Asiakirjan ovat allekirjoittaneet

Nimi	Tunnistautuminen	Aika
Anne Väisänen	Suomi.fi	05.03.2024 12:52:51 UTC+02:00

Sisäisen tarkastuksen raportti vuodelta 2023

Sisäisen valvonnan ja riskienhallinnan ohjeen noudattaminen

Vuonna 2022 laadittujen riskienhallinnan osalta tarkastettiin:

- Onko sisäisen valvonnan ja riskienhallinnan suunnitelmissa kuvattuja toimenpiteitä toteutettu, onko riskienhallintasuunnitelmissa kuvattuja riskejä seurattu ja toteutuneiden riskien käsittely dokumentoitu
- Onko merkittävistä riskeistä raportoitu sisäisen valvonnan ja riskienhallinnan ohjeen mukaisesti johtoryhmälle

Hallintosäännön mukaisesti Maakuntahallitus vastaa sisäisen valvonnan ja riskienhallinnan järjestämisestä. Maakuntajohtaja vastaa maakuntahallituksen sisäisen valvonnan ja riskienhallinnan tehtävien valmistelusta ja yhteensovittamisesta johtoryhmän avustamana. Vastuualuejohtajat vastaavat vastuualueensa riskien tunnistamisesta, arvioinnista, riskienhallinnan toimenpiteiden toteutuksesta ja toimivuudesta ja järjestävät vastuualueensa riskien seurannan ja raportoivat riskeistä johtoryhmälle.

Riskien seurannassa käytettävät mittarit ja muut keinot on valittava siten, että erityisesti nopeasti etenevät tai merkitykseltään suuret riskit voidaan havaita ilman tarpeetonta viivytystä. Riskien seuranta kuvataan riskienhallintasuunnitelmissa. Johtoryhmä kokoaa maakuntajohtajan johdolla tiedot organisaatiossa tehdyistä riskihavainnoista ja niiden käsittelystä. Maakuntahallitus antaa johtoryhmän keräämien tietojen perusteella toimintakertomuksessa tiedot keskeisistä johtopäätöksistä sekä selvityksen merkittävimmistä riskeistä ja epävarmuustekijöistä.

Rajaus ja menetelmät

Tarkastusta varten vastuualuejohtajat vastasivat sisäiselle tarkastukselle kirjallisesti sisäisen valvonnan ja riskienhallinnan havainnoistaan. Lisäksi tarkastusta varten käytiin läpi johtoryhmän muistioiden vakiopykälänä olevien sisäisen valvonnan ja riskienhallinnan kirjaukset. Tarkastus koski Pohjois-Pohjanmaan liiton toiminnan riskienhallintaa, eikä tarkastuksessa tarkastettu rahoituksen saaneiden, liiton ulkopuolisten organisaatioiden hankkeiden riskienhallintaa, joita varten on erilliset kontrollitoimenpiteet.

Havainnot

Riskienhallintasuunnitelmat on laadittu vuosien 2022-2023 aikana. Johtoryhmässä on keskusteltu riskienhallinnan toimeenpanon jalkauttamisesta ja seurannasta. Riskienhallintaan on kartoitettu kaupallisia sovellus/järjestelmävaihtoehtoja, mutta toistaiseksi on päädytty jatkamaan riskienhallinnan kehittämistä jo käytössä olevalla ratkaisulla, vaikka se koetaan osin vaikeaksi käyttää. Johtoryhmässä on käsitelty hallinnon vastuualueen ENI-CBC-ohjelman henkilöstöriskit.

Riskienhallintasuunnitelman kohonneita tai toteutuneita riskejä ei ole käsitelty säännönmukaisesti johtoryhmän kokouksissa. Johtoryhmän työskentelyssä on ollut vuonna 2023 aikana muutoksia mm. maakuntajohtajan tehtäväjärjestelyiden vuoksi. Vuodelle 2024 johtoryhmälle on aikataulutettu säännölliset kokoontumisajat, joiden puitteissa myös riskienhallinnan havaintojen käsittely on mahdollista toteuttaa säännöllisin väliajoin. **Vastuualueilla ei ole toteutettu systemaattisesti sisäisen valvonnan ja riskienhallinnan toimenpiteitä, eikä riskienhallintasuunnitelmia ole päivitetty vuoden 2023 aikana. Riskienhallintaa on kuitenkin**

toteutettu kaikilla vastuualueilla osana vastuualueiden työtä, sillä sisäistä valvontaa ovat kaikki ne toimenpiteet, jotka lisäävät asetettujen tavoitteiden saavuttamisen todennäköisyyttä. Vastuualueiden työntekijät ovat olleet mukana laatimassa riskienhallintasuunnitelmia, joten he havaitsevat työtehtäviinsä liittyvät tunnistetut riskit. Riskienhallintaa on toteutettu osana työtehtäviä mm. vastuualueiden palavereissa. Lisäksi tehtäväkuviin on määritelty riskien seurannan ja raportoinnin vastuita. Vastuualueilla on jo toteutettu tai on suunnitteilla riskienhallintaa parantavia toimenpiteitä.

