# EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS (EU) 2016/679

| **Vain ne asetuksen resitaalit, joissa mainittu riski, uhka tai vaikutus** | **Pitäisikö huomioida organisaatiossani? Miten?** |
| --- | --- |
| (9) Direktiivin 95/46/EY tavoitteet ja periaatteet ovat edelleen pätevät, mutta sen avulla ei ole pystytty estämään tietosuojan täytäntöönpanon hajanaisuutta eri puolilla unionia, oikeudellista epävarmuutta tai laajalle levinnyttä näkemystä, jonka mukaan erityisesti verkkoympäristössä toimimiseen liittyy luonnollisten henkilöiden suojelun kannalta huomattavia riskejä. Jäsenvaltioiden väliset eroavuudet henkilötietojen käsittelyssä suhteessa luonnollisten henkilöiden oikeuksien ja vapauksien suojeluun, erityisesti oikeudessa henkilötietojen suojaan, voivat estää henkilötietojen vapaan liikkuvuuden unionin alueella. Nämä eroavuudet voivat muodostua esteeksi unionin taloudelliselle toiminnalle, vääristää kilpailua ja estää viranomaisia suorittamasta unionin oikeuden mukaisia velvollisuuksiaan. Tällaiset suojelun tasossa ilmenevät eroavuudet johtuvat direktiivin 95/46/EY täytäntöönpanossa ja soveltamisessa esiintyvistä eroista. |  |
| (15) Vakavan väärinkäytösten riskin välttämiseksi luonnollisten henkilöiden suojelun olisi oltava teknologianeutraalia eli se ei saisi riippua käytetystä tekniikasta. Luonnollisten henkilöiden suojelun olisi koskettava myös henkilötietojen automaattista käsittelyä sekä niiden manuaalista käsittelyä, jos henkilötiedot sisältyvät tai ne on tarkoitus sisällyttää rekisteriin. Tämän asetuksen soveltamisalaan ei ole tarkoitus sisällyttää sellaisia asiakirjoja tai asiakirjakokoelmia kansilehtineen, joita ei ole järjestetty tiettyjen perusteiden mukaisesti. |  |
| (28) Pseudonymisoinnin soveltaminen henkilötietoihin voi vähentää asianomaisiin rekisteröityihin kohdistuvia riskejä sekä auttaa rekisterinpitäjiä ja henkilötietojen käsittelijöitä noudattamaan tietosuojavelvoitteitaan. ”Pseudonymisoinnin” nimenomaisella sisällyttämisellä tähän asetukseen ei ole tarkoitus sulkea pois mitään muita tietosuoja­ toimenpiteitä. |  |
| (38) Erityisesti lasten henkilötietoja on pyrittävä suojaamaan, koska he eivät välttämättä ole kovin hyvin perillä henkilötietojen käsittelyyn liittyvistä riskeistä, seurauksista, asianomaisista suojatoimista tai omista oikeuksistaan. Tällaista erityistä suojaa olisi sovellettava etenkin lasten henkilötietojen käyttämistä markkinointitarkoituksiin tai henkilö- tai käyttäjäprofiilien luomiseen ja lapsia koskevien henkilötietojen keräämistä, kun käytetään suoraan lapsille tarjottuja palveluja. Vanhempainvastuunkantajan suostumuksen ei olisi oltava tarpeen tarjottaessa ennalta ehkäiseviä palveluja tai neuvontapalveluja suoraan lapselle. |  |
| (39) Henkilötietojen käsittelyn olisi oltava laillista ja asianmukaista. Luonnollisille henkilöille olisi oltava läpinäkyvää, miten heitä koskevia henkilötietoja kerätään ja käytetään ja niihin tutustutaan tai niitä käsitellään muulla tavoin sekä selvillä siitä, missä määrin henkilötietoja käsitellään tai on määrä käsitellä. Läpinäkyvyyden periaatteen mukaisesti kyseisten henkilötietojen käsittelyyn liittyvien tietojen ja viestinnän on oltava helposti saatavilla ja ymmärrettävissä ja niissä on käytettävä selkeää ja yksinkertaista kieltä. Tämä periaate koskee erityisesti rekisteröityjen tietoja rekisterinpitäjän identiteetistä ja käsittelyn tarkoituksista sekä lisätietoja, joilla varmistetaan kyseisiä luonnollisia henkilöitä koskevan käsittelyn asianmukaisuus ja läpinäkyvyys, sekä heidän oikeuttaan saada vahvistus ja ilmoitus heitä koskevien henkilötietojen käsittelystä. Luonnollisille henkilöille olisi tiedotettava henkilötietojen käsittelyyn liittyvistä riskeistä, säännöistä, suojatoimista ja oikeuksista sekä siitä, miten he voivat käyttää tällaista käsittelyä koskevia oikeuksiaan. Varsinkin henkilötietojen käsittelyn nimenomaiset tarkoitukset olisi määritettävä ja ilmoitettava henkilötietojen keruun yhteydessä yksiselitteisesti ja lainmukaisesti. Henkilötietojen olisi oltava riittäviä ja olennaisia ja rajoituttava siihen, mikä on välttämätöntä niiden käsittelyn tarkoitusten kannalta. Tämä edellyttää erityisesti