DIGITALEUROPE

EU:n verkko- ja tietoturvadirektiivin (NIS-direktiivi) saattaminen osaksi kansallista lainsäädäntöä

Bryssel, 5 Heinäkuu 2016

TIIVISTELMÄ

Euroopan unionin neuvosto julkaisi verkko- ja tietoturvadirektiivin (NIS-direktiivi) lopullisen version 21. huhtikuuta 2016. Vaikka Euroopan parlamentin onkin muodollisesti allekirjoitettava direktiivi tänä kesänä, kolme EU:n toimielintä on hyväksynyt itse tekstin eikä sen odoteta muuttuvan. Jäsenvaltioiden on saatettava direktiivi osaksi kansallista lainsäädäntöään 21 kuukauden kuluessa direktiivin hyväksymisestä. Tätä prosessia auttaaksemme olemme laatineet liitteeksi ohjeet parhaiksi käytännöiksi, joiden avulla teknologia-alalle olennaiset asiat voidaan panna tehokkaasti täytäntöön direktiivin laatijoiden tarkoitusperien mukaisesti.

EU:n NIS-direktiivi on ensimmäinen yleiseurooppalainen kyberturvallisuutta käsittelevä lainsäädäntö. Se keskittyy kyberturvallisuusviranomaisten toiminnan vahvistamiseen kansallisella tasolla ja viranomaisten välisen yhteistyön lisäämiseen. Direktiivi tuo mukanaan myös avaintoimialoja koskevia turvallisuusvaatimuksia.

Kaiken kansallisen toimeenpanolainsäädännön pitää huomioida direktiivin kaksi päätavoitetta: (1) maan kriittisten infrastruktuurien kyberturvallisuuden korkean tason varmistaminen, (2) EU:n jäsenvaltioiden välisen tehokkaan yhteistyömekanismin vakiinnuttaminen ensimmäisen tavoitteen edistämiseksi. Resursseja olisi varattava ennen kaikkea näiden kahden tärkeän tavoitteen saavuttamiseen.

Teknologia-alalla erityisen kiinnostuksen kohteena ovat ns. digitaalisen palvelun tarjoajiin liittyvät säännökset. Direktiivissä todetaan selvästi, että keskeisten palvelujen tarjoajien ja digitaalisen palvelun tarjoajien välillä on perustavanlaatuisia eroja. Viimeksi mainittuja ei pidetä sinänsä kriittisenä infrastruktuurina. Kuten lainsäädännössä todetaan, näihin digitaalipalveluihin vaikuttava poikkeama aiheuttaisi selvästi alhaisemman riskin maan taloudelliselle ja yleiselle turvallisuudelle. On olennaista pitää mielessä tämä ero, jotta sääntöjä valvovien ja täytäntöönpanevien viranomaisten vähäiset resurssit voidaan hyödyntää vaikuttavasti ja tehokkaasti.

Edellä esitetyn vuoksi, kehotamme pitämään tiukasti mielessä, mikä on direktiivin tarkoitettu **soveltamisala.** Päätöksentekijöiden tulisi kansallisessa lainsäädännössä kohdistaa turvallisuusvaatimuksia vain niihin sektoreihin, jotka on määritelty keskeisten palvelujen tarjoajiksi ja digitaalisen palvelun tarjoajiksi.

Lainkäyttövallan osalta digitaalisen palvelun tarjoajien pitäisi pystyä vetoamaan päätoimipaikkansa sijaintimaassa sovellettavaan lakiin myös tapauksissa, joihin liittyy useamman kuin yhden maan toimivaltaisia viranomaisia. Valvonnan osalta toimivaltaisten viranomaisten olisi noudatettava jälkikäteistä toimintatapaa sen sijaan, että määrättäisiin digitaalisen palvelun tarjoajien valvontaa koskeva yleinen velvoite. Lisäksi viranomaisten olisi keskityttävä tuloksiin ja säilytettävä keskeisten palvelujen tarjoajien ja digitaalisen palvelun tarjoajien välinen ero siten, ettei viimeksi mainittuihin sovelleta vaatimuksia, joita direktiivi ei edellytä, kuten tarkastuksia ja sitovia ohjeita.