Hallinnon vastuualueella on tunnistettu erityisesti tietoturvaan ja tietohallintoon liittyvät riskit. Tietoturvaan liittyen henkilöstölle on pidetty tietoturvaiskuja, mutta ohjeistaminen ei ole järjestelmällistä, eikä annetut ohjeet löydy keskitetysti yhdestä paikasta. Tietohallinnon riskienhallintatehtäviä ovat hoitaneet hallinto- ja henkilöstöjohtaja, viestintä- ja hallintopäällikkö, hallinnon kehittämispäällikkö sekä tietohallintopäällikkö. Myös Karelia ENI-CBC-ohjelman henkilöstöön ja takaisinperintään liittyvät riskit on havaittu ja toimenpiteet aloitettu.

Hallinnon vastuualueella on pyritty ennaltaehkäisemään tunnistettuja riskejä. Riskien ennaltaehkäiseviä keinoja ovat riskien minimoimiseen tähtäävien ohjeiden laatiminen ja päivittäminen, kuten hankinta- ja hyvän hallinnon ohjeet, sekä annetuista ohjeista järjestetyt infotilaisuudet henkilöstölle, liiton hallinnoimien hankkeiden säännöllinen talous- ja hallintopalaveri sekä toimeksianto johtoryhmän sihteerille valmistella päättyvien sopimusten seuranta johtoryhmään kaksi kertaa vuodessa. Vuoden 2023 aikana on otettu käyttöön ilmoittajansuojelulain mukainen ilmoituskanava, jota varten ilmoitusten käsittelyn ja tutkimisen prosessi on kuvattu. Liiton sisäisten hankkeiden ohjeen laatiminen on aloitettu.

Maakunnan kehittämisen ja rahoituksen vastuualueella keväällä 2023 havaittiin, että hakemusten ja rahoitustoimien määrän kasvaessa käsittely valmisteluaikojen piteneminen ja työn kuormittavuuden lisääntyminen. Riskiin reagoitiin lisäämällä tehtävään henkilöstöresurssia. Lisäksi havaittiin tarve parantaa osaamista mm. jääviysriskin hallintaan ja vuoden 2023 aikana henkilöstö on osallistunut TEM:n järjestämiin koulutuksiin. Koulutukset jatkuvat vuonna 2024.

Suunnittelun ja osaamisen vastuualueella riskienhallintasuunnitelmat ovat ajantasaisia maakuntakaavoituksen ja maakuntaohjelman osalta, mutta maakuntaohjelman osalta suunnitelmaa tarkastellaan uudelleen loppuvuodesta 2024 työsuunnitelman laatimisen yhteydessä, osana maakuntaohjelmien ulkoista arviointia. Vastuualueella on tehty riskienhallintasuunnitelmien lisäksi keskeisistä riskeistä nelikenttäanalyyseja. Sisäisen tarkastuksen vastuuhenkilö on käynyt perehdyttämässä riskienhallintasuunnitelmien toimeenpanoa ja seurantaa Suunnittelu- ja osaaminen – vastuualueen henkilöstölle tarkastusjakson aikana.

Tarkastusjakson aikana on tunnistettu riskejä, joita ei ole kuvattu nykyisissä riskienhallintasuunnitelmissa. Tällaisia riskejä ovat mm. erilaiset henkilöstöön ja toimitiloihin liittyvät riskit sekä varautumiseen liittyvät riskit. Uusien tunnistettujen tai toteutuneiden riskien ja niihin liittyvien toimenpiteiden kirjaaminen riskienhallintasuunnitelmiin on tärkeää, jotta vastaavanlainen riski voitaisiin jatkossa välttää.

Sopimukset ja päätökset ovat asiakirjoja, jotka luovat liitolle mm. taloudellisia oikeuksia ja velvollisuuksia. Riskienhallintasuunnitelmien ja riskien seurannan lisäksi **sopimustenhallinta on keskeinen riskien- ja kustannustenhallinnan väline**. Puutteellinen sopimustenhallinta tai sopimusosaaminen ovat riskejä, joiden toteutuminen on mahdollinen kaikilla vastuualueilla.

