TIETOSUOJATYÖRYHMÄ

17/FI

WP 253

Asetuksessa 2016/679 tarkoitettujen hallinnollisten sakkojen soveltamista ja määräämistä koskevat suuntaviivat

Annettu 3. lokakuuta 2017

Tietosuojatyöryhmä on perustettu direktiivin 95/46/EY 29 artiklalla. Se on riippumaton EU:n neuvoa-antava elin, joka käsittelee tietosuojaan ja yksityisyyden suojaan liittyviä kysymyksiä. Sen tehtävät määritellään direktiivin 95/46/EY 30 artiklassa ja direktiivin 2002/58/EY 15 artiklassa.

Työryhmän sihteeristön tehtävistä huolehtii Euroopan komission oikeus- ja kuluttaja-asioiden pääosaston linja C (Perusoikeudet ja oikeusvaltioperiaate), toimisto MO-59 03/075, B-1049 Bryssel, Belgia.

Verkkosivusto: http://ec.europa.eu/justice/data-protection/index_en.htm

TIETOSUOJATYÖRYHMÄ, joka

on perustettu 24 päivänä lokakuuta 1995 annetulla Euroopan parlamentin ja neuvoston direktiivillä 95/46/EY,

ottaa huomioon mainitun direktiivin 29 ja 30 artiklan,

ottaa huomioon työjärjestyksensä,

ON ANTANUT SEURAAVAT SUUNTAVIIVAT:

Sisällysluettelo

I. Johdanto

EU on saanut valmiiksi laajan tietosuojasääntöjen uudistuksen Euroopassa. Uudistus perustuu useisiin pilareihin tai keskeisiin osatekijöihin, joita ovat johdonmukaiset säännöt, yksinkertaistetut menettelyt, koordinoidut toimet, käyttäjien osallistaminen, tiedottamisen tehostaminen ja valvontavaltuuksien lujittaminen.

Rekisterinpitäjillä ja henkilötietojen käsittelijöillä on yhä suurempi vastuu tehokkaan henkilötietosuojan varmistamisesta. Valvontaviranomaisilla on valtuudet varmistaa, että yleisen tietosuoja-asetuksen (jäljempänä ’asetus’) periaatteita ja yksilöiden oikeuksia noudatetaan asetuksen sanamuodon ja hengen mukaisesti.

Tietosuojasääntöjen yhdenmukaisella täytäntöönpanolla on olennainen merkitys yhdenmukaistetun tietosuojajärjestelmän kannalta. Hallinnolliset sakot ovat asetuksella käyttöön otetun uuden valvontajärjestelmän keskeinen osa ja valvontaviranomaisten tehokas täytäntöönpanoväline yhdessä muiden 58 artiklassa säädettyjen toimenpiteiden kanssa.

Tämä asiakirja on tarkoitettu valvontaviranomaisten käyttöön, ja sillä pyritään varmistamaan asetuksen tehokkaampi soveltaminen ja täytäntöönpano. Asiakirjassa esitetään valvontaviranomaisten yhteinen näkemys asetuksen 83 artiklan säännöksistä ja sen soveltamisesta yhdessä 58 ja 70 artiklan ja asiaa koskevien johdanto-osan kappaleiden kanssa.

Asetuksen 70 artiklan 1 kohdan e alakohdan mukaan Euroopan tietosuojaneuvostolle (jäljempänä ’tietosuojaneuvosto’) annetaan erityisesti valtuudet antaa suuntaviivoja, suosituksia ja parhaita käytänteitä, joilla tuetaan asetuksen johdonmukaista soveltamista, ja 70 artiklan 1 kohdan k alakohdassa se valtuutetaan laatimaan suuntaviivoja, jotka koskevat hallinnollisten sakkojen määräämistä.

Nämä suuntaviivat eivät ole tyhjentäviä, eikä niissä selvennetä hallinnollisten sakkojen määräämiseen liittyviä hallinto-, siviili- tai rikosoikeusjärjestelmien välisiä eroja.

Jotta hallinnollisten sakkojen määräämiseen voitaisiin soveltaa yhdenmukaista lähestymistapaa, joka ilmentäisi asianmukaisesti kaikkia näissä suuntaviivoissa esitettyjä periaatteita, tietosuojaneuvosto on sopinut asetuksen 83 artiklan 2 kohdassa esitettyjä arviointiperusteita koskevasta yhteisestä tulkinnasta. Tietosuojaneuvosto ja yksittäiset valvontaviranomaiset ovat sopineet käyttävänsä näitä suuntaviivoja yhteisen lähestymistavan perustana.

II. Periaatteet

Kun tapauksen tosiseikkojen arvioinnin perusteella on todettu, että asetusta on rikottu, toimivaltaisen valvontaviranomaisen on määritettävä kaikkein asianmukaisin korjaava toimenpide (tai korjaavat toimenpiteet) rikkomiseen puuttumiseksi. Asetuksen 58 artiklan 2 kohdan b–j alakohdan[1] säännöksistä käy ilmi, mitä välineitä valvontaviranomaiset voivat käyttää rekisterinpitäjän tai henkilötietojen käsittelijän rikkomisten korjaamiseksi. Käyttäessään näitä valtuuksia valvontaviranomaisten on noudatettava seuraavia periaatteita:

1. Asetuksen rikkomisen olisi johdettava ”samantasoisten seuraamusten” määräämiseen

Käsite ”samantasoinen” on keskeisessä asemassa määritettäessä valvontaviranomaisten velvoitteiden laajuutta. Sillä halutaan varmistaa, että valvontaviranomaiset toimivat yhdenmukaisesti käyttäessään 58 artiklan 2 kohdassa tarkoitettuja korjaavia toimivaltuuksiaan ja erityisesti määrätessään hallinnollisia sakkoja[2].

Jotta voitaisiin varmistaa yhdenmukainen ja korkeatasoinen luonnollisten henkilöiden suojelu ja poistaa henkilötietojen liikkuvuuden esteet unionissa, ***luonnollisten henkilöiden oikeuksien ja vapauksien suojelun tason*** *olisi oltava vastaava kaikissa jäsenvaltioissa* (johdanto-osan 10 kappale). Johdanto-osan 11 kappaleessa selvennetään, että henkilötietojen samantasoinen suojelu kaikkialla unionissa edellyttää muun muassa ”samantasoisia valtuuksia valvoa henkilötietojen suojaa koskevien sääntöjen noudattamista ja samantasoisia seuraamuksia sääntöjen rikkomisesta jäsenvaltioissa”. Lisäksi kun varmistetaan samantasoiset seuraamukset kaikissa jäsenvaltioissa sekä eri jäsenvaltioiden valvontaviranomaisten välinen tehokas yhteistyö, voidaan ”estää eroavuudet, jotka haittaavat henkilötietojen vapaata liikkuvuutta sisämarkkinoilla”, kuten todetaan asetuksen johdanto-osan 13 kappaleessa.

Asetuksessa korostetaan yhdenmukaisuutta voimakkaammin kuin direktiivissä 95/46/EY, sillä asetusta sovelletaan jäsenvaltioissa sellaisenaan. Valvontaviranomaiset toimivat ”täysin riippumattomasti” (52 artikla) kansallisiin viranomaisiin, rekisterinpitäjiin tai henkilötietojen käsittelijöihin nähden, mutta niiden odotetaan tekevän yhteistyötä, ”jotta varmistetaan tämän asetuksen johdonmukainen soveltaminen ja täytäntöönpano” (57 artiklan 1 kohdan g alakohta).