sitä, että henkilötietojen säilytysaika on mahdollisimman lyhyt. Henkilötietoja olisi käsiteltävä vain jos käsittelyn tarkoitusta ei voida kohtuullisesti toteuttaa muilla keinoin. Rekisterinpitäjän olisi asetettava määräajat henkilötietojen poistoa tai niiden säilyttämisen tarpeellisuuden määräaikaistarkastelua varten, jotta voidaan varmistaa, ettei henkilötietoja säilytetä pidempään kuin on tarpeen. Olisi toteutettava kaikki kohtuulliset toimenpiteet, jotta varmistetaan, että virheelliset henkilötiedot oikaistaan tai poistetaan. Henkilötietoja olisi käsiteltävä siten, että varmistetaan henkilötietojen asianmukainen turvallisuus ja luottamuksellisuus, millä muun muassa ehkäistään luvaton pääsy henkilötietoihin tai niiden käsittelyyn käytettyihin laitteistoihin sekä tällaisten tietojen tai laitteistojen luvaton käyttö. |  |
| (50) Henkilötietojen käsittely muita tarkoituksia varten kuin niitä tarkoituksia, joita varten henkilötiedot on alun perin kerätty, olisi sallittava vain, jos käsittely sopii yhteen niiden tarkoitusten kanssa, joita varten henkilötiedot on alun perin kerätty. Tällöin henkilötietojen keruun oikeuttaneen käsittelyn oikeusperusteen lisäksi ei edellytetä muuta erillistä käsittelyn oikeusperustetta. Jos käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi, unionin oikeudessa tai jäsenvaltion lainsäädännössä voidaan määrittää ja täsmentää tehtävät ja tarkoitukset, joiden myöhempää käsittelyä olisi pidettävä yhteensopivana ja laillisena. Myöhempi käsittely yleisen edun mukaisiin arkistointitarkoituksiin taikka tieteellisiä tai historiallisia tutkimustarkoituksia varten tai tilastollisiin tarkoituksiin olisi katsottava yhteensopiviksi laillisiksi käsittelytoimiksi. Myös unionin oikeuden tai jäsenvaltion lainsäädännön tarjoama käsittelyn oikeusperuste henkilötietojen käsittelylle voi muodostaa käsittelyn oikeusperusteen myöhemmälle käsittelylle. Jotta voidaan varmistaa, onko myöhemmän käsittelyn tarkoitus yhteensopiva sen tarkoituksen kanssa, jota varten henkilötiedot alun perin kerättiin, rekisterinpitäjän olisi kaikki alkuperäisen käsittelyn laillisuutta koskevat vaatimukset ensin täytettyään otettava huomioon muun muassa kyseisten tarkoitusten ja suunnitellun myöhemmän käsittelyn tarkoitusten väliset yhteydet, tilanne, jossa henkilötiedot on kerätty, erityisesti myöhempään käsittelyyn liittyvät rekisteröidyn kohtuulliset odotukset, jotka perustuvat hänen ja rekisterinpitäjän väliseen suhteeseen; henkilötietojen luonne; suunnitellun myöhemmän käsittelyn seuraukset rekisteröidyille; ja asianomaisten suojatoimien olemassaolo sekä alkuperäisessä että suunnitellussa käsittelyssä. Jos rekisteröity on antanut suostumuksensa tai käsittely perustuu unionin oikeuteen tai jäsenvaltion lainsäädäntöön, joka muodostaa demokraattisessa yhteiskunnassa välttämättömän ja oikeasuhteisen toimenpiteen, jolla pyritään turvaamaan erityisesti yleiseen julkiseen etuun liittyviä tärkeitä tavoitteita, rekisterinpitäjälle olisi sallittava henkilötietojen myöhempi käsittely riippumatta tarkoitusten yhteensopivuudesta. Kaikissa tapauksissa olisi kuitenkin varmistettava, että sovelletaan tässä asetuksessa vahvistettuja periaatteita ja varmistettava erityisesti, että rekisteröidylle ilmoitetaan näistä muista tarkoituksista ja hänen oikeuksistaan, kuten oikeudesta vastustaa henkilötietojenkäsittelyä. Rekisterinpitäjän oikeutetun edun mukaiseksi on katsottava se, että tämä ilmoittaa mahdollisista rikollisista teoista tai yleiseen turvallisuuteen kohdistuvista uhkista ja toimittaa olennaiset henkilötiedot toimivaltaisille viranomaisille yksittäistapauksissa tai useissa tapauksissa, jotka liittyvät samaan rikolliseen tekoon tai yleiseen turvallisuuteen kohdistuvaan uhkaan. Tällaisen tietojen siirron rekisterinpitäjän oikeutetun edun nimissä tai henkilötietojen myöhemmän käsittelyn olisi kuitenkin oltava kiellettyä, mikäli käsittely on ristiriidassa johonkin oikeudelliseen, ammatilliseen tai muuhun sitovaan salassapitovelvollisuuteen nähden. |  |