Suositukset

Tavoitteena on saada jatkossa sisäinen valvonta ja riskienhallinta johtoryhmätyöskentelyn avulla ennakoivaksi, säännölliseksi, järjestelmälliseksi ja dokumentoiduksi kuntalain ja hallintosäännön edellyttämällä tavalla vastuualueilla jo tehtävän riskienhallinnan lisäksi. Jotta sisäisen valvonnan riskienhallinnan havainnot saataisiin jatkossa säännöllisesti käsiteltyä ja rekisteröityä, **suositellaan, että johtoryhmä suunnittelee johtoryhmän kokoontumisen aikatauluun sopivan säännöllisen tarkastusvälin vuosikellomallin mukaisesti** esimerkiksi kolme kertaa vuodessa. Tarvittaessa sisäiseen valvonnan ja riskienhallinnan ad hoc -asiat otetaan johtoryhmän esityslistalle käsiteltäväksi vuosikellon aikataulusta riippumatta.

Vuosikellomallin avulla vastuualueiden **henkilöstö rekisteröi säännöllisin väliajoin havainnot kohonneista tai toteutuneista riskeistä ja tarpeen mukaan ne käsitellään vastuualueiden palavereissa, jotta vastuualuejohtaja voi arvioida riskin merkittävyyttä ja tarvetta raportoida johtoryhmälle**. Sisäisen valvonnan ja riskienhallinnan seuraamiselle suositellaan avattavaksi vastuualueittain asiarekisteriin vuosiasiat, joihin vastuualueen viran- ja toimenhaltijat rekisteröivät mahdolliset toteutuneet ja kohonneet riskit taulukoihin sekä tiedon, että toteutuneita tai kohonneita riskejä ei ole havaittu. Myös tieto siitä, että riskejä ei ole havaittu, on osa toimivaa sisäistä valvontaa ja riskienhallintaa.

Sopimusten hallintaan ja sopimusosaamiseen suositellaan kiinnitettävän aiempaa enemmän huomiota. Sopimuksiin ja päätöksiin liittyviä riskejä voidaan ehkäistä mm. kahden valmistelijan toimintatavalla, jossa asiakirjat, jotka luovat Pohjois-Pohjanmaan liitolle merkittäviä taloudellisia oikeuksia ja velvollisuuksia, tarkistettaisiin vähintään kahden valmistelijan toimesta ennen päätöksen tai sopimuksen tekemistä. Mikäli liitolla on lakimiesresurssia käytettävissä, **tapauskohtaista harkintaa käyttäen on suositeltavaa hyödyntää lakimiehen konsultaatiota** etenkin niissä tapauksissa, joissa sopimusta ei laadita liiton tekemälle sopimuspohjalle. Liiton toimintaympäristö on kansallinen sekä kansainvälinen, jonka vuoksi kansainvälisten sopimusten ja muiden asiakirjojen hyväksyntään suositellaan kiinnitettävän erityistä huomiota kielen ja sovellettavan lainsäädännön osalta. Suositeltavaa olisi, jos liitto voisi **hankkia harkintaan perustuen käännös- sekä laki- ja sopimusteknistä palvelua.**

Riskienhallintasuunnitelmia suositellaan täydennettäväksi henkilöstöriskien osalta, kuten varahenkilöjärjestelyt ydintoiminnoissa, henkilöstön riittävä ohjeistus ja osaaminen tietojärjestelmien käytössä, matkustaminen sekä työskentelyolosuhteet työpaikalla. Jatkuvuudenhallinta normaaliajan häiriötilanteissa ja varautuminen poikkeusoloissa ovat osa riskienhallintaa. **Riskienhallinnan tai varautumisen suunnitelmissa suositellaan huomioitavaksi aiempaa laajemmin mm. kyberhyökkäykset ja tiloihin liittyvät riskit, kuten tulipalot ja vesivahingot.** Liiton ydintehtävien osalta varautuminen on huomioitava myös kriittisten sopimuskumppanien kanssa tehtävissä sopimuksissa ja sopimuksiin täytyy sisällyttää varautuminen ja jatkuvuudenhallinta jo hankinnan tarjouspyyntövaiheessa. Varautumisen ja jatkuvuudenhallinnan tavoitteet täytyy sisällyttää hankinta- ja sopimusohjeistukseen siten, että ydintehtävien ja kriittisten toimintojen jatkuvuus voidaan turvata myös sopimussuhteisesti järjestetyissä palveluissa, jotta kriittinen tukipalvelu ei pysäytä liiton toimintaa häiriötilanteessa.