Asetuksessa edellytetään suurempaa yhdenmukaisuutta seuraamusten määräämisessä kuin direktiivissä 95/46/EY. Rajat ylittävissä tapauksissa yhdenmukaisuus on saavutettava ensisijaisesti yhteistyöhön perustuvalla järjestelmällä (yhden luukun järjestelmä) ja jossain määrin uudessa asetuksessa vahvistetun yhdenmukaisuusmekanismin avulla.

Asetuksen soveltamisalaan kuuluvissa kansallisissa tapauksissa valvontaviranomaiset soveltavat näitä suuntaviivoja 57 artiklan 1 kohdan g alakohdan ja 63 artiklan mukaisen yhteistyön hengessä, jotta varmistetaan asetuksen yhdenmukainen soveltaminen ja täytäntöönpano. Vaikka valvontaviranomaiset

[1] Asetuksen 58 artiklan 2 kohdassa säädetään, että varoituksia voidaan antaa, kun käsittelytoimet todennäköisesti ovat asetuksen säännösten vastaisia. Toisin sanoen säännöksen soveltamisalaan kuuluvassa tapauksessa asetusta ei ole vielä rikottu.

[2] Vaikka joidenkin EU:n jäsenvaltioiden lait eivät salli asetuksen mukaisten hallinnollisten sakkojen määräämistä, kyseisten jäsenvaltioiden sääntöjen soveltamisella on oltava vastaava vaikutus kuin valvontaviranomaisten määräämillä hallinnollisilla sakoilla (johdanto-osan 151 kappale). Toisin kuin nämä tietosuojaneuvoston suuntaviivat, asetus sitoo tuomioistuimia.

voivat valita riippumattomasti 58 artiklan 2 kohdassa esitetyt korjaavat toimenpiteet, on vältettävä sitä, että valvontaviranomaiset valitsevat erilaisia korjaavia toimenpiteitä samankaltaisissa tapauksissa.

Periaatetta sovelletaan myös, kun tällaisia korvaavia toimenpiteitä määrätään sakkoina.

---

2. Kuten kaikkien valvontaviranomaisten valitsemien korjaavien toimenpiteiden, myös hallinnollisten sakkojen olisi oltava "tehokkaita, oikeasuhteisia ja varoittavia"

Kuten kaikkien korjaavien toimenpiteiden yleisesti, myös hallinnollisten sakkojen olisi vastattava asianmukaisesti rikkomisen luonnetta, vakavuutta ja seurauksia, ja valvontaviranomaisten on arvioitava tapauksen kaikkia tosiseikkoja yhdenmukaisesti ja objektiivisesti perustellulla tavalla. Arvioitaessa, mikä on kussakin tapauksessa tehokasta, oikeasuhteista ja varoittavaa, on myös otettava huomioon valitun korjaavan toimenpiteen tavoite eli joko sääntöjenmukaisuuden palauttaminen tai sääntöjenvastaisesta toiminnasta rankaiseminen (tai molemmat).

Valvontaviranomaisten on yksilöitävä korjaava toimenpide, joka on "tehokas, oikeasuhteinen ja varoittava" (83 artiklan 1 kohta), sekä silloin, kun kyse on jäsenvaltion alueella suoritettavasta henkilötietojen käsittelystä (55 artikla), että silloin, kun kyse henkilötietojen rajat ylittävästä käsittelystä (siten kuin se on määritelty 4 artiklan 23 kohdassa).

Näissä suuntaviivoissa on otettu huomioon se, että kansallisessa lainsäädännössä voidaan asettaa lisävaatimuksia valvontaviranomaisten noudattamalle täytäntöönpanomenettelylle. Ne voivat koskea esimerkiksi osoitteen ilmoittamista, muotovaatimusta, määräaikaa tietojen esittämiselle, muutoksenhakua, täytäntöönpanoa tai maksamista.[3]

Tällaisten vaatimusten ei kuitenkaan pitäisi estää sitä, että seuraamus on tehokas, oikeasuhteinen ja varoittava.

Se, minkälainen on tehokas, oikeasuhteinen tai varoittava seuraamus, täsmentyy valvontaviranomaisten tulevan käytännön (tietosuoja-alan käytännön ja sääntelyaloilta saatujen kokemusten) sekä näiden periaatteiden tulkintaa koskevan oikeuskäytännön perusteella.

Tehokkaiden, oikeasuhteisten ja varoittavien sakkojen määräämiseksi valvontaviranomaisten on käytettävä Euroopan unionin tuomioistuimen vahvistamaa yrityksen käsitteen määritelmää, jota sovelletaan SEUT-sopimuksen 101 ja 102 artiklan yhteydessä, toisin sanoen yritys **on ymmärrettävä siten, että sillä tarkoitetaan** taloudellista yksikköä, jonka voivat muodostaa emoyhtiö ja kaikki toimintaan osallistuvat tytäryhtiöt. Unionin oikeuden ja oikeuskäytännön[4] mukaan yrityksen käsitteellä on katsottava tarkoitettavan taloudellista yksikköä, joka harjoittaa kaupallista/taloudellista toimintaa, oikeudellisista muodoista riippumatta (johdanto-osan 150 kappale).

---

[3] Esimerkiksi Irlannin perustuslaissa ja tietosuojaa koskevassa lainsäädäntöluonnoksessa säädetään, että itse rikkomista koskeva virallinen päätös, joka ilmoitetaan asianomaisille osapuolille, tehdään ennen seuraamusasteikon arviointia. Itse rikkomista koskevaa päätöstä ei voida arvioida uudelleen seuraamusasteikon arvioinnin yhteydessä.

[4] Euroopan unionin tuomioistuimen oikeuskäytännössä yritys on määritelty seuraavasti: "Yrityksen käsite kattaa kaikki taloudellista toimintaa harjoittavat yksiköt riippumatta niiden oikeudellisesta muodosta ja rahoitustavasta" (unionin tuomioistuimen tuomio 23.4.1991, Höfner ja Elsner, C-41/90, ECLI:EU:C:1991:161, 21 kohta). Käsitteellä yritys on "katsottava tarkoitettavan taloudellista kokonaisuutta [– –], vaikkakin oikeudellisesti tämän taloudellisen kokonaisuuden muodostaa useampi kuin yksi luonnollinen henkilö tai oikeushenkilö" (unionin tuomioistuimen tuomio 14.12.2006, Confederación Española de Empresarios de Estaciones de Servicio, C-217/05, ECLI:EU:C:2006:784, 40 kohta).

3. Toimivaltainen valvontaviranomainen tekee arvion ”kussakin yksittäisessä tapauksessa”

Hallinnollisia sakkoja voidaan määrätä monista erilaisista rikkomisista. Asetuksen 83 artiklassa säädetään sen 4–6 kohdassa nimenomaisesti esitettyjen velvoitteiden rikkomista koskevasta yhdenmukaistetusta lähestymistavasta. Jäsenvaltion lainsäädännössä voidaan laajentaa 83 artiklan soveltamisalaa kattamaan kyseisen jäsenvaltion viranomaiset ja julkishallinnon elimet. Lisäksi jäsenvaltion lainsäädännössä voidaan sallia sakon määrääminen tai jopa velvoittaa siihen myös muista kuin 83 artiklan 4–6 kohdassa esitettyjen säännösten rikkomisesta.

Asetuksessa edellytetään, että jokainen yksittäinen tapaus arvioidaan erikseen.[5] Asetuksen 83 artiklan 2 kohta on tällaisen yksittäisen arvioinnin lähtökohta. Siinä todetaan, että ”kun päätetään hallinnollisen sakon määräämisestä ja hallinnollisen sakon määrästä, kussakin yksittäisessä tapauksessa on otettava asianmukaisesti huomioon seuraavat seikat – –”. Näin ollen, ja kun otetaan huomioon johdanto-osan 148 kappale[6], valvontaviranomaisen velvollisuutena on valita kaikkein asianmukaisin toimenpide (tai toimenpiteet). Asetuksen 83 artiklan 4–6 kohdassa mainituissa tapauksissa tämän valinnan yhteydessä **on harkittava** kaikkia korjaavia toimenpiteitä, mukaan lukien asianmukaisen hallinnollisen sakon määräämistä joko 58 artiklan 2 kohdan mukaisen korjaavan toimenpiteen lisäksi tai yksinään.