| (51) Henkilötietoja, jotka ovat erityisen arkaluonteisia perusoikeuksien ja -vapauksien kannalta, on suojeltava erityisen tarkasti, koska niiden käsittelyn asiayhteys voisi aiheuttaa huomattavia riskejä perusoikeuksille ja -vapauksille. Tällaisiin henkilötietoihin olisi sisällyttävä myös henkilötiedot, joista ilmenee rotu tai etninen alkuperä. Ilmaisun ”rotu” käyttäminen tässä asetuksessa ei kuitenkaan tarkoita sitä, että unioni hyväksyisi teorioita, joilla yritetään määrittää eri ihmisrotujen olemassaolo. Valokuvien käsittelyä ei olisi automaattisesti katsottava henkilötietojen erityisryhmien käsittelyksi, koska valokuvat kuuluvat biometristen tietojen määritelmän piiriin ainoastaan siinä tapauksessa, että niitä käsitellään erityisin teknisin menetelmin, jotka mahdollistavat luonnollisen henkilön yksilöllisen tunnistamisen tai todentamisen. Tällaisia henkilötietoja ei pitäisi käsitellä, ellei käsittelyä sallita tässä asetuksessa vahvistetuissa erityistapauksissa, ottaen huomioon, että jäsenvaltioiden lainsäädännössä voidaan vahvistaa erityisiä tietosuojasäännöksiä tämän asetuksen sääntöjen soveltamisen mukauttamiseksi lakisääteisen velvoitteen noudattamista tai yleistä etua koskevan tehtävän suorittamista tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämistä varten. Tällaista käsittelyä koskevien erityisvaatimusten lisäksi olisi sovellettava tämän asetuksen yleisiä periaatteita ja muita sääntöjä erityisesti lainmukaisen tietojenkäsittelyn osalta. Olisi kuitenkin nimenomaisesti säädettävä poikkeuksista yleiseen kieltoon, joka koskee erityisiin henkilötietojen ryhmiin kuuluvien tietojen käsittelyä, muun muassa silloin, kun rekisteröity antaa nimenomaisen suostumuksensa tai silloin, kun kyseisten tietojen käsittely suoritetaan tiettyjen yhdistysten tai säätiöiden sellaisen oikeutetun toiminnan yhteydessä, jonka tarkoituksena on mahdollistaa perusvapauksien toteutuminen. |  |
| (65) Luonnollisella henkilöllä olisi oltava oikeus saada häntä koskevat virheelliset henkilötiedot oikaistuiksi ja oikeus ”tulla unohdetuksi”, jos tietojen säilyttäminen rikkoo tätä asetusta tai rekisterinpitäjään sovellettavaa unionin oikeutta tai jäsenvaltion lainsäädäntöä. Rekisteröidyllä olisi erityisesti oltava oikeus siihen, että hänen henkilötietonsa poistetaan ja ettei niitä käsitellä sen jälkeen kun henkilötietoja ei enää tarvita niitä tarkoituksia varten, joita varten ne kerättiin tai jota varten niitä muutoin käsiteltiin, tai kun rekisteröity on perunut tietojenkäsittelyä koskevan suostumuksensa tai kun hän on vastustanut henkilötietojensa käsittelyä tai kun hänen henkilötietojensa käsittely ei muutoin ole tämän asetuksen säännösten mukaista. Tämä oikeus tulee kyseeseen erityisesti silloin kun rekisteröity on antanut suostumuksensa lapsena, eikä ole ollut täysin tietoinen tietojenkäsittelyyn liittyvistä riskeistä, ja haluaa myöhemmin poistaa tällaiset tiedot erityisesti internetistä. Rekisteröidyn olisi voitava käyttää tätä oikeutta siitä huolimatta, että hän ei enää ole lapsi. Henkilötietojen edelleen säilyttämisen tulisi kuitenkin olla lainmukaista, jos se on tarpeen sananvapautta ja tiedonvälityksen vapautta koskevan oikeuden käyttämiseksi, lakisääteisen velvoitteen noudattamiseksi yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi, kansanterveyteen liittyvää yleistä etua koskevista syistä, yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia taikka tilastollisia tarkoituksia varten tai oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi. |  |
| (71) Rekisteröidyllä olisi oltava oikeus olla joutumatta hänen henkilökohtaisia ominaisuuksiaan arvioivan, mahdollisesti toimenpiteen sisältävän päätöksen kohteeksi, joka on tehty yksinomaan automaattisen tietojenkäsittelyn perusteella, josta hänelle aiheutuu oikeudellisia vaikutuksia tai joka vaikuttaa häneen vastaavalla merkittävällä tavalla, kuten online-luottohakemuksen automaattinen epääminen tai sähköisen rekrytoinnin käytännöt ilman ihmisen osallistumista. Kyseinen tietojenkäsittely sisältää ”profiloinnin”, joka tarkoittaa mitä tahansa henkilötietojen automaattista käsittelyä luonnollisen henkilön henkilökohtaisten ominaisuuksien arvioimiseksi, erityisesti rekisteröidyn työsuorituksen, taloudellisen tilanteen, terveyden, henkilökohtaisten mieltymysten tai kiinnostuksen kohteiden, luotettavuuden tai