Ohjeet 4/2019 25 artiklan mukaisesta sisäänrakennetusta ja oletusarvoisesta tietosuojasta

Versio 2.0

Annettu 20. lokakuuta 2020

Aiemmat versiot

Versio 1.0	13. marraskuuta 2019	Ohjeiden hyväksyminen julkista kuulemista varten
Versio 2.0	20. lokakuuta 2020	Ohjeiden hyväksyminen Euroopan tietosuojaneuvostossa julkisen kuulemisen jälkeen

Sisällysluettelo

Euroopan tietosuojaneuvosto, joka

ottaen huomioon luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta 27 päivänä huhtikuuta 2016 annetun Euroopan parlamentin ja neuvoston asetuksen 2016/679/EU, jäljempänä yleinen tietosuoja-asetus, 70 artiklan 1 kohdan e alakohdan,

ottaen huomioon ETA-sopimuksen sekä erityisesti sen liitteen XI ja pöytäkirjan 37, sellaisina kuin ne ovat muutettuina 6 päivänä heinäkuuta 2018 annetulla ETA:n sekakomitean päätöksellä N:o 154/2018,

ottaen huomioon työjärjestyksensä 12 ja 22 artiklan,

ON ANTANUT SEURAAVAT OHJEET:

<u>Tiivistelmä</u>

Maailman digitalisoituessaon ensisijaisen tärkeää, että noudatetaan sisäänrakennettua ja oletusarvoista tietosuojaa koskevia vaatimuksia yksityisyyden suojan ja tietosuojan parantamiseksi yhteiskunnassa. Tämän vuoksi rekisterinpitäjien on otettava tämä vastuu vakavasti ja täytettävä yleisen tietosuoja-asetuksen mukaiset velvollisuutensa henkilötietojen käsittelytoimia suunnitellessaan.

Näissä ohjeissa annetaan yleisiä ohjeita yleisen tietosuoja-asetuksen 25 artiklassa säädetystä sisäänrakennettua ja oletusarvoista tietosuojaa koskevasta velvoitteesta. Sisäänrakennettu ja oletusarvoinen tietosuoja velvoittaa kaikkia rekisterinpitäjiä riippumatta siitä, miten laajaa tai monimutkaista käsittely on. Jotta sisäänrakennettua ja oletusarvoista tietosuojaa koskevat vaatimukset voidaan täyttää, on olennaisen tärkeää, että rekisterinpitäjä ymmärtää tietosuojaperiaatteet ja rekisteröidyn oikeudet ja vapaudet.

Keskeisenä velvoitteena on sellaisten *asianmukaisten* toimenpiteiden ja tarvittavien suojatoimien toteuttaminen, joilla taataan *tietosuojaperiaatteiden* ja siten *rekisteröityjen oikeuksien ja vapauksien täytäntöönpano sisäänrakennetusti ja oletusarvoisesti.* Asetuksen 25 artiklassa kuvataan sekä sisäänrakennettuun että oletusarvoiseen tietosuojaan liittyviä tekijöitä, jotka on otettava huomioon. Näissä ohjeissa tekijöitä käsitellään yksityiskohtaisemmin.

Asetuksen 25 artiklan 1 kohdassa säädetään, että rekisterinpitäjien on otettava sisäänrakennettu ja oletusarvoinen tietosuoja huomioon ajoissa uutta henkilötietojen käsittelytoimea suunnitellessaan. Rekisterinpitäjien on pantava sisäänrakennettu ja oletusarvoinen tietosuoja täytäntöön sekä *ennen* käsittelyä että *jatkuvasti* käsittelyn aikana arvioimalla valittujen toimenpiteiden ja suojatoimien tehokkuutta. Sisäänrakennettua ja oletusarvoista tietosuojaa edellytetään myös olemassa olevilta järjestelmiltä, joissa käsitellään henkilötietoja.

Näissä ohjeissa annetaan myös ohjeita siitä, miten 5 artiklan 1 kohdan mukaiset tietosuojaperiaatteet pannaan täytäntöön tehokkaasti. Lisäksi ohjeissa luetellaan sisäänrakennetun ja oletusarvoisen tietosuojan keskeiset osa-alueet ja havainnollistetaan niitä käytännön esimerkein. Rekisterinpitäjän on arvioitava ehdotettujen toimenpiteiden asianmukaisuutta kyseessä olevan nimenomaisen käsittelyn kannalta.

Euroopan tietosuojaneuvosto antaa suosituksia siitä, miten rekisterinpitäjät, henkilötietojen käsittelijät ja tuottajat voivat yhteistyössä saada aikaan sisäänrakennetun ja oletusarvoisen tietosuojan. Se kannustaa toimialojen rekisterinpitäjiä, henkilötietojen käsittelijöitä ja tuottajia käyttämään sisäänrakennettua ja oletusarvoista tietosuojaa keinona saada kilpailuetua, kun ne markkinoivat tuotteitaan rekisterinpitäjille ja rekisteröidyille. Se kannustaa myös kaikkia rekisterinpitäjiä hyödyntämään sertifiointeja ja käytännesääntöjä.

1 SOVELTAMISALA

1. Näissä ohjeissa käsitellään sitä, miten rekisterinpitäjät toteuttavat sisäänrakennetun ja oletusarvoisen tietosuojan, joka perustuu yleisen tietosuoja-asetuksen 25 artiklan mukaiseen velvollisuuteen.[1] Näistä ohjeista voi olla hyötyä myös muille toimijoille, kuten henkilötietojen käsittelijöille sekä tuotteiden, palvelujen ja sovellusten tuottajille, jäljempänä ”tuottajat”, joita 25 artikla ei suoraan koske, kun ne suunnittelevat yleisen tietosuoja-asetuksen vaatimukset täyttäviä tuotteita ja palveluja, joiden avulla rekisterinpitäjät voivat täyttää tietosuojaa koskevat velvollisuutensa.[2] Yleisen tietosuoja-asetuksen johdanto-osan 78 kappaleessa lisätään, että sisäänrakennettu ja oletusarvoinen tietosuoja on otettava huomioon myös julkisissa tarjouskilpailuissa. Rekisterinpitäjä vastaa sisäänrakennettua ja oletusarvoista tietosuojaa koskevien velvoitteiden täyttämisestä sen henkilötietojen käsittelijöiden ja alikäsittelijöiden toteuttaman käsittelyn osalta. Siksi rekisterinpitäjän on otettava sisäänrakennettu ja oletusarvoinen tietosuoja huomioon tehdessään sopimuksia näiden osapuolten kanssa.

2. Asetuksen 25 artiklan vaatimuksen mukaan rekisterinpitäjien on sisällytettävä tietosuoja henkilötietojen käsittelyyn oletusarvoisesti. Tämä koskee koko käsittelyn elinkaarta. Sisäänrakennettua ja oletusarvoista tietosuojaa koskeva vaatimus koskee myös ennen yleisen tietosuoja-asetuksen voimaantuloa käytössä olleita käsittelyjärjestelmiä. Rekisterinpitäjien täytyy päivittää käsittelyä johdonmukaisesti yleisen tietosuoja-asetuksen mukaisesti. Näiden ohjeiden alaluvussa 2.1.4 on lisätietoa siitä, miten olemassa oleva järjestelmä pidetään sisäänrakennetun ja oletusarvoisen tietosuojan mukaisena. Säännöksen ytimenä on varmistaa *asianmukainen* ja *tehokas* tietosuoja, joka on sekä *sisäänrakennettu* että *oletusarvoinen*. Se tarkoittaa, että rekisterinpitäjien on voitava osoittaa, että henkilötietojen käsittelyn yhteydessä käytössä ovat asianmukaiset toimenpiteet ja suojatoimet, jotta varmistetaan, että tietosuojaperiaatteita noudatetaan ja rekisteröityjen oikeuksia ja vapauksia suojataan tehokkaasti.

3. Ohjeiden luvussa 2 käsitellään 25 artiklassa säädettyjen vaatimusten tulkintaa ja selvitetään, mitä lakisääteisiä velvollisuuksia säännökseen liittyy. Luvussa 3 annetaan esimerkkejä siitä, miten sisäänrakennettua ja oletusarvoista tietosuojaa sovelletaan tiettyjen tietosuojaperiaatteiden yhteydessä.

4. Ohjeiden luvussa 4 käsitellään sertifiointimekanismeja, jolla osoitetaan, että 25 artiklaa noudatetaan henkilötietojen käsittelyssä. Luvussa 5 kerrotaan siitä, miten valvontaviranomaiset valvovat 25 artiklan

[1] Tässä esitetyt tulkinnat koskevat yhtä lailla direktiivin (EU) 2016/680 20 artiklaa ja asetuksen 2018/1725 27 artiklaa.

[2] Tämä tarve sanotaan selvästi yleisen tietosuoja-asetuksen johdanto-osan 78 kappaleessa: ”Kehitettäessä, suunniteltaessa, valittaessa ja käytettäessä sovelluksia, palveluja ja tuotteita, jotka perustuvat henkilötietojen käsittelyyn tai käsittelevät henkilötietoja tehtävänsä täyttämiseksi, tuotteiden, palvelujen ja sovellusten tuottajia olisi kannustettava ottamaan huomioon oikeus tietosuojaan niiden kehittäessä ja suunnitellessa tällaisia tuotteita, palveluja ja sovelluksia ja varmistamaan viimeisin tekniikka asianmukaisesti huomioon ottaen, että rekisterinpitäjät ja henkilötietojen käsittelijät pystyvät täyttämään tietosuojavelvoitteensa.”

noudattamista. Ohjeiden lopussa sidosryhmille annetaan lisää suosituksia siitä, miten sisäänrakennetun ja oletusarvoisen tietosuojan toteuttaminen onnistuu parhaiten. Euroopan tietosuojaneuvosto on tietoinen siitä, että pienillä ja keskisuurilla yrityksillä, jäljempänä ”pk-yritykset”, on haasteita sisäänrakennettua ja oletusarvoista tietosuojaa koskevien velvoitteiden täysimääräisessä noudattamisessa. Siksi se antaa luvussa 6 lisäsuosituksia erityisesti pk-yrityksille.

2 ASETUKSEN 25 ARTIKLAN SISÄÄNRAKENNETTUA TIETOSUOJAA KOSKEVAN 1 KOHDAN JA OLETUSARVOISTA TIETOSUOJAA KOSKEVAN 2 KOHDAN ANALYYSI

5. Tässä luvussa selitetään sisäänrakennettua tietosuojaa koskevia vaatimuksia (25 artiklan 1 kohta) ja oletusarvoista tietosuojaa koskevia vaatimuksia (25 artiklan 2 kohta) ja annetaan niistä ohjeita. Sisäänrakennettu tietosuoja ja oletusarvoinen tietosuoja ovat toisiaan täydentäviä ja vahvistavia käsitteitä. Rekisteröidyt hyötyvät enemmän oletusarvoisesta tietosuojasta, jos sisäänrakennettu tietosuoja on pantu samanaikaisesti täytäntöön – ja päinvastoin.

6. Sisäänrakennettua ja oletusarvoista tietosuojaa koskevaa vaatimusta sovelletaan kaikkiin rekisterinpitäjiin, niin pieniin yrityksiin kuin monikansallisiin yrityksiinkin. Näin ollen se, miten monimutkaista sisäänrakennetun ja oletusarvoisen tietosuojan toteuttaminen on, voi vaihdella yksittäisten käsittelytoimien mukaan. Sisäänrakennetun ja oletusarvoisen tietosuojan täytäntöönpano voi kuitenkin kaikissa tapauksissa tuoda etuja rekisterinpitäjälle ja rekisteröidylle koosta riippumatta.

2.1 25 artiklan 1 kohta: Sisäänrakennettu tietosuoja

2.1.1 Rekisterinpitäjän velvollisuus toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet ja tarvittavat suojatoimet käsittelyn yhteydessä

7. Asetuksen 25 artiklan 1 kohdan mukaisesti rekisterinpitäjän on toteutettava tietosuojaperiaatteiden täytäntöönpanoa varten *asianmukaiset* tekniset ja organisatoriset *toimenpiteet* ja sisällytettävä *tarvittavat suojatoimet* osaksi käsittelyä, jotta käsittely vastaisi vaatimuksia ja rekisteröityjen oikeuksia ja vapauksia suojattaisiin. Sekä asianmukaiset toimenpiteet että tarvittavat suojatoimet palvelevat samaa tarkoitusta eli rekisteröityjen oikeuksien suojaamista ja sen varmistamista, että heidän henkilötietojensa suojaaminen sisällytetään osaksi käsittelyä.

8. *Tekniset ja organisatoriset toimenpiteet* ja tarvittavat *suojatoimet* voidaan ymmärtää laajasti miksi tahansa menetelmäksi tai keinoksi, jota rekisterinpitäjä voi käyttää henkilötietojen käsittelyssä. *Asianmukaisuus* tarkoittaa, että toimenpiteiden ja tarvittavien suojatoimien pitäisi soveltua aiotun tarkoituksen saavuttamiseen, eli niillä on voitava panna tietosuojaperiaatteet täytäntöön *tehokkaasti*[3]. Asianmukaisuuden vaatimus liittyy siis läheisesti tehokkuuden vaatimukseen.

9. Tekninen tai organisatorinen toimenpide ja suojatoimi voi olla niin kehittyneiden teknisten ratkaisujen käyttöä kuin peruskoulutuksen järjestämistä henkilökunnalle. Sen mukaan, mikä on kyseessä olevan käsittelyn tausta ja mitä riskejä käsittelyyn liittyy, esimerkkejä voisivat olla muun muassa henkilötietojen pseudonymisointi[4], henkilötietojen tallentaminen rakenteelliseen, yleiseen koneellisesti luettavaan muotoon, rekisteröityjen mahdollisuus puuttua käsittelyyn, tietojen

[3] ”Tehokkuutta” käsitellään jäljempänä alaluvussa 2.1.2.
[4] Määritellään yleisen tietosuoja-asetuksen 4 artiklan 5 kohdassa.

antaminen henkilötietojen tallentamisesta, haittaohjelmien havaitsemisjärjestelmien käyttö, työntekijöiden kouluttaminen, yksityisyyden ja tietoturvan hallintajärjestelmien luominen, henkilötietojen käsittelijöiden velvoittaminen sopimusperusteisesti panemaan täytäntöön erityisiä tietojen minimointia koskevia käytäntöjä jne.

10. Rekisterinpitäjien tai henkilötietojen käsittelijöiden ryhmiä edustavien yhdistysten tai muiden elimien tunnustamat standardit, parhaat käytännöt ja käytännesäännöt voivat olla avuksi asianmukaisten toimenpiteiden määrittämisessä. Rekisterinpitäjän on kuitenkin varmistettava toimenpiteiden asianmukaisuus kyseessä olevan nimenomaisen käsittelyn kannalta.

2.1.2 Tavoitteena noudattaa tietosuojaperiaatteita tehokkaasti ja suojata rekisteröityjen oikeuksia ja vapauksia

11. Asetuksen 5 artiklassa esitetään *tietosuojaperiaatteet*, jäljempänä ”periaatteet”. *Rekisteröityjen oikeudet ja vapaudet* ovat luonnollisten henkilöiden perusoikeuksia ja -vapauksia, ja erityisesti heidän oikeutensa henkilötietojen suojaan, joka nimetään 1 artiklan 2 kohdassa yleisen tietosuoja-asetuksen tavoitteeksi (jäljempänä ”oikeudet”)[5]. Oikeudet esitetään yksityiskohtaisesti Euroopan unionin perusoikeuskirjassa. Rekisterinpitäjän on olennaisen tärkeää ymmärtää *periaatteiden* ja *oikeuksien* merkitys yleisen tietosuoja-asetuksen ja erityisesti sisäänrakennettua ja oletusarvoista tietosuojaa koskevan velvoitteen tarjoaman suojan perustana.