Sakot ovat tärkeä väline, jota valvontaviranomaisten olisi käytettävä tarkoituksenmukaisesti. Valvontaviranomaisia kannustetaan käyttämään harkittua ja tasapainoista lähestymistapaa korjaavia toimenpiteitä soveltaessaan, jotta rikkomiseen vastattaisiin tehokkaasti, varoittavasti ja oikeasuhteisesti. Tavoitteena ei ole luokitella sakkoja viimeiseksi keinoksi eikä saada luopumaan sakkojen määräämisestä, vaan tavoitteena on, ettei sakkoja käytetä siten, että heikennetään tämän välineen tehokkuutta.

Kun tietosuojaneuvosto on asetuksen 65 artiklan mukaan toimivaltainen, se antaa sitovan päätöksen viranomaisten välisissä kiistoissa, jotka liittyvät etenkin rikkomisen toteamiseen. Kun merkityksellisessä ja perustellussa vastalauseessa tuodaan esiin kysymys, onko korjaava toimenpide

[5] Asetuksen 83 artiklassa esitettyjen perusteiden lisäksi tämän lähestymistavan perustaa voidaan lujittaa soveltamalla myös muita säännöksiä, kuten

- johdanto-osan 141 kappaletta: ”Valitus olisi tutkittava siinä määrin kuin kussakin tapauksessa on asianmukaista, ja ratkaisu olisi voitava saattaa tuomioistuimen käsiteltäväksi.”
- johdanto-osan 129 kappaletta: ”Valvontaviranomaisten valtuuksia olisi käytettävä unionin oikeudessa ja jäsenvaltioiden lainsäädännössä vahvistettujen asianmukaisten menettelytakeiden mukaisesti puolueettomasti, asianmukaisesti ja kohtuullisessa ajassa. Jokaisen toimenpiteen olisi erityisesti oltava tarkoituksenmukainen, tarpeellinen ja oikeasuhteinen, jotta voidaan varmistaa tämän asetuksen noudattaminen siten, että otetaan huomioon kunkin yksittäisen tapauksen olosuhteet – –”.
- 57 artiklan 1 kohdan f alakohtaa: ”käsiteltävä rekisteröidyn tai 80 artiklan mukaisen elimen, järjestön tai yhdistyksen tekemiä valituksia ja tutkittava siinä määrin kuin se on asianmukaista valituksen kohdetta – –.”

[6] ”Tämän asetuksen sääntöjen täytäntöönpanon vahvistamiseksi asetuksen säännösten rikkomisesta olisi määrättävä seuraamuksia, kuten hallinnollisia sakkoja, valvontaviranomaisen tämän asetuksen mukaisesti määräämien asianmukaisten toimenpiteiden lisäksi tai niiden sijasta. Jos kyseessä on vähäinen rikkominen tai jos määrättävä sakko olisi kohtuuton rasitus luonnolliselle henkilölle, voidaan sakon sijasta antaa huomautus. Rikkomisen luonteeseen, vakavuuteen ja kestoon, sen tahallisuuteen, aiheutuneen vahingon lieventämiseksi toteutettuihin toimiin, vastuun asteeseen tai mahdollisiin vastaaviin aiempiin rikkomisiin, tapaan, jolla rikkominen tuli valvontaviranomaisen tietoon, rekisterinpitäjälle tai henkilötietojen käsittelijälle määrättyjen toimenpiteiden noudattamiseen, käytännesääntöjen noudattamiseen ja mahdollisiin muihin raskauttaviin tai lieventäviin tekijöihin olisi kuitenkin kiinnitettävä asianmukaista huomiota. Seuraamusten, kuten hallinnollisten sakkojen, määräämiseen olisi sovellettava riittäviä menettelytakeita unionin lainsäädännön ja perusoikeuskirjan yleisten periaatteiden mukaisesti, tehokkaat oikeussuojakeinot ja asianmukainen prosessi mukaan luettuina.”

yhdenmukainen tietosuoja-asetuksen kanssa, tietosuojaneuvoston päätöksessä tarkastellaan myös, onko toimivaltaisen valvontaviranomaisen päätösehdotuksessa mainittu hallinnollinen sakko tehokkuutta, oikeasuhteisuutta ja varoittavuutta koskevien periaatteiden mukainen. Tietosuojaneuvosto laatii myöhemmin erikseen asetuksen 65 artiklan soveltamista koskevia ohjeita, joissa annetaan yksityiskohtaista tietoa tietosuojaneuvoston tämän tyyppisestä päätöksestä.

---

4. Hallinnollisia sakkoja tietosuojan alalla koskeva yhdenmukaistettu lähestymistapa edellyttää, että valvontaviranomaiset osallistuvat aktiivisesti toimiin ja vaihtavat keskenään tietoja

---

Näissä suuntaviivoissa on otettu huomioon, että sakotustoimivalta on joillekin kansallisille valvontaviranomaisille uusi toimivalta tietosuoja-alalla, ja siksi se herättää useita resursseihin, organisaatioon ja menettelyyn liittyviä kysymyksiä. Kansallisiin tuomioistuimiin voidaan valittaa erityisesti päätöksistä, joissa valvontaviranomaiset käyttävät niille annettua sakotustoimivaltaa.

Valvontaviranomaisten on tehtävä yhteistyötä keskenään ja tarvittaessa Euroopan komission kanssa käyttämällä asetuksessa tarkoitettuja yhteistyömekanismeja. Tarkoituksena on edistää virallista ja epävirallista tiedonvaihtoa, esimerkiksi säännöllisesti järjestettävien työpajojen avulla. Tällaisessa yhteistyössä keskityttäisiin valvontaviranomaisten kokemuksiin ja käytäntöihin sakotustoimivallan soveltamisen alalla, jotta varmistetaan lopulta suurempi yhdenmukaisuus.

Ennakoiva tietojen jakaminen ja toimivallan käyttöä koskeva muodostumassa oleva oikeuskäytäntö voivat johtaa siihen, että periaatteita tai näiden suuntaviivojen tiettyjä yksityiskohtia on tarkasteltava uudelleen.

III. Asetuksen 83 artiklan 2 kohdassa esitetyt arviointikriteerit

Asetuksen 83 artiklan 2 kohdassa esitetään luettelo kriteereistä, joita valvontaviranomaisten odotetaan käyttävän sekä sakon määräämisen että sakon määrän arvioinnin yhteydessä. Samoihin kriteereihin perustuvan arvioinnin toistamista ei suositella, vaan arvioinnissa olisi otettava huomioon kaikki yksittäisen tapauksen olosuhteet, kuten 83 artiklassa säädetään.[7]

Arvioinnin ensimmäisessä vaiheessa tehtyjä päätelmiä voidaan käyttää sakon määrää koskevassa toisessa vaiheessa, jolloin vältetään tarve tehdä arviointi käyttämällä samoja kriteerejä kahdesti.