Perustuen direktiivin toteamukseen, jonka mukaan digitaalisen palvelun tarjoajat edustavat selvästi alhaisempaa turvallisuusriskiä, digitaalisen palvelun tarjoajiin olisi sovellettava erilaisia turvallisuustoimenpiteitä kuin

DIGITALEUROPE
Rue de la Science, 14 - 1040 Bryssel [Belgia]
Puh.: +32 (0) 2 609 53 10 Faksi: +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Komission avoimen datan portaalin jäsen: 64270747023-20

keskeisten palvelujen tarjoajiin. Näiden palvelujen osalta päätöksentekijöiden olisi toteutettava yhdenmukaistamistavoite, otettava huomioon alan käytössä olevat kansainväliset standardit, vältettävä teknologia-mandaatteja ja kunnioitettava direktiiviin kirjattua digitaalisen palvelun tarjoajien oikeutta määritellä parhaiten järjestelmiinsä sopivat turvallisuustoimenpiteet. Poikkeamista ilmoittaminen olisi myös niin pitkälle kuin mahdollista yhdenmukaistettava Euroopan tasolla. Tällöin olisi keskityttävä palvelun jatkuvuuteen vaikuttaviin poikkeamiin, sovellettava joustavuutta ilmoitusten ajoituksessa ja luotava luotettava ympäristö, joka rohkaisee tiedonjakoon kasvattamatta ilmoittavan osapuolen vastuuta.

Keskeisten palvelujen tarjoajille määrätyt toimenpiteet vaikuttavat myös muihin toimialoihin, kun turvallisuustoimenpiteet ja poikkeamista ilmoittaminen siirtyvät ketjussa alaspäin sopimusehtoihin. Tämä pätee etenkin pilvipalveluihin. Sen vuoksi digitaalisen palvelun tarjoajiin saatetaan välillisesti soveltaa niiden asiakkaiden kansallisia lakeja ja siksi tarvitsemme näihin palveluihin sovellettavia, kansainvälisesti tunnustettuja turvallisuustoimenpiteitä. Ehdotamme myös keskeisten palvelujen tarjoajien ja digitaalisen palvelun tarjoajien **ilmoitusvaatimusten** mahdollisimman hyvää yhteensovittamista ja synergiaa, koska digitaalisen palvelun tarjoajat todennäköisesti joutuvat tekemään ilmoituksensa kahdesti.

Direktiivin tavoite on verkko- ja tietojärjestelmien yhteinen korkeatasoinen turvallisuus, joka parantaa sisäisten markkinoiden toimintaa. Jotta tämä vaativa tavoite saavutettaisiin, direktiivin **saattamisessa osaksi kansallista lainsäädäntöä on keskityttävä riskiperustaiseen, yhdenmukaistettuun ja kansainväliseen lähestymistapaan**. Siten yksityisen sektorin toimijat voivat joustavasti sopeutua jatkuvasti muuttuvaan uhkaympäristöön, kyberviranomaiset voivat keskittää rajalliset resurssit tärkeimpiin haasteisiin ja voidaan huomioida se, että ongelmaan, joka ei tunnusta valtiorajoja, on löydettävä globaali ratkaisu. Toivomme, että näistä neuvoista on hyötyä tavoitteen saavuttamisessa ja vastaamme mielellämme mahdollisiin lisäkysymyksiin.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Bryssel [Belgia]
Puh.: +32 (0) 2 609 53 10 Faksi: +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Komission avoimen datan portaalin jäsen: 64270747023-20

Liite: Parhaat käytännöt NIS-direktiivin saattamiseksi osaksi kansallista lainsäädäntöä