käyttäytymisen, sijainnin tai liikkumisen analysoimiseksi tai ennakoimiseksi, siltä osin kuin sillä on rekisteröityyn kohdistuvia oikeudellisia vaikutuksia tai se vaikuttaa häneen vastaavasti merkittävällä tavalla. Kyseiseen tietojenkäsittelyyn, mukaan lukien profilointiin, perustuva päätöksenteko olisi kuitenkin sallittava, jos siihen annetaan nimenomainen lupa rekisterinpitäjään sovellettavassa unionin oikeudessa tai jäsenvaltion lainsäädännössä, mukaan lukien lainsäädäntö, joka on annettu petosten ja verovilpin valvomiseksi ja torjumiseksi unionin toimielinten tai kansallisten valvontaelinten antamien asetusten, standardien ja suositusten mukaisesti, sekä rekisterinpitäjän tarjoaman palvelun turvallisuuden ja luotettavuuden varmistamiseksi, tai jos se on tarpeen rekisteröidyn ja rekisterinpitäjän välisen sopimuksen tekemistä tai täytäntöönpanoa varten tai jos rekisteröity on antanut siihen nimenomaisen suostumuksensa. Tällaiseen käsittelyyn olisi kuitenkin aina sovellettava asianmukaisia suojatoimia, joihin olisi kuuluttava käsittelystä ilmoittaminen rekisteröidylle ja oikeus vaatia ihmisen osallistumista tietojen käsittelemiseen, rekisteröidyn oikeus esittää kantansa, saada selvitys kyseisen arvioinnin jälkeen tehdystä päätöksestä ja riitauttaa päätös. Tällaista toimenpidettä ei saisi kohdistaa lapseen. Rekisteröityä koskevan asianmukaisen ja läpinäkyvän käsittelyn varmistamiseksi, ottaen huomioon henkilötietojen käsittelyn erityiset olosuhteet ja asiayhteys, rekisterinpitäjän olisi käytettävä profiloinnissa asianmukaisia matemaattisia tai tilastollisia menetelmiä, toteutettava teknisiä ja organisatorisia toimenpiteitä, jotka soveltuvat erityisesti sen varmistamiseen, että henkilötietojen virheellisyyteen johtavat tekijät korjataan ja virheriski minimoidaan, sekä turvattava henkilötiedot siten, että rekisteröidyn etuihin ja oikeuksiin kohdistuvat mahdolliset riskit otetaan huomioon ja estetään muun muassa luonnollisten henkilöiden syrjintä rodun tai etnisen alkuperän, poliittisten mielipiteiden, uskonnon tai vakaumuksen, ammattiliittoon kuulumisen, geneettisen tilan, terveydentilan tai seksuaalisen suuntautumisen perusteella taikka vaikutukset, joiden johdosta toteutetaan toimenpiteitä, joilla on tällaisia seurauksia. Henkilötietojen erityisluokitteluun perustuva automaattinen päätöksenteko ja profilointi olisi sallittava vain erityistilanteissa. |  |
| (74) Olisi vahvistettava rekisterinpitäjän vastuu tämän suorittamasta tai rekisterinpitäjän puolesta suoritetusta henkilötietojen käsittelystä. Erityisesti rekisterinpitäjällä olisi oltava velvollisuus toteuttaa asianmukaisia ja tehokkaita toimenpiteitä, ja sen olisi voitava osoittaa, että käsittelytoimet ovat tämän asetuksen mukaisia, toimenpiteiden tehokkuus mukaan luettuna. Näitä toimenpiteitä toteutettaessa olisi otettava huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuva riski. |  |
| (75) 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. |  |
| (76) Rekisteröidyn oikeuksiin ja vapauksiin kohdistuvan riskin todennäköisyys ja vakavuus olisi määriteltävä tietojen­ käsittelyn luonteen, laajuuden, asiayhteyden ja tarkoitusten mukaan. Riski olisi arvioitava objektiivisen arvioinnin perusteella, jolla todetaan, liittyykö tietojenkäsittelytoimiin riski tai korkea riski. |  |
| (77) Asianmukaisten toimenpiteiden toteuttamista koskevaa opastusta ja opastusta sen osoittamiseksi, onko rekisterinpitäjä tai henkilötietojen käsittelijä täyttänyt vaatimukset, erityisesti tietojenkäsittelyyn liittyvien riskien tunnistamisen ja niiden alkuperän, luonteen, todennäköisyyden ja vakavuuden arvioinnissa sekä riskien minimoinnin kannalta parhaiden käytäntöjen määrittelyssä, voitaisiin antaa erityisesti hyväksyttyjen käytänne­ sääntöjen, hyväksyttyjen todistusten tai tietosuojaneuvoston suuntaviivojen avulla taikka tietosuojavastaavan tiedotteilla. Tietosuojaneuvosto voi myös antaa suuntaviivoja käsittelytoimista, joiden ei katsota todennäköisesti aiheuttavan suurta riskiä luonnollisten henkilöiden oikeuksille ja vapauksille, ja mainita, mitkä toimenpiteet voivat tällaisissa tilanteissa olla riittäviä tällaisen riskin torjumiseksi. |  |