Tässä osassa valvontaviranomaisia opastetaan, miten asian yksittäisiä tosiseikkoja olisi tulkittava 83 artiklan 2 kohdassa esitettyjen kriteerien mukaisesti.

a) rikkomisen luonne, vakavuus ja kesto

Lähes kaikki asetuksen mukaiset rekisterinpitäjien ja henkilötietojen käsittelijöiden velvoitteet luokitellaan 83 artiklan 4–6 kohdassa niiden **luonteen** mukaan. Asetuksessa vahvistetaan hallinnollisen sakon kaksi enimmäismäärää (10 ja 20 miljoonaa euroa), mikä ilmentää sitä, että asetuksen joidenkin säännösten rikkominen voi olla vakavampaa kuin toisten. Arvioituaan asiaan liittyviä tosiseikkoja 83 artiklan 2 kohdassa esitettyjen yleisten kriteerien perusteella toimivaltainen valvontaviranomainen voi kuitenkin päättää, että kyseisessä tapauksessa on – enemmän tai vähemmän – tarvetta sakon muodossa toteutettavaan korjaavaan toimenpiteeseen. Jos sakko on valittu ainoaksi asianmukaiseksi korjaavaksi toimenpiteeksi tai yhdeksi useista asianmukaisista korjaavista toimenpiteistä, sovelletaan asetuksen porrastettua järjestelmää (83 artiklan 4–6 kohta), jotta voidaan määrittää kyseisen rikkomisen luonteen perusteella määrättävä enimmäissakko.

Johdanto-osan 148 kappaleessa selostetaan käsitettä ”vähäinen rikkominen”. Tällaisessa rikkomisessa voi olla kyse yhden tai useamman 83 artiklan 4 tai 5 kohdassa esitetyn säännöksen rikkomisesta. Asetuksen 83 artiklan 2 kohdassa esitettyjen kriteerien arvioinnin perusteella valvontaviranomaiset voivat kuitenkin esimerkiksi katsoa, että rikkominen ei tapauksen konkreettisissa olosuhteissa muodosta huomattavaa riskiä asianomaisten rekisteröityjen oikeuksille eikä se vaikuta rikotun velvoitteen olennaiseen sisältöön. Tällaisissa tapauksissa sakon sijaan voidaan antaa huomautus (ei kuitenkaan aina).

Johdanto-osan 148 kappaleessa valvontaviranomaisia ei aina velvoiteta korvaamaan sakko huomautuksella, kun kyse on vähäisestä rikkomisesta (”…voidaan sakon sijasta antaa huomautus”), vaan siinä pikemminkin säädetään mahdollisuudesta antaa huomautus asiaan liittyvien kaikkien olosuhteiden konkreettisen arvioinnin perusteella.

Johdanto-osan 148 kappaleessa annetaan myös mahdollisuus korvata sakko huomautuksella, jos rekisterinpitäjä on luonnollinen henkilö ja jos todennäköinen sakko olisi kohtuuton rasitus. Lähtökohtana on, että valvontaviranomaisen on arvioitava, onko sakon määrääminen tarpeen, kun otetaan huomioon kyseisen tapauksen olosuhteet. Jos valvontaviranomainen toteaa sakon määräämisen tarpeelliseksi, sen on arvioitava myös, olisiko määrättävä sakko kohtuuton rasitus luonnolliselle henkilölle.

Asetuksessa ei vahvisteta tiettyä hintalappua tietyille rikkomisille, ainoastaan sakkojen enimmäismäärä. Tämä voi ilmentää sitä, että 83 artiklan 4 kohdassa lueteltujen velvoitteiden rikkomista pidetään vähemmän vakavina kuin 83 artiklan 5 kohdassa esitettyjen velvoitteiden

[7] Joidenkin maiden perustuslaillisiin vaatimuksiin perustuvien kansallisten menettelysääntöjen vuoksi seuraamusta voidaan arvioida erikseen, kun on ensin arvioitu, onko sääntöjä rikottu. Tämä voi näin ollen rajoittaa tällaisten maiden johtavien valvontaviranomaisten antaman päätösluonnoksen sisältöä ja yksityiskohtaisuutta.

rikkomista. Asetuksen 83 artiklan 5 kohdan rikkomisesta annettava tehokas, oikeasuhteinen ja varoittava seuraamus määräytyy kuitenkin tapauksen olosuhteiden perusteella.

On huomautettava, että asetuksen rikkomiset, joista määrättävä sakko voisi rikkomuksen luonteen perusteella olla enintään 10 miljoonaa euroa tai enintään kaksi prosenttia vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta, kuten säädetään 83 artiklan 4 kohdassa, voivat täyttää korkeamman tason (20 miljoonaa euroa) luokitusta koskevat ehdot tietyissä olosuhteissa. Tämä olisi todennäköistä tapauksissa, joissa valvontaviranomaiset ovat aiemmin antaneet rikkomista koskevan määräyksen[8] mutta rekisterinpitäjä tai henkilötietojen käsittelijä on jättänyt noudattamatta[9] kyseistä määräystä (83 artiklan 6 kohta). Kansallisen lainsäädännön säännöksillä voi käytännössä olla vaikutusta tähän arviointiin.[10] Rikkomisen luonne mutta myös ”kyseisen tietojenkäsittelyn – – laajuus tai tarkoitus – – sekä niiden rekisteröityjen lukumäärä, joihin rikkominen vaikuttaa, ja heille aiheutuneen vahingon suuruus” ilmentävät rikkomisen **vakavuutta**. Jos tietyssä yksittäisessä tapauksessa rikkomisia on useita, valvontaviranomainen voi määrätä hallinnollisia sakkoja vakavimman rikkomisen rajoissa siinä määrin kuin on tehokasta, oikeasuhteista ja varoittavaa. Näin ollen, jos todetaan, että 8 ja 12 artiklaa on rikottu, valvontaviranomainen voi soveltaa niitä 83 artiklan 5 kohdassa esitettyjä korjaavia toimenpiteitä, jotka vastaavat vakavimman rikkomisen luokkaa, tarkemmin sanottuna 12 artiklan rikkomista. Näissä suuntaviivoissa ei tässä vaiheessa tarkastella asiaa yksityiskohtaisemmin (yksityiskohtaista laskentaa tarkastellaan näiden suuntaviivojen mahdollisessa myöhemmässä osassa).

Jäljempänä esitettyjä seikkoja olisi arvioitava yhdessä, esimerkiksi rekisteröityjen määrää olisi arvioitava yhdessä niihin mahdollisesti kohdistuvan vaikutuksen kanssa.

Asianomaisten rekisteröityjen **määrä** olisi arvioitava, jotta voidaan määrittää, onko kyse yksittäisestä tapauksesta vai ilmentääkö tapaus järjestelmällisempää rikkomista tai asianmukaisten käytäntöjen puutetta. Tämä ei tarkoita sitä, että yksittäiset tapaukset eivät ole täytäntöönpanokelpoisia, sillä yksittäisellä tapauksella voi silti olla vaikutusta moniin rekisteröityihin. Tämä riippuu tapauksen

---

[8] Asetuksen 58 artiklan 2 kohdan mukaan valvontaviranomaisella on valtuudet

- määrätä rekisterinpitäjä tai henkilötietojen käsittelijä noudattamaan rekisteröidyn pyyntöjä, jotka koskevat tähän asetukseen perustuvien rekisteröidyn oikeuksien käyttöä;
- määrätä rekisterinpitäjä tai henkilötietojen käsittelijä saattamaan käsittelytoimet tämän asetuksen säännösten mukaisiksi, tarvittaessa tietyllä tavalla ja tietyn määräajan kuluessa;
- määrätä rekisterinpitäjä ilmoittamaan henkilötietojen tietoturvaloukkauksesta rekisteröidylle;
- asettaa väliaikainen tai pysyvä rajoitus käsittelylle, mukaan lukien käsittelykielto;
- määrätä henkilötietojen oikaisemisesta tai poistamisesta tai käsittelyn rajoittamisesta 16, 17 ja 18 artiklan perusteella sekä näistä toimenpiteistä ilmoittamisesta niille vastaanottajille, joille henkilötietoja on luovutettu 17 artiklan 2 kohdan ja 19 artiklan mukaisesti;
- määrätä sertifiointielin peruuttamaan 42 ja 43 artiklan mukaisesti annettu sertifiointi tai kieltää sertifiointielintä antamasta sertifiointia silloin kun sertifiointia koskevat vaatimukset eivät täyty tai eivät enää täyty;
- määrätä tiedonsiirtojen keskeyttämisestä kolmannessa maassa olevalle vastaanottajalle tai kansainväliselle järjestölle.