12. Asianmukaisia teknisiä ja organisatorisia toimenpiteitä toteutettaessa kunkin edellä mainitun periaatteen tehokas noudattaminen ja siitä johtuva oikeuksien ja vapauksien suojaaminen on *sisällytettävä* näihin toimenpiteisiin ja suojatoimiin.

Tehokkuuden varmistaminen

13. Tehokkuus on keskeinen osa sisäänrakennetun tietosuojan käsitettä. Vaatimus periaatteiden tehokkaasta täytäntöönpanosta tarkoittaa, että rekisterinpitäjien on otettava käyttöön näiden periaatteiden suojaamiseksi tarvittavat toimenpiteet ja suojatoimet, jotta rekisteröityjen oikeudet voidaan turvata. Kunkin toteutetun toimenpiteen pitäisi tuottaa halutut tulokset rekisterinpitäjän suunnittelemassa käsittelyssä. Tämä tarkoittaa kahta asiaa.

14. Ensinnäkin se tarkoittaa, että 25 artiklassa ei edellytetä minkään tiettyjen teknisten ja organisatoristen toimenpiteiden toteuttamista vaan sitä, että valittujen toimenpiteiden ja suojatoimien on sovelluttava tietosuojaperiaatteiden täytäntöönpanoon juuri kyseessä olevassa käsittelyssä. Näin ollen toimenpiteet ja suojatoimet olisi rakennettava kestäviksi, ja rekisterinpitäjän pitäisi pystyä toteuttamaan lisätoimenpiteitä riskien mahdollisen leviämisen estämiseksi[6]. Se, ovatko toimenpiteet tehokkaita, määräytyy aina kulloisenkin käsittely-yhteyden mukaan. Lisäksi on arvioitava, mitkä tekijät on otettava huomioon käsittelytapoja määritettäessä. Edellä mainittuja tekijöitä käsitellään jäljempänä alaluvussa 2.1.3.

[5] Ks. yleisen tietosuoja-asetuksen johdanto-osan 4 kappale.

[6] ”Rekisterinpitäjiin sovellettavien perusperiaatteiden (esimerkiksi legitimiteetti, tietojen minimointi, käyttötarkoitussidonnaisuus, avoimuus, tietojen eheys ja tietojen täsmällisyys) on oltava samat käsittelystä ja rekisteröityihin kohdistuvista riskeistä riippumatta. Käsittelyn luonteen ja laajuuden asianmukainen huomioon ottaminen on ollut aina kiinteä osa näiden periaatteiden soveltamista, joten ne ovat luontaisesti skaalattavissa.” 29 artiklan mukainen tietosuojatyöryhmä. ”Statement on the role of a risk-based approach in data protection legal frameworks.” WP 218, 30. toukokuuta 2014, s. 3. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

15. Toiseksi rekisterinpitäjien pitäisi pystyä osoittamaan, että periaatteita on ylläpidetty.

16. Toteutetuilla toimenpiteillä ja suojatoimilla pitäisi saada aikaan haluttu vaikutus tietosuojan kannalta, ja rekisterinpitäjän pitäisi dokumentoida toteutetut tekniset ja organisatoriset toimenpiteet[7]. Jotta tämä onnistuisi, rekisterinpitäjä voi määrittää asianmukaisia keskeisiä tulosindikaattoreita (KPI), joilla tehokkuus voidaan osoittaa. Keskeinen tulosindikaattori on rekisterinpitäjän valitsema mitattavissa oleva arvo, joka osoittaa, miten tehokkaasti rekisterinpitäjä saavuttaa tietosuojatavoitteensa. Keskeinen tulosindikaattori voi olla *määrällinen*, kuten väärien positiivisten tai väärien negatiivisten tulosten osuus, valitusten väheneminen, reagointiajan lyheneminen, kun rekisteröidyt käyttävät oikeuksiaan, tai *laadullinen*, kuten tulosten arviointi, arviointiasteikkojen käyttö tai asiantuntija-arvioinnit. Keskeisten tulosindikaattorien sijasta rekisterinpitäjät voivat osoittaa periaatteiden tehokkaan täytäntöönpanon antamalla perustelut valittujen toimenpiteiden ja suojatoimien tehokkuuden arvioinnille.

2.1.3 Huomioon otettavat tekijät

17. Yleisen tietosuoja-asetuksen 25 artiklan 1 kohdassa luetellaan tekijät, jotka rekisterinpitäjän on otettava huomioon, kun päätetään tiettyä käsittelytoimea koskevista toimenpiteistä. Seuraavassa annetaan ohjeita siitä, miten näitä tekijöitä sovelletaan toimenpiteiden suunnitteluprosessissa, joka sisältää oletusarvoisten asetusten suunnittelun. Kaikki nämä tekijät auttavat määrittämään, onko toimenpide asianmukainen periaatteiden tehokasta täytäntöönpanoa varten. Mikään tekijä ei siis ole itsessään päämäärä, vaan ne kaikki ovat tekijöitä, jotka on otettava yhdessä huomioon tavoitteen saavuttamiseksi.

2.1.3.1 ”Viimeisin tekniikka”

18. ”Viimeisin tekniikka” -käsitettä käytetään monissa EU:n säännöstöissä, esimerkiksi ympäristönsuojelun ja tuoteturvallisuuden alalla. Yleisessä tietosuoja-asetuksessa ”viimeisimpään tekniikkaan”[8] viitataan paitsi 32 artiklassa, jossa käsitellään käsittelyn turvallisuuteen liittyviä toimenpiteitä[9][10], myös 25 artiklassa, joten tämä kriteeri koskee kaikkia käsittelyyn liittyviä teknisiä ja organisatorisia toimenpiteitä.

19. Yleisen tietosuoja-asetuksen 25 artiklan osalta viittauksella ”viimeisimpään tekniikkaan” asetetaan rekisterinpitäjille velvollisuus **ottaa huomioon** markkinoilla saatavilla olevan **tekniikan nykyinen kehitys**, kun ne määrittävät asianmukaisia teknisiä ja organisatorisia toimenpiteitä. Vaatimuksen mukaan rekisterinpitäjien on seurattava teknistä kehitystä ja pysyteltävä siitä ajan tasalla. Rekisterinpitäjien on myös tiedettävä, millaisia tietosuojaan liittyviä riskejä tai mahdollisuuksia käsittelytoimille valittu tekniikka voi aiheuttaa ja miten toteutetaan ja päivitetään sellaiset toimenpiteet ja suojatoimet, joilla *varmistetaan*, että periaatteet *pannaan täytäntöön* ja

[7] Ks. johdanto-osan 74 ja 78 kappale.
[8] Ks. Saksan perustuslakituomioistuimen vuonna 1978 asiassa ”Kalkar” antama päätös, johon käsitteen objektiivisen määrittelemisen menetelmä voi perustua: https://germanlawarchive.iuscomp.org/?p=67 Tällä perusteella ”viimeisimmän tekniikan” taso määritettäisiin ”nykyisen tieteellisen tietämyksen ja tutkimuksen” tason ja vakiintuneempien ”yleisesti hyväksyttyjen tekniikan sääntöjen” välille. ”Viimeisin tekniikka” voidaan siis määrittää sellaiseksi palvelun tai tekniikan tai tuotteen tekniseksi tasoksi, joka vastaa markkinoilla vallitsevaa tasoa ja joka on kaikkein tehokkain määritettyjen tavoitteiden saavuttamisen kannalta.
[9] https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security
[10] www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/

rekisteröityjen oikeuksia *suojataan tehokkaasti* kehittyvä tekninen toimintaympäristö huomioon ottaen.

20. ”Viimeisin tekniikka” on liukuva käsite, jota on arvioitava jatkuvasti teknisen kehityksen yhteydessä. Tekniikan kehittyessä voi olla, että rekisterinpitäjä toteaa, että aikanaan riittävän suojan tason antanut toimenpide ei tee sitä enää. Jos rekisterinpitäjä ei pysyttele ajan tasalla tekniikan muutoksista, voi olla, etteivät 25 artiklan vaatimukset täyty.

21. ”Viimeisin tekniikka” -kriteeriä sovelletaan teknisten toimenpiteiden lisäksi myös organisatorisiin toimenpiteisiin. Asianmukaisten organisatoristen toimenpiteiden puute voi heikentää valitun tekniikan tehokkuutta tai vaarantaa sen kokonaan. Organisatorisia toimenpiteitä ovat esimerkiksi sisäisten toimintalinjojen hyväksyminen, teknologiaa, turvallisuutta ja tietosuojaa koskeva ajantasainen koulutus sekä tietotekniikan turvallisuuden hallinto- ja hallintakäytännöt.

22. Eri alojen voimassa olevilla ja hyväksytyillä kehyksillä, standardeilla, sertifioinneilla, käytännesäännöillä jne. voi olla osansa osoitettaessa, mikä on kulloinkin ”viimeisintä tekniikkaa” kullakin käyttöalalla. Jos tällaisia standardeja on ja ne takaavat rekisteröidylle korkeatasoisen suojan lakisääteisten vaatimusten mukaisesti – tai niitä paremmin – rekisterinpitäjien on otettava ne huomioon tietosuojatoimenpiteiden suunnittelussa ja toteuttamisessa.

2.1.3.2 ”Toteuttamiskustannukset”

23. Rekisterinpitäjä voi ottaa toteuttamiskustannukset huomioon valitessaan ja soveltaessaan asianmukaisia teknisiä ja organisatorisia toimenpiteitä ja tarvittavia suojatoimia, joilla periaatteet pannaan asianmukaisesti täytäntöön rekisteröityjen oikeuksien suojelemiseksi. Kustannuksilla tarkoitetaan yleisesti resursseja, mukaan lukien aika- ja henkilöresurssit.

24. Kustannustekijä ei edellytä, että rekisterinpitäjä käyttää suhteettoman määrän resursseja, kun on olemassa vähemmän resursseja vaativia, mutta tehokkaita, vaihtoehtoisia toimenpiteitä. Toteuttamiskustannukset ovat kuitenkin tekijä, joka on otettava huomioon sisäänrakennetun tietosuojan täytäntöönpanossa, eikä syy olla panematta sitä täytäntöön.

25. Valituilla toimenpiteillä varmistetaan näin ollen, että rekisterinpitäjän suunnittelemassa käsittelytoimessa ei käsitellä henkilötietoja periaatteiden vastaisesti kustannuksista riippumatta. Rekisterinpitäjien pitäisi pystyä hallinnoimaan yleisiä kustannuksia, jotta kaikki periaatteet voidaan panna täytäntöön tehokkaasti ja suojella siten oikeuksia.

2.1.3.3 ”Käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset”

26. Rekisterinpitäjien on otettava tarvittavia toimenpiteitä määrittäessään huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset.

27. Näitä tekijöitä on tulkittava johdonmukaisesti sen kanssa, mikä niiden rooli on muissa yleisen tietosuoja-asetuksen säännöksissä, kuten 24, 32 ja 35 artiklassa, jotta tietosuojaperiaatteet voidaan sisällyttää käsittelyyn.

28. L**uonne**-käsitteen voidaan ymmärtää tarkoittavan käsittelyn luontaisia[11] ominaisuuksia. **Laajuus** tarkoittaa käsittelytoimien kokoa ja laajuutta. **Asiayhteys** liittyy käsittelyn olosuhteisiin, jotka voivat vaikuttaa rekisteröidyn odotuksiin, kun taas **tarkoitus** viittaa käsittelyn tavoitteisiin.

2.1.3.4 ”Henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit”

29. Monissa yleisen tietosuoja-asetuksen säännöksissä sovelletaan yhtenäistä riskiperusteista lähestymistapaa, ja 24, 25, 32 ja 35 artikloissa käsitellään sitä, miten määritetään asianmukaiset tekniset ja organisatoriset toimenpiteet, joiden avulla suojataan yksilöitä ja heidän henkilötietojaan ja täytetään yleisen tietosuoja-asetuksen vaatimukset. Suojelun kohteet ovat aina samat (yksilöt heidän henkilötietojensa suojaamisen välityksellä) ja myös (yksilöiden oikeuksiin kohdistuvat) riskit, joilta suojaudutaan, ovat samat. Lisäksi otetaan huomioon samat edellytykset (henkilötietojen käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset).

30. Kun tehdään riskianalyysia 25 artiklan noudattamisesta, rekisterinpitäjän on tunnistettava rekisteröidyn oikeuksiin kohdistuvat riskit, joita periaatteiden loukkaaminen aiheuttaa, ja määritettävä niiden todennäköisyys ja vakavuus, jotta tunnistettujen riskien tehokasta lieventämistä varten voidaan toteuttaa toimenpiteitä. Riskinarvioinnissa on ratkaisevan tärkeää arvioida käsittelyä järjestelmällisesti ja perusteellisesti. Esimerkiksi vapaaehtoisen suostumuksen puuttuminen rikkoo lainmukaisuuden periaatetta. Kun kyse on heikossa asemassa olevan ryhmän muodostavien alle 18-vuotiaiden lasten ja nuorten henkilötietojen käsittelystä eikä käsittelyyn ole muuta laillista perustetta, rekisterinpitäjä arvioi toimintaan liittyvät erityiset riskit ja toteuttaa asianmukaiset toimenpiteet tähän rekisteröityjen ryhmään liittyviin tunnistettuihin riskeihin puuttumiseksi ja niiden lieventämiseksi tehokkaasti.

31. Euroopan tietosuojaneuvoston julkaisussa ”Euroopan tietosuojaneuvoston ohjeet tietosuojaa koskevasta vaikutustenarvioinnista”[12] käsitellään sitä, miten määritetään, liittyykö käsittelyyn todennäköisesti korkea riski rekisteröidylle vai ei. Lisäksi siinä annetaan ohjeita tietosuojariskien arvioimisesta ja tietosuojaan liittyvän riskinarvioinnin tekemisestä. Näistä ohjeista voi olla hyötyä tehtäessä kaikkiin edellä mainittuihin artikloihin, myös 25 artiklaan, liittyvää riskinarviointia.

32. Riskiperusteinen lähestymistapa ei sulje pois perustasojen, parhaiden käytäntöjen ja standardien käyttöä. Ne voivat olla rekisterinpitäjille hyödyllisiä työkaluja käsiteltäessä samanlaisia riskejä samanlaisissa tilanteissa (käsittelyn luonne, laajuus, asiayhteys ja tarkoitus). Tästä huolimatta 25 artiklan (sekä 24, 32 ja 35 artiklan 7 kohdan c alakohdan) mukaista velvollisuutta ottaa huomioon ”*käsittelyn aiheuttamat todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit luonnollisten henkilöiden oikeuksille ja vapauksille*” on noudatettava. Vaikka rekisterinpitäjillä onkin apunaan tällaisia työkaluja, on niiden tehtävä aina tapauskohtainen arviointi kulloisenkin käsittelytoimen aiheuttamista tietosuojariskeistä ja varmistettava, että ehdotetut asianmukaiset toimenpiteet ja suojatoimet ovat tehokkaita. Lisäksi voidaan edellyttää tietosuojaa koskevaa vaikutustenarviointia tai olemassa olevan vaikutustenarvioinnin päivittämistä.

---

[11] Esimerkkejä ovat erityiset tietoryhmät, automaattinen päätöksenteko, vääristyneet valtasuhteet, ennakoimaton käsittely, rekisteröidyn vaikeudet oikeuksien käyttämisessä jne.

[12] 29 artiklan mukaisen tietosuojatyöryhmän ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittyykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu ”korkea riski”. WP 248 rev.01, 4. lokakuuta 2017. ec.europa.eu/newsroom/document.cfm?doc_id=47711 – Euroopan tietosuojaneuvoston hyväksymä.