| (80) Jos unionin alueella olevien rekisteröityjen henkilötietoja käsittelee rekisterinpitäjä tai henkilötietojen käsittelijä, joka ei ole sijoittautunut unioniin, ja käsittely liittyy tavaroiden tai palvelujen tarjoamiseen näille rekisteröidyille unionin alueella riippumatta siitä, edellytetäänkö rekisteröidyltä maksua, tai heidän käyttäytymisensä seurantaan niiltä osin kuin käyttäminen tapahtuu unionissa, rekisterinpitäjän tai henkilötietojen käsittelijän olisi nimettävä edustaja, paitsi jos käsittely on satunnaista eikä kohdistu laajasti henkilötietojen erityisryhmiin tai rikostuomioita tai rikkomuksia koskeviin tietoihin, eikä siihen todennäköisesti liity luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä ottaen huomioon käsittelyn luonne, asiayhteys, laajuus ja tarkoitukset tai jos rekisterinpitäjä on viranomainen tai julkishallinnon elin. Edustajan olisi toimittava rekisterinpitäjän tai henkilötietojen käsittelijän puolesta, ja edustajaan voivat ottaa yhteyttä kaikki valvontaviranomaiset. Edustaja olisi nimenomaisesti nimettävä rekisterinpitäjän tai henkilötietojen käsittelijän antamalla kirjallisella valtuutuksella hoitamaan tämän puolesta tämän asetuksen mukaiset velvoitteet. Edustajan nimeämisellä ei ole vaikutusta tämän asetuksen mukaisiin rekisterinpitäjän tai henkilötietojen käsittelijän velvollisuuksiin tai vastuisiin. Edustajan olisi suoritettava tehtävänsä rekisterinpitäjältä tai henkilötietojen käsittelijältä saadun toimeksiannon mukaisesti, mukaan lukien yhteistyö toimivaltaisten valvontaviranomaisten kanssa kaikissa tämän asetuksen noudattamisen varmistamiseksi toteutettavissa toimissa. Nimettyyn edustajaan olisi sovellettava täytäntöönpanotoimia, jos rekisterinpitäjä tai henkilötietojen käsittelijä ei noudata asetuksen säännöksiä. |  |
| (81) Jotta voidaan varmistaa, että henkilötietojen käsittelijä noudattaa tämän asetuksen vaatimuksia rekisterinpitäjän puolesta suorittamassaan käsittelyssä, rekisterinpitäjän olisi antaessaan käsittelytoiminnat henkilötietojen käsittelijän tehtäväksi käytettävä ainoastaan sellaisia henkilötietojen käsittelijöitä, joilla on antaa riittävät takeet erityisesti asiantuntemuksesta, luotettavuudesta ja resursseista, jotta ne voivat panna täytäntöön tämän asetuksen vaatimusten mukaiset tekniset ja organisatoriset toimenpiteet, käsittelyn turvallisuus mukaan lukien. Sitä, että henkilötietojen käsittelijä noudattaa hyväksyttyjä käytännesääntöjä tai hyväksyttyä sertifiointimekanismia, voidaan käyttää osoittamaan rekisterinpitäjälle asetettujen velvollisuuksien noudattamista. Henkilötietojen käsittelijän suorittamaa käsittelyä olisi säänneltävä unionin oikeuden tai jäsenvaltion lainsäädännön mukaisella sopimuksella tai muulla oikeudellisella asiakirjalla, joka sitoo henkilötietojen käsittelijän rekisterinpitäjään ja jossa vahvistetaan käsittelyn kohde ja kesto, käsittelyn luonne ja tarkoitukset, henkilötietojen tyyppi ja rekisteröityjen ryhmät, ja siinä olisi otettava huomioon henkilötietojen käsittelijän erityistehtävät ja vastuualueet suoritettavan käsittelyn yhteydessä sekä rekisteröidyn oikeuksiin ja vapauksiin liittyvä riski. Rekisterinpitäjä ja henkilötietojen käsittelijä voivat päättää käyttää yksittäistä sopimusta tai sellaisia vakiosopimuslausekkeita, jotka hyväksyy joko suoraan komissio tai valvontaviranomainen yhdenmukaisuusmekanismin mukaisesti komission hyväksymänä. Kun henkilötietojen käsittelijä on saattanut käsittelyn loppuun rekisterinpitäjän puolesta, sen olisi rekisterinpitäjän valinnan mukaisesti palautettava tai poistettava henkilötiedot, paitsi jos henkilötietojen käsittelijään sovellettavassa unionin oikeudessa tai jäsenvaltion lainsäädännössä vaaditaan säilyttämään henkilötiedot. |  |
| (83) Turvallisuuden ylläpitämiseksi ja asetuksen säännösten vastaisen käsittelyn estämiseksi rekisterinpitäjän tai henkilötietojen käsittelijän olisi arvioitava käsittelyyn liittyvät riskit ja toteutettava toimenpiteitä näiden riskien lieventämiseksi esimerkiksi salauksella. Näiden toimenpiteiden avulla olisi varmistettava asianmukainen turvallisuustaso, muun muassa luottamuksellisuus, ottaen huomioon uusin tekniikka ja toteuttamiskustannukset suhteessa tietojenkäsittelyn riskeihin ja suojeltavien henkilötietojen luonteeseen. Tietosuojariskiä arvioitaessa olisi otettava huomioon henkilötietojen käsittelyyn liittyvät riskit, kuten siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai laiton tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen tai henkilötietoihin pääsy, mikä voi aiheuttaa etenkin fyysisiä, aineellisia tai aineettomia vahinkoja. |  |