Tietoturva ja tietosuoja

Tietoturvan ja tietosuojan osalta tarkastettiin:

- Onko tietoturva- ja tietosuojasäännössä kuvattuja keskeisiä toimenpiteitä noudatettu Pohjois-Pohjanmaan liiton toiminnassa
- Onko tietoturva- ja tietosuojasäännössä kuvattuihin keskeisistä toimenpiteistä annettu tarkentavat ohjeet ja tarpeellinen koulutus henkilöstölle

Pohjois-Pohjanmaan liiton tietoturva- ja tietosuojasääntö on hyväksytty Maakuntahallituksessa 23.5.2022 § 82. Tietoturvan ja tietosuojan organisointi ja johdon vastuut perustuvat liiton hallintosääntöön. Maakuntajohtajalla on kokonaisvastuu maakunnan liiton tehtävien yhteensovittamisesta. Hallinto- ja henkilöstöjohtaja toimii hallinnon vastuualueelle kuuluvan tietohallinnon hallinnollisena esimiehenä, sekä vastaa tehtävien taloudellisesta ja tuloksellisesta hoidosta ja asetettujen tavoitteiden saavuttamisesta. Tietohallintopäällikkö vastaa tietoturvan ja tietosuojan toteuttamisesta ja toimeenpanosta tehtävänkuvansa mukaisesti. Tietosuojavastaavana toimii tietohallintopäällikkö. Tietoturvaan ja tietosuojaan liittyviä asioita on hoitanut tietohallintopäällikön lisäksi hallintojohtaja, viestintä- ja hallintopäällikkö sekä hallinnon kehittämispäällikkö.

ICT-palveluita tuottaa Pohjois-Pohjanmaan liitolle Kuntien Tiera Oy ja Loihde Oyj. Loihde vastaa tietoliikenneyhteyksistä, palomuurista, tietoliikenneyhteyksien kahdentamisesta, sisäverkon kytkimistä ja nimipalveluista. Palvelimiin ja työasemiin liittyvät palvelut tuottaa Tiera. Vuoden 2023 aikana on jatkettu ICT-palveluiden palvelutuotannon siirtämistä Tieralle mm. mobiililaitteiden hallinnan osalta. ICT-kokonaisuuden hallinta on vielä tällä hetkellä hajanainen, koska palveluiden ulkoistaminen on toteutettu vasta osittain.

Tietosuojalainsäädännön perusteella henkilötietoja ovat sellaiset tiedot, joiden perusteella henkilö voidaan tunnistaa suoraan tai välillisesti esimerkiksi yhdistämällä yksittäinen tieto johonkin toiseen tietoon, joka mahdollistaa tunnistamisen. Tietosuoja-asetus suojaa henkilötietoja riippumatta siitä, mitä tekniikkaa tietojenkäsittelyssä käytetään. Tietojen säilytystavalla ei myöskään ole merkitystä. Tietoja voidaan säilyttää esimerkiksi tietojärjestelmässä tai fyysisessä tilassa paperiarkistossa. Tietoturva tarkoittaa organisatorisia ja teknisiä toimenpiteitä, joilla varmistetaan tiedon luottamuksellisuus ja eheys sekä järjestelmien käytettävyys.

Rajaus ja menetelmät

Tarkastus toteutettiin haastattelemalla tietohallintopäällikköä annetusta ohjeistuksesta ja henkilöstön koulutuksista, perehtymällä liiton Teamsin eri kanavissa oleviin ohjeisiin sekä tutustumalla liiton tilaratkaisuihin, joissa viranomaisen asiakirjoja säilytetään ja hävitetään. Tarkastuksessa ei tarkastettu ulkoisten palveluntuottajien toimintaa ja niiden tehtävien tietoturvan ja tietosuojan ohjeistuksia, joissa liitto ei toimi rekisterinpitäjänä.

Havainnot

Tietohallintopäällikkö seuraa tietoturvapoikkeamia lokeista Microsoftin sivuilta. Vuonna 2023 tietoturvapoikkeamia ja tietoturvaloukkauksia ei ole havaittu, eikä palveluntuottaja Tieralle ole ilmoitettu tietoturvapoikkeamista. Vuonna 2023 tietoturvaa on parannettu ottamalla käyttöön Multi-Factor Authentication (MFA) eli kaksivaiheinen käyttäjän tunnistaminen sekä käyttäjän tunnistamisen työkalu Microsoft Authenticator -sovellus.

