (erityisesti tietoturvapäivitykset) tulee olla ajan tasalla. Tietojen käsittelyssä käytettävät laitteet tulee olla suojattu varastamisen ja katoamisen varalta.

Hakijan/Luvan saajan pitää olla toteuttanut ja dokumentoinut tietojen käsittelyyn liittyvät haittaohjelmatorjuntatoimenpiteet ja niiden tulee olla ajan tasalla. Hakijan/Luvan saajan tulee huolehtia siitä, että käyttäjä osaa tietoturvalliset toimintatavat eri työskentely-ympäristöissä kuten etätöissä.

Tietojen käsittelyyn liittyvien palomuurien ja muiden suodatuslaitteiden suodatussäännöt pitää olla toteutettuina, dokumentoituina ja ajan tasalla.

Hakijan/Luvan saajan tulee toteutuksissaan huomioida ja dokumentoida kansalliset turvaluokitellun tiedon käsittelyohjeet. Hakijan/Luvan saajan pitää myös varmistaa, että salassa pidettäviä tietoja käsitellään salattuna. Salassapitovelvoitteet ovat voimassa myös luvan päättymisen jälkeen. Salassapitovelvollisuus ei koske tietoa, joka on yleisesti saatavilla tai julkista.

Hakijan/Luvan saajan pitää suojata verkkoympäristönsä siten, että muut kuin käsittelijät eivät pääse käsittelemään tietoa.

Mikäli Hakija/Luvan saaja käyttää sellaisia alihankkijoita, jotka pääsevät käsittelemään tietoja, Hakijan/Luvan saajan on huolehdittava siitä, että myös alihankkijat noudattavat tässä mainittuja tietoturva- ja tietosuojavaatimuksia.

Hakijan/Luvan saajan tulee varmistaa, että tietoa ei joudu asiattomille Hakijan/Luvan saajan tietovälineiden huollon tai poiston yhteydessä.

Poikkeamien hallinta

Hakijan/Luvan saajan tulee huolehtia, että käsittelijät on koulutettu ja ohjeistettu turvallisuus-, tietoturva- ja tietosuojapoikkeamien varalta. Hakijan/Luvan saajan tulee ilmoittaa mahdollisista tietoon liittyvistä turvallisuus-, tietoturva- ja tietosuojapoikkeamista tai niiden uhasta Suomen ympäristökeskukselle ilman aiheetonta viivytystä saatuaan sen tietoonsa ja viimeistään 72 tunnin kuluessa. Tietosuojapoikkeamista ilmoitetaan osoitteeseen tietosuojaSyke@syke.fi ja tietoturvapoikkeamasta turvasähköpostilla osoitteeseen ryhti@syke.fi.sec. Ilmoituksesta tulee käydä ilmi, miten ja milloin poikkeama ilmeni/ilmenee, mitä tietoja poikkeama koskee sekä mihin henkilötietoihin tietoturvaloukkaukset mahdollisesti kohdistui ja kuinka montaa rekisteröitynyttä tietoturvaloukkaukset koskee. Ilmoituksessa on myös ilmoitettava tietosuojavastaava tai muu vastuhenkilö, jolta voi saada asiassa lisätietoja, kuvattava henkilötietojen tietoturvaloukkauksen todennäköiset seuraukset sekä kuvattava toimenpiteet, joita kyseinen henkilötietojen käsittelijä ehdottaisi tai joita se on toteuttanut henkilötietojen tietoturvaloukkauksen johdosta ja tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi. Tietojen käyttöön liittyvissä tarkastuksissa todetuista



Liite

poikkeamista tulee ilmoittaa edellä kuvatulla tavalla sekä korjata ne viivytyksettä ja raportoida suoritetuista korjaustoimenpiteistä Suomen ympäristökeskukselle.