| (84) Tämän asetuksen noudattamisen edesauttamiseksi tapauksissa, joissa käsittelytoimiin todennäköisesti liittyy luonnollisten henkilöiden oikeuksiin ja vapauksiin liittyvä korkea riski, rekisterinpitäjän olisi vastattava tietosuojaa koskevan vaikutustenarvioinnin suorittamisesta erityisesti kyseisen riskin alkuperän, luonteen, erityisluonteen ja vakavuuden arvioimiseksi. Arvioinnin tulos olisi otettava huomioon määriteltäessä asianmukaisia toimia, jotka on toteutettava, jotta voidaan osoittaa, että henkilötietojen käsittely on tämän asetuksen säännösten mukaista. Jos tietosuojaa koskevan vaikutustenarvioinnin perusteella osoitetaan, että käsittelytoimiin liittyy korkea riski, jota rekisterinpitäjä ei voi asianmukaisin toimenpitein vähentää saatavilla olevan tekniikan ja toteuttamiskustannusten suhteen, ennen tietojenkäsittelyä olisi kuultava valvontaviranomaista. |  |
| (85) Jos henkilötietojen tietoturvaloukkaukseen ei puututa riittävän tehokkaasti ja nopeasti, siitä voi aiheutua luonnollisille henkilöille fyysisiä, aineellisia tai aineettomia vahinkoja, kuten omien henkilötietojen valvomiskyvyn menettäminen tai oikeuksien rajoittaminen, syrjintää, identiteettivarkaus tai petos, taloudellisia menetyksiä, pseudonymisoitumisen luvaton kumoutuminen, maineen vahingoittuminen, salassapitovelvollisuuden alaisten henkilötietojen luottamuksellisuuden menetys tai muuta merkittävää taloudellista tai sosiaalista vahinkoa. Sen vuoksi rekisterinpitäjän olisi ilmoitettava henkilötietojen tietoturvaloukkauksesta valvontaviranomaiselle ilman aiheetonta viivytystä heti, kun se on tullut rekisterinpitäjän tietoon, ja mahdollisuuksien mukaan 72 tunnin kuluessa, paitsi jos rekisterinpitäjä pystyy osoittamaan tilivelvollisuusperiaatteen mukaisesti, että henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä. Jos tällaista ilmoitusta ei voida tehdä 72 tunnin kuluessa, ilmoitukseen olisi liitettävä selvitys viivytyksen syistä, ja tietoa voidaan antaa vaiheittain ilman aiheetonta lisäviivytystä. |  |
| (86) Rekisterinpitäjän olisi ilmoitettava henkilötietojen tietosuojaloukkauksesta rekisteröidylle viipymättä, jos tämä tietosuojaloukkaus todennäköisesti aiheuttaa luonnollisen henkilön oikeuksia ja vapauksia koskevan suuren riskin, jotta rekisteröity voi toteuttaa tarvittavat varotoimet. Ilmoituksessa olisi kuvattava henkilötietojen tietoturva­ loukkauksen luonne ja esitettävä suosituksia siitä, miten asianomainen luonnollinen henkilö voi lieventää sen mahdollisia haittavaikutuksia. Tällainen ilmoitus rekisteröidylle olisi tehtävä niin pian kuin se on kohtuudella mahdollista ja tiiviissä yhteistyössä valvontaviranomaisen kanssa noudattaen valvontaviranomaisen tai muiden asiaankuuluvien viranomaisten (kuten lainvalvontaviranomaisten) antamia ohjeita. Esimerkiksi tarve lieventää välittömien haittojen riskiä edellyttää sitä, että rekisteröidyille ilmoitetaan viipymättä, kun taas tarve toteuttaa asianmukaiset toimenpiteet tietoturvaloukkauksen jatkumisen tai vastaavien henkilötietojen tietoturvaloukkausten estämiseksi voivat olla perusteena pidemmälle ilmoitusajalle. |  |
| (87) Olisi tarkistettava, onko kaikki asianmukaiset tekniset suojatoimenpiteet ja organisatoriset toimenpiteet toteutettu, jotta voidaan selvittää välittömästi, onko tapahtunut henkilötietojen tietoturvaloukkaus, ja saattaa asia viipymättä valvontaviranomaisen ja rekisteröidyn tiedoksi. Se, että ilmoitus tehtiin ilman aiheetonta viivytystä, olisi selvitettävä ottaen huomioon erityisesti henkilötietojen tietoturvaloukkauksen luonne ja vakavuus sekä tästä rekisteröidylle aiheutuvat seuraukset ja haittavaikutukset. Kyseinen ilmoitus voi johtaa siihen, että valvontaviran­ omainen puuttuu asiaan sille tässä asetuksessa säädettyjen tehtävien ja toimivaltuuksien mukaisesti. |  |