1. Digitaalisen palvelun tarjoajat

a) Soveltamisala

- Direktiivin mukaan verkossa toimivia markkinapaikkoja, verkossa toimivia hakukoneita ja pilvipalveluja pidettäisiin digitaalisen palvelun tarjoajina ja ne sisältyisivät siten direktiivin soveltamisalaan. Vaikka kyseessä on vähimmäistason yhdenmukaistamista koskeva direktiivi (3 artikla), on tärkeää säilyttää johdonmukaisuus koko EU:n alueella, eikä jäsenvaltioiden siten pitäisi soveltaa kansallisen lainsäädännön turvallisuusvaatimuksia muihin kuin keskeisten palvelujen tarjoajiksi tai digitaalisen palvelun tarjoajiksi määriteltyihin aloihin siten kuin ne on määritelty 4 artiklassa.

- Direktiivissä mainitaan nimenomaisesti, että laitteistojen valmistajat tai ohjelmistojen kehittäjät eivät ole keskeisten palvelujen tarjoajia tai digitaalisen palvelun tarjoajia, eivätkä ne siten kuulu kansallisten direktiivin täytäntöönpanolakien piiriin (johdanto-osan kappale 50).

- Direktiivissä suljetaan nimenomaisesti soveltamisalan ulkopuolelle verkkokauppojen osalta ne verkkopalvelut, jotka toimivat välittäjinä kolmansien osapuolien tarjoamille palveluille, joiden kautta myynti- tai palvelusopimus lopulta tehdään (esim. vertailusivustot) (johdanto-osan kappale 15).

- Verkossa toimivan hakukoneen määritelmän ei tulisi kattaa hakutoimintoja, jotka rajoittuvat tietyn verkkosivuston sisältöön, vaikka toiminnoissa hyödynnettäisiin ulkopuolista palveluntarjoajaa (johdanto-osan kappale 16).

- Direktiivin mukainen pilvipalvelujen määritelmä riippuu siitä, jaetaanko pilvipalveluresursseja useampien käyttäjien kesken (4 artiklan 19 kohta ja johdanto-osan kappale 17). Koska yksityiset pilvipalvelut (toisin kuin julkiset pilvipalvelut) on tarkoitettu yksittäiselle organisaatiolle, niiden ei pitäisi katsoa kuuluvan määritelmän piiriin.

- Direktiivissä korostetaan, että keskeisten palvelujen tarjoajien ja digitaalisen palvelun tarjoajien välillä on perustavanlaatuisia eroja, ja siksi digitaalisen palvelun tarjoajiin sovelletaan erilaisia sääntöjä (johdanto-osan kappale 57). Tämä ero pitäisi säilyttää direktiivin täytäntöönpanon yhteydessä.

b) Lainkäyttövalta ja valvonta

- Digitaalisen palvelun tarjoajia koskeva lainkäyttövalta olisi annettava vain yhdelle jäsenvaltiolle, jossa digitaalisen palvelun tarjoajalla on päätoimipaikka EU:ssa. Se vastaa periaatteessa paikkaa, jossa palvelun tarjoajalla on pääkonttori EU:ssa (18 artiklan 1 kohta ja johdanto-osan kappale 64). Mielestämme digitaalisen palvelun tarjoajien olisi määriteltävä asia itse, ja päätöstä olisi tarkistettava vain, jos toimivaltaiset viranomaiset kiistävät sen jälkikäteen toteutettavien valvontatoimien yhteydessä.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Bryssel [Belgia]
Puh.: +32 (0) 2 609 53 10 Faksi: +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Komission avoimen datan portaalin jäsen: 64270747023-20

- Kun digitaalisen palvelun tarjoajilla on verkko- ja tietojärjestelmiä muualla kuin siinä maassa, jossa niiden päätoimipaikka sijaitsee, 17 artiklan 3 kohdassa säädetään toimivaltaisten viranomaisten yhteistyöstä. Digitaalisen palvelun tarjoajien näkökulmasta on kuitenkin tärkeää, että sovelletaan edelleen päätoimipaikan maan lakia ja että ne ovat vastuussa vain tämän lainkäyttövallan toimivaltaiselle viranomaiselle, joka toimii vuoropuhelun osapuolena.