[9] Asetuksen 83 artiklan 6 kohdan soveltamisessa on otettava huomioon menettelyä koskeva kansallinen lainsäädäntö. Kansallisessa lainsäädännössä määritetään, miten määräys annetaan, miten siitä ilmoitetaan, milloin se tulee voimaan ja sovelletaanko rikkomuksen poistamiseen siirtymäaikaa. Erityisesti olisi otettava huomioon muutoksenhaun vaikutus määräyksen täytäntöönpanokelpoisuuteen.

[10] Laissa olevat vanhentumissäännökset voivat johtaa siihen, että valvontaviranomaisen aiempaa määräystä ei voida enää ottaa huomioon, jos kyseisen määräyksen antamisesta on kulunut aikaa. Joidenkin oikeudenkäyttöalueiden säännöissä vahvistetaan, että kun määräyksen vanhentumisaika on kulunut umpeen, 83 artiklan 6 kohdan nojalla ei voida antaa sakkoa kyseisen määräyksen noudattamatta jättämisestä. Kunkin oikeudenkäyttöalueen valvontaviranomaiset vahvistavat, mitä vaikutuksia tällä on niihin.

olosuhteet huomioon ottaen esimerkiksi kyseiseen tietokantaan rekisteröityjen määrästä, palvelun käyttäjien määrästä, asiakkaiden määrästä tai maan väestömäärästä tapauksen mukaan.

Myös käsittelyn **tarkoitusta** on arvioitava. Tietosuojatyöryhmän 29 lausunnossa käyttötarkoituksen rajaamisesta[11] on analysoitu tämän periaatteen kahta keskeistä osatekijää tietosuojalainsäädännössä: käyttötarkoituksen määrittelyä ja tarkoituksenmukaista käyttöä. Arvioidessaan käsittelyn tarkoitusta 83 artiklan 2 kohdan yhteydessä valvontavalvontaviranomaisten olisi tarkasteltava, missä määrin käsittelyssä noudatetaan tämän periaatteen kahta keskeistä osatekijää.[12] Valvontaviranomainen voi tietyissä tilanteissa katsoa tarpeelliseksi laatia perusteellisemman selvityksen käsittelyn tarkoituksesta 83 artiklan 2 kohdan mukaisessa analyysissa.

Jos rekisteröidyt ovat kärsineet **vahinkoa**, vahingon suuruus on otettava huomioon. Henkilötietojen käsittelystä voi aiheutua henkilöiden oikeuksiin ja vapauksiin liittyviä riskejä, kuten todetaan johdanto-osan 75 kappaleessa:

> ”Nämä todennäköisyydeltään ja vakavuudeltaan vaihtelevat luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat riskit voivat aiheutua henkilötietojen käsittelystä, joka voi aiheuttaa fyysisiä, aineellisia tai aineettomia vahinkoja, erityisesti jos käsittely saattaa johtaa syrjintään, identiteettivarkauteen tai petokseen, taloudellisiin menetyksiin, maineen vahingoittumiseen, salassapitovelvollisuuden alaisten henkilötietojen luottamuksellisuuden menetykseen, pseudonymisoitumisen luvattomaan kumoutumiseen tai aiheuttaa muuta merkittävää taloudellista tai sosiaalista vahinkoa; kun rekisteröidyiltä saatetaan evätä heidän oikeuksiaan ja vapauksiaan tai estää heitä valvomasta omia henkilötietojaan; kun käsitellään sellaisia henkilötietoja, jotka koskevat rotua tai etnistä alkuperää, poliittisia mielipiteitä, uskonnollista tai filosofista vakaumusta ja ammattiliittoon kuulumista, tai käsitellään geneettisiä tietoja tai terveyttä ja seksuaalista käyttäytymistä tai rikostuomioita ja rikkomuksia tai niihin liittyviä turvaamistoimenpiteitä koskevia tietoja; kun arvioidaan henkilökohtaisia ominaisuuksia, erityisesti jos kyseessä on henkilöprofiilin luomista tai käyttämistä varten suoritettu analyysi tai ennakointi työsuorituksesta, taloudellisesta tilanteesta, terveydestä, henkilökohtaisista mieltymyksistä tai kiinnostuksen kohteista, luotettavuudesta tai käyttäytymisestä, sijainnista tai liikkeistä; kun käsitellään heikossa asemassa olevien luonnollisten henkilöiden, erityisesti lasten, henkilötietoja; tai kun käsitellään suuria määriä henkilötietoja ja käsittely koskee suurta rekisteröityjen määrää.”

Jos rekisteröity on kärsinyt tai todennäköisesti kärsii vahinkoa asetuksen rikkomisen vuoksi, valvontaviranomaisen olisi otettava tämä huomioon valitessaan korjaavaa toimenpidettä, vaikka valvontaviranomainen ei itse ole toimivaltainen myöntämään erityistä korvausta kärsitystä vahingosta.

Sakon määrääminen ei ole riippuvainen siitä, kykeneekö valvontaviranomainen vahvistamaan syy-yhteyden rikkomisen ja aineellisen menetyksen välillä (ks. esim. 83 artiklan 6 kohta).

Rikkomisen **kesto** voi ilmentää esimerkiksi

a) rekisterinpitäjän tarkoituksellista toimintaa tai

b) asianmukaisten ehkäisevien toimenpiteiden laiminlyöntiä tai

c) kyvyttömyyttä toteuttaa tarvittavia teknisiä ja organisatorisia toimenpiteitä.

---

[11] WP 203, lausunto 3/2013 käyttötarkoituksen rajaamisesta, saatavilla osoitteessa http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[12] Ks. myös WP 217, lausunto 6/2014 direktiivin 95/46/EY 7 artiklan mukaisesta rekisterinpitäjän oikeutetun intressin käsitteestä, s. 26, kun tarkastellaan kysymyksiä ”Mikä tekee intressistä ’oikeutetun’ tai ’perusteettoman’?”

b) rikkomisen tahallisuus tai tuottamuksellisuus

Tahallisuus edellyttää yleensä tietoista ja tarkoituksellista rikkomista, kun taas tahattomuudella tarkoitetaan sitä, että rikkominen ei ollut tahallista, vaikka rekisterinpitäjä / henkilötietojen käsittelijä rikkoikin laissa edellytettyä huolellisuusvelvoitetta.

Tahallisia rikkomisia, jotka ilmentävät piittaamattomuutta lainsäädännöstä, pidetään yleisesti vakavampina kuin tahattomia rikkomisia, ja siksi tahallisista teoista olisi todennäköisemmin määrättävä hallinnollinen sakko kuin tahattomista. Tahallisuutta tai tuottamuksellisuutta koskevat päätelmät tehdään määrittämällä tapauksen tosiseikkoihin perustuvat, toimintaan liittyvät objektiiviset seikat. Lisäksi asetuksen soveltamisalaan kuuluvaa tietosuojaa koskevan muodostumassa olevan oikeuskäytännön ja muun käytännön perusteella voidaan tulevaisuudessa päätellä selkeämmin, missä olosuhteissa rikkomista on pidettävä tahallisena.

Tahallista rikkomista ilmentäviä olosuhteita voivat olla laiton tietojenkäsittely, johon rekisterinpitäjän ylin johto on nimenomaisesti antanut valtuudet tai joka toteutetaan tietosuojavastaavan ohjeista tai voimassa olevista toimintaperiaatteista välittämättä. Esimerkkinä voidaan mainita kilpailijan työntekijöitä koskevien tietojen hankkiminen ja käsittely, millä pyritään saattamaan kyseinen kilpailija huonoon maineeseen markkinoilla.

Muita tällaisia esimerkkejä voivat olla tilanteet, joissa

- henkilötietoja muutetaan siten, että annetaan harhaanjohtava (myönteinen) käsitys tavoitteiden saavuttamisesta (tällaista on ilmennyt sairaaloiden tavoiteodotusaikojen yhteydessä), tai
- henkilötietoja kaupitellaan markkinointitarkoituksiin, toisin sanoen tietoja myydään aivan kuin niiden käyttö perustuisi suostumukseen (tarkistamatta rekisteröityjen suostumusta tietojensa käyttöön tai heidän kiellostaan välittämättä).

Muut seikat, kuten inhimillinen erehdys tai se, että voimassa oleviin toimintaperiaatteisiin ei ole perehdytty eikä niitä ole noudatettu, julkaistuista tiedoista ei ole tarkistettu henkilötietoja, teknisiä päivityksiä ei ole tehty oikea-aikaisesti tai toimintaperiaatteita ei ole hyväksytty (sen sijaan, että niitä on yksinkertaisesti jätetty soveltamatta), voivat viitata tuottamuksellisuuteen.

Yritysten pitäisi kantaa vastuu siitä, että niiden rakenteet ja resurssit ovat riittäviä niiden liiketoiminnan luonteeseen ja monimutkaisuuteen nähden. Rekisterinpitäjät ja henkilötietojen käsittelijät eivät voi perustella tietosuojalainsäädännön rikkomista vetoamalla puutteellisiin resursseihin. Tietojenkäsittelytoimia koskevissa käytännöissä ja niiden dokumentoinnissa noudatetaan asetuksen mukaista riskiperusteista lähestymistapaa.

On olemassa harmaita alueita, joilla on vaikutusta mahdollisen korjaavan toimenpiteen määräämistä koskevaan päätökseen, ja viranomaisen on ehkä tehtävä perusteellisempi tutkimus varmistuakseen tapauksen tosiseikoista ja taatakseen, että kunkin yksittäisen tapauksen erityiset olosuhteet on otettu huomioon.

c) rekisterinpitäjän tai henkilötietojen käsittelijän toteuttamat toimet rekisteröidyille aiheutuneen vahingon lieventämiseksi

Rekisterinpitäjät ja henkilötietojen käsittelijät ovat velvollisia toteuttamaan teknisiä ja organisatorisia toimenpiteitä varmistaakseen riskiin nähden asianmukaisen turvallisuustason, suorittamaan tietosuojaa koskevan vaikutustenarvioinnin ja lieventämään henkilötietojen käsittelystä aiheutuvia, henkilöiden oikeuksiin ja vapauksiin liittyviä riskejä. Jos sääntöjä kuitenkin rikotaan ja rekisteröidylle on aiheutunut vahinkoa, vastuussa olevan osapuolen olisi tehtävä kaikki voitavansa lieventääkseen rikkomisesta asianomaiselle (asianomaisille) aiheutuvia seurauksia. Valvontaviranomainen ottaa huomioon tällaisen vastuullisen toiminnan (tai sen puuttumisen) korjaavaa toimenpidettä valitessaan ja sakkoa laskiessaan.

Vaikka raskauttavat ja lieventävät tekijät soveltuvat erityisesti sakon määrän hienosäätämiseen tapauksen erityisten olosuhteiden mukaan, niiden merkitystä ei pitäisi aliarvioida myöskään asianmukaisten korjaavien toimenpiteiden valinnassa. Tapauksissa, joissa muihin kriteereihin perustuva arviointi saa valvontaviranomaisen epäilemään hallinnollisen sakon asianmukaisuutta joko ainoana korjaavana toimenpiteenä tai yhdessä muiden 58 artiklan mukaisten toimenpiteiden kanssa, tällaiset raskauttavat tai lieventävät olosuhteet voivat auttaa valitsemaan asianmukaiset toimenpiteet siirtämällä painopistettä sellaisiin toimenpiteisiin, jotka osoittautuvat tehokkaiksi, oikeasuhteisiksi ja varoittaviksi tietyssä tapauksessa.

Tämän säännöksen pohjalta arvioidaan rekisterinpitäjän vastuun astetta rikkomisen jälkeen. Sitä voidaan soveltaa tapauksiin, joissa rekisterinpitäjä / henkilötietojen käsittelijä ei selvästikään ole toiminut piittaamattomasti tai tuottamuksellisesti ja joissa se on tehnyt kaiken voitavansa toimintansa korjaamiseksi saatuaan tietää rikkomisesta.

Valvontaviranomaisten direktiivin 95/46/EY soveltamisesta saama kokemus on aiemmin osoittanut, että jonkinasteisen joustavuuden salliminen saattaa olla järkevää, kun kyse on rekisteripitäjistä / henkilötietojen käsittelijöistä, jotka ovat myöntäneet rikkomisensa ja ottaneet vastuulleen toimintansa vaikutusten korjaamisen tai rajoittamisen. Esimerkkejä tällaisesta ovat seuraavat (tämä ei kuitenkaan aina johda joustavampaan lähestymistapaan):

- Rekisterinpitäjä / henkilötietojen käsittelijä ottaa yhteyttä muihin rekisteripitäjiin / henkilötietojen käsittelijöihin, jotka ovat saattaneet olla osallisina laajennetussa tietojenkäsittelyssä, toisin sanoen, jos tietoa on jaettu vahingossa kolmansille osapuolille.
- Rekisterinpitäjä / henkilötietojen käsittelijä toteuttaa oikea-aikaisia toimia siten, että rikkomista estetään jatkumasta tai sitä estetään laajentumasta sellaiselle tasolle tai sellaiseen vaiheeseen, jossa vaikutukset olisivat paljon vakavampia.

d) rekisterinpitäjän tai henkilötietojen käsittelijän vastuun aste, ottaen huomioon heidän 25 ja 32 artiklan nojalla toteuttamansa tekniset ja organisatoriset toimenpiteet

Asetuksella on lisätty selvästi rekisterinpitäjän vastuuta verrattuna EU:n tietosuojadirektiiviin 95/46/EY.

Kun rekisterinpitäjän tai henkilötietojen käsittelijän vastuun astetta arvioidaan sen suhteen, onko sovellettu asianmukaista korjaavaa toimenpidettä, seuraavat seikat voidaan ottaa huomioon:

- Onko rekisterinpitäjä toteuttanut teknisiä toimenpiteitä, jotka vastaavat erityisesti sisäänrakennetun ja oletusarvoisen tietosuojan periaatteita (25 artikla)?
- Onko rekisterinpitäjä toteuttanut organisatorisia toimenpiteitä, joilla varmistetaan sisäänrakennetun ja oletusarvoisen tietosuojan periaatteiden (25 artikla) noudattaminen kaikilla organisaatiotasoilla?
- Onko rekisterinpitäjä tai henkilötietojen käsittelijä varmistanut asianmukaisen turvallisuustason (32 artikla)?
- Ovatko kaikki asiaa koskevat tietosuojakäytännöt/-toimintaperiaatteet tiedossa ja sovelletaanko niitä asianmukaisella tasolla organisaation hallinnossa? (24 artikla).

Asetuksen 25 ja 32 artiklassa edellytetään, että rekisterinpitäjät ottavat huomioon ”uusimman tekniikan ja toteuttamiskustannukset sekä käsittelyn luonteen, laajuuden, asiayhteyden ja tarkoitukset sekä käsittelyn aiheuttamat todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit luonnollisten henkilöiden oikeuksille ja vapauksille”. Mainituilla säännöksillä ei aseteta päämäärään liittyvää velvoitetta vaan keinoihin liittyvä velvoite, toisin sanoen rekisterinpitäjän on huolehdittava tarpeellisista arvioinneista ja tehtävä asianmukaiset päätelmät. Tämän jälkeen valvontaviranomaisen on vastattava siihen, missä määrin rekisterinpitäjä ”teki sen, mitä siltä voitiin odottaa”, kun otetaan

huomioon tietojenkäsittelyn luonne, tarkoitus tai laajuus sekä rekisterinpitäjälle asetuksessa asetetut velvoitteet.

Tässä arvioinnissa olisi otettava asianmukaisesti huomioon parhaisiin käytänteisiin perustuvat menettelyt tai menetelmät, jos sellaiset on laadittu ja jos niitä sovelletaan. Toimialan standardeihin ja kyseisellä alalla tai ammatissa sovellettaviin käytännesääntöihin on tärkeää kiinnittää huomiota. Käytännesäännöt voivat antaa viitteitä siitä, mikä on alan yleinen käytäntö ja miten hyvin tietojenkäsittelyyn liittyvien tyypillisten turvallisuuskysymysten ratkaisemiseen käytettävissä olevat erilaiset keinot ovat toimijoiden tiedossa.

Vaikka parhaita käytänteitä olisi yleensä pyrittävä soveltamaan, vastuun asteen arvioimisessa on otettava huomioon kunkin yksittäisen tapauksen erityiset olosuhteet.

e) rekisterinpitäjän tai henkilötietojen käsittelijän mahdolliset aiemmat vastaavat rikkomiset

Tämän kriteerin perusteella on tarkoitus arvioida rikkomiseen syyllistyneen yksikön historiatietoja. Valvontaviranomaisten olisi otettava huomioon, että tältä osin arviointi voi olla hyvin laaja, sillä minkä tahansa tyyppinen rikkominen, vaikka se poikkeaisi luonteeltaan valvontaviranomaisen nyt tutkimasta rikkomisesta, voi olla merkityksellinen arvioinnin kannalta, sillä se saattaa antaa yleisellä tasolla viitteitä riittämättömistä tiedoista tai tietosuojasäännösten noudattamatta jättämisestä.

Valvontaviranomaisen olisi arvioitava seuraavia seikkoja:

- Onko rekisterinpitäjä tai henkilötietojen käsittelijä syyllistynyt samaan rikkomiseen aiemmin?
- Onko rekisterinpitäjä tai henkilötietojen käsittelijä aiemmin rikkonut asetusta vastaavalla tavalla (esimerkiksi sen seurauksena, että organisaatiossa ei ole tunnettu voimassa olevia käytäntöjä, riskinarviointi on ollut epätarkoituksenmukaista, rekisteröidyn pyyntöihin ei ole vastattu oikea-aikaisesti tai pyyntöihin vastaamisessa on ilmennyt aiheetonta viivästystä)?

f) yhteistyön aste valvontaviranomaisen kanssa rikkomisen korjaamiseksi ja sen mahdollisten haittavaikutusten lieventämiseksi

Asetuksen 83 artiklan 2 kohdassa säädetään, että yhteistyön aste voidaan ottaa ”asianmukaisesti huomioon”, kun päätetään hallinnollisen sakon määräämisestä ja sen määrästä. Asetuksessa ei anneta täsmällistä vastausta siihen, miten rekisterinpitäjän tai henkilötietojen käsittelijän toimet, joilla pyritään korjaamaan valvontaviranomaisen jo toteama rikkominen, otetaan huomioon. On kuitenkin selvää, että tätä kriteeriä tavallisesti sovelletaan sakon suuruutta laskettaessa.

Jos rekisterinpitäjän toimien ansiosta yksilöiden oikeuksiin ei kohdistunut kielteisiä seurauksia tai vaikutukset olivat vähäisemmät kuin ne muutoin olisivat saattaneet olla, myös tämä voidaan ottaa huomioon, kun valitaan kussakin tapauksessa oikeasuhteista korjaavaa toimenpidettä.

Yksi näkökohta, joka voitaisiin ottaa huomioon merkityksellisenä seikkana arvioitaessa yhteistyötä valvontaviranomaisen kanssa, on se,

- onko toimija reagoinut valvontaviranomaisen pyyntöihin kyseisen tapauksen tutkinnan aikana siten, että sillä on rajoitettu merkittävästi yksilöiden oikeuksiin kohdistuvaa vaikutusta?

Tästä huolimatta ei olisi kuitenkaan tarkoituksenmukaista korostaa jo lainsäädännössä vaadittua yhteistyötä. Toimijan esimerkiksi edellytetään joka tapauksessa sallivan valvontaviranomaiselle pääsyn tiloihinsa tarkastuksia varten.

g) henkilötietoryhmät, joihin rikkominen vaikuttaa

Esimerkkejä olennaisista kysymyksistä, joihin vastaamista valvontaviranomainen voi tapauksen mukaan pitää tässä yhteydessä tarpeellisena, ovat:

- Koskeeko rikkominen asetuksen 9 tai 10 artiklassa esitettyjen erityisten henkilötietoryhmien käsittelyä?
- Ovatko tiedot tunnistettavissa suoraan tai välillisesti?
- Koskeeko käsittely tietoja, joiden levittäminen aiheuttaisi välitöntä vahinkoa/haittaa yksilölle (jos tiedot jäävät 9 tai 10 artiklassa tarkoitetun ryhmän ulkopuolelle)?
- Ovatko tiedot saatavilla suoraan ilman teknistä suojausta vai onko ne salattu?[13]

[13] Sitä, että rikkominen koskee vain välillisesti tunnistettavia tai pseudonymisoituja/salattuja tietoja, ei tulisi aina pitää seikkana, jonka johdosta lieventävä vaikutus on suurempi. Kun kyse on tällaisesta rikkomisesta, muihin kriteereihin perustuva kokonaisarvio voi antaa jonkin asteisia tai merkittäviä viitteitä siitä, että sakko olisi määrättävä.

h) tapa, jolla rikkominen tuli valvontaviranomaisen tietoon, erityisesti se, ilmoittiko rekisterinpitäjä tai henkilötietojen käsittelijä rikkomisesta ja missä laajuudessa

Rikkominen voi tulla valvontaviranomaisen tietoon tutkinnan, valitusten, lehtiartikkelien, nimettömien vihjeiden tai rekisterinpitäjän ilmoituksen perusteella. Asetuksessa rekisterinpitäjä velvoitetaan ilmoittamaan valvontaviranomaiselle henkilötietojen tietoturvaloukkauksista. Jos rekisterinpitäjä vain täyttää tämän velvoitteen, velvoitteen noudattamista ei voida pitää lieventävänä tekijänä. Sitä vastoin valvontaviranomainen voi katsoa, että rekisterinpitäjälle / henkilötietojen käsittelijälle, joka on toiminut huolimattomasti ilmoittamatta tai ilmoittamatta ainakaan kaikista rikkomisen yksityiskohdista, koska se ei ole arvioinut riittävästi rikkomisen laajuutta, on syytä määrätä vakavampi seuraamus, toisin sanoen tällaista rikkomista ei todennäköisesti luokiteltaisi vähäiseksi rikkomiseksi.

i) jos kyseiselle rekisterinpitäjälle tai henkilötietojen käsittelijälle on aikaisemmin määrätty samasta asiasta 58 artiklan 2 kohdassa tarkoitettuja toimenpiteitä, näiden toimenpiteiden noudattaminen

Valvontaviranomainen voi seurata jo aiemman rikkomisen vuoksi, miten rekisterinpitäjä tai henkilötietojen käsittelijä noudattaa sääntöjä, ja yhteydenpito tietosuojavastaavaan, jos sellainen on olemassa, on jo todennäköisesti ollut laajaa. Siksi valvontaviranomainen ottaa huomioon aiemman yhteydenpidon.

Toisin kuin edellä e kohdassa mainitun kriteerin osalta, tämän arviointikriteerin tarkoituksena on ainoastaan muistuttaa valvontaviranomaisia siitä, että niiden on otettava huomioon toimenpiteet, jotka ne itse ovat aiemmin määränneet samalle rekisterinpitäjälle tai henkilötietojen käsittelijälle ”*samasta asiasta*”.

j) 40 artiklan mukaisten hyväksyttyjen käytännesääntöjen tai 42 artiklan mukaisten hyväksyttyjen sertifiointimekanismien noudattaminen

Valvontaviranomaisten on ”valvottava tämän asetuksen soveltamista ja pantava se täytäntöön” (57 artiklan 1 kohdan a alakohta). Rekisterinpitäjä tai henkilötietojen käsittelijä voi käyttää hyväksyttyjen käytännesääntöjen noudattamista tekijänä, jolla osoitetaan sääntöjenmukaisuus 24 artiklan 3 kohdan, 28 artiklan 5 kohdan tai 32 artiklan 3 kohdan mukaisesti.

Jos yhtä asetuksen säännöksistä rikotaan, hyväksyttyjen käytännesääntöjen noudattaminen voi olla osoitus siitä, miten kattavasti valvontaviranomaisen on puututtava tilanteeseen ja määrättävä tehokas, oikeasuhteinen ja varoittava hallinnollinen sakko tai muua korjaava toimenpide. Asetuksen 40 artiklan 4 kohdan mukaan hyväksyttyihin käytännesääntöihin sisältyvät ”mekanismit, joiden avulla (valvonta)elin voi velvoitteen mukaisesti valvoa, että käytännesääntöjä soveltavat rekisterinpitäjät tai henkilötietojen käsittelijät noudattavat niitä”.

Jos rekisterinpitäjä tai henkilötietojen käsittelijä on sitoutunut noudattamaan hyväksyttyjä käytännesääntöjä, valvontaviranomainen voi tyytyä siihen, että käytännesääntöjen hallinnoinnista vastaava yhteisö ryhtyy itse asianmukaisiin toimenpiteisiin jäsentään vastaan, esimerkiksi turvautumalla käytännesääntöjen seuranta- ja täytäntöönpanojärjestelmiin. Siksi valvontaviranomainen voi katsoa, että tällaiset toimenpiteet ovat riittävän tehokkaita, oikeasuhteisia tai varoittavia kyseisessä tapauksessa, jolloin valvontaviranomaisen ei ole tarpeen määrätä lisätoimenpiteitä. Asetuksen 41 artiklan 2 kohdan c alakohdan ja 42 artiklan 4 kohdan mukaisesti sääntöjenvastaisesta toiminnasta voidaan langettaa seuraamuksia soveltamalla tällaista seurantajärjestelmää, mukaan lukien rekisterinpitäjän tai henkilötietojen käsittelijän määräaikainen pidättäminen tehtävästä tai jättäminen käytännesääntöjä hallinnoivan yhteisön ulkopuolelle. Joka tapauksessa valvontaelimen valtuuksilla *ei rajoiteta toimivaltaisen valvontaviranomaisen tehtäviä ja valtuuksia*, mikä tarkoittaa sitä, että valvontaviranomainen ei ole velvollinen ottamaan huomioon aiemmin määrättyjä seuraamuksia, jotka liittyvät itsesääntelyjärjestelmään.

Itsesääntelytoimenpiteiden toteuttamatta jättäminen voi myös paljastaa rekisterinpitäjän tai henkilötietojen käsittelijän sääntöjenvastaisuuteen liittyvän tuottamuksellisuuden tai tahallisuuden.

k) mahdolliset muut tapaukseen sovellettavat raskauttavat tai lieventävät tekijät, kuten rikkomisesta suoraan tai välillisesti saadut mahdolliset taloudelliset edut tai rikkomisella vältetyt tappiot

Säännöksessä esitetään esimerkkejä muista tekijöistä, jotka voidaan ottaa huomioon, kun päätetään 83 artiklan 4–6 kohdassa mainittujen säännösten rikkomisesta määrättävän hallinnollisen sakon asianmukaisuudesta.

Rikkomisella saatua hyötyä koskevat tiedot voivat olla valvontaviranomaisten kannalta erityisen merkityksellisiä, sillä rikkomisesta saatua taloudellista etua ei voida kompensoida toimenpiteillä, joihin ei liity maksuseuraamusta. Se, että rekisterinpitäjä on hyötynyt asetuksen rikkomisesta, voi olla selkeä merkki siitä, että sakko olisi määrättävä.

IV. Päätelmät

Edellä esitettyjen kaltaisia kysymyksiä koskevat pohdinnat auttavat valvontaviranomaisia määrittämään tapaukseen liittyvien tosiseikkojen pohjalta kriteerit, joista on eniten hyötyä, kun ne päättävät, olisiko 58 artiklassa tarkoitettujen muiden toimenpiteiden lisäksi tai niiden sijasta määrättävä asianmukainen hallinnollinen sakko. Valvontaviranomainen määrittää tähän arviointiin liittyvän asiayhteyden perusteella, mikä on tehokkain, oikeasuhteisin ja varoittavin toimenpide, jolla rikkomiseen vastataan.

Asetuksen 58 artiklassa opastetaan, mitä toimenpiteitä valvontaviranomainen voi valita, sillä korjaavat toimenpiteet ovat luonteeltaan erilaisia ja sopivat erilaisten tavoitteiden saavuttamiseen. Jotkin 58 artiklassa säädetyistä toimenpiteistä voidaan myös yhdistää, jolloin valvontatoimi muodostuu useammasta kuin yhdestä korjaavasta toimenpiteestä.

Toimenpidettä ei ole aina välttämätöntä täydentää käyttämällä toista korjaavaa toimenpidettä. Esimerkiksi kun valvontaviranomaiset ottavat asianmukaisesti huomioon, mikä on oikeasuhteista jossakin tapauksessa, toimenpiteen tehokkuutta ja varoittavuutta koskeva tavoite on mahdollista saavuttaa pelkästään sakolla.

Viranomaisten on palautettava sääntöjenmukaisuus ja tällöin hyödynnettävä kaikkia niiden käytettävissä olevia korjaavia toimenpiteitä. Valvontaviranomaisten on myös valittava kaikkein tarkoituksenmukaisin kanava sääntelytoimien toteuttamiseksi. Tähän voi sisältyä esimerkiksi rikosoikeudellisten seuraamusten määrääminen (jos ne ovat mahdollisia kansallisella tasolla).

Hallinnollisten sakkojen soveltaminen yhdenmukaisesti kaikkialla Euroopan unionissa on työtä, joka eteneee koko ajan. Valvontaviranomaisten on toimittava yhdessä parantaakseen jatkuvasti yhdenmukaisuutta. Tämä voidaan saavuttaa vaihtamalla säännöllisesti tietoa tapauksia käsittelevissä työpajoissa ja muissa tapahtumissa, jotka mahdollistavat alueellisten, kansallisten ja rajat ylittävien tapausten vertailun. Tämän jatkuvan toiminnan tukemiseksi on suositeltavaa perustaa pysyvä alaryhmä asiaa käsittelevän tietosuojaneuvoston yhteyteen.