2.1.4 Aikaan liittyvät näkökohdat

2.1.4.1 Käsittelytapojen määrittämisen yhteydessä

33. Sisäänrakennettu tietosuoja on pantava täytäntöön ”*käsittelytapojen määrittämisen yhteydessä*”.

34. ”*Käsittelytavat*” vaihtelevat yleisistä yksityiskohtaisesti suunniteltuihin käsittelyn osa-alueisiin, joita ovat esimerkiksi arkkitehtuuri, menettelyt, protokollat, layout ja ulkoasu.

35. *Käsittelytapojen määrittämisen yhteydellä* tarkoitetaan sitä ajanjaksoa, jolloin rekisterinpitäjä päättää, miten käsittely toteutetaan, tapaa, jolla käsittely tapahtuu, sekä mekanismeja, joita kyseisen käsittelyn tekemiseen käytetään. Tässä prosessissa tehdään siis päätökset siitä, että rekisterinpitäjän on arvioitava asianmukaiset toimenpiteet ja suojatoimet, joilla periaatteet ja rekisteröityjen oikeudet sisällytetään käsittelyyn tehokkaasti. Lisäksi sen on otettava huomioon esimerkiksi ”uusimman tekniikan”, toteutuskustannusten sekä käsittelyn luonteen, laajuuden, asiayhteyden ja tarkoituksen ja riskien kaltaiset osatekijät. Tämä sisältää tietojenkäsittelyssä käytettävien ohjelmistojen, laitteistojen ja palvelujen hankinnan ja käyttöönoton.

36. Sisäänrakennetun ja oletusarvoisen tietosuojan varhainen huomioon ottaminen on ratkaisevan tärkeää tietosuojaperiaatteiden ja rekisteröityjen oikeuksien suojelun onnistuneelle täytäntöönpanolle. Kustannus-hyötysuhteen kannalta on myös rekisterinpitäjien edun mukaista ottaa sisäänrakennettu ja oletusarvoinen tietosuoja huomioon mieluummin aikaisemmin kuin myöhemmin, sillä jo tehtyjen suunnitelmien ja jo suunniteltujen käsittelytoimien muuttaminen myöhemmin voi olla haasteellista ja kallista.

2.1.4.2 Itse käsittelyn yhteydessä (tietosuojavaatimusten ylläpito ja arviointi)

37. Kun käsittely on alkanut, rekisterinpitäjän on pidettävä jatkuvasti yllä sisäänrakennettua ja oletusarvoista tietosuojaa eli pantava periaatteita täytäntöön koko ajan tehokkaasti, oikeuksien suojaamiseksi. Tämä tehdään muun muassa pysymällä ajan tasalla uusimmasta tekniikasta ja uudelleen arvioimalla riskitasoa. Käsittelytoimien luonne, laajuus ja asiayhteys sekä riskit voivat muuttua käsittelyn aikana. Siksi rekisterinpitäjän on arvioitava käsittelytoimiaan uudelleen tarkastamalla ja arvioimalla säännöllisesti valitsemiensa toimenpiteiden ja suojatoimien tehokkuutta.

38. Käsittelytoimien ylläpitoa, tarkastamista ja päivittämistä koskevaa velvollisuutta sovelletaan myös jo käytössä oleviin järjestelmiin. Tämä tarkoittaa, että ennen yleisen tietosuoja-asetuksen voimaantuloa suunnitellut käytössä olleet järjestelmät on arvioitava ja niitä on ylläpidettävä siten, että varmistetaan sellaisten toimenpiteiden ja suojatoimien toteuttaminen, joilla pannaan periaatteet ja rekisteröityjen oikeudet täytäntöön tehokkaasti näiden ohjeiden mukaisesti.

39. Tämä velvollisuus koskee myös kaikkea henkilötietojen käsittelijöiden tekemää käsittelyä. Rekisterinpitäjien on tarkastettava ja arvioitava käsittelijöiden toimia säännöllisesti, jotta varmistetaan, että ne ovat jatkuvasti periaatteiden mukaisia ja että ne omalta osaltaan auttavat rekisterinpitäjiä täyttämään velvollisuutensa.

2.2 25 artiklan 2 kohta oletusarvoinen tietosuoja

2.2.1 Oletusarvoisesti käsitellään vain käsittelyn kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja

40. Tietojenkäsittelytieteessä ”oletusarvolla” tarkoitetaan yleensä jonkin sellaisen konfiguroitavan asetuksen olemassa olevaa tai esivalittua arvoa, joka liittyy ohjelmistosovellukseen,

tietokoneohjelmaan tai laitteeseen. Tällaisia asetuksia kutsutaan myös ”esiasetuksiksi” tai ”tehdasasetuksiksi”, eritoten elektroniikkalaitteissa.

41. Käsitteellä ”oletusarvoinen” tarkoitetaan henkilötietojen käsittelyssä henkilötietojen käsittelyyn vaikuttavien konfigurointiarvojen tai käsittelyvaihtoehtojen, asettamista. Näitä ovat esimerkiksi kerättyjen henkilötietojen määrään, käsittelyn laajuuteen, säilytysaikaan ja saatavilla oloon vaikuttavat asetukset muun muassa ohjelmistosovelluksissa, palveluissa tai laitteissa.

42. Rekisterinpitäjän on valittava oletusarvoiset käsittelyasetukset ja -vaihtoehdot ja vastattava niiden täytäntöönpanosta siten, että oletusarvoisesti toteutetaan vain asetetun lainmukaisen tavoitteen saavuttamiseksi ehdottoman välttämätön henkilötietojen käsittely. Rekisterinpitäjien on siis tukeuduttava arvioonsa käsittelyn tarpeellisuudesta 6 artiklan 1 kohdan mukaisten laillisten perusteiden mukaisesti. Tämä tarkoittaa, että oletusarvoisesti rekisterinpitäjän ei pidä kerätä enemmän tietoja kuin on välttämätöntä, sen ei pidä käsitellä kerättyjä tietoja pidempään kuin niiden tarkoituksia varten on välttämätöntä eikä sen pidä säilyttää tietoja pidempään kuin on välttämätöntä. Perusvaatimuksena on, että tietosuoja on sisällytetty käsittelyyn oletusarvoisesti.

43. Rekisterinpitäjän on määritettävä etukäteen, mitä tiettyä, nimenomaista ja laillista tarkoitusta varten henkilötietoja kerätään ja käsitellään.[13] Toimenpiteillä on voitava oletusarvoisesti varmistaa, että vain sellaisia henkilötietoja käsitellään, jotka ovat tarpeen kunkin nimenomaisen käsittelytarkoituksen kannalta. Euroopan tietosuojavaltuutetun ohjeet siitä, miten arvioidaan sellaisten toimenpiteiden tarpeellisuutta ja oikeasuhteisuutta, joilla rajoitetaan oikeutta henkilötietojen suojaan, voivat olla hyödyllisiä, kun selvitetään, minkä tietojen käsittely on tarpeen tietyn tarkoituksen saavuttamiseksi.[14] [15] [16]

44. Jos rekisterinpitäjä käyttää kolmannen osapuolen ohjelmistoa tai valmisohjelmistoa, rekisterinpitäjän on tehtävä tuotteelle riskienarviointi ja varmistettava, että toiminnot, joille ei ole laillista perustetta tai jotka eivät vastaa käsittelyn aiottuja tarkoituksia, poistetaan käytöstä.

45. Samoja näkökohtia sovelletaan myös organisatorisiin toimenpiteisiin, joilla tuetaan käsittelytoimia. Ne on suunniteltava siten, että alusta lähtien käsitellään vain niin vähän henkilötietoja kuin tietyissä käsittelytoimissa on tarpeen. Tämä on otettava huomioon etenkin silloin, kun annetaan tietoihinpääsyoikeuksia työntekijöille, joilla on erilaisia rooleja ja erilaisia käyttötarpeita.

46. Oletusarvoisen tietosuojan yhteydessä asianmukaiset ”tekniset ja organisatoriset toimenpiteet” tarkoittavat siten samaa kuin on kuvattu edellä alaluvussa 2.1.1, mutta niitä sovelletaan eritoten tietojen minimoinnin periaatteen noudattamiseen.

47. Edellä mainittua velvollisuutta käsitellä vain sellaisia henkilötietoja, jotka ovat tarpeen kunkin nimenomaisen tarkoituksen kannalta, sovelletaan seuraaviin seikkoihin.

---

[13] Yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan b, c, d ja e alakohta.

[14] Euroopan tietosuojavaltuutettu. ”Guidelines on assessing the necessity and proportionality of measures that limit the right to data protection”. 25. helmikuuta 2019. edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf

[15] Euroopan tietosuojavaltuutettu, ”Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit” https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en

[16] Ks. lisätietoja tarpeellisuudesta 29 artiklan mukaisen tietosuojatyöryhmän julkaisusta ”Lausunto 6/2014 direktiivin 95/46/EY 7 artiklan mukaisesta rekisterinpitäjän oikeutetun intressin käsitteestä.” WP 217, 9. huhtikuuta 2014. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_fi.pdf

2.2.2 Tietojen minimointia koskevan velvollisuuden näkökohdat

48. Asetuksen 25 artiklan 2 kohdassa luetellaan oletusarvoisen käsittelyn tietojen minimointia koskevan velvollisuuden näkökohdat. Siinä todetaan, että velvollisuus koskee kerättyjen henkilötietojen määrää, käsittelyn laajuutta, säilytysaikaa ja saatavilla oloa.

2.2.2.1 ”Kerättyjen henkilötietojen määrä”

49. Rekisterinpitäjien on otettava huomioon sekä käsittelyssä tarvittava henkilötietojen määrä että niiden tyypit, ryhmät ja yksityiskohtaisuus. Näissä suunnitteluvalinnoissa on otettava huomioon, että eheyteen ja luottamuksellisuuteen, tietojen minimointiin ja säilytyksen rajoittamisen periaatteisiin kohdistuvat riskit kasvavat, kun kerätään suuria määriä yksityiskohtaisia henkilötietoja, verrattuna siihen, että riskit pienenevät, kun kerätään pienempiä määriä ja/tai vähemmän yksityiskohtaisia tietoja rekisteröidyistä. Oletusasetuksena ei saa olla, että kerätään sellaisia henkilötietoja, jotka eivät ole tarpeen tietyn käsittelytarkoituksen kannalta. Toisin sanoen jos tietyt henkilötietoryhmät ovat tarpeettomia tai jos yksityiskohtaisia tietoja ei tarvita, koska vähemmän yksityiskohtaisetkin tiedot riittävät, henkilötietoja ei saa kerätä yhtään enempää kuin on tarpeen.

50. Samat oletusarvoiset vaatimukset koskevat palveluja riippumatta siitä, mitä alustaa tai laitetta käytetään. Vain kyseessä olevan tarkoituksen kannalta välttämättömiä henkilötietoja kerätään.

2.2.2.2 ”Käsittelyn laajuus”

51. Henkilötietoihin kohdistuvat käsittelytoimet[17] on rajoitettava vain siihen, mikä on välttämätöntä. Monet käsittelytoimet voivat liittyä tiettyyn käsittelytarkoitukseen. Pelkästään se, että tämän tarkoituksen täyttämiseen tarvitaan tiettyjä henkilötietoja, ei kuitenkaan tarkoita sitä, että tiedoilla saataisiin tehdä kaikenlaisia käsittelytoimia toistuvasti. Rekisterinpitäjien on myös varottava laajentamasta 6 artiklan 4 kohdan ”yhteensopivien tarkoitusten” rajoja ja pidettävä mielessä, millainen käsittely on rekisteröityjen kohtuullisten odotusten mukaista.

2.2.2.3 ”Tietojen säilytysaika”

52. Kerättyjä henkilötietoja ei saa tallentaa, jos se ei ole välttämätöntä käsittelyn tarkoitusta varten eikä 6 artiklan 4 kohdan mukaan ole muuta yhteensopivaa tarkoitusta ja laillista perustetta. Rekisterinpitäjän on perusteltava objektiivisesti ja osoitusvelvollisuuden periaatteen mukaisesti, että tietojen mahdollinen säilyttäminen on välttämätöntä.

53. Rekisterinpitäjän on rajoitettava säilytysaika siihen, mikä on käsittelytarkoituksen kannalta välttämätöntä. Jos henkilötietoja ei enää tarvita käsittelyä varten, on ne oletusarvoisesti poistettava tai anonymisoitava. Säilytysajan pituus riippuu näin ollen kyseessä olevan käsittelyn tarkoituksesta. Tämä velvollisuus liittyy suoraan 5 artiklan 1 kohdan e alakohdan mukaiseen säilytyksen rajoittamisen periaatteeseen, ja se on pantava täytäntöön oletusarvoisesti. Toisin sanoen rekisterinpitäjällä on oltava järjestelmälliset menettelyt käsittelyyn sisältyvien tietojen poistamiseen tai anonymisointiin.

[17] Yleisen tietosuoja-asetuksen 4 artiklan 2 kohdan mukaan tällä tarkoitetaan tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista.

54. Henkilötietojen anonymisointi[18] on vaihtoehto poistamiselle, kunhan otetaan huomioon kaikki oleelliset tilannekohtaiset tiedot ja kunhan riskin, myös henkilön uudelleentunnistamisen riskin, todennäköisyyttä ja vakavuutta arvioidaan säännöllisesti[19].

2.2.2.4 "Tietojen saatavilla olo"

55. Rekisterinpitäjän on rajoitettava sitä, kuka voi käyttää henkilötietoja ja millä tavoin, sen perusteella, mikä on tarpeellista, ja varmistettava, että henkilötiedot ovat niiden työntekijöiden saatavilla, jotka tarvitsevat niitä esimerkiksi kriittisissä tilanteissa. Tietojen käyttöä on valvottava koko tiedonsiirron ajan käsittelyn aikana.

56. Yleisen tietosuoja-asetuksen 25 artiklan 2 kohdassa todetaan myös, ettei tietoihinpääsyoikeuksia saa antaa rajoittamattomalle määrälle luonnollisia henkilöitä ilman yksilön mahdollisuutta myötävaikuttaa asiaan. Rekisterinpitäjän on siis oletusarvoisesti rajoitettava tietoihinpääsyoikeuksia ja annettava rekisteröidylle mahdollisuus puuttua asiaan ennen itseään koskevien henkilötietojen julkaisemista tai niiden saattamista muutoin rajoittamattoman henkilöjoukon saataville.

57. Henkilötietojen saattaminen rajoittamattoman henkilömäärän saataville voi johtaa siihen, että tietoja jaetaan laajemmalle kuin alun perin oli tarkoitettu. Tämä koskee erityisesti internetiä ja hakukoneita. Rekisterinpitäjien on siksi annettava rekisteröidyille oletusarvoisesti mahdollisuus puuttua asiaan ennen kuin henkilötiedot annetaan saataville avoimessa internetissä. Tämä on erityisen tärkeää, kun kyse on lapsista ja heikossa asemassa olevista ryhmistä.

58. Puuttumismahdollisuudet voivat vaihdella käsittelyn asiayhteyden mukaan sen perusteella, mikä on käsittelyn laillinen peruste. Se voi esimerkiksi olla suostumuksen pyytäminen henkilötietojen asettamiseen julkisesti saataville tai yksityisyysasetusten asettaminen siten, että rekisteröidyt voivat itse hallita julkista saatavuutta.

59. Silloinkaan, kun henkilötietoja asetetaan julkisesti saataville rekisteröidyn luvalla ja yhteisymmärryksessä hänen kanssaan, kyse ei ole siitä, että jokin toinen rekisterinpitäjä, jonka saatavilla henkilötiedot ovat, saisi vapaasti käsitellä niitä omiin tarkoituksiinsa, vaan sillä on oltava käsittelylle oma laillinen perusteensa.[20]

3 TIETOSUOJAPERIAATTEIDEN TÄYTÄNTÖÖNPANO HENKILÖTIETOJEN KÄSITTELYSSÄ HYÖDYNTÄMÄLLÄ SISÄÄNRAKENNETTUA JA OLETUSARVOISTA TIETOSUOJAA

60. Kaikissa käsittelytoimien suunnittelun vaiheissa, myös hankinnan, tarjouskilpailun, ulkoistamisen, kehityksen, tuen, ylläpitämisen, testauksen, säilyttämisen, poistamisen jne. yhteydessä, rekisterinpitäjän on otettava huomioon sisäänrakennetun ja oletusarvoisen tietosuojan eri seikkoja ja

[18] 29 artiklan mukainen tietosuojatyöryhmä. "Lausunto 5/2014 anonymisointitekniikoista". WP 216, 10. huhtikuuta 2014. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_fi.pdf

[19] Ks. myös yleisen tietosuoja-asetuksen 4 artiklan 1 kohta, johdanto-osan 26 kappale sekä 29 artiklan mukaisen tietosuojatyöryhmän "Lausunto 5/2014 anonymisointitekniikoista". Ks. myös tämän asiakirjan kohdassa 3 oleva alakohta "Säilytyksen rajoittaminen", jossa mainitaan, että rekisterinpitäjän on varmistettava käytetyn anonymisointitekniikan (käytettyjen anonymisointitekniikoiden) tehokkuus.

[20] Ks. asia 931/13, Satakunnan Markkinapörssi oy ja Satamedia oy v. Suomi.

arvioitava niitä. Tätä havainnollistetaan myöhemmin tässä luvussa esimerkeillä, joissa on kyse periaatteiden täytäntöönpanoon liittyvistä tilanteista.[21] [22] [23]

61. Rekisterinpitäjien on pantava periaatteet täytäntöön sisäänrakennetun ja oletusarvoisen tietosuojan aikaan saamiseksi. Nämä periaatteet ovat läpinäkyvyys, lainmukaisuus, kohtuullisuus, käyttötarkoitussidonnaisuus, tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen, eheys ja luottamuksellisuus sekä osoitusvelvollisuus. Periaatteet esitetään yleisen tietosuoja-asetuksen 5 artiklassa ja johdanto-osan 39 kappaleessa. Sisäänrakennetun ja oletusarvoisen tietosuojan täytäntöönpanon täydellinen ymmärtäminen edellyttää kunkin periaatteen merkityksen ymmärtämistä.

62. Laatiessamme esimerkkejä siitä, miten sisäänrakennetun ja oletusarvoisen tietosuojan periaatteita otetaan käyttöön, olemme tehneet luettelot **sisäänrakennettua ja oletusarvoista tietosuojaa koskevista keskeisistä osatekijöistä** jokaisen periaatteen osalta. Esimerkit, joissa korostetaan kyseessä olevan tietosuojaperiaatteen erityispiirteitä, voivat limittyä myös muihin niihin läheisesti liittyviin periaatteisiin. Euroopan tietosuojaneuvosto korostaa, että jäljempänä esitetyt keskeiset osatekijät ja esimerkit eivät ole tyhjentäviä eivätkä sitovia, vaan niillä on tarkoitus antaa ohjausta kustakin periaatteesta. Rekisterinpitäjien on arvioitava, miten periaatteiden noudattaminen taataan kulloisessakin konkreettisessa käsittelytoimessa.

63. Vaikka tässä osassa keskitytään periaatteiden täytäntöönpanoon, rekisterinpitäjän on myös otettava käyttöön *asianmukaisia* ja *tehokkaita* tapoja suojella rekisteröityjen oikeuksia, yleisen tietosuoja-asetuksen III luvun mukaisesti, jos niitä ei jo edellytetä itse periaatteissa.

64. Osoitusvelvollisuuden periaate on kaikenkattava: sen mukaan rekisterinpitäjä on vastuussa tarvittavien teknisten ja organisatoristen toimenpiteiden valitsemisesta.

3.1 Läpinäkyvyys[24]

65. Rekisterinpitäjän on kerrottava rekisteröidylle selvästi ja avoimesti miten se kerää, käyttää ja jakaa henkilötietoja. Läpinäkyvyydellä tarkoitetaan sitä, että rekisteröidyt ymmärtävät 15–22 artiklan mukaiset oikeutensa ja sen, että he tarvittaessa voivat käyttää niitä. Periaate sisältyy 12, 13, 14 ja 34 artiklaan. Läpinäkyvyyden periaatteen tukemiseksi käytettävien toimenpiteiden ja suojatoimien tulisi tukea myös näiden artiklojen täytäntöönpanoa.

66. Sisäänrakennetun ja oletusarvoisen tietosuojan läpinäkyvyyttä koskevia keskeisiä tekijöitä ovat seuraavat:

- Selkeys – tiedot on esitettävä selvällä ja yksinkertaisella kielellä, tiiviisti ja ymmärrettävästi.
- Semantiikka – viestinnällä on oltava ymmärrettävä kyseiselle yleisölle.
- Saatavuus – tietojen on oltava helposti rekisteröidyn saatavilla.
- Asiayhteys – tiedot on annettava oikeaan aikaan ja asianmukaisessa muodossa.

[21] Lisää esimerkkejä on Norjan tietosuojaviranomaisen verkkosivulla ”Software Development with Data Protection by Design and by Default”. 28. marraskuuta 2017 www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?id=7729

[22] https://www.cnil.fr/en/cnil-publishes-gdpr-guide-developers

[23] https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf

[24] Sitä, miten läpinäkyvyyden käsite tulisi ymmärtää, on selvitetty 29 artiklan mukaisen tietosuojatyöryhmän julkaisussa ”Asetuksen 2016/679 mukaista läpinäkyvyyttä koskevat suuntaviivat”. WP 260 rev.01, 11. huhtikuuta 2018. ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025 – Euroopan tietosuojaneuvoston hyväksymä.

- Olennaisuus – tietojen on oltava asiaankuuluvia ja liityttävä tiettyyn rekisteröityyn.
- Universaali rakenne – tietojen on oltava kaikkien rekisteröityjen käytettävissä ja niissä on käytettävä koneellisesti luettavia esitysmuotoja luettavuuden ja selkeyden parantamiseksi ja automatisoimiseksi.
- Ymmärrettävyys – rekisteröidyillä on oltava asianmukainen käsitys siitä, mitä he voivat odottaa omien henkilötietojensa käsittelyltä etenkin, kun rekisteröidyt ovat lapsia tai muita heikossa asemassa olevia ryhmiä.
- Monikanavaisuus – tietoa on annettava eri kanavissa ja medioissa myös muita kuin tekstimuotoisia välineitä hyödyntämällä. Tämä parantaa sen todennäköisyyttä, että tieto saavuttaa rekisteröidyn tehokkaasti.
- Kerroksellisuus – tiedot on kerrostettava siten, että niistä saadaan sekä täydellisiä että ymmärrettäviä ja että niissä otetaan huomioon rekisteröityjen kohtuulliset odotukset.

Esimerkki[25]

Rekisterinpitäjä suunnittelee verkkosivustollaan tietosuojakäytännön, jotta se täyttäisi läpinäkyvyyttä koskevat vaatimukset. Tietosuojakäytännön ei pitäisi sisältää sellaista tekstiä, joita tyypillisen rekisteröidyn on vaikeaa ymmärtää ja käsittää. Tiedot on esitettävä selkeästi ja tiiviisti, ja verkkosivuston käyttäjän on pystyttävä niiden avulla ymmärtämään helposti, miten henkilötietoja käsitellään. Siksi rekisterinpitäjä esittää tiedot kerroksittain jäsennettyinä ja tärkeimmät kohdat korostettuina. Lisätietoja annetaan saataville helposti. Sivustolla on pudotusvalikoita ja linkkejä muille sivuille, joilla eri kohtia ja käytännön käsitteitä selitetään tarkemmin. Lisäksi rekisterinpitäjä varmistaa, että tietoa annetaan monilla eri kanavilla. Siinä hyödynnetään myös videoleikkeitä, joissa selitetään tärkeimmät kohdat kirjallisista tiedoista. Eri sivujen yhteisvaikutus on ensiarvoisen tärkeää, jotta voidaan varmistaa, että kerroksellinen toimintamalli ei lisää hämmennystä vaan vähentää sitä.

Rekisteröityjen on voitava löytää tietosuojakäytäntö sivustolta helposti. Siksi tietosuojakäytäntö asetetaan saataville ja näkyville kaikille kyseisen sivuston verkkosivuille. Rekisteröity saa tämän käytännön siis nähtäväkseen aina vain yhdellä näpäytyksellä. Esitetyt tiedot on myös laadittu parhaiden käytäntöjen ja universaalia rakennetta koskevien standardien mukaisesti, jotta ne olisivat kaikkien saatavilla.

Tarvittavat tiedot on myös esitettävä oikeassa asiayhteydessä ja oikeaan aikaan. Koska rekisterinpitäjä toteuttaa useita käsittelytoimia verkkosivustolle kerättyjen tietojen avulla, rekisterinpitäjä ei täytä läpinäkyvyyden vaatimuksia pelkästään verkkosivustolla olevan yleisen tietosuojakäytännön avulla. Sen vuoksi rekisterinpitäjä suunnittelee sellaisen tietovirran, jossa asiaankuuluvat tiedot esitetään rekisteröidylle oikeissa asiayhteyksissä käyttämällä vaikkapa erilaisia tietoikkunoita tai ponnahdusikkunoita. Esimerkiksi kun rekisteröityä pyydetään antamaan henkilötietoja, rekisterinpitäjä ilmoittaa hänelle, miten henkilötietoja käsitellään ja miksi näitä henkilötietoja tarvitaan käsittelyä varten.

3.2 Lainmukaisuus

67. Rekisterinpitäjän on määritettävä pätevä laillinen peruste henkilötietojen käsittelylle. Toimenpiteiden ja suojatoimien pitäisi varmistaa, että koko käsittelyn elinkaari on linjassa käsittelyn oleellisten laillisten perusteiden kanssa.

[25] Ranskan tietosuojaviranomainen on julkaissut useita esimerkkejä, joissa kuvataan käyttäjille tiedottamisen parhaita käytäntöjä ja muita läpinäkyvyyteen liittyviä periaatteita: https://design.cnil.fr/en/

68. Sisäänrakennetun ja oletusarvoisen tietosuojan lainmukaisuutta koskevia keskeisiä tekijöitä ovat seuraavat:
    - Oleellisuus – käsittelyssä on sovellettava asianmukaista laillista perustetta.
    - Erottaminen[26] – kullakin käsittelytoimella on oltava erillinen laillinen peruste.
    - Tietty tarkoitus – asianmukaisen laillisen perusteen on liityttävä selvästi tiettyyn käsittelytarkoitukseen.[27]
    - Tarpeellisuus – käsittelyn on oltava käyttötarkoituksen kannalta tarpeen, jotta se olisi lainmukaista.
    - Itsemääräämisoikeus – rekisteröidylle on annettava laillisen perusteen rajoissa mahdollisimman laaja itsemääräämisoikeus omien henkilötietojensa valvontaan.
    - Suostumuksen saaminen – suostumuksen on oltava vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen.[28] Erityistä huomiota on kiinnitettävä lasten ja nuorten kykyyn antaa tietoinen suostumus.
    - Suostumuksen peruuttaminen – kun suostumus on laillinen peruste, suostumus on voitava peruuttaa käsittelyssä. Peruutuksen on oltava yhtä helppoa kuin suostumuksen antaminen. Jos se ei ole, rekisterinpitäjän suostumusmekanismi ei ole yleisen tietosuoja-asetuksen mukainen.[29]
    - Etujen arviointi – jos oikeutetut edut ovat laillinen peruste, rekisterinpitäjän on tehtävä painotettu etujen arviointi, jossa kiinnitetään erityistä huomiota vallan epätasapainoon, etenkin alle 18-vuotiaisiin lapsiin ja muihin heikossa asemassa oleviin ryhmiin. Rekisteröityihin kohdistuvan kielteisen vaikutuksen lieventämiseksi on oltava käytössä toimenpiteitä ja suojatoimia.
    - Ennalta määrittäminen – laillinen peruste on määritettävä ennen kuin käsittely aloitetaan.
    - Käsittelyn lopettaminen – jos laillista perustetta ei enää voida soveltaa, käsittely on lopetettava.
    - Mukauttaminen – jos käsittelyn laillinen peruste muuttuu pätevästä syystä, varsinaista käsittelyä on mukautettava uuden laillisen perusteen mukaisesti[30].
    - Vastuunjako – aina kun suunnitellaan yhteisrekisterinpitoa, osapuolten on määritettävä selvästi ja avoimesti vastuunsa rekisteröityyn nähden ja suunniteltava käsittelyn toimenpiteet tämän määrityksen mukaisesti.

Esimerkki

Pankki suunnittelee tarjoavansa palvelua, jonka tarkoituksena on parantaa lainahakemusten käsittelyn tehokkuutta. Palvelu perustuu ajatukseen siitä, että kun pankki pyytää asiakkaalta luvan, se voi hakea asiakkaasta tietoja suoraan veroviranomaisilta. Tämä esimerkki ei koske muista lähteistä saatavien henkilötietojen käsittelyä.

[26] Euroopan tietosuojaneuvosto. ”Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects”. Versio 2.0, 8. lokakuuta 2019. edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf

[27] Ks. käyttötarkoitussidonnaisuutta koskeva kohta jäljempänä.

[28] Ks. Guidelines 05/2020 on consent under Regulation 2016/679. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

[29] Ks. Guidelines 05/2020 on consent under Regulation 2016/679, s. 24. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

[30] Jos alkuperäinen laillinen peruste on suostumus, ks. Guidelines 05/2020 on consent under Regulation 2016/679. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

Henkilötietojen saaminen rekisteröidyn taloudellisesta tilanteesta on tarpeen, jotta voitaisiin ryhtyä toimiin rekisteröidyn pyynnöstä ennen lainasopimuksen tekemistä.[31] Henkilötietojen keräämistä suoraan verohallinnolta ei kuitenkaan katsota tarpeelliseksi, koska asiakas voi tehdä sopimuksen antamalla verohallinnon tiedot itse. Vaikka asiakirjojen hankkiminen suoraan veroviranomaisilta voi olla pankin kannalta oikeutettu etu, esimerkiksi lainan käsittelyn tehokkuuden varmistamiseksi, tällaisen suoran käyttöoikeuden antaminen pankeille hakijoiden henkilötietoihin aiheuttaa käyttöoikeuksien käyttöä tai mahdollista väärinkäyttöä koskevia riskejä.

Lainmukaisuuden periaatetta noudattaessaan rekisterinpitäjä havaitsee, ettei se voi tässä yhteydessä käyttää perustetta ”tarpeellinen sopimuksen tekemisen vuoksi” siihen käsittelyn vaiheeseen, jossa pyydetään henkilötietoja suoraan veroviranomaisilta. Se, että tämä nimenomainen käsittely aiheuttaa riskin siitä, että rekisteröidyllä on vähemmän mahdollisuuksia myötävaikuttaa omien tietojensa käsittelyyn, on oleellinen tekijä kun arvioidaan varsinaisen käsittelyn laillisuutta. Pankki toteaa, että käsittelyn tässä osassa on turvauduttava muuhun lailliseen perusteeseen. Tässä nimenomaisessa jäsenvaltiossa, johon rekisterinpitäjä on sijoittautunut, kansallisten lakien mukaan pankki voi kerätä tietoa suoraan veroviranomaisilta, jos rekisteröity antaa siihen etukäteen suostumuksen.