- Direktiivissä korostetaan, että koska digitaalisen palvelun tarjoajiin sovelletaan reaktiivisia jälkikäteen toteutettavia valvontatoimia, toimivaltaisella viranomaisella ei ole yleistä velvoitetta valvoa digitaalisen palvelun tarjoajia ja sen olisi ryhdyttävä toimenpiteisiin vain, jos sille esitetään näyttöä. (17 artiklan 1 kohta ja johdanto-osan kappale 60). Näitä säännöksiä olisi noudatettava direktiivin täytäntöönpanon yhteydessä.

- Toisin kuin keskeisten palvelujen tarjoajien ollessa kyseessä, viranomaiset voivat digitaalisen palvelun tarjoajilta vain pyytää tietoja ja vaatia, että digitaalisen palvelun tarjoajat korjaavat kaikki virheet. Direktiivissä tehdään selväksi, että viranomaisilla ei ole tarkastusvaltuuksia eivätkä ne voi antaa sitovia ohjeita. Näitä säännöksiä olisi noudatettava myös kansallisella tasolla.

c) Lisävaatimukset

- Digitaalisen palvelun tarjoajien turvallisuus- ja ilmoitusvaatimuksiin sovelletaan mahdollisimman voimakasta yhdenmukaistamista (16 artiklan 10 kohta). Tämän artiklan tulisi ajatella koskevan palvelun tarjoajien verkko- ja tietojärjestelmien perustana olevia tuotteita, palveluja ja ratkaisuja. Sen vuoksi lisävaatimuksia, kuten tuotetestausta, ei tule asettaa, jos tuotteita ja palveluja käytetään tässä yhteydessä.

d) Turvallisuustoimenpiteet ja -standardit

- Digitaalisen palvelun tarjoajiin olisi sovellettava kevyempiä turvallisuustoimenpiteitä kuin keskeisten palvelujen tarjoajiin. Digitaalisen palvelun tarjoajien olisi voitava vapaasti määritellä, kuinka ne hoitavat turvallisuusasiat ja kuinka ne varmistavat verkko- ja tietojärjestelmiensä suojan niihin kohdistuvan riskin suuruuteen sopeutetusti (johdanto-osan kappale 49).

- Turvallisuustoimenpiteiden olisi oltava prosessisuuntautuneita ja keskityttävä riskinhallintaan. Ne eivät saisi edellyttää, että tieto- tai viestintäteknologiatuotteet suunnitellaan, kehitetään tai valmistetaan tietyllä tavalla (johdanto-osan kappale 51).

- Direktiivissä korostetaan, että jäsenvaltio ei saa määrätä mitään lisäturvallisuusvaatimuksia digitaalisen palvelun tarjoajille (16 artiklan 10 kohta).

- Odotamme ohjeita useilta toimijoilta. Jäsenvaltiot varmistavat, että direktiivissä hahmotellut toimenpiteet hyväksytään (16 artiklan 1 kohta). Ne voivat kannustaa käyttämään toimenpiteiden käyttöönottoon tähtääviä standardeja (19 artiklan 1 kohta) ja keskustella standardeista eurooppalaisten standardointijärjestöjen kanssa yhteistyöryhmässä (11 artiklan 3 kohdan h alakohta). ENISA antaa neuvoja asianmukaisista standardeista (19 artiklan 2 kohta) ja Euroopan komission vastuulla on hyväksyä turvallisuustoimenpiteitä koskevia täytäntöönpanosäädöksiä (16 artiklan 8 kohta).

- Kun otetaan huomioon toiminnan monimutkaisuus ja yhdenmukaistamisesta saatavat edut, suosittelemme, että kansallisessa menettelyssä pääosin odotetaan täytäntöönpanosäädöksiä ennen kuin sovitaan asianmukaisista toimenpiteistä. Täytäntöönpanosäädökset on joka tapauksessa saatettava valmiiksi vuoden kuluessa direktiivin voimaantulosta. Täytäntöönpanosäädökset eivät itsessään saa vaarantaa digitaalisen palvelun tarjoajien kykyä määrittää niiden järjestelmiin parhaiten soveltuvat turvallisuustoimenpiteet.

