INNOFACTOR®

GDPR:n mukainen tietosuojakuvaus Dynasty ja Dynasty TOJ

Selvitys
19. kesäkuu 2019

Public

Versiohistoria

Vastuuhenkilöt: Niko Lappalainen

Tarkastajat: Camillo Särs, Sami Huotari

Versio	Päivämäärä	Laatija (t)	Kuvaus	Tarkastaja	Hyväksyjä
1.0	3.5.2018	TNa, JNe	Ensimmäinen versio	CaSä, SaHu 26.4.2018	CaSä
1.1	3.1.2018	NLa	Päivitetty versio	CaSä, SaHu	

Sisältö

Keilaranta 9
FI-02150 Espoo Finland
contact@innofactor.com
www.innofactor.fi
tel.: +358 10 272 9000
fax: +358 10 272 9001

1 Dynasty asianhallinta ja Dynasty tiedonohjaus

Innofactorin Dynasty asianhallintajärjestelmä (case management system) ja Dynasty TOJ tiedonohjausjärjestelmä ovat kunnan **asianhallintaan**, **asiankäsittelyyn** ja **arkistointiin** tarkoitettuja järjestelmiä. Niiden avulla organisaatio hoitaa toimintaan kuuluvien asioiden, asiakirjojen ja töiden hallintaa, valmistelua, päätöksentekoa ja arkistointia.

Asianhallinta on asioiden ja niihin liittyvien asiakirjojen käsittelyn ohjaamista niiden koko elinkaaren ajan. Asianhallintaan sisältyy asiankäsittely, asiakirjahallinta ja arkistointi. **Asiankäsittely** tarkoittaa viranomaisen prosessia, jossa asia käsitellään laissa määritellyn hallintomenettelyn mukaisesti. Asiankäsittelyn päävaiheet ovat vireilletulo, valmistelu, päätöksenteko, tiedoksianto, muutoksenhaku ja seuranta.

Tiedonohjaus tuottaa asiakirjatiedon käsittelyn ja hallinnan edellyttämät metatiedot asiakirjatietoa käsitteleviin tietojärjestelmiin. Pysyvästi säilytettävän asiakirja-aineiston sähköinen arkistoiminen ei ole mahdollista ilman tiedonohjauksen tuottamia metatietoja.

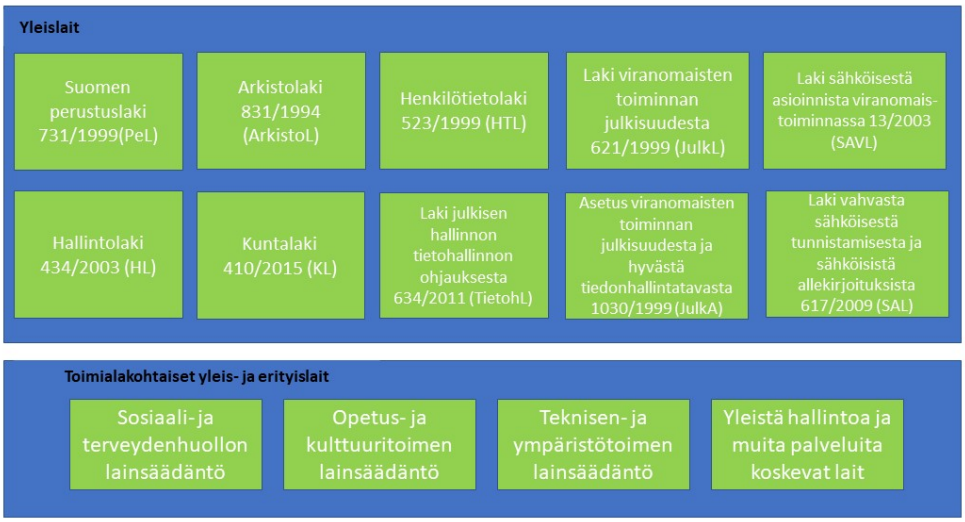
Dynasty-tuoteperheeseen kuuluu edellä mainittujen tietojärjestelmien lisäksi myös useita julkaisusovelluksia, joiden avulla kunnassa hoidetaan kuntalain edellyttämää kuntalaisten tiedonsaantioikeutta. Näitä ovat: esityslistojen ja pöytäkirjojen julkaisusovellus, jonka avulla julkaistaan yleiseen tietoverkkoon kunnan esityslistat ja pöytäkirjat liitteineen ja muutoksenhakuohjeineen; viranhaltijapäätösten julkaisusovellus, joka mahdollistaa julkisten viranhaltijapäätösten julkaisemisen kunnan verkkosivuilla; sekä kuulutusten julkaisusovellus, jonka avulla voidaan hallita kuulutusten nähtävilläoloaikaa.

Dynasty-tuoteperheen tietojärjestelmät ovat kunnan toiminnassa keskeisessä asemassa. Järjestelmien avulla kunta voi toteuttaa kuntalain mukaista perustarkoitustaan, joka on luoda edellytykset kunnan asukkaiden itsehallinnon sekä osallistumis- ja vaikuttamismahdollisuuksien toteutumiselle kunnan toiminnassa. Keskeisen aseman vuoksi järjestelmien tulee noudattaa korkeita tietoturva- ja tietosuojavaatimuksia. Asianhallintajärjestelmällä hallitaan kunnan päätöksentekoon liittyvät prosessit ja riskienhallinnan näkökulmasta se on yksi kunnan tärkeimmistä tietojärjestelmistä, jonka toimimattomuus vaarantaisi tai viivästyttäisi kunnassa tapahtuvaa päätöksentekoa ja asioiden käsittelyä.

Asianhallintajärjestelmässä käsitellään henkilötietoja, mutta järjestelmään kerätään henkilötietoja vain niiltä osin kuin asioiden vireillesaattaminen vaatii. Järjestelmään ei tule kerätä henkilötietoja, ellei asioiden vireilletulo, päätöksenteko tai tiedoksianto sitä välttämättä vaadi.

Asianhallintaa säätelee joukko yleis- ja erityislakeja. Asioiden käsittelyä ja niihin liittyviä toimenpiteitä sekä asiakirjatiedon tuottamista ohjaava lainsäädäntö voidaan kuvata alla olevan kuvan mukaisesti. Järjestelmät on suunniteltu siten, että niiden avulla voidaan toteuttaa yksityiselämän suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistämään hyvän tietojenkäsittelytavan kehittämistä ja noudattamista kunnissa.

Asianhallintaa säätelevä lainsäädäntö



Tiedonhallinnan lainsäädäntöön on tulossa muutoksia. Dokumentin laadintahetkellä Talvella 2019 eduskunnan vireilletulotiedon mukaan eduskunta käsittelee lakiehdotuksen kevätistuntokaudella 2019. Laki tulisi voimaan vuonna 2019. Dokumentaatiota tullaan päivittämään siinä vaiheessa, kun tiedetään, millä tavalla laki tulee vaikuttamaan toimintaa ohjaavaan lainsäädäntöön.

2 Henkilötietojen käsittelyä koskevat periaatteet (artikla 5)

EU:n tietosuoja-asetuksen mukaan rekisterinpitäjän (organisaatio xxx) on varmistettava, että henkilötietojen käsittelyyn käytettävä järjestelmä täyttää sisäänrakennetun ja oletusarvoisen tietosuojan vaatimukset. Dynasty-tuoteperheen näkökulmasta sisäänrakennetun tietosuojan vaatimukset täyttyvät seuraavassa kuvatulla tavalla.

Rekisterinpitäjä huolehtii siitä, että kerättyjä henkilötietoja käsitellään lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi (**”lainmukaisuus, kohtuullisuus ja läpinäkyvyys”**). Dynasty tiedonohjausjärjestelmä sisältää rekisteriseloste-moduulin, jolla rekisterinpitäjä laatii ja ylläpitää kirjalliset selosteet käsittelytoimista (artikla 30) sekä rekisteröidyn informoimiseen tarkoitetut julkiset tietosuojakuvaukset.

Rekisterinpitäjän on seurattava, että henkilötietoja kerätään tiettyä, nimenomaista ja laillista tarkoitusta varten. Henkilötietoja ei myöskään käsitellä alkuperäiseen tarkoitukseen sopimattomalla tavalla (**”käyttötarkoitussidonnaisuus”**).

Rekisterinpitäjän on huolehdittava siitä, että henkilötietojen on oltava asianmukaisia ja olennaisia. Henkilötietoja on kerättävä vain tarpeellinen määrä, jotta asian käsittely ei vaarantuisi. Rekisterinpitäjä huolehtii siitä, että henkilötietoja kerätään vain minimimäärä kutakin tarkoitusta varten (**”tietojen minimointi”**).

Rekisterinpitäjä vastaa siitä, että organisaatiossa henkilötietoja käsittelevällä henkilöstöllä on riittävä ja ajanmukainen koulutus henkilötiedon käsittelyyn. Ohjeistuksen on myös oltava ajan tasalla (määräykset, sitoumukset, tilivalvonta, omavalvonta). Henkilötietojen käsittelijän (Innofactor Oyj) on huolehdittava oman henkilöstönsä koulutuksesta asiakkaan henkilötietojen käsittelyssä. Rekisterinpitäjä voi tarvittaessa ohjeistaa henkilötietojen käsittelijää. Asiakas ja toimittaja (Innofactor) sopivat erikseen siitä henkilötietojen käsittelystä, jota toimittaja tekee asiakkaan lukuun (artikla 28). Olemassa olevia sopimuksia on täydennetty sopimusliitteellä *Sopimus henkilötietojen käsittelystä*.

Rekisterinpitäjän vastuulla on, että kerätyt henkilötiedot ovat täsmällisiä ja oikein. Epätarkat ja virheelliset henkilötiedot poistetaan tai tarvittaessa oikaistaan viivytyksettä (**”täsmällisyys”**).

Henkilötietoja on säilytettävä muodossa, josta rekisteröity on tunnistettavissa vain niin kauan kuin on tarpeen alkuperäisen tarkoituksen toteuttamiseksi. Henkilötietoja voidaan säilyttää pidempiä aikoja, jos niitä käsitellään ainoastaan yleisen edun mukaisia arkistointitarkoituksia varten (**”säilytyksen rajoittaminen”**). Jotta rekisterinpitäjän on käytännössä mahdollista rajoittaa säilytystä, on sen luokiteltava tietovarantonsa. Tiedon luokittelua varten on olemassa tiedonohjausjärjestelmä Dynasty TOJ. Jotta GDPR:n vaatimukset täyttyvät, Innofactor suosittelee tiedonohjausjärjestelmän käyttöönottoa ja integroimista asianhallintajärjestelmään, sillä tämä mahdollistaa mm. säilytysaikojen määrittelyn rekisterinpitäjän tuottamalle tiedolle. Tiedonohjausjärjestelmä tuottaa metatietona myös henkilötietoluonnetiedon (ei sisällä henkilötietoja, sisältää henkilötietoja, sisältää arkaluonteisia henkilötietoja) kaikelle järjestelmässä tuotettavalle tiedolle.

Henkilötietoja on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus. Dynasty TOJ tuottaa metatietona säilytysaikojen ja henkilötietoluonteen ohella myös tiedon turvallisuusluokittelun ja suojaustason. Tiedot on suojattava luvattomalta ja lainvastaiselta käsittelyltä käyttäen asianmukaisia teknisiä ja organisatorisia toimia (**”eheys ja luottamuksellisuus”**). Luvussa henkilötietojen käsittelyn turvallisuus (luku 4) kuvataan järjestelmien tekniset keinot suojata tietoa järjestelmissä.

Rekisterinpitäjän on lisäksi pystyttävä osoittamaan, että edellä mainittuja kohtia on noudatettu (**”osoitusvelvollisuus”**). Rekisterinpitäjän on dokumentoitava tehdyt toimenpiteet. Järjestelmä tarjoaa teknisinä turvaamistoimina seuraavia keinoja:

-

3 Sisäänrakennettu ja oletusarvoinen tietosuoja (Privacy by Design ja Privace by Default) (artikla 25)

Tietoaineisto jaetaan loogisesti kahteen osaan: järjestelmän operatiivinen tieto eli asia, käsittelyvaihe, toimenpide/asiakirja ja dokumenttitiedot metatietoineen sekä järjestelmää tukevat tiedot, kuten esimerkiksi loki- ja käyttäjätiedot. Näiden tietoaineistojen turvaamisessa noudatetaan VAHTI-ohjeiden mukaista turvallisuustasoa.

3.1 Järjestelmän operatiivinen tieto ja sen suojaaminen

3.1.1 Pääsynvalvonta ja käyttövaltuusperiaatteet

Rekisterinpitäjän on varmistettava, että oletusarvoisesti käsitellään vain kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja. Pääsynvalvontaperiaatteet järjestelmille on määritelty siten, että järjestelmissä tietoon pääsevät vain organisaation sisäiset käyttäjät, kenelläkään ulkopuolisella ei ilman rekisterinpitäjän myötävaikutusta ole pääsyä järjestelmässä oleviin tietoihin. Näin ollen henkilötietoja ei missään tilanteessa saateta rajoittamattoman henkilömäärän saataville ilman luonnollisen henkilön myötävaikutusta.

Järjestelmiin ja niissä oleviin tietoihin pääsevät kirjautumaan vain ne käyttäjät, joille on luotu henkilökohtainen käyttäjätunnus. Henkilökohtainen käyttäjätunnus on suojattu salasanalla. Kun autentikointi tehdään käyttäjätunnuksella ja salasanalla, salasanapolitiikka on määritelty ja vaatimustenmukainen. Lähtökohtaisesti käyttäjätunnusta luotaessa kukin organisaatio rajaa itse henkilön käyttöoikeudet käyttäjän tehtävien ja roolien mukaisiksi. Rekisterinpitäjä vastaa myös vanhentuneiden käyttäjätunnusten poistamisesta järjestelmästä. Käyttäjähallinta voidaan esimerkiksi integroida Microsoftin Active Directoryyn, jolloin käyttäjien tunnistamisesta huolehtii Windows verkkoympäristö, eikä ohjelmakohtaisia salasanoja ja niiden hallintaa tarvita. Kirjautumisessa voidaan tällöin vaatia myös muita tunnistautumismenetelmiä, kuten esimerkiksi toimikortti. Tällöin tunnistautuminen täyttää vahvan sähköisen tunnistautumisen ominaispiirteet.

Kun henkilökohtainen käyttäjätunnus on luotu, pääsyä järjestelmässä olevaan tietoon sekä käsittelyn laajuutta voidaan rajata monella eri tavalla. Käyttöoikeutta voidaan rajata moduuleittain (asiat, asiakirjat, viranhaltijapäätökset, kokoukset, sopimukset, yhteystiedot jne.) mutta myös käyttöoikeustasojen ja roolien avulla.

Salassapidettävään ja arkaluontoista henkilötietoa sisältävään aineistoon on pääsy organisaation erikseen määrittämillä henkilöillä, kuten esim. pääkäyttäjillä. Näkyvyyttä ja käyttöoikeutta voidaan rajata myös aineistorajauksin. Käyttöoikeuksia voidaan rajata myös asiakirjakohtaisesti. Jotta henkilötietojen käsittely olisi asianmukaista, rekisterinpitäjän on mahdollista luokitella tietoaineistonsa tiedonohjausjärjestelmän avulla. Mikäli rekisterinpitäjä on luokitellut tietoaineistonsa, luokittelutiedosta voidaan ottaa myös raportteja riskienhallinnan työvälineeksi.

3.1.2 Varmuuskopiointi

Hyvä tiedonhallintatapa edellyttää, että käsiteltävän tiedon saatavuus, suoja, eheys ja laatu turvataan. Tietojen saatavuus turvataan mm. varmuuskopioinnilla. Varmuuskopiointi tapahtuu tietokantojen ajastetuilla varmuuskopioinneilla. Yleinen periaate on, että Innofactorin asennustiimi tekee asiakkaan kanssa varmuuskopiointisuunnitelman, joka yleensä pitää tietokantojen tiedot kolmen päivän ajan saatavana. Aika voi olla pidempi, esimerkiksi viikko, asiakkaan levytilasta riippuen. Silloin kun organisaation sovellusinstanssi on asennettu jaettuun käyttöpalveluun, on varmuuskopiointiasetukset vakiotuna kaikille samassa jaetussa käyttöpalvelussa oleville organisaatioiden sovellusintansseille. **Varmuuskopiointisuunnitelma tällöin säilyttää tietokantojen tiedot viikon ajan**.

3.2 Loki ja käyttäjätiedot sekä niiden suojaaminen

Asianhallintajärjestelmässä on mahdollista suorittaa valvontaa myös jälkikäteen järjestelmän lokitietojen avulla. Tämä edellyttää, että järjestelmä tuottaa lokia järjestelmän tapahtumista. Tietojen luominen, muokkaus ja poisto (käyttäjä, aika, muutoksen kohde sekä tarkemmat tiedot tapahtumasta) on nähtävissä suoraan lokitiedoista. Myös tietojen lukemisesta ja asiakirjojen esikatselusta (käyttäjä, aika, kohde) jää jälki lokitietoihin. Lokitietoa syntyy kaikesta järjestelmässä käsitellystä tiedosta.

Rekisterinpitäjän ja käsittelijän tulee varmistaa, että lokitiedot ovat turvassa asiattomalta pääsyltä sekä vahingossa tai luvattomasti tapahtuvalta hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä tai muulta käsittelyltä. Kohdekohtaiseen muutoslokiin oikeudet määräytyvät kohteen näkymisen oikeuksien mukaan. Auditointilokeihin eli muutos- ja lukulokiin ei ole pääsyä tavallisella käyttäjällä. Lukutapahtumien lokien näkeminen vaatii organisaatiossa asetetun järjestelmän käyttöoikeusryhmään kuulumisen. Ainoastaan auktorisoidut henkilöt pääsevät lukemaan auditointilokiin tallennettua tietoa, joten lokitietojen asiaton häviäminen tai hävittäminen ei ole mahdollista. Tietokantatasolla auditointilokeja pääsevät muokkaamaan tai poistamaan ne henkilöt, joilla on muokkausoikeus ylläpitäjätileihin eli organisaation ICT-henkilöt ja muut tietokantojen hallinnoinnista vastaavat henkilöt.

Lokitiedot varastoidaan järjestelmän tietokantoihin. Järjestelmätason lokitukset menevät käyttöjärjestelmän tapahtumalokiin tai tietokantajärjestelmän lokitusjärjestelmään. Lokien lukemisesta, muokkaamisesta tai poistamisesta jää lokimerkintä lokiin itseensä.

4 Henkilötietojen käsittelyn turvallisuus (artikla 32)

Asianmukaisen turvallisuustason arvioimisessa on kiinnitettävä huomiota erityisesti käsittelyn sisältämiin riskeihin, erityisesti siirrettyjen, tallennettujen tai muutoin käsiteltyjen henkilötietojen vahingossa tapahtuvan tai laittoman tuhoamisen, häviämisen, muuttamisen, luvattoman luovuttamisen tai henkilötietoihin pääsyn vuoksi. Tarvittavia toimia arvioitaessa tulee huomioida uusin tekniikka ja toteuttamiskustannukset sekä käsittelyn aiheuttamat riskit rekisteröidyn oikeuksille ja vapauksille, käsittelyn luonne ja laajuus huomioon ottaen.

Rekisterinpitäjän (organisaatio xxx) ja henkilötietojen käsittelijän (Innofactor Oyj) on toteutettava toimenpiteet sen varmistamiseksi, että jokainen rekisterinpitäjän tai henkilötietojen käsittelijän alaisuudessa toimiva luonnollinen henkilö, jolla on pääsy henkilötietoihin, käsittelee niitä ainoastaan rekisterinpitäjän ohjeiden mukaisesti.

Ylläpitotason pääsy järjestelmään on rekisterinpitäjän omien pääkäyttäjien lisäksi vain Innofactorin asentajilla ja kolmannen tason tuella. Ylläpitäjät ovat tehneet salassapitosopimuksen työnantajan kanssa sekä saaneet tarvittavan tietoturva- ja tietosuojakoulutuksen sekä perehdytyksen. Ylläpitotason toimia henkilötietojen käsittelijä tekee vain siinä tapauksessa, että rekisterinpitäjä sitä erikseen pyytää ja tarvitsee.

4.1 Tietojen poistaminen

Tiedot ja syntyneet asiakirjat ovat poistettavissa järjestelmästä. Tämä edellyttää tiedon luokittelua tiedonohjaussuunnitelman avulla. Asianhallintajärjestelmä mahdollistaa määräajan säilytettävän aineiston hävittämisen. Dynasty asiahallintajärjestelmään sisältyy hävitystoiminnallisuus, joka tuottaa hävitysesityksen määriteltyjen hävittämiskriteerien mukaisesti. Tämä mahdollistaa asiakirjojen keskitetyn hävittämisen järjestelmästä. Asiakirjoissa henkilötiedot säilyvät rekisterinpitäjän tiedonohjaussuunnitelmaan määrittelemien säilytysaikojen mukaisesti.

Käyttöliittymä näyttää tietokannoissa olevaa tietoa. Tiedot poistetaan tietokannasta. Tiedot poistuvat backupeista määräajan kuluttua. Lähtökohtaisesti tiedot poistuvat sitä mukaa, kun backupit korvautuvat uudemmilla, joissa tieto ei ole enää mukana.

4.2 Henkilötietojen suojaaminen

Rekisterinpitäjän on arvioitava prosessien, käsittelyn ja järjestelmien turvallisuustaso koko käsittelyn ja henkilötietojen elinkaaren ajan. Ottaen huomioon uusin tekniikka ja totauttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet (artikla 32).

Mikäli rekisterinpitäjä toteaa, että järjestelmässä käsitellään arkaluonteisia henkilötietoja tai rekisterinpitäjän tekemän riskikartoituksen tulos näin vaatii, tiedot tulee suojata. Arkaluonteisia henkilötietoja voidaan suojata erilaisilla suojausmekanismeilla, joita järjestelmä tarjoaa. Esimerkiksi järjestelmässä voidaan käyttää suojatoimena henkilötiedon tai henkilön yhteystietojen peittäminen yhteystietorekisterissä silloin, kun se riskiarvion perusteella on tarpeellista. Asioita voidaan käsitellä myös rajoitetuin henkilötiedoin. Tällöin asian käsittelijällä oikeustasosta riippuen ei ole välttämättä oikeutta nähdä kaikkia yhteystietoja. Henkilötietoihin voidaan merkitä myös esimerkiksi turvakielto, jolloin kyseisten henkilötietojen käsittelyn arkaluonteisuuden tuomaa vastuuta korostetaan käyttäjälle.

4.3 Turvalliset tiedonsiirrot

Asianmukaisen turvallisuustason arvioimisessa on kiinnitettävä huomiota erityisesti käsittelyn sisältämiin riskeihin, erityisesti siirrettyjen, tallennettujen tai muutoin käsiteltyjen henkilötietojen vahingossa tapahtuvan tai laittoman tuhoamisen, häviämisen, muuttamisen, luvattoman luovuttamisen tai henkilötietoihin pääsyn vuoksi.

Tiedonsiirrot ulkoisiin järjestelmiin on suojattu asianmukaisesti käyttäen salattuja tiedonsiirtoprotokollia. Tiedonsiirrossa käytetään HTTPS-protokollaa. Järjestelmään otetaan yhteyksiä käyttäjien työasemista, huoltoyhteyden kautta tai mahdollisten asiakkaille toteutettujen integraatioiden seurauksena. Integraatiot ovat asiakaskohtaisia, mutta yleisimpiä järjestelmiä ovat Lupapiste, Suomi.fi-viestit, lomakepalvelujärjestelmä jne. Järjestelmä ottaa yhteyksiä internet/ekstranet alustoille, julkaisujärjestelmiin mukaan lukien sähköinen kokous (Cloud Meeting). Asiakaskohtaisissa integraatioissa järjestelmä voi ottaa yhteyttä Lupapiste, Suomi.fi-viestit tai muihin asiakaskohtaisiin toteutuksiin.

Dynasty-tuoteperheeseen kuuluu julkaisusovelluksia, kuten esityslista- ja pöytäkirja-, viranhaltijapäätös- sekä kuulutussovellukset. Niissä lähdejärjestelmänä toimii Dynasty-asianhallintajärjestelmä. Julkaisujärjestelmiin on toteutettu niin sanottu peittämistyökalu, jonka avulla tietoja voidaan mustata julkaistavista asiakirjoista. Sovelluksia on kehitetty niin, että toiminnallisuudet toteuttavat kuntalain (410/2015) 1.6.2017 voimaantulleita säädöksiä.

4.4 Sovelluskehityksen tietosuojavaatimukset

Järjestelmän kehittämisestä, kuten alustan ja sovelluksesta vastaa Innofactorin tuotekehitys. Sovelluksen osalta myös asiakkailla on rooli osallistua testaamiseen ja vaikuttaa kehittämiseen. Asiakkaat voivat esittää kehitysehdotuksia erillisen palvelun kautta.

Tekninen tietoturvatestaus on toteutettu osana tuotekehitystä. Tietyin menettelyin testataan, tutkitaan ja arvoidaan säännöllisesti teknisten toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi. Kehityksessä seurataan ja huomioidaan ilmenneitä haavoittuvuuksia. Myös OWASP 10 listojen kohdat huomioidaan.

Tuotteille suoritetaan ajoittain ulkopuolisen kolmannen osapuolen tekemiä tietoturva-auditointeja. Tuotekehitys ja testaus ei käytä asiakkaan tuotantodataa eikä näin ollen käsittele henkilötietoja. Innofactorin oma tietosuojavastaava toimii yhteistyössä tuote-omistajien kanssa käyden läpi ohjelmistojen tietosuojaan liittyviä kehitystarpeita. Innofactorilla toimii myös oma tietosuojaryhmä.

Lisätietoja tietosuojasta ja tietoturvasta pyydetään ensisijaisesti kysymään tuotteen toimittaneilta projektipäälliköiltä. Kysymyksen luonteesta riippuen he ottavat tarvittaessa yhteyttä tuotekehitykseen tai Innofactorin tietosuojavastaavaan.

Keilaranta 9
FI-02150 Espoo Finland

contact@innofactor.com
www.innofactor.fi

tel.: +358 10 272 9000
fax: +358 10 272 9001

5 Dynasty-tuoteperhe ja tuotteiden GDPR-vaatimusten täyttyminen

5.1 Dynasty asianhallintajärjestelmä

Vaatimusten täyttyminen	Dynasty 10.0	Dynasty 6.4	Dynasty 6.3	Dynasty 6.2	Dynasty 6.1
Vaatimuksen-mukainen	X				
Lähes		X	X		
Osin				X	X
Työ käynnis-tetty					
Ei vaatimus-ten mukainen					

5.2 Dynasty tiedonohjausjärjestelmä

Vaatimus-ten täytty-minen	Dynasty TOJ 1.7 SP1	Dynasty TOJ 1.7	Dynasty TOJ 1.6	Dynasty TOJ 1.5	Dynasty TOJ 1.4	Dynasty TOJ 1.3
Vaatimuk-sen-mukai-nen	X					
Lähes		X	X	X	X	X
Osin						
Työ käyn-nistetty						
Ei vaati-musten mukainen						

Dynasty asianhallinta- ja Dynasty tiedonohjausjärjestelmät on suunniteltu toimimaan yhdessä sekä tukemaan hyvän tiedonhallintatavan toteuttamista. Innofactor suosittelee vahvasti vanhojen Dynasty-versioiden 6.1 ja 6.2 päivittämistä uusimpaan myös tietosuojan toteutumisen varmistamiseksi. Tuki näiden järjestelmien osalta on päättynyt, emmekä voi taata niiden GDPR-vaatimustenmukaisuutta. Asianhallintajärjestelmän versioihin 6.3 ja 6.4. on toteutettu tiedonohjausintegraatio, jolloin tiedonohjaus ohjaa suoraan myös henkilötietojen käsittelyä ja syntyvän tiedon luokittelua. Dynasty 10.0 versio on GDPR:n vaatimusten mukainen. Uusimpaan versioon tullaan toteuttamaan muutamia rekisteröidyn informointia helpottavia toiminnallisuuksia.

Dynasty Tiedonohjausjärjestelmään on lisätty versiossa 1.7 SP1 GDPR:n vaatimia metatietokenttiä niin TOS-moduuliin kuin Rekisteriselostemoduuliin. Aiemmista versioista nämä metatietokentät puuttuvat ja siksi versiot eivät ole täysin GDPR-yhteensopivia.