Niinpä pankki antaa tietoa käsittelystä lainahakemusten tekemiseen tarkoitetulla verkkoalustalla siten, että rekisteröityjen on helppo ymmärtää, millainen käsittely on pakollista ja millainen vapaaehtoista. Oletusarvoisesti käsittelyvaihtoehdot eivät anna lupaa siihen, että tietoa haetaan muista lähteistä kuin rekisteröidyltä itseltään, ja vaihtoehto pyytää tietoja suoraan esitetään siten, että rekisteröidyllä on mahdollisuus kieltäytyä siitä. Mahdollinen suostumus tietojen hankkimiseen suoraan muilta rekisterinpitäjiltä tarkoittaa vain tilapäistä oikeutta päästä tiettyihin tietoihin.

Mahdollisesti annettu suostumus käsitellään sähköisesti siten, että se voidaan dokumentoida, ja rekisteröidyille annetaan helppokäyttöinen mahdollisuus valvoa, mihin he ovat antaneet suostumuksensa ja miten he voivat peruuttaa sen.

Rekisterinpitäjä on arvioinut nämä sisäänrakennettua ja oletusarvoista tietosuojaa koskevat vaatimukset etukäteen, ja se sisällyttää kaikki nämä kriteerit vaatimusmäärittelyihinsä, jotka koskevat lainahakemusten tekemiseen tarkoitetun verkkoalustan hankintaa. Rekisterinpitäjä tietää, että jos se ei sisällytä sisäänrakennettua ja oletusarvoista tietosuojaa koskevia vaatimuksia tarjouspyyntöön, tietosuojan toteuttaminen jälkeenpäin voi olla joko liian myöhäistä tai hyvin kallista.

3.3 Kohtuullisuus

69. Kohtuullisuus on yleisperiaate, joka edellyttää sitä, ettei henkilötietoja saa käsitellä rekisteröidyn kannalta perusteettoman haitallisella, lainvastaisen syrjivällä, odottamattomalla tai harhaanjohtavalla tavalla. Toimenpiteillä ja suojatoimilla, joilla kohtuullisuuden periaate pannaan täytäntöön, tuetaan myös rekisteröityjen oikeuksia ja vapauksia. Niitä ovat erityisesti oikeus saada ilmoitus tietojenkäsittelystä (läpinäkyvyys), puuttumisoikeus (pääsy tietoihin, niiden poistaminen, henkilötietojen siirtäminen järjestelmästä toiseen ja niiden oikaiseminen) ja oikeus rajoittaa käsittelyä (oikeus kieltäytyä automaattisista yksittäispäätöksistä ja rekisteröityjen syrjimättömyys tällaisissa prosesseissa).

70. Sisäänrakennetun ja oletusarvoisen tietosuojan kohtuullisuutta koskevia keskeisiä tekijöitä ovat seuraavat:

[31] Ks. yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan b alakohta.

- Itsemääräämisoikeus – rekisteröidyille on taattava mahdollisimman suuri itsemääräämisoikeus omien henkilötietojen käytön määrittämisessä sekä kyseisen käytön tai käsittelyn laajuuden ja ehtojen osalta.
- Vuorovaikutus – rekisteröityjen on voitava viestiä rekisterinpitäjän kanssa ja käyttää oikeuksiaan rekisterinpitäjän käsittelemien henkilötietojen osalta.
- Odotukset – käsittelyn on vastattava rekisteröityjen kohtuullisia odotuksia.
- Syrjimättömyys – rekisterinpitäjä ei saa syrjiä rekisteröityjä epäoikeudenmukaisesti.
- Ei hyväksikäyttöä – rekisterinpitäjä ei saa käyttää rekisteröityjen tarpeita tai haavoittuvuuksia hyväkseen.
- Kuluttajan valinta – rekisterinpitäjä ei saa sitoa kuluttajaa epäoikeudenmukaisesti. Aina, kun henkilötietoja käsittelevä palvelu on suljettu, se voi edellyttää sitoutumista palveluun. Se ei taas ehkä ole kohtuullista, jos se heikentää rekisteröityjen mahdollisuutta käyttää tietojen siirrettävyyttä koskevaa oikeuttaan 20 artiklan mukaisesti.
- Vallan tasapaino – vallan tasapainon on oltava keskeinen tavoite rekisterinpitäjän ja rekisteröidyn välisessä suhteessa. Vallan epätasapainoa on vältettävä. Kun se ei ole mahdollista, se on tiedostettava ja siitä on huolehdittava soveltuvin vastatoimin.
- Ei riskin siirtoa – rekisterinpitäjät eivät saa siirtää yrityksen riskejä rekisteröidyille.
- Ei harhaanjohtamista – tietojenkäsittelyä koskevat tiedot ja vaihtoehdot on annettava puolueettomasti ja neutraalisti ja vältettävä harhaanjohtavaa tai ohjailevaa kielenkäyttöä tai esittämistä.
- Oikeuksien kunnioittaminen – rekisterinpitäjän on kunnioitettava rekisteröityjen perusoikeuksia ja toteutettava asianmukaiset toimenpiteet ja suojatoimet, eikä rekisterinpitäjä saa estää kyseisiä oikeuksia, ellei sitä ole nimenomaisesti perusteltu laissa.
- Eettisyys – rekisterinpitäjän on nähtävä myös käsittelyn laajempi vaikutus yksilöiden oikeuksiin ja ihmisarvoon.
- Oikeellisuus – rekisterinpitäjän on annettava saataville tietoa siitä, miten se käsittelee henkilötietoja, sen on toimittava ilmoittamallaan tavalla, eikä se saa johtaa rekisteröityjä harhaan.
- Ihmisen osallistuminen – rekisterinpitäjän on sisällytettävä käsittelyyn mahdollisuus, että tietojen käsittelyyn voi tarvittaessa osallistua *pätevä* ihminen, jotta pystyttäisiin havaitsemaan vinoutumat, joita koneet voivat luoda. Tämä liittyy oikeuteen kieltäytyä automaattisista yksittäispäätöksistä 22 artiklan mukaisesti.[32]
- Tasapuoliset algoritmit – arvioidaan säännöllisesti, toimivatko algoritmit tarkoitusten mukaisesti, ja muokataan algoritmeja havaittujen vinoutumien lieventämiseksi ja käsittelyn tasapuolisuuden varmistamiseksi. Rekisteröidyille on annettava tietoa sellaisiin algoritmeihin perustuvasta henkilötietojen käsittelystä, joilla tehdään analyyseja tai ennusteita esimerkiksi heidän työssä suoriutumisestaan, taloudellisesta tilanteestaan, terveydestään, henkilökohtaisista mieltymyksistään, luotettavuudestaan tai käyttäytymisestään sekä sijainnistaan tai liikkeistään.[33]

Esimerkki 1

[32] Ks. suuntaviivat automatisoiduista yksittäispäätöksistä ja profiloinnista asetuksen (EU) 2016/679 täytäntöön panemiseksi. https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826
[33] Ks. yleisen tietosuoja-asetuksen johdanto-osan 71 kappale.

Rekisterinpitäjä ylläpitää hakukonetta, joka käsittelee useimmiten käyttäjien luomia henkilötietoja. Rekisterinpitäjälle koituu tästä se etu, että se saa suuria määriä henkilötietoja, joita se voi käyttää kohdennettuun mainontaan. Sen vuoksi rekisterinpitäjä haluaa vaikuttaa rekisteröityihin siten, että he sallisivat henkilötietojensa laajamittaisemman keräämisen ja käytön. Suostumus on hankittava esittämällä käsittelyvaihtoehdot rekisteröidylle.

Kohtuullisuuden periaatetta noudattaessaan rekisterinpitäjä ottaa huomioon käsittelyn luonteen, laajuuden, asiayhteyden ja tarkoituksen ja havaitsee, ettei se voi esittää vaihtoehtoja tavalla, joka ohjaisi rekisteröityä sallimaan rekisterinpitäjän kerätä tarvittavaa enemmän henkilötietoja kuin silloin, kun vaihtoehdot esitetään tasapuolisella ja neutraalilla tavalla. Toisin sanoen se ei voi esittää käsittelyvaihtoehtoja siten, että rekisteröityjen on vaikea kieltäytyä tietojensa jakamisesta tai muuttaa yksityisyysasetuksiaan ja rajoittaa käsittelyä. Nämä ovat esimerkkejä käyttäjän johdattelusta, joka on vastoin 25 artiklan henkeä. Käsittelyn oletusvaihtoehdot eivät saa olla invasiivisia, ja muunlaista käsittelyä koskeva valinta on esitettävä siten, ettei rekisteröityä painosteta antamaan suostumusta. Siksi rekisterinpitäjän on esitettävä suostumuksen antamista tai epäämistä koskevat vaihtoehdot yhtä näkyvästi, ja niissä on esitettävä rekisteröidyille täsmällisesti kunkin valinnan seuraukset.

Esimerkki 2

Toinen rekisterinpitäjä käsittelee henkilötietoja suoratoistopalvelun tarjoamista varten, ja käyttäjät voivat valita vakiolaatuisen säännöllisen tilauksen tai premium-luokan tilauksen, jonka laatu on vakiolaatua parempi. Premium-tilauksen tehneitä tilaajat asetetaan myös etusijalle asiakaspalvelussa.

Kohtuullisuuden periaatteen perusteella premium-tilauksen tehneiden tilaajien asettamisella etusijalle asiakaspalvelussa ei voida syrjiä vakiotilaajien mahdollisuuksia käyttää oikeuksiaan yleisen tietosuoja-asetuksen 12 artiklan mukaisesti. Tämä tarkoittaa sitä, että vaikka premium-tilauksen tehneitä tilaajia asetetaan etusijalle asiakaspalvelussa, tällainen etusijalle asettaminen ei voi johtaa siihen, että ei toteuteta riittäviä toimia, jotta tavallisten tilaajien pyyntöihin voitaisiin vastata ilman aiheetonta viivästystä ja joka tapauksessa kuukauden kuluessa pyyntöjen vastaanottamisesta.

Vaikka etusijalle asetetut asiakkaat kenties maksavatkin saadakseen parempaa palvelua, kaikilla rekisteröidyillä on oltava tasaveroinen ja syrjimättömyyteen perustuva mahdollisuus käyttää 12 artiklan mukaisia oikeuksiaan ja vapauksiaan.

3.4 Käyttötarkoitussidonnaisuus[34]

71. Rekisterinpitäjän on kerättävä tietoja tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin niiden keräämistarkoituksen kanssa yhteensopimattomalla tavalla.[35] Käsittely on siis suunniteltava sen mukaan, mikä on tarpeen tarkoitusten täyttämiseksi. Jos tietoja on suunniteltu käytettäväksi myöhemmin, rekisterinpitäjän on ensin varmistettava, että tämän käsittelyn tarkoitukset

[34] 29 artiklan mukainen tietosuojatyöryhmä on antanut ohjeita siitä, miten direktiivin 95/46/EY mukainen käyttötarkoitussidonnaisuuden periaate tulisi ymmärtää. Vaikka lausunto ei ole Euroopan tietosuojaneuvoston hyväksymä, se voi silti olla merkityksellinen, sillä periaatteen sanamuoto on sama myös yleisessä tietosuoja-asetuksessa. 29 artiklan mukainen tietosuojatyöryhmä. ”Opinion 03/2013 on purpose limitation”. WP 203, 2. huhtikuuta 2013. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[35] Yleisen tietosuoja-asetuksen 5 artiklan 1 kohta.

ovat yhteensopivat alkuperäisten tarkoitusten kanssa, ja suunniteltava käsittely tämän mukaisesti. Se, onko uusi käyttötarkoitus yhteensopiva vai ei, on arvioitava 6 artiklan 4 kohdan mukaisesti.

72. Sisäänrakennetun ja oletusarvoisen tietosuojan käyttötarkoitussidonnaisuutta koskevia keskeisiä tekijöitä ovat seuraavat:
    - Ennalta määrittäminen – lailliset tarkoitukset on määritettävä ennen käsittelyn suunnittelemista.
    - Nimenomaisuus – tarkoitukset on yksilöitävä ja on selitettävä nimenomaisesti, miksi henkilötietoja käsitellään.
    - Tarkoituksenmukaisuus – käsittely on suunniteltava käsittelyn tarkoituksen perusteella, ja sen mukaan on määritettävä myös käsittelyn rajat.
    - Tarpeellisuus – käsittelyn tarkoitus määrää sen, mitä henkilötietoja käsittelyssä tarvitaan.
    - Yhteensopivuus – kaikkien uusien tarkoitusten on oltava yhteensopivia sen alkuperäisen tarkoituksen kanssa, jota varten tietoja kerättiin, ja sen on ohjattava myös käsittelyn rakenteeseen tehtäviä mahdollisia muutoksia.
    - Jatkokäsittelyn rajoittaminen – rekisterinpitäjä ei saa yhdistää tietueita tai tehdä jatkokäsittelyä uusia yhteensopimattomia tarkoituksia varten.
    - Uudelleenkäytön rajoitukset – rekisterinpitäjän on käytettävä teknisiä toimenpiteitä, esimerkiksi tiivistämistä ja salausta, rajoittaakseen mahdollisuutta käyttää henkilötietoja toiseen käyttötarkoitukseen. Rekisterinpitäjällä on myös oltava organisatorisia toimenpiteitä, kuten toimintalinjoja ja sopimusvelvoitteita, joilla rajoitetaan henkilötietojen uudelleenkäyttöä.
    - Arviointi – rekisterinpitäjän on arvioitava säännöllisesti, onko tietojen käsittely tarpeellista sitä tarkoitusta varten, johon tietoja kerättiin, ja testattava rakennetta käyttötarkoitussidonnaisuuteen nähden.

Esimerkki

Rekisterinpitäjä käsittelee asiakkaidensa henkilötietoja. Käsittelyn tarkoituksena on täyttää sopimus, jotta voidaan esimerkiksi toimittaa tavarat oikeaan osoitteeseen ja saada maksu. Tallennettuja henkilötietoja ovat ostohistoria, nimi, osoite, sähköpostiosoite ja puhelinnumero.

Rekisterinpitäjä harkitsee sellaisen asiakastietojen hallintaohjelman ostamista, joka kerää kaikki asiakastiedot myynnistä, markkinoinnista ja asiakaspalvelusta yhteen paikkaan. Tällä ohjelmalla voidaan tallentaa kaikki puhelut, toimet, asiakirjat, sähköpostiviestit ja markkinointikampanjat, jotta saadaan asiakkaasta kattava kuva. Asiakastietojen hallintaohjelma pystyy myös analysoimaan asiakkaiden ostovoiman automaattisesti julkisia tietoja hyödyntämällä. Analyysin tarkoituksena on parantaa mainostoimien kohdentamista. Nämä toimet eivät kuuluu käsittelyn alkuperäiseen lainmukaiseen tarkoitukseen.

Jotta tämä olisi käyttötarkoitussidonnaisuuteen liittyvän periaatteen mukaista, rekisterinpitäjä edellyttää, että ohjelmistotuotteen toimittaja määrittää eri käsittelytoimet, joissa käytetään henkilötietoja, rekisterinpitäjän kannalta oleellisten tarkoitusten mukaisesti.

Saatuaan määrityksen tulokset rekisterinpitäjä arvioi, ovatko uudet markkinointia ja kohdennettua mainontaa koskevat tarkoitukset yhteensopivia tietojen keräämisen aikana määritettyjen alkuperäisten tarkoitusten kanssa ja onko käsittelylle niiden osalta riittävä laillinen peruste. Jos arvioinnin tulos ei ole myönteinen, rekisterinpitäjä ei saa käyttää kyseisiä toimintoja. Vaihtoehtoisesti rekisterinpitäjä voi päättää ohittaa arvioinnin ja vain olla käyttämättä tuotteen kuvattuja toimintoja.

3.5 Tietojen minimointi

73. Vain sellaisia henkilötietoja saa käsitellä, jotka ovat asianmukaisia ja olennaisia ja rajoitettu siihen, mikä on **tarpeellista** suhteessa siihen tarkoitukseen, jota varten niitä käsitellään.[36] Näin ollen rekisterinpitäjän on määritettävä etukäteen, mitkä käsittelyjärjestelmien ominaisuudet ja parametrit ja niitä tukevat toiminnot ovat sallittuja. Tiedon minimointi toteuttaa henkilötietojen tarpeellisuusvaatimusta. Jatkokäsittelyn yhteydessä rekisterinpitäjän on arvioitava säännöllisin väliajoin, ovatko käsitellyt henkilötiedot yhä asianmukaisia, oleellisia ja tarpeellisia vai onko tiedot poistettava tai anonymisoitava.

74. Ennen kaikkea rekisterinpitäjien on määritettävä, onko niiden edes käsiteltävä henkilötietoja itselleen olennaisissa tarkoituksissa. Rekisterinpitäjän on tarkastettava, voidaanko asiaankuuluvat tarkoitukset saavuttaa käsittelemällä vähemmän henkilötietoja tai siten, että henkilötiedot eivät ole niin yksityiskohtaisia tai ne on yhdistetty, taikka siten, että henkilötietoja ei käsitellä lainkaan[37]. Tällainen tarkastus on tehtävä ennen mitään käsittelyä, mutta se voidaan tehdä myös missä tahansa käsittelyn elinkaaren vaiheessa. Tämä on myös 11 artiklan mukaista.

75. Minimoinnilla voidaan tarkoittaa myös tunnistamisen astetta. Jos käsittelyn tarkoitus ei vaadi lopullista tietokokonaisuutta, joka liittyy tunnistettuun tai tunnistettavissa olevaan henkilöön (kuten vaikkapa tilastoissa) mutta jos alkuperäinen käsittelytarkoitus vaatii sitä (esimerkiksi ennen tietojen yhdistelemistä), rekisterinpitäjän on poistettava tai anonymisoitava henkilötiedot niin pian kuin mahdollista sen jälkeen, kun tunnistamista ei enää tarvita. Jos tunnistaminen on vielä tarpeen muita käsittelytoimia varten, henkilötiedot on pseudonymisoitava, jotta pienennetään rekisteröityjen oikeuksiin kohdistuvia riskejä.

76. Sisäänrakennetun ja oletusarvoisen tietosuojan tietojen minimointia koskevia keskeisiä tekijöitä ovat seuraavat:
    - Henkilötietojen käsittelyn välttäminen – vältetään käyttämästä henkilötietoja ollenkaan, jos se on mahdollista kunkin tarkoituksen yhteydessä.
    - Rajoittaminen – rajoitetaan kerättävien henkilötietojen määrä vain siihen, mikä on tarpeen tarkoituksen kannalta.
    - Käytön rajoittaminen – muokataan tietojenkäsittelyä siten, että mahdollisimman pieni määrä ihmisiä käsittelee henkilötietoja tehtäviensä täyttämiseksi, ja rajoitetaan käyttöä sen mukaan.
    - Olennaisuus – henkilötietojen on oltava kyseisen käsittelyn kannalta olennaisia, ja rekisterinpitäjän on voitava osoittaa olennaisuus.
    - Tarpeellisuus – jokaisen henkilötietoryhmän on oltava tarpeen määritetyissä tarkoituksissa, ja niitä on käsiteltävä vain, jos tarkoitusta ei voida täyttää muilla keinoilla.
    - Yhdisteleminen – käytetään yhdistelmätietoja, mikäli mahdollista.
    - Pseudonymisointi – pseudonymisoidaan henkilötiedot heti, kun henkilötietoja ei enää tarvita suoraan tunnistamiseen, ja säilytetään tunnistamisavaimet erikseen.
    - Anonymisointi ja poistaminen – kun henkilötietoja ei tarvita tai ei enää tarvita tiettyyn tarkoitukseen, ne on anonymisoitava tai hävitettävä.
    - Tiedonsiirto – tiedonsiirron on oltava riittävän tehokasta, jotta ei luoda enempää kopioita kuin on tarpeen.

[36] Yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan c alakohta.
[37] Yleisen tietosuoja-asetuksen johdanto-osan 39 kappaleessa todetaan: ”Henkilötietoja olisi käsiteltävä vain jos käsittelyn tarkoitusta ei voida kohtuullisesti toteuttaa muilla keinoin.”

- ”Viimeisin tekniikka” – rekisterinpitäjän on käytettävä ajan tasalla olevaa ja asianmukaista tekniikkaa, jotta voidaan välttää henkilötietojen käsittely ja varmistaa tietojen minimointi.

Esimerkki 1

Kirjakauppa haluaa kasvattaa tulojaan myymällä kirjoja verkossa. Kirjakaupan omistaja haluaa ottaa käyttöön vakiomuotoisen tilausprosessin. Varmistaakseen, että asiakkaat antavat kaikki tarvittavat tiedot, kirjakaupan omistaja tekee kaikista tilauslomakkeen kentistä pakollisia (ts. jos asiakas ei täytä kaikkia kenttiä, hän ei voi tehdä tilausta). Verkkokaupan omistaja käyttää vakiomuotoista yhteydenottolomaketta, jossa pyydetään antamaan tietoja, muun muassa asiakkaan syntymäaika, puhelinnumero ja kotiosoite. Kaikki lomakkeen kentät eivät kuitenkaan ole välttämättömiä kirjojen ostamista ja toimittamista varten. Jos tässä nimenomaisessa tapauksessa rekisteröity maksaa tuotteen etukäteen, rekisteröidyn syntymäaikaa ja puhelinnumeroa ei tarvita tuotteen ostamiseen. Ne eivät siksi voi olla pakollisia kenttiä tuotteen tilaukseen käytettävässä verkkolomakkeessa, ellei rekisterinpitäjä pysty selkeästi osoittamaan, että se on muutoin välttämätöntä, sekä sen, miksi kentät ovat välttämättömiä. On myös tilanteita, joissa osoitetta ei tarvita. Esimerkiksi sähkökirjan tilaava asiakas voi ladata tuotteen suoraan laitteelleen.

Niinpä verkkokaupan omistaja päättää tehdä kaksi verkkolomaketta: yhden kirjojen tilaamista varten, ja siinä on kenttä asiakkaan osoitteelle, ja toisen sähköisten kirjojen tilaamista varten ilman tätä kenttää.

Esimerkki 2

Julkinen kuljetusyhtiö haluaa kerätä matkustajien reitteihin perustuvaa tilastotietoa. Nämä tiedot ovat hyödyllisiä, jotta yhtiö voi tehdä asianmukaisia päätöksiä julkisen liikenteen aikataulumuutoksista ja reitittää junat asianmukaisesti. Matkustajien on käytettävä matkalippunsa lukijassa joka kerta, kun he nousevat kulkuvälineeseen tai poistuvat siitä. Kun rekisterinpitäjä on tehnyt matkustajien reittitietojen keräämiseen liittyvän riskinarvioinnin matkustajien oikeuksista ja vapauksista, se toteaa, että matkustajat, jotka asuvat tai työskentelevät harvaan asutuilla alueilla, voidaan tunnistaa yksinomaan matkustusreitin perusteella lipputunnisteen avulla. Koska tunnistamista ei tarvita sitä varten, että julkisen liikenteen aikataulut ja junien reititykset voitaisiin optimoida, rekisterinpitäjä ei tallenna lipputunnistetta. Kun matkustaja on tehnyt matkansa, rekisterinpitäjä säilyttää tiedot yksittäisistä matkustusreiteistä siten, ettei niiden perusteella voida tunnistaa yksittäiseen lippuun liittyviä matkoja, ja säilyttää vain erillisiä matkustusreittejä koskevat tiedot.

Jos on riski, että henkilö voidaan tunnistaa yksinomaan heidän käyttämänsä julkisen liikennevälineen reitin perusteella, rekisterinpitäjä toteuttaa riskin vähentämiseksi tilastollisia toimenpiteitä ja poistaa tiedoista vaikkapa reitin alku- ja päätepisteen.

Esimerkki 3

Kuriiriyhtiö haluaa arvioida toimitustensa tehokkuutta toimitusaikojen, työmäärän suunnittelun ja polttoaineenkulutuksen kannalta. Tämän tavoitteen saavuttamiseksi kuriiriyhtiön on käsiteltävä monenlaisia henkilötietoja, jotka liittyvät sekä työntekijöihin (kuljettajiin) että asiakkaisiin (osoitteet,

toimitettavat tuotteet jne.). Tähän käsittelytoimeen sisältyy riskejä, jotka liittyvät sekä työntekijöiden valvontaan, joka edellyttää tiettyjä oikeudellisia takeita, että asiakkaiden tapojen seurantaan, kun kuriiriyhtiö saa tietoa esimerkiksi tietyn ajan kuluessa toimitetuista tuotteista. Näitä riskejä voidaan pienentää tuntuvasti sillä, että työntekijät ja asiakkaat pseudonymisoidaan asianmukaisesti. Etenkin se, että pseudonymisointiavaimia kierrätetään säännöllisesti ja että käytetään laajempia alueita tarkkojen osoitteiden sijasta, edistää tietojen minimointia, ja rekisterinpitäjä voi keskittyä yksinomaan toimitusprosessiin ja resurssien optimointiin liittyvään tarkoitukseen ilman, että henkilöiden (asiakkaiden tai työntekijöiden) käyttäytymisen valvontaa merkitsevä raja ylittyisi.

Esimerkki 4

Sairaala kerää potilaistaan tietoa sairaalan tietojärjestelmään (sähköinen potilaskertomus) Sairaalan henkilöstön on voitava käyttää potilastiedostoja, jotta he voivat tehdä päätöksiä potilaiden hoidosta ja lääkityksestä sekä kaikkien diagnosointia, hoitoa ja lääkitystä koskevien toimien kirjaamiseksi. Käyttöoikeus annetaan oletusarvoisesti vain niille terveydenhoidon työntekijöille, jotka on osoitettu kyseessä olevan potilaan hoitoon siinä erityisosastossa, jossa potilas on. Niiden ihmisten ryhmää, joilla on pääsy potilaan tiedostoihin, laajennetaan, jos hoitoon osallistuu muita osastoja tai diagnostiikkayksikköjä. Kun potilas on kotiutettu ja laskutus on valmis, käyttöoikeutta vähennetään erityisosastojen pieneen työntekijäryhmään, joka vastaa lääketieteellistä tietoa tai konsultaatiota koskeviin pyyntöihin, joita muiden lääketieteellisten palvelujen tarjoajat esittävät kyseessä olevan potilaan luvalla.

3.6 Täsmällisyys

77. Henkilötietojen on oltava täsmällisiä ja päivitettyjä. Lisäksi on toteutettava kaikki mahdolliset kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä.[38]

78. Näitä vaatimuksia on tarkasteltava suhteessa tietojen konkreettiseen käyttöön liittyviin riskeihin ja seurauksiin. Epätäsmälliset henkilötiedot voivat aiheuttaa rekisteröidyn oikeuksiin ja vapauksiin kohdistuvan riskin, esimerkiksi jos niiden perusteella tehdään terveysprotokollassa virheellinen diagnoosi tai määritetään vääränlainen hoito. Virheellinen kuva henkilöstä voi johtaa myös siihen, että päätöksiä tehdään väärin perustein joko manuaalisesti, automaattisessa päätöksenteossa tai tekoälyn välityksellä.

79. Sisäänrakennetun ja oletusarvoisen tietosuojan täsmällisyyttä koskevia keskeisiä tekijöitä ovat seuraavat:
    - Tiedonlähde – henkilötietojen lähteiden on oltava tietojen täsmällisyyden kannalta luotettavia.
    - Täsmällisyyden aste – kunkin henkilötietoelementin on oltava niin täsmällinen kuin on tarpeen määritettyjen tarkoitusten kannalta.
    - Mitattavissa oleva täsmällisyys – vähennetään väärien positiivisten/negatiivisten tulosten määrää, esimerkiksi vinoutumia automaattisessa päätöksenteossa ja tekoälyssä.

[38] Yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan d alakohta.

- Varmentaminen – tietojen luonteen mukaan ja sen mukaan, miten usein ne voivat muuttua, rekisterinpitäjän on varmennettava henkilötietojen oikeellisuus rekisteröidyltä ennen käsittelyn aloittamista ja sen eri vaiheissa (esim. ikävaatimukset).
- Poistaminen/oikaiseminen – rekisterinpitäjän on poistettava tai oikaistava epätäsmälliset tiedot viipymättä. Rekisterinpitäjän on edistettävä tätä erityisesti, jos rekisteröidyt ovat lapsia tai olivat lapsia ja haluavat myöhemmin poistaa kyseiset henkilötiedot.[39]
- Virheiden leviämisen välttäminen – rekisterinpitäjien on vähennettävä kumuloituvan virheen vaikutusta käsittelyketjussa.
- Pääsy tietoihin – rekisteröidyille on annettava tietoa henkilötiedoista ja helppo pääsy niihin, jotta he voivat tarkistaa tietojen täsmällisyyden ja oikaista niitä tarvittaessa yleisen tietosuoja-asetuksen 12–15 artiklan mukaisesti.
- Jatkuva täsmällisyys – henkilötietojen on oltava täsmällisiä kaikissa käsittelyn vaiheissa, ja kriittisissä vaiheissa on tehtävä täsmällisyyteen liittyviä testejä.
- Ajantasaisuus – henkilötiedot on päivitettävä, jos se on tarpeen käsittelyn tarkoituksen kannalta.
- Tietojen suunnittelu – käytetään teknisiä ja organisatorisia suunnittelutoimintoja vähentämään epätäsmällisyyttä, esimerkiksi esittämällä ytimekkäitä etukäteen määritettyjä vaihtoehtoja vapaan tekstin kenttien sijasta.

Esimerkki 1

Vakuutusyhtiö haluaa käyttää tekoälyä vakuutuksia ostavien asiakkaiden profiloimiseksi. Tekoälyä käytettäisiin perustana päätöksenteolle vakuutusriskiä laskettaessa. Määrittäessään, miten tällaisia tekoälyratkaisuja olisi kehitettävä, vakuutusyhtiö määrittää myös käsittelytavat, ja sen on otettava huomioon sisäänrakennettu tietosuoja, kun se valitsee tekoälysovelluksen toimittajaa ja päättää, miten tekoälyä opetetaan.

Kun rekisterinpitäjä määrittää, miten tekoälyä opetetaan, sillä on oltava täsmällistä tietoa, jotta saataisiin tarkat tulokset. Niinpä rekisterinpitäjän on varmistettava, että tekoälyn opettamisessa käytettävät tiedot ovat täsmällisiä.

Olettaen, että rekisterinpitäjällä on pätevä laillinen peruste opettaa tekoälyä käyttämällä henkilötietoja suuresta joukosta nykyisiä asiakkaitaan, rekisterinpitäjä valitsee koko asiakaspopulaation kannalta edustavan joukon asiakkaita, jotta vältettäisiin myös vinoutumat.

Sitten asiaankuuluvasta tietojenkäsittelyjärjestelmästä kerätään asiakastiedot, myös tiedot vakuutuslajista, esimerkiksi siitä, onko kyseessä sairausvakuutus, kotivakuutus, matkavakuutus jne., sekä tiedot julkisista rekistereistä, joihin rekisterinpitäjällä on laillinen käyttöoikeus. Kaikki tiedot pseudonymisoidaan ennen kuin ne siirretään tekoälymallin opettamista koskevaan järjestelmään.

Sen varmistamiseksi, että tekoälyn opettamiseen käytettävät tiedot ovat mahdollisimman täsmällisiä, rekisterinpitäjä kerää tietoa vain sellaisista tietolähteistä, joissa olevat tiedot ovat oikeita ja ajantasaisia.

Vakuutusyhtiö testaa tekoälyn luotettavuutta ja sitä, antaako se syrjimättömiä tuloksia sekä sen kehittämisen aikana että lopuksi ennen tuotteen julkistamista. Kun tekoäly on kokonaan opetettu ja toiminnassa, vakuutusyhtiö käyttää tuloksia vakuutusriskin arviointien tukena. Se ei kuitenkaan turvaudu pelkästään tekoälyyn tehdessään myönteisen vakuutuspäätöksen, ellei päätöstä tehdä yleisen tietosuoja-asetuksen 22 artiklan 2 kohdan poikkeusten mukaisesti.

[39] Ks. johdanto-osan 65 kappale.

Vakuutusyhtiö myös arvioi säännöllisesti tekoälystä saatavat tulokset, jotta luotettavuutta voidaan pitää yllä ja tarvittaessa mukauttaa algoritmia.

Esimerkki 2

Rekisterinpitäjä on terveydenhuollon laitos, joka etsii menetelmiä, joilla varmistetaan sen asiakasrekistereissä olevien henkilötietojen eheys ja täsmällisyys.

Tilanteissa, joissa kaksi henkilöä saapuu laitokseen samaan aikaan ja saa saman hoidon, on olemassa riski, että heidät sekoitetaan, jos ainoa heitä erottava parametri on nimi. Täsmällisyyden varmistamiseksi rekisterinpitäjä tarvitsee yksilöllisen tunnisteen jokaiselle henkilölle, ja siksi se tarvitsee muutakin tietoa kuin vain asiakkaan nimen.

Laitos käyttää useita järjestelmiä, jotka sisältävät asiakkaiden henkilötietoja, ja sen on varmistettava, että kuhunkin asiakkaaseen liittyvät tiedot ovat oikeita, täsmällisiä ja yhdenmukaisia kaikissa järjestelmissä missä tahansa aikapisteessä. Laitos on määrittänyt useita riskejä, joita voi aiheutua, jos jokin tieto muutetaan vain yhdessä järjestelmässä muttei kaikissa.

Rekisterinpitäjä päättää lieventää tätä riskiä tiivistetekniikalla, jota voidaan käyttää sairauskertomuksen tietojen eheyden varmistamisessa. Niinpä sairauskertomustietueisiin ja niihin liittyville asiakkaille kehitetään pysyviä salattuja aikaleimoja, jotta kaikki muutokset voidaan tunnistaa, liittää toisiinsa ja jäljittää, jos se on tarpeen.

3.7 Säilytyksen rajoittaminen

80. Rekisterinpitäjän on varmistettava, että henkilötietoja säilytetään sellaisessa muodossa, jonka avulla rekisteröityjen tunnistaminen on mahdollista vain sen aikaa kuin on tarpeen niiden tarkoitusten kannalta, joita varten henkilötietoja käsitellään.[40]
On hyvin tärkeää, että rekisterinpitäjä tietää tarkasti, mitä henkilötietoja yritys käsittelee ja miksi. Käsittelyn tarkoitus on ratkaiseva kriteeri, kun määritetään, kauanko henkilötietoja on säilytettävä.

81. Toimenpiteillä ja suojatoimilla, joilla säilytyksen rajoittamisen periaate pannaan täytäntöön, on täydennettävä rekisteröityjen oikeuksia ja vapauksia, etenkin oikeutta poistaa tietoja sekä oikeutta vastustaa tietojen käsittelyä.

82. Sisäänrakennetun ja oletusarvoisen tietosuojan säilytyksen rajoittamista koskevia keskeisiä tekijöitä ovat seuraavat:
    - Poistaminen ja anonymisointi – rekisterinpitäjällä on oltava selkeät sisäiset menettelyt ja toiminnot henkilötietojen poistamista ja/tai anonymisointia varten.
    - Anonymisoinnin/poistamisen tehokkuus – rekisterinpitäjän on varmistettava, ettei anonymisoitujen tietojen perusteella voida tunnistaa henkilöitä uudelleen tai ettei poistettuja tietoja voida palauttaa. Rekisterinpitäjän on testattava, onko tämä mahdollista.
    - Automatisointi – tiettyjen henkilötietojen poistaminen on automatisoitava.
    - Säilytyskriteerit – rekisterinpitäjän on määritettävä, mitkä tiedot ovat tarpeen tarkoituksen kannalta ja kauanko niitä on säilytettävä.

[40] Yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan c alakohta.

- Perustelut – rekisterinpitäjän on pystyttävä perustelemaan, miksi säilytysaika on tarpeen tarkoitusta ja kyseessä olevia henkilötietoja varten, sekä pystyttävä esittämään säilytysajan syyt ja lailliset perusteet.
- Säilytyskäytäntöjen valvonta – rekisterinpitäjän on valvottava sisäisiä säilytyskäytäntöjä ja tehtävä testejä, joilla varmistetaan, noudattaako organisaatio näitä käytäntöjä.
- Varmuuskopiot/lokit – rekisterinpitäjien on määritettävä, mitkä henkilötiedot ovat tarpeen varmuuskopioita ja lokeja varten ja kauanko niitä on säilytettävä.
- Tiedon kulku – rekisterinpitäjän on valvottava henkilötietojen kulkua ja niiden jäljennösten säilyttämistä sekä pyrittävä rajoittamaan niiden ”väliaikaista” säilyttämistä.

Esimerkki

Rekisterinpitäjä kerää henkilötietoja, kun käsittelyn tarkoituksena on hallinnoida rekisteröidyn jäsenyyttä. Henkilötiedot on poistettava, kun jäsenyys päättyy eikä tietojen säilyttämiselle pidempään ole laillista perustetta.

Rekisterinpitäjä laati ensin sisäisen menettelyn tietojen säilyttämistä ja poistamista varten. Menettelyn mukaan työntekijöiden on poistettava henkilötiedot manuaalisesti, kun säilytysaika päättyy. Työntekijä noudattaa menettelyä ja poistaa ja oikaisee tietoja säännöllisesti kaikista laitteista, varmuuskopioista, lokeista ja sähköpostiviesteistä sekä muista oleellisista tallennusvälineistä.

Jotta poistamista voidaan tehostaa ja vähentää sen virhealttiutta, rekisterinpitäjä ottaa käyttöön automaattisen järjestelmän, joka poistaa tietoja automaattisesti, luotettavasti ja aiempaa säännöllisemmin. Järjestelmä on konfiguroitu siten, että se poistaa henkilötietoja tietyn menettelyn mukaan säännöllisin ja ennalta määritetyin väliajoin kaikista yrityksen tallennusvälineistä. Rekisterinpitäjä tarkastaa ja testaa säilyttämismenettelyn säännöllisesti ja varmistaa, että se on ajantasaisten säilytyskäytäntöjen mukainen.

3.8 Eheys ja luottamuksellisuus

83. Eheyden ja luottamuksellisuuden periaate tarkoittaa tietojen suojaamista luvattomalta ja laittomalta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta asianmukaisia teknisiä tai organisatorisia toimenpiteitä hyödyntäen. Henkilötietojen turvallisuus edellyttää asianmukaisia toimenpiteitä, joiden tarkoituksena on estää ja hallita tietoturvaloukkauksia, taata tietojenkäsittelytehtävien asianmukainen toteuttaminen ja muiden periaatteiden noudattaminen sekä helpottaa henkilöiden oikeuksien tehokasta käyttämistä.

84. Johdanto-osan 78 kappaleessa todetaan, että sisäänrakennettua ja oletusarvoista tietosuojaa koskeviin toimenpiteisiin voi kuulua esimerkiksi se, että rekisterinpitäjä voi ”luoda ja parantaa turvaominaisuuksia”. Muiden sisäänrakennettua ja oletusarvoista tietosuojaa koskevien toimenpiteiden ohella johdanto-osan 78 kappaleessa ehdotetaan, että rekisterinpitäjille asetetaan velvollisuus arvioida jatkuvasti, käyttääkö se asianmukaisia käsittelytapoja aina ja voidaanko valituilla toimenpiteillä tosiasiallisesti torjua olemassa olevia haavoittuvuuksia. Lisäksi rekisterinpitäjien on tarkastettava henkilötietoihin liittyvät ja niitä suojaavat tietoturvatoimenpiteet sekä tietoturvaloukkausten käsittelymenettely säännöllisesti.

85. Sisäänrakennetun ja oletusarvoisen tietosuojan eheyttä ja luottamuksellisuutta koskevia keskeisiä tekijöitä ovat seuraavat:
    - Tietoturvallisuuden hallintajärjestelmä (ISMS) – käytössä on oltava operatiiviset keinot hallita tietoturvaan liittyviä käytäntöjä ja menettelyjä.

- Riskianalyysi – arvioidaan henkilötietojen turvallisuuteen kohdistuvia riskejä ottamalla huomioon vaikutus henkilöiden oikeuksiin ja torjutaan havaittuja riskejä. Riskinarvioinnissa käytettäväksi laaditaan kokonaisvaltainen, järjestelmällinen ja realistinen uhkamalli ja suunnitellun ohjelmiston hyökkäyspinta-alan analyysi ja pidetään niitä yllä, jotta voidaan pienentää hyökkäysvektoreita ja mahdollisuuksia heikkojen kohtien ja haavoittuvuuksien hyödyntämiseen.
- Sisäänrakennettu turvallisuus – otetaan turvallisuusvaatimukset huomioon mahdollisimman varhain järjestelmän suunnittelemisessa ja kehittämisessä sekä integroidaan ja tehdään asiaankuuluvia testejä jatkuvasti.
- Ylläpito – arvioidaan ja testataan ohjelmistoja, laitteistoja, järjestelmiä, palveluja jne. säännöllisesti, jotta voidaan havaita käsittelyjä tukevien järjestelmien haavoittuvuudet.
- Käyttöoikeuksien hallinta – vain luvan saanut henkilöstö, joka tarvitsee henkilötietoja käsittelytehtäviään varten, ja rekisterinpitäjä on erotettava luvan saaneen henkilöstön käyttöoikeuksissa.
    - Käytön rajoittaminen (asiamiehet) – muokataan tietojenkäsittelyä siten, että mahdollisimman pieni määrä ihmisiä tarvitsee henkilötietoja tehtäviensä täyttämiseksi, ja rajoitetaan käyttöä sen mukaan.
    - Käytön rajoittaminen (sisältö) – kunkin käsittelytoimen yhteydessä rajoitetaan käyttöä vain niihin tietokokonaisuuden määreisiin, joita tarvitaan kyseisen toimen tekemiseen. Lisäksi rajoitetaan käyttö niiden rekisteröityjen tietoihin, jotka ovat kyseessä olevan työntekijän vastuualueella.
    - Käytön eriyttäminen – muokataan tietojenkäsittelyä siten, että yksikään henkilö ei tarvitse kokonaisvaltaista pääsyä kaikkeen rekisteröidystä kerättyyn tietoon ja vielä vähemmän tietystä rekisteröityjen ryhmästä kerättyihin kaikkiin henkilötietoihin.
- Turvalliset siirrot – tiedonsiirto on suojattava luvattomalta ja tahattomalta käytöltä ja luvattomilta ja tahattomilta muutoksilta.
- Turvallinen säilytys – tietojen säilytys on suojattava luvattomalta käytöltä ja luvattomilta muutoksilta. Keskitetyn tai hajautetun säilyttämisen riskin arvioimiseen on oltava menettelyjä sen mukaan, mitä henkilötietoryhmiä se koskee. Jotkin tiedot voivat tarvita lisäturvatoimia tai ne on eristettävä muista.
- Pseudonymisointi – henkilötiedot ja varmuuskopiot/lokit on pseudonymisoitava varotoimena, jotta minimoidaan mahdollisten tietoturvaloukkausten riskit käyttämällä esimerkiksi tiivistämistä tai salausta.
- Varmuuskopiot/lokit – huolehditaan varmuuskopioinnista ja lokeista siinä määrin kuin on tarpeen tietoturvan kannalta, käytetään jäljitysketjuja ja tapahtumaseurantaa tavanomaisena turvallisuusvalvonnan toimenpiteenä. Ne on suojattava luvattomalta ja tahattomalta käytöltä ja luvattomilta ja tahattomilta muutoksilta ja arvioitava säännöllisesti. Häiriöt on käsiteltävä ripeästi.
- Palautumissuunnitelma / liiketoiminnan jatkuvuus – käsitellään tietojärjestelmän palautussuunnitelmaa ja liiketoiminnan jatkuvuutta koskevia vaatimuksia, jotta henkilötietojen käytettävyys voidaan palauttaa suurten häiriöiden jälkeen.
- Riskien mukainen suoja – Kaikkia henkilötietoryhmiä on suojattava toimenpiteillä, jotka ovat asianmukaisia tietoturvaloukkauksen riskiin nähden. Erityisiä riskejä aiheuttavat tiedot on mahdollisuuksien mukaan pidettävä erillään muista henkilötiedoista.
- Turvallisuuden vaarantumistapauksiin reagoimisen hallinta – käytössä on oltava rutiineja, menettelyjä ja resursseja, joilla havaitaan, rajoitetaan ja käsitellään tietoturvaloukkauksia sekä ilmoitetaan ja opitaan niistä.

- Tietoturvahäiriöiden hallinta – rekisterinpitäjällä on oltava käytössä prosessit tietoturvaloukkausten ja -häiriöiden hallitsemiseksi, jotta käsittelyjärjestelmää voidaan vankistaa. Tähän kuuluvat ilmoitusmenettelyt, kuten (valvontaviranomaiselle tehtävien) ilmoitusten hallinta ja (rekisteröidyille annettavien) tietojen hallinta.

Esimerkki

Rekisterinpitäjä haluaa hakea suuria määriä henkilötietoja lääketieteellisestä tietokannasta, jossa on sähköisiä potilaskertomuksia, yrityksen erityiselle tietokantapalvelimelle, jotta haettuja tietoja voidaan käsitellä laadunvarmistusta varten. Yritys on arvioinut, että riski, joka liittyy tiedonsiirtoon palvelimelle, joka on kaikkien yrityksen työntekijöiden käytettävissä, on rekisteröityjen oikeuksien ja vapauksien kannalta todennäköisesti suuri. Koska yrityksessä on vain yksi osasto, jonka on käsiteltävä potilastieto-otteita, rekisterinpitäjä päättää rajoittaa erityispalvelimelle pääsyn tuon osaston työntekijöille. Riskin vähentämiseksi entisestään tiedot myös pseudonymisoidaan ennen niiden siirtämistä.

Säännelläkseen käyttöoikeuksia ja lieventääkseen mahdollisia haittaohjelmista johtuvia vaurioita yritys päättää eristää verkon ja ryhtyy valvomaan palvelimen käyttöoikeuksia. Lisäksi yritys ottaa käyttöön turvallisuuden valvontajärjestelmän sekä tunkeutumisen havaitsemis- ja ehkäisyjärjestelmän ja eristää sen rutiinikäytöstä. Käyttöön otetaan myös automaattinen jäljitysjärjestelmä, joka tarkkailee käyttöoikeuksia ja näiden muutoksia. Tämä järjestelmä antaa raportteja ja automaattisia hälytyksiä, jos se havaitsee tiettyjä käyttöön liittyviä tapahtumia. Rekisterinpitäjä varmistaa, että käyttäjien käyttöoikeudet perustuvat siihen, mitä heidän täytyy tietää, asianmukaisella käyttöoikeustasolla. Epäasianmukainen käyttö voidaan havaita nopeasti ja helposti.

Joitakin siirretyistä tiedoista on verrattava uusiin tietoihin, minkä vuoksi niitä on säilytettävä kolme kuukautta. Rekisterinpitäjä päättää panna ne erillisiin tietokantoihin samalla palvelimella ja käyttää sekä avointa että saraketason suojausta niiden säilyttämisessä. Sarakkeiden tietojen suojauskoodit tallennetaan erityisiin turvamoduuleihin, joita voi käyttää vain luvan saanut henkilöstö, mutta niitä ei voida siirtää.

Tulevien häiriöiden käsittely lisää järjestelmän vakautta ja luotettavuutta. Rekisterinpitäjä ymmärtää, että ehkäisevät ja tehokkaat toimenpiteet ja suojatoimet on sisällytettävä kaikkeen nyt ja tulevaisuudessa tehtävään henkilötietojen käsittelyyn ja että näin toimiminen voi auttaa estämään tulevia tietoturvaloukkauksia.

Rekisterinpitäjä ottaa nämä turvallisuustoimenpiteet käyttöön varmistaakseen tietojen täsmällisyyden, eheyden ja luottamuksellisuuden mutta myös ehkäistäkseen kyberhyökkäyksistä johtuvien haittaohjelmien leviämisen. Näin tietojärjestelmästä tulee entistäkin vankempi. Vankat turvatoimet lisäävät rekisteröityjen luottamusta.

3.9 Osoitusvelvollisuus[41]

86. Osoitusvelvollisuuden periaatteen mukaan rekisterinpitäjä on vastuussa kaikkien edellä mainittujen periaatteiden noudattamisesta, ja sen on myös voitava osoittaa se.

87. Rekisterinpitäjän on pystyttävä osoittamaan periaatteiden noudattaminen. Sitä varten rekisterinpitäjä voi osoittaa rekisteröityjen oikeuksien suojelemiseksi toteutettujen toimenpiteiden vaikutukset ja sen, miksi toimenpiteiden katsotaan olevan asianmukaisia ja tehokkaita. Se voi esimerkiksi osoittaa, miksi toimenpide on asianmukainen säilytyksen rajoittamisen periaatteen tehokkaan noudattamisen varmistamisessa.

[41] Ks. johdanto-osan 74 kappale, jonka mukaan rekisterinpitäjien on osoitettava toimenpiteidensä tehokkuus.

88. Jotta henkilötietoja voidaan käsitellä vastuullisesti, rekisterinpitäjällä on oltava sekä tietoa tietosuojasta että kyky panna se täytäntöön. Rekisterinpitäjän on siis ymmärrettävä yleisen tietosuoja-asetuksen mukaiset tietosuojavelvollisuutensa ja pystyttävä noudattamaan kyseisiä velvollisuuksia.

4 SERTIFIOINTIA KOSKEVA 25 ARTIKLAN 3 KOHTA

89. Yleisen tietosuoja-asetuksen 25 artiklan 3 kohdan mukaan 42 artiklan mukaista sertifiointia voidaan käyttää yhtenä tekijänä sen osoittamiseksi, että sisäänrakennettua ja oletusarvoista tietosuojaa noudatetaan. Sisäänrakennetun ja oletusarvoisen tietosuojan noudattamisen osoittavat asiakirjat voivat puolestaan olla hyödyllisiä sertifiointiprosessissa. Tämä tarkoittaa sitä, että jos rekisterinpitäjän tai henkilötietojen käsittelijän käsittelytoimi on sertifioitu 42 artiklan mukaisesti, valvontaviranomaiset ottavat sen huomioon tehdessään arviointia siitä, miten yritys noudattaa yleisen tietosuoja-asetuksen vaatimuksia varsinkin sisäänrakennetun ja oletusarvoisen tietosuojan osalta.

90. Kun rekisterinpitäjän tai henkilötietojen käsittelijän käsittelytoimi sertifioidaan 42 artiklan mukaisesti, tekijöitä, jotka auttavat osoittamaan 25 artiklan 1 ja 2 kohdan noudattamisen, ovat suunnitteluprosessit eli käsittelykeinojen määrittämisprosessi, hallinto ja tekniset ja organisatoriset toimenpiteet, joilla tietosuojaperiaatteet pannaan täytäntöön. Sertifiointielimet tai sertifiointijärjestelmän omistajat määrittävät tietosuojan sertifiointikriteerit ja toimivaltainen valvontaviranomainen tai Euroopan tietosuojaneuvosto hyväksyy ne. Sertifiointimekanismeista on lisätietoa Euroopan tietosuojaneuvoston sertifiointiohjeissa[42] sekä muissa asiaankuuluvissa ohjeissa, jotka on julkaistu Euroopan tietosuojaneuvoston verkkosivustolla.

91. Vaikka käsittelytoimelle myönnetään sertifiointi 42 artiklan mukaisesti, rekisterinpitäjä on edelleen vastuu siitä, että 25 artiklan sisäänrakennettua ja oletusarvoista tietosuojaa koskevien kriteerien noudattamista seurataan ja parannetaan jatkuvasti.

5 25 ARTIKLAN TÄYTÄNTÖÖNPANON VALVONTA JA SEN SEURAUKSET

92. Valvontaviranomaiset voivat arvioida 25 artiklan vaatimusten noudattamista 58 artiklassa lueteltujen menettelyjen mukaisesti. Korjaavat valtuudet on lueteltu 58 artiklan 2 kohdassa. Niitä ovat esimerkiksi varoitusten antaminen, huomautusten antaminen, määräykset noudattaa rekisteröityjen oikeuksia, määräykset rajoittaa tai kieltää tietojen käsittely, hallinnollisten sakkojen määrääminen jne.

93. Sisäänrakennettu ja oletusarvoinen tietosuoja on lisätekijä, kun määritetään yleisen tietosuoja-asetuksen säännösten noudattamatta jättämisestä johtuvan sakon määrää (ks. 83 artiklan 4 kohta).[43] [44]

[42] Euroopan tietosuojaneuvosto. ”Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation”. Versio 3.0, 4. kesäkuuta 2019. edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf

[43] Yleisen tietosuoja-asetuksen 83 artiklan 2 kohdan d alakohdassa säädetään, että määrättäessä asetuksen noudattamatta jättämisestä johtuvaa sakkoa ”on otettava asianmukaisesti huomioon [– –] rekisterinpitäjän tai henkilötietojen käsittelijän vastuun aste, ottaen huomioon heidän 25 ja 32 artiklan nojalla toteuttamansa tekniset ja organisatoriset toimenpiteet”.

[44] Lisätietoja sakoista on 29 artiklan mukaisen tietosuojatyöryhmän julkaisussa ”Guidelines on application and setting of administrative fines for the purposes of the Regulation 2016/679”. WP 253, 3. lokakuuta 2017. ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 – Euroopan tietosuojaneuvoston hyväksymä.

6 SUOSITUKSET

94. Vaikka henkilötietojen käsittelijöitä ja tuottajia ei suoraan käsitellä 25 artiklassa, ne tunnustetaan myös sisäänrakennetun ja oletusarvoisen tietosuojan keskeisiksi edistäjiksi. Näiden tulisikin olla myös tietoisia siitä, että rekisterinpitäjien edellytetään käsittelevän henkilötietoja vain järjestelmissä ja tekniikoissa, joissa on sisäänrakennettu suoja.

95. Käsitellessään tietoja rekisterinpitäjien toimeksiannosta tai tarjotessaan niille ratkaisuja henkilötietojen käsittelijöiden ja tuottajien on käytettävä asiantuntemustaan, jotta ne voivat saada asiakkaidensa luottamuksen ja ohjata asiakkaita, myös pk-yrityksiä, suunnittelemaan/hankkimaan sellaisia ratkaisuja, joissa tietosuoja sisällytetään mukaan tietojenkäsittelyyn. Tämä puolestaan tarkoittaa, että tuotteiden ja palvelujen suunnittelulla on vastattava rekisterinpitäjien tarpeisiin.

96. Yleisen tietosuoja-asetuksen 25 artiklaa täytäntöön pantaessa on muistettava, että suunnittelun päätavoite on periaatteiden ja rekisteröityjen oikeuksien *suojelun* sisällyttäminen tehokkaasti tietojenkäsittelyn asianmukaisiin toimenpiteisiin. Sisäänrakennetun ja oletusarvoisen tietosuojan omaksumisen helpottamiseksi ja edistämiseksi rekisterinpitäjille sekä tuottajille ja henkilötietojen käsittelijöille annetaan seuraavat suositukset:
    - Rekisterinpitäjien on huomioitava tietosuoja jo käsittelytoimien suunnittelun alkuvaiheissa, jo ennen käsittelytapojen määrittämistä.
    - Jos rekisterinpitäjällä on tietosuojavastaava, Euroopan tietosuojaneuvosto kannustaa tietosuojavastaavaa osallistumaan aktiivisesti sisäänrakennetun ja oletusarvoisen tietosuojan yhdistämiseen hankinta- ja kehittämismenettelyihin sekä koko käsittelyn elinkaareen.
    - Käsittelytoimia voidaan *sertifioida*. Käsittelytoimen sertifiointi tuo rekisterinpitäjälle lisäarvoa tämän valitessa tuottajilta tai henkilötietojen käsittelijöiltä ohjelmistoja, laitteistoja, palveluja ja/tai järjestelmiä käsittelyä varten. Tuottajien on siksi pyrittävä osoittamaan sisäänrakennettu ja oletusarvoinen tietosuoja käsittelyratkaisunsa kehittämisen elinkaaressa. Sertifiointisinetti voi myös ohjata rekisteröityjä näiden tehdessä valintoja eri tavaroiden ja palvelujen välillä. Käsittelyn sertifioinnin saaminen voi toimia kilpailuetuna tuottajille, henkilötietojen käsittelijöille ja rekisterinpitäjille, ja se voi jopa lisätä rekisteröityjen luottamusta heidän henkilötietojaan käsittelevään tahoon. Jos sertifiointia ei saada, rekisterinpitäjien kannattaa hankkia muita *takeita* siitä, että tuottajat tai henkilötietojen käsittelijät noudattavat sisäänrakennettua ja oletusarvoista tietosuojaa koskevia vaatimuksia.
    - Rekisterinpitäjien, henkilötietojen käsittelijöiden ja tuottajien on otettava huomioon velvollisuutensa taata alle 18-vuotiaille lapsille ja muille heikossa asemassa oleville ryhmille erityissuoja sisäänrakennetun ja oletusarvoisen tietosuojan noudattamisessa.
    - Tuottajien ja henkilötietojen käsittelijöiden on pyrittävä helpottamaan sisäänrakennetun ja oletusarvoisen tietosuojan täytäntöönpanoa, jotta rekisterinpitäjää voidaan auttaa noudattamaan 25 artiklan velvollisuuksia. Toisaalta rekisterinpitäjien ei tule valita sellaisia tuottajia tai henkilötietojen käsittelijöitä, jotka eivät voi tarjota järjestelmiä, joiden avulla rekisterinpitäjä voi täyttää 25 artiklan vaatimukset tai joilla sitä voidaan tukea, koska tällöin katsotaan, että rekisterinpitäjä on vastuussa artiklan noudattamatta jättämisestä.
    - Tuottajien ja henkilötietojen käsittelijöiden olisi syytä toimia aktiivisesti sen varmistamisessa, että ”viimeisintä tekniikkaa” koskevat kriteerit täyttyvät. Heidän pitäisi myös ilmoittaa rekisterinpitäjille sellaisista mahdollisista ”viimeisimmässä tekniikassa” tapahtuneista muutoksista, jotka voivat vaikuttaa käytössä olevien toimenpiteiden tehokkuuteen.

Rekisterinpitäjien on hyvä sisällyttää tämä vaatimus sopimusehtoihin sen varmistamiseksi, että ne pysyvät ajan tasalla.

- Euroopan tietosuojaneuvosto suosittelee, että rekisterinpitäjät vaativat tuottajia ja henkilötietojen käsittelijöitä osoittamaan, miten rekisterinpitäjä pystyy niiden laitteiston, ohjelmiston, palvelujen tai järjestelmien avulla noudattamaan osoitusvelvollisuuden vaatimuksia sisäänrakennetun ja oletusarvoisen tietosuojan mukaisesti. Tämä voidaan tehdä esimerkiksi käyttämällä keskeisiä tulosindikaattoreita osoittamaan toimenpiteiden ja suojatoimien tehokkuus periaatteiden ja oikeuksien täytäntöönpanossa.
- Euroopan tietosuojaneuvosto korostaa, että on tärkeää noudattaa yhdenmukaistettua lähestymistapaa, jotta periaatteet ja oikeudet voidaan toteuttaa tehokkaasti. Lisäksi se kehottaa yhdistyksiä ja muita elimiä laatimaan 40 artiklassa tarkoitetut käytännesäännöt siten, että myös niihin sisällytetään sisäänrakennettua ja oletusarvoista tietosuojaa koskevat alakohtaiset ohjeet.
- Rekisterinpitäjien on kohdeltava rekisteröityjä oikeudenmukaisesti ja oltava avoimia siinä, miten ne arvioivat ja osoittavat, että sisäänrakennettu ja oletusarvoinen tietosuoja on pantu täytäntöön tehokkaasti, samalla tavalla kuin ne osoittavat noudattavansa yleistä tietosuoja-asetusta vastuuvelvollisuuden periaatteen mukaisesti.
- Uusimman tekniikan tason saavuttaneita yksityisyyden suojaa parantavia tekniikoita voidaan hyödyntää soveltuvin osin toimenpiteenä sisäänrakennettua ja oletusarvoista tietosuojaa koskevien vaatimusten mukaisesti riskiin perustuvassa toimintamallissa. Yksityisyyden suojaa parantavat tekniikat eivät itse välttämättä täytä 25 artiklan velvollisuuksia. Rekisterinpitäjien on arvioitava, onko toimenpide asianmukainen ja tehokas tietosuojaperiaatteiden noudattamisessa ja rekisteröityjen oikeuksien toteuttamisessa.
- Käytössä oleviin aiempiin järjestelmiin sovelletaan samoja sisäänrakennettua ja oletusarvoista tietosuojaa koskevia velvollisuuksia kuin uusiin järjestelmiin. Jos aiemmat järjestelmät eivät jo noudata sisäänrakennettua ja oletusarvoista tietosuojaa eikä velvollisuuksien noudattamiseksi voida tehdä muutoksia, aiempi järjestelmä ei yksinkertaisesti täytä yleisen tietosuoja-asetuksen velvoitteita eikä sitä voida käyttää henkilötietojen käsittelemiseen.
- Asetuksen 25 artiklassa ei alenneta vaatimustasoa pk-yritysten osalta. Seuraavat kohdat voivat helpottaa 25 artiklan noudattamista pk-yrityksissä:
    - Tee riskinarvioinnit varhain.
    - Aloita pienestä käsittelystä – laajenna sen soveltamisalaa ja tarkkuutta myöhemmin.
    - Pyydä tuottajalta ja henkilötietojen käsittelijältä takeita sisäänrakennetusta ja oletusarvoisesta tietosuojasta, esimerkiksi sertifiointia ja käytännesääntöjen noudattamista.
    - Käytä kumppaneita, joilla on aiempia saavutuksia.
    - Keskustele tietosuojavastaavien kanssa.
    - Lue tietosuojavastaavien ja Euroopan tietosuojaneuvoston ohjeet.
    - Noudata käytännesääntöjä, kun ne ovat saatavilla.
    - Hae ammattiapua ja -neuvontaa.

Euroopan tietosuojaneuvosto

Puheenjohtaja

(Andrea Jelinek)