- Standardeja koskevan artiklan mukaisesti voidaan vedota eurooppalaisiin tai kansainvälisesti hyväksyttyihin standardeihin (19 artiklan 1 kohta). Kun otetaan huomioon alalla olemassa olevien kansainvälisten standardien kypsyysaste, suosittelemme asianmukaisten standardien ollessa olemassa, että sertifiointi tällaisen standardin mukaisesti (kuten ISO 27001) olisi riittävä osoitus vaatimusten noudattamisesta.

- Standardisertifioinnin pitäisi joka tapauksessa olla vapaaehtoista, ei pakollista. 19 artiklassa painotetaan, että minkä tahansa standardin käyttöön voidaan vain kannustaa ilman että jäsenvaltiot ”määräävät käyttämään jotain tiettyä teknologiaa tai harjoittavat syrjintää jonkin tietyn teknologian käytön suosimiseksi.”

e) Turvapoikkeamista ilmoittaminen

- NIS-direktiivin mukaisesti sekä turvallisuustoimenpiteiden että myös poikkeamien ilmoittamismenettelyjen muokkaamiseen osallistuvat useat osapuolet. Jäsenvaltioiden on varmistettava, että digitaalisen palvelun tarjoajat ilmoittavat niistä turvapoikkeamista, joilla on merkittävä vaikutus niiden tarjoaman (direktiivin soveltamisalaan kuuluvan) palvelun tarjoamiseen (16 artiklan 3 kohta), yhteistyöryhmän tehtävänä on keskustella ilmoituksia koskevista järjestelyistä (11 artiklan 3 kohdan m alakohta) ja komissio hyväksyy täytäntöönpanosäädökset (16 artiklan 8 ja 9 kohta).

- Suosittelemme tämänkin osalta, että kansalliseen lainsäädäntöön saattamisessa odotetaan täytäntöönpanosäädöksiä, joiden puitteissa ilmoittamiskynnystä koskeva täytäntöönpanosäädös on hyväksyttävä vuoden kuluessa direktiivin voimaantulosta.

- Mitä tulee ilmoitettavaa poikkeamatyyppiä koskeviin ehtoihin, digitaalisen palvelun tarjoajien on ilmoitettava “kaikista poikkeamista, joilla on merkittävä vaikutus [niiden] palvelun tarjoamiseen” (16 artiklan 3 kohta). Kuten televiestintäoperaattorien puitedirektiivin 13a artiklan vastaavien säännösten täytäntöönpanossa, uskomme että tämänkin tulkinnassa olisi painotettava tarjottujen palvelujen **jatkuvuutta (tai saatavuutta)**. Toisin sanoen, palvelukatkoksista jotka ylittävät tietyn kynnysrajan (joka määritetään täytäntöönpanosäädöksissä) olisi ilmoitettava ennemminkin kuin muun tyyppisistä turvapoikkeamista. Näin voidaan keskittyä talouteen tai yhteiskuntaan kaikkein todennäköisimmin vaikuttaviin poikkeamiin ja samalla minimoida (vaikkakaan ei kokonaan poistaa) päällekkäisyys, joka syntyy yleistä tietosuojaa koskevan asetuksen ilmoitusvaatimuksista henkilötietoja koskevissa rikkomuksissa.