| (89) Direktiivissä 95/46/EY on säädetty yleisestä velvollisuudesta ilmoittaa henkilötietojen käsittelystä valvontaviranomaisille. Vaikka tämä velvollisuus aiheuttaa hallinnollista ja taloudellista rasitusta, se ei aina ole edistänyt henkilötietojen suojaa. Tällaisista yleisistä ilmoitusvelvollisuuksista olisi luovuttava ja korvattava ne tehokkailla menettelyillä ja mekanismeilla, jotka keskittyvät sen sijaan niihin käsittelytoimien tyyppeihin, joihin niiden luonteen, laajuuden, asiayhteyden ja tarkoitusten vuoksi todennäköisesti liittyy luonnollisten henkilöiden oikeuksien ja vapauksien kannalta korkea riski. Tällaisiin käsittelytoimien tyyppeihin kuuluvat erityisesti toimet, jotka perustuvat erityisesti uusien tekniikoiden käyttöön tai jotka ovat uudenlaisia ja joiden osalta rekisterinpitäjä ei ole ensin tehnyt tietosuojaa koskevaa vaikutustenarviointia, tai tietosuojaa koskeva vaikutustenarviointi on tullut tarpeelliseksi, koska aikaa on kulunut siitä kun käsittely alkoi. |  |
| (90) Tapauksissa, joissa luonnollisten henkilöiden oikeuksiin tai vapauksiin kohdistuu korkea riski, rekisterinpitäjän olisi kyseisen riskin erityisen todennäköisyyden ja vakavuuden arvioimiseksi käsittelyn luonteen, laajuuden, asiayhteyden ja tarkoitusten sekä riskin alkuperän huomioon ottaen tehtävä ennen tietojenkäsittelyä tietosuojaa koskeva vaikutustenarviointi. Tässä vaikutustenarvioinnissa olisi tarkasteltava erityisesti suunniteltuja toimenpiteitä sekä suojatoimia ja mekanismeja, joiden avulla lievennetään edellä mainittua riskiä ja varmistetaan henkilötietojen suoja ja osoitetaan, että tätä asetusta on noudatettu. |  |
| (91) Tätä olisi sovellettava erityisesti laajoihin käsittelytoimiin, joissa on tarkoitus käsitellä huomattavia määriä henkilötietoja alueellisella, kansallisella tai ylikansallisella tasolla, jotka voivat vaikuttaa suureen määrään rekisteröityjä ja joihin todennäköisesti liittyy korkea suuri riski esimerkiksi tietojen arkaluonteisuuden vuoksi, jos uutta tekniikkaa käytetään saavutetun teknologisen osaamistason mukaisesti hyvin laajasti myös muihin käsittelytoimiin, joihin liittyy rekisteröityjen oikeuksiin ja vapauksiin vaikuttava korkea riski, varsinkin silloin kun rekisteröityjen on kyseisten toimien johdosta hankalampi käyttää oikeuksiaan. Tietosuojaa koskeva vaikutustenarviointi olisi toteutettava myös tapauksissa, joissa henkilötietoja käsitellään tiettyjä luonnollisia henkilöitä koskevien päätösten tekemiseksi kyseisten tietojen profilointiin perustuvan luonnollisten henkilöiden henkilökohtaisten ominaisuuksien järjestelmällisen ja kattavan arvioinnin perusteella tai erityisiä henkilötietoryhmiä, biometrisiä tietoja taikka tietoja, jotka koskevat rikostuomioita ja rikkomuksia tai niihin liittyviä turvaamistoimenpiteitä, koskevan käsittelyn perusteella. Tietosuojaa koskeva vaikutustenarviointi on tarpeen myös yleisölle avoimien alueiden laaja-alaisessa valvonnassa, erityisesti jos käytetään optoelektronisia laitteita, tai kaikissa muissa toimissa, jos toimivaltainen valvontaviranomainen katsoo, että käsittelyyn todennäköisesti liittyy korkea riski rekisteröityjen oikeuksien ja vapauksien kannalta erityisesti siitä syystä, että ne estävät rekisteröityjä käyttämästä oikeutta tai palvelua tai sopimusta tai siitä syystä, että kyseisiä toimia toteutetaan järjestelmällisesti laajassa mittakaavassa. Henkilötietojen käsittelyä ei saisi pitää laaja-alaisena, jos käsittely koskee yksittäisen lääkärin, muun terveydenhuollon ammattilaisen tai lakimiehen asiakkaiden henkilötietoja. Tällaisissa tapauksissa tietosuojaa koskevan vaikutustenarvioinnin ei pitäisi olla pakollista. |  |
| (92) Joissain olosuhteissa voi olla järkevää ja taloudellista laatia tietosuojaa koskeva vaikutustenarviointi, jossa tarkastellaan asioita laajemmin kuin yhden projektin kannalta, esimerkiksi kun viranomaiset tai julkishallinnon elimet aikovat luoda yhteisen sovelluksen tai käsittelyalustan tai kun useat rekisterinpitäjät aikovat ottaa käyttöön yhteisen sovelluksen tai käsittely-ympäristön kokonaista teollisuuden alaa tai segmenttiä tai jotakin laajalti käytettävää horisontaalista toimintoa varten. |  |
| (94) Jos tietosuojaa koskeva vaikutustenarviointi osoittaa, että käsittelyyn liittyisi riskin lieventämistä koskevien suojatoimien, suojaustoimenpiteiden ja -keinojen puuttumisen vuoksi suuri luonnollisten henkilöiden oikeuksiin ja vapauksiin vaikuttava riski, ja rekisterinpitäjä katsoo, että tätä riskiä ei voida kohtuullisin toimenpitein vähentää saatavilla olevan tekniikan ja toteuttamiskustannusten suhteen, ennen käsittelytoimien aloittamista olisi kuultava valvontaviranomaista. On todennäköistä, että tällainen korkea riski liittyy tietyntyyppiseen henkilötietojen käsittelyyn ja käsittelyn laajuuteen ja toistumistiheyteen, mikä voi aiheuttaa vahinkoa myös luonnollisen henkilön oikeuksille ja vapauksille tai merkitä niihin puuttumista. Valvontaviranomaisen olisi vastattava kuulemispyyntöön määrätyn ajan kuluessa. Valvontaviranomaisen reagoimattomuus määräajan puitteissa ei kuitenkaan saisi vaikuttaa valvontaviranomaisen mahdollisiin toimiin sille tässä asetuksessa annettujen tehtävien ja valtuuksien puitteissa, kuten valtaan kieltää käsittelytoimia. Osana kuulemismenettelyä valvontaviranomaiselle voidaan toimittaa käsittelyn osalta toteutetun tietosuojaa koskevan vaikutustenarvioinnin tulos, etenkin toimenpiteet, joiden tarkoituksena on vähentää luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä. |  |
| (95) Henkilötietojen käsittelijän olisi tarvittaessa ja pyydettäessä avustettava rekisterinpitäjää, joka varmistaa tietosuojaa koskevan vaikutustenarvioinnin toteuttamisesta ja valvontaviranomaisen ennakkokuulemisesta aiheutuvien velvoitteiden noudattamisen. |  |
| (96) Valvontaviranomaista olisi kuultava myös silloin, kun valmistellaan henkilötietojen käsittelyä koskevaa lainsäädäntö- tai sääntelytoimenpidettä, jotta voitaisiin varmistaa, että aiotussa käsittelyssä noudatetaan tätä asetusta, ja erityisesti pienentää rekisteröityyn henkilöön kohdistuvia riskejä. |  |
| (98) Rekisterinpitäjien tai henkilötietojen käsittelijöiden ryhmiä edustavia yhdistyksiä tai muita elimiä olisi kannustettava laatimaan käytännesääntöjä tässä asetuksessa asetetuissa rajoissa, jotta voitaisiin helpottaa tämän asetuksen soveltamista ottaen huomioon tietyillä aloilla suoritettavan käsittelyn erityispiirteet ja mikroyritysten sekä pienten ja keskisuurten yritysten erityistarpeet. Erityisesti käytännesäännöillä voitaisiin sopeuttaa rekisterin­ pitäjien tai henkilötietojen käsittelijöiden velvoitteita ottaen huomioon luonnollisten henkilöiden oikeuksiin ja vapauksiin todennäköisesti kohdistuva tietojenkäsittelyn riski. |  |
| (122) Jokaisen valvontaviranomaisen olisi oltava oman jäsenvaltionsa alueella toimivaltainen käyttämään toimivaltaa ja suorittamaan tehtäviä, jotka sille on annettu tämän asetuksen mukaisesti. Tämän olisi katettava erityisesti käsittely, jota suoritetaan sen oman jäsenvaltion alueella sijaitsevassa rekisterinpitäjän tai henkilötietojen käsittelijän toimipaikassa toteutettavan toiminnan yhteydessä, viranomaisten tai yleisen edun hyväksi toimivien yksityisten elinten suorittama henkilötietojen käsittely, käsittely, joka vaikuttaa sen alueella oleviin rekisteröityihin tai sellaisen rekisterinpitäjän tai henkilötietojen käsittelijän suorittama käsittely, joka ei ole sijoittautunut unioniin, kun käsittely kohdistuu sen alueella asuviin rekisteröityihin. Tähän olisi kuuluttava rekisteröidyn tekemien valitusten käsittely, asetuksen soveltamista koskevien tutkimusten suorittaminen sekä yleisen tietoisuuden edistäminen henkilötietojen käsittelyyn liittyvistä riskeistä, säännöistä, suojatoimista ja oikeuksista. |  |
| (170) Jäsenvaltiot eivät voi riittävällä tavalla saavuttaa tämän asetuksen tavoitteita eli varmistaa luonnollisten henkilöiden yhdenmukaista suojelua ja henkilötietojen vapaata liikkuvuutta unionissa, vaan ne voidaan toiminnan laajuuden ja vaikutusten vuoksi saavuttaa paremmin unionin tasolla. Sen vuoksi unioni voi toteuttaa toimenpiteitä Euroopan unionista tehdyn sopimuksen (SEU) 5 artiklassa vahvistetun toissijaisuusperiaatteen mukaisesti. Kyseisessä artiklassa vahvistetun suhteellisuusperiaatteen mukaisesti tässä asetuksessa ei ylitetä sitä, mikä on tarpeen näiden tavoitteiden saavuttamiseksi. |  |