Tietojärjestelmien käyttäjähallinta ei ole keskitettyä, eikä käyttöoikeuksien hakemiseen, myöntämiseen ja poistamiseen ole suunniteltua toimintatapaa, vaan eri järjestelmien pääkäyttäjät myöntävät ja poistavat käyttöoikeudet. Toimintatavan puuttuessa työntekijälle voidaan myöntää liian laajat oikeudet tarkastella ja käsitellä salassa pidettäviä tai henkilötietoja sisältäviä asiakirjoja tai tietoja. Käyttöoikeudet voivat myös jäädä poistamatta työtehtävien muuttuessa tai palvelussuhteen päättyessä.

Henkilöstön koulutus tietoturvaan ja tietosuojaan liittyen ei ole ollut säännöllistä ja koulutus on toteutettu henkilöstöinfoissa ns. tietoiskuina. Vuonna 2023 henkilöstölle on annettu info nettihuijauksista. Myös tietojen kalasteluviesteistä on varoitettu henkilökuntaa. Käytössä ei ole ollut toimintatapaa, jossa henkilöstö olisi velvoitettu osallistumaan infoihin tai koulutuksien suorittamista olisi seurattu tai dokumentoitu.

Tietoturva- ja tietosuojasäännön tarkentavat ohjeistukset ovat hajallaan Teamsin eri kanavien tiedostoissa tai ne on annettu sähköpostiviesteissä vapaamuotoisesti. Tietyiltä osin ohjeet puuttuvat. Pohjois-Pohjanmaan liitolla ei ole ohjeistusta, mihin tietojärjestelmiin voi tallentaa henkilötietoja tai salassa pidettäviä tietoja tai salassa pidettävien tietojen ja henkilötietojen lähettämistä sähköisesti ei ole ohjeistettu. Liiton käyttämä sähköposti on Microsoftin pilvisähköposti**, eikä liitolla ole käytössä ns. turvasähköpostipalvelua, jolla salassa pidettävä tai henkilötietoja sisältävät tiedot ja asiakirjat voisi lähettää tai vastaanottaa tietoturvallisesti.** Tiedonohjaussuunnitelmassa ei ole huomioitu sähköisten tietojen säilyttämistä ja hävittämistä muissa tietojärjestelmissä kuin asianhallintajärjestelmässä tai palvelun tuottajan tietojärjestelmissä.

Liitolla on kaksi päätearkistokäytössä olevaa arkistotilaa, jotka eivät kuitenkaan täytä Kansallisarkiston arkistotilalle asettamia vaatimuksia. Arkistotiloissa säilytetään henkilötietoja sekä salassa pidettäviä tietoja sisältäviä viranomaisen asiakirjoja. **Tiloihin kulkua ei ole rajoitettu asianmukaisella tavalla vain niille työntekijöille, joiden työtehtäviin arkiston hoitaminen kuuluu. Toimistokerroksessa olevassa arkistotilassa ei ole ovea, eikä lukkoa**. Toinen arkistotila on samassa kiinteistössä, mutta erillään muista liiton käytössä olevista tiloista. **Arkistotilana käytetty tila ei ole pelkästään liiton käytössä, vaan tila on yhteiskäytössä yksityisen toimijan kanssa, joka toimii samassa kiinteistössä**.

Tietoturvaan ja tietosuojaan kuuluu myös, että viranomaisen asiakirjat ja tiedot on hävitettävä tietoturvallisesti, kun ennalta määritelty säilytysaika päättyy. **Paperilla tai muussa fyysisessä muodossa olevien asiakirjojen ja tietojen tietoturvallista säilyttämistä ja hävittämistä ei ole ohjeistettu Tiedonhallinta ja arkistointisäännössä**. Asiakirjojen ja tietojen hävittäminen ei ole ollut järjestelmällistä. Liitto ostaa palveluna lukittavia tietosuojasäiliöitä, joihin henkilötietoja ja salassa pidettäviä tietoja sisältävät asiakirjat laitetaan ja palvelun tuottaja noutaa säiliöt sekä hoitaa asiakirjojen hävittämisen tietoturvallisella tavalla. **Tietosuojasäiliöitä on pidetty lukitsemattomina tyhjennysten välillä.** Salassa pidettäviä ja henkilötietoja sisältäviä asiakirjoja on jouduttu hävittämään perinteisellä silppurilla, eikä hankittu tietoturvasäiliöpalvelu ole tarkoituksen mukaisessa ja täysimääräisessä käytössä.

Suositukset

ICT-palveluiden ulkoistamisesta huolimatta Pohjois-Pohjanmaan liitolla viranomaisena säilyy edelleen vastuu ICT-palveluiden järjestämisestä ja tietojen käsittelemisestä lainsäädännön mukaisesti. **Tämän vuoksi on varmistettava, että liitolla on riittävä tilaajaosaaminen ICT-palveluiden hankinnassa ja neuvotteluissa sekä tietoturvaan ja tietosuojaan liittyvässä ohjeistamisessa.**

Tietoturvaan ja tietosuojaan liittyvä ohjeistus suositellaan koottavaksi intranetiin yhteen paikkaan, jotta ohjeistus on löydettävissä helposti. Ohjeet suositellaan annettavan asiakirjamuotoisina ilman ulkoisia

hyperlinkkejä, jotta ohjeistuksen eheys ja muuttumattomuus pystytään varmistamaan. Soveltuvin osin ohjeet suositellaan tehtäväksi yhteistyössä palvelun tuottajan kanssa, mikäli se on mahdollista palvelusopimuksen puitteissa. **Tarvittaessa suositellaan hankittavan ajankohtaista tietoturva- ja tietosuojakoulutusta henkilöstölle myös organisaation ulkopuolelta.** Suositeltavaa on, että tiettyihin koulutuksiin työntekijät velvoitetaan osallistumaan ja osallistuminen dokumentoidaan.

Tietojärjestelmien käyttöoikeuksien hakeminen määrämuotoisesti suositellaan ohjeistettavaksi. Tietoturva- ja tietosuojasääntöä täydentäviä ohjeita suositellaan laadittavaksi myös muista kuin varsinaisista asiakäsittely- ja rekisteröintijärjestelmistä. Ohjeistus suositellaan laadittavaksi etenkin niistä tietojärjestelmistä, joissa käsitellään henkilötietoja tai mikäli tiedot liittyvät hankintaan tai tilaamiseen. Tällaisia järjestelmiä ovat mm. Teams, Outlook, Gmail, WhatsApp tai Instagram. Tiedonohjaussuunnitelmia suositellaan täydennettäväksi niiltä osin, kun tietoja käsitellään muissa tietojärjestelmissä kuin asiarekisterissä. **Ohjeistuksessa täytyy huomioida erilaiset käytössä olevat päätelaitteet, kuten pc:t ja mobiililaitteet.**

Pohjois-Pohjanmaan liiton kokoisessa organisaatiossa ei ole tarkoituksenmukaista tai kustannustehokasta hankkia yksittäisiä tehtäviä varten erillisiä sähköisen asioinnin järjestelmiä tai muita tietojärjestelmiä, vaan viranomaistehtäviä hoidetaan myös sähköpostilla. **Liitolle suositellaan hankittavaksi kustannustehokas turvasähköpostipalvelu, jotta salassa pidettävät tiedot ja asiakirjat sekä henkilötiedot voidaan tarvittaessa vastaanottaa ja lähettää tietoturvallisesti.**

Toimistotiloissa olevaan arkistotilaan suositellaan asennettavaksi lukollinen ovi, **jotta paperiasiakirjojen säilytys toteutuu tietoturvallisesti.** Arkistojen järjestämisen ja asiakirjojen hävittämisen yhteydessä suositellaan selvitettäväksi, voidaanko pysyvästi säilytettäville ja pitkään säilytettäville sekä henkilötietoja ja salassa pidettäviä tietoja sisältävälle aineistolle järjestää toimiston yhteyteen tila, jossa asiakirjat voidaan säilyttää asianmukaisesti. **Kulkuoikeudet arkistontiloihin annetaan työntekijöille, joiden työtehtäviin arkiston hoitaminen kuuluu.**

Tiedonhallinta- ja arkistosääntöä suositellaan täydennettäväksi asiakirjojen hävittämisen osalta. Tietosuojasäiliöt suositellaan pidettävän jatkossa lukittuina myös tyhjennysten välillä, jotta hävitettävät asiakirjat voidaan laittaa niihin tietoturvallisesti ja hankittu palvelu vastaa tarkoitustaan.

Hankinnat

Hankintojen osalta tarkastettiin:

- Onko sisäisessä tarkastuksessa vuonna 2022 annettuja toimenpide-ehdotuksia huomioitu hankintojen toteutuksessa
- Onko hankinnoissa havaittujen puutteiden ja virheiden määrä vähentynyt vuoteen 2022 verrattuna

Rajaus ja menetelmät

Tarkastus toteutettiin niihin hankintoihin, joissa Pohjois-Pohjanmaan liitto toimii hankintayksikkönä, yhteishankintoihin osallistumista ei tarkastettu. Tarkastuksessa ei tarkastettu hankkeiden rahoittajan antamien ohjeiden täyttymistä hankinnoissa, vaan kansallisen lainsäädännön ja Maakuntahallituksen antaman hankintaohjeen noudattamista. Tarkastuksessa ei myöskään arvioitu hankintojen tarkoituksenmukaisuutta. Tarkastus toteutettiin asiarekisterissä vuonna 2023 avattujen ja päättyneiden hankinta-asioiden ja niiden asiakirjojen avulla.

Havainnot

Valtaosa Pohjois-Pohjanmaan liiton vuoden 2023 hankinnoista ovat olleet kansallisen kynnysarvon alittavia, ns. pienhankintoja, joita ei tarvitse kilpailuttaa hankintalain mukaisesti, vaan niiden kilpailuttamiseen sovelletaan kuntalakia ja hallintolakia, Pohjois-Pohjanmaan liiton hallintosääntöä sekä hankintaohjetta. Hallintosäännön mukaisesti hankintalain kynnysarvot ylittävistä hankinnoista päättää Maakuntahallitus. Maakuntajohtajan hankintaraja on 60 000 € ja vastuualuejohtajien hankintaraja on 10 000 €.

Virheiden määrä hankinnoissa on vähentynyt jonkin verran (n. 10 %) vuoteen 2022 verrattuna. Tarkastuksessa havaittiin, että valtaosassa (78 %) hankinnoissa hankintaohjeen vaatimukset hankintaprosessin rekisteröinnistä, tarjouspyynnöstä, hankintapäätöksen sisällöstä ja täytäntöönpanosta täyttyvät pääosin. Hankintapäätökset on yleensä tehty oikea-aikaisesti ennen hankintaa. **Puutteet hankintaprosessissa eivät ole tarkastuksen perusteella aiheuttaneet Pohjois-Pohjanmaan liitolle sellaisia riskejä, joista olisi aiheutunut vähäistä suurempia taloudellisia tai toiminnallisia riskejä. Tarkastusjaksolla ei ole rekisteröity hankintoihin kohdistuvia hankintaoikaisuja tai valituksia markkinaoikeuteen.** Tarkastuksessa havaittiin, että olemassa olevaa hankintaohjeistusta sekä lainsäädäntöä, kuten hallinto- tiedonhallinta- ja hankintalakia, noudattamalla sekä hankintaohjeen täydentämisellä ja koulutuksella tarkastuksessa havaittuja virheitä olisi voitu ja voidaan jatkossa tehokkaammin välttää.

Tiedonhallintalaki velvoittaa viranomaista rekisteröimään kaikki asian käsittelyn vaiheet ja niihin liittyvät asiakirjat. **Hankintojen rekisteröinti on ollut puutteellista joidenkin hankintaprosessin vaiheiden ja asiakirjojen osalta.** Esimerkiksi lisätietopyyntöjä ja vastauksia niihin ei ole kaikissa hankinnoissa rekisteröity asiarekisteriin. Myös tarjousten avauspöytäkirjojen rekisteröinnissä sekä päätösten tiedoksi antamisen ja päätöksen täytäntöönpanon ja ko. käsittelyvaiheen tietojen rekisteröinnissä on puutteita.

Pohjois-Pohjanmaan liiton hankintaohjeen mukaan hankintapäätöksestä tai sen liitteistä on käytävä ilmi hankinnan kohde, valittu hankintamenettely ja perustelu, tarjousten vertailu, hankinnan kokonaisarvo, hankinnan

kustannusten kohdentaminen, tieto, mikäli päätös toimii tilausvahvistuksena sekä mahdollinen hankinnan keskeyttäminen perusteluineen. Lisäksi hankinta-asialle on rekisteröitävä tarjouspyyntö tai vaihtoehtoisesti tarjouspyynnön korvaava hintavertailu täytyy löytyä hankintapäätöksestä, päätöksen tiedoksianto sekä tarvittavat toimeenpanotiedot, kuten hankintasopimus tai tieto, että hankintapäätös toimii tilausvahvistuksena.

Hankintapäätöksissä on jonkin verran puutteita kaikilla osa-alueilla. Esimerkiksi hankinnan kohteen kuvailussa tulisi käydä selkeästi ilmi, hankintaanko tavaraa vai palvelua tai molempia. Etenkin 3000 € ylittävistä **suorahankintapäätöksistä puuttuivat hankintaohjeen mukaiset perustelut, miksi hankinta oli toteutettu suora hankintana tietyltä toimittajalta.** Tilanteissa, joissa hankinta toteutetaan **yhteishankintana toisen viranomaisen kanssa tai toinen viranomainen toimii hankintayksikkönä ja Pohjois-Pohjanmaanliitto osallistuu hankintaan, täytyy käydä selkeästi ilmi, mikä tai mitkä viranomaiset toimivat hankintayksikkönä ko. hankinnassa.**

Hankintaohjeessa on ohjeistettu toteuttamaan hankinta hankintalain kynnysarvon ylittävänä hankinta, mikäli hankinnan arvo on arvioitu lähelle hankintalain mukaista kynnysarvoa. **Tarkastusjaksolla arvoltaan kansallista kynnysarvoa lähellä oleva hankinta on toteutettu ns. pienhankintana. Tämän kaltaisissa tilanteissa riskinä on, että tarjouspyyntö ei välttämättä tavoita kaikkia potentiaalisia tarjoajia ja useampia tarjouksia ei saada, hankinnan todellista arvoa ei saada selville, päätöksen tekijä ylittää toimivaltansa tai päätökseen kohdistuu muutoksenhaku puutteellisen hankintamenettelyn vuoksi, mikäli hankinnan kokonaisarvo ylittää hankintalain mukaisen kynnysarvon.**

Osassa hankinnoissa ei ole tehty hankintasopimusta, vaikka kyseessä on arvoltaan suhteellisen suuri hankinta liiton kokoisessa organisaatiossa, vaan hankintapäätös toimii samalla tilauksena ja sopimuksena. Kaikissa päätöksissä ei ole mainittu, että päätös toimii tilauksena, mutta erillistä hankintasopimusta ei kuitenkaan ole tehty tästä huolimatta. Hankintaohjeessa ei ole ohjeistettu hankintasopimusvaihetta, joka voi osaksi selittää hankintasopimusten puuttumisen osassa hankinnoissa.

Suositukset

Hankintaohjetta suositellaan tarkennettavaksi hankinnan eri vaiheiden ja niiden asiakirjojen, kuten lisätietopyyntöjen tai tarjousten avauspöytäkirjojen**, rekisteröinnin osalta, jotta rekisteröinti vastaa tiedonhallintalain vaatimuksia**. Rekisteröinnillä varmistetaan myös viranomaisen asiakirjojen säilyttäminen ja hävittäminen asianmukaisesti.

Asiarekisterin asiakirjapohjiin suositellaan lisättäväksi valmistelijaa ohjaavia tekstejä, kuten valittu hankintamenettely ja tarvittaessa perustelu valitulle hankintamenettelylle, hintavertailu, tieto valitusta toimittajasta sekä maininta erillisen hankintasopimuksen laatimisesta tai hankintapäätöksen toimimisesta tilauksena. **Etenkin suorahankinnalle täytyy esittää päätöksessä perustelu, miksi suorahankinta on valittu menettelyksi kilpailutuksen sijaan. Lisäksi päätöksestä täytyy käydä selkeästi ilmi, toimiiko liitto hankintayksikkönä hankinnassa, mikäli hankinta toteutetaan yhdessä toisen viranomaisen kanssa.**

Hankintalain mukaisissa kynnysarvon ylittävissä hankinnoissa sopimuksen keskeiset ehdot täytyy olla esitettynä jo tarjouspyyntövaiheessa. Suuri osa liiton hankinnoista alittaa hankintalain mukaisen kansallisen kynnysarvon. **Myös kansallisen kynnysarvon alittavissa hankinnoissa on suositeltavaa laatia hankintasopimus, ellei se ole ilmeisen tarpeetonta.** Hankintasopimuksen tekeminen on molempien sopimusosapuolten etu mahdollisissa hankintaan liittyvissä erimielisyyksissä. **Sopimuksen laatiminen on keskeinen hankintojen riskien- ja kustannusten hallintakeino.**

Tällä hetkellä hankintaohjeessa on ohjeistettu käyttämään tarjouspyyntöpohjaa, jossa on kuvattu hankinnassa ja tarjouksessa noudatetaan tiettyjä yleisiä ehtoja ja vaatimuksia. **Hankintaohjetta suositellaan täydennettäväksi päätöksen täytäntöönpano- ja hankintasopimusosiolla**. Tapauskohtaisesti arvioidaan, millaisessa pienhankinnassa sopimusta ei tarvitse laatia.

Hankintaohjeen päivittämisen jälkeen, **suositellaan, että hankintatiimi järjestää vuoden 2024 aikana Pohjois-Pohjanmaan liiton henkilöstölle koulutuksen tai infon, jossa koulutetaan hankintaohjeen uudet ja päivitetyt osiot sekä käydään läpi niitä hankintaprosessin vaiheita, joissa on havaittu puutteita**.