- Lisäksi keskeisten palvelujen tarjoajia koskevassa ilmoitusvelvoitteessa määritellään, että näiden toimijoiden on ilmoitettava “poikkeamista, joilla on merkittävä vaikutus niiden tarjoamien palvelujen jatkuvuuteen”. Tässä painotetaan jälleen selkeästi palvelun jatkuvuutta (tai saatavuutta). Lainsäätäjien

mukaan digitaalisen palvelun tarjoajien velvoitteiden olisi oltava kevyempiä kuin keskeisten palvelujen tarjoajien velvoitteiden (johdanto-osan kappale 49). NIS-direktiivin mukaisen digitaalisen palvelun tarjoajien poikkeamien ilmoittamisvelvoitteen ei siten pitäisi olla laajempi kuin keskeisten palvelujen tarjoajien velvoitteen ja tämän eron pitäisi näkyä velvoitteiden kynnysarvoissa. Samalla korostuu edelleen, että digitaalisen palvelun tarjoajien poikkeamailmoitukset olisi rajoitettava poikkeamiin, jotka ylittävät tietyn kynnysarvon ja **vaikuttavat palvelun jatkuvuuteen/saatavuuteen.** Ilmoituksia ei tulisi edellyttää poikkeamista, jotka liittyvät tietojen eheyteen tai luottamuksellisuuteen, koska nämä tapaukset on jo suurelta osin katettu GDPR- ja eIDAS-asetusten mukaisissa ilmoitusvaatimuksissa.

- Ilmoittamisen ajoituksen osalta olemme tyytyväisiä ilmaisun "ilman aiheetonta viivytystä" sisältämään joustavuuteen (16 artiklan 3 kohta). Täytäntöönpanon ei pitäisi johtaa ehdottomiin määräaikoihin, koska poikkeamien monimutkaisuus vaihtelee suuresti. Yhtäläiset ilmoitusmääräajat johtaisivat epätarkkaan raportointiin, jolloin jäisi epäselväksi kuinka laajasti poikkeamat alun perin kohdistuivat järjestelmiin. Ne vaikuttaisivat myös poikkeamista vastuussa olevien ammattilaisten kykyyn priorisoida poikkeamaan reagointi sen sijaan että he käyttäisivät aikaansa poikkeamaa koskevaan raportointiin.

- Kuten edellä on mainittu, direktiivin mukaisesti ilmoitettavat turvapoikkeamat saattavat edellyttää ilmoittamista myös tietosuojalain mukaisesti, riippuen siitä onko henkilötietoja loukattu. Tämä ei tarkoita ainoastaan sitä, että samasta poikkeamasta on ilmoitettava eri viranomaisille, vaan että nämä viranomaiset voivat jopa sijaita eri jäsenvaltioissa sen mukaan, mitä lainkäyttövaltaa digitaalisen palvelun tarjoajiin sovelletaan näissä kahdessa laissa. Suosittelemme, että jäsenvaltiot huomioivat tämän ongelman ja pyrkivät siihen, että poikkeamista tehdään vain yksi ilmoitus ja että luodaan viestintäkanavat jäsenvaltioiden välisten tärkeiden tietojen jakamiseksi vaarantamatta liiketoiminnan luottamuksellisuutta.

- Toimivaltaisten viranomaisten olisi otettava huomioon digitaalisen palvelun tarjoajien maineeseen kohdistuvat vaikutukset sekä kaupalliset vaikutukset ennen poikkeamatietojen julkistamista. Vielä tärkeämpää on huomioida se, että poikkeamatiedon julkistaminen saattaa lisätä turvallisuusriskiä. Sen vuoksi on tärkeää koordinoida toimintaa kyseessä olevien toimijoiden kesken ennen minkäänlaista julkistamista.

- Direktiivissä korostetaan, että luottamuksellisia tietoja olisi käsiteltävä luottamuksellisina (johdanto-osan kappaleet 41 ja 59 sekä 1 artiklan 5 kohta).

- 16 artiklan 3 kohdassa korostetaan, että turvapoikkeamasta ilmoittaminen ei saa lisätä ilmoittavan osapuolen vastuuta.

2. Keskeisten palvelujen tarjoajat

a) Turvallisuustoimenpidevaatimusten siirtyminen toimittajaketjussa

- Digitaalisen palvelun tarjoajiin, joilla on asiakkaina keskeisten palvelujen tarjoajia, kohdistuu sopimusneuvottelujen yhteydessä soveltuvia turvallisuustoimenpidevaatimuksia, jotka perustuvat keskeisten palvelujen tarjoajia koskeviin säännösvelvoitteisiin (14 artiklan 1 kohta). Näin ollen,

digitaalisen palvelun tarjoajiin voidaan välillisesti soveltaa niiden asiakkaiden kansallista lakia riippumatta digitaalisen palvelun tarjoajien eurooppalaisen pääkonttorin sijaintimaassa sovellettavasta laista.

- Keskeisten palvelujen tarjoajia koskevia turvallisuustoimenpiteitä olisikin pyrittävä yhdenmukaistamaan. Vaikka jäsenvaltioilla on oikeus määrätä keskeisten palvelujen tarjoajille tiukempia velvoitteita kuin mitä direktiivissä on säädetty (3 artikla), suosittelemme pidättäytymään tästä ja rohkaisemme jäsenvaltioita pyrkimään yhdenmukaiseen lähestymistapaan. Tämä voidaan saada aikaan välttämällä lisätoimenpiteitä, jotka liittyvät saattamiseen osaksi kansallista lainsäädäntöä ja määrittämällä asianmukaisia turvallisuustoimenpiteitä yhteistyöryhmässä sen sijaan, että keskityttäisiin kansalliseen menettelyyn.

- Turvallisuustoimenpiteiden olisi perustuttava mahdollisimman pitkälti kansainvälisiin standardeihin (kuten ISO 27x -sarja) ja tunnustettuihin parhaisiin turvallisuuskäytäntöihin.

- Keskeisten palvelujen tarjoajille määrätyissä turvallisuustoimenpiteissä ei saisi missään tapauksessa edellyttää tietyn tieto- ja viestintäteknologiatuotteen suunnittelua, kehittämistä tai valmistamista tietyllä tavalla (johdanto-osan kappale 51).

b) Turvapoikkeamien ilmoittamisvaatimusten siirtyminen toimittajaketjussa

- Keskeisten palvelujen tarjoajien on ilmoitettava turvapoikkeamista, jotka koskevat niiden kanssa sopimussuhteessa olevia digitaalisen palvelun tarjoajia ja jotka vaikuttavat keskeisten palvelujen tarjoamiseen (16 artiklan 5 kohta). Digitaalisen palvelun tarjoajien on siten sopimuksen mukaisesti ilmoitettava kyseiselle keskeisten palvelujen tarjoajalle näihin mahdollisesti vaikuttavista turvapoikkeamista.

- Arvostamme ajoituksen joustavuutta ilmoittamisessa keskeisten palvelujen tarjoajille, mikä ilmenee ilmaisussa “ilman aiheetonta viivytystä” (14 artiklan 3 kohta). Kun direktiiviä saatetaan osaksi kansallista lainsäädäntöä, ei pitäisi ottaa käyttöön tarkkoja määräaikoja. Joka tapauksessa, jos keskeisten palvelujen tarjoajia pyydetään perustelemaan ilmoittamiseen kulunut aika, niitä koskevan arviointijakson pitäisi alkaa siitä hetkestä, jolloin keskeisten palvelujen tarjoaja on saanut tiedon poikkeamasta eikä siitä hetkestä, jolloin digitaalisen palvelun tarjoaja on tullut tietoiseksi poikkeamasta.

- 14 artiklan 7 kohdassa mainitaan, että yhteistyöryhmä voisi luoda suuntaviivoja niistä tilanteista, joissa keskeisten palvelujen tarjoajien edellytetään ilmoittavan poikkeamista sen sijaan, että komissio yhdenmukaistaisi digitaalisen palvelun tarjoajien ilmoitustehtävää. Kun otetaan huomioon digitaalisen palvelun tarjoajien kaksinkertainen ilmoitusvaatimus, on tärkeää, että ilmoitusvelvoitteet eivät ole ristiriitaisia ja niitä yhdenmukaistetaan mahdollisimman paljon. Menettelyä olisi tarkasteltava tätä tavoitetta vastaan. Lisäksi digitaalisen palvelun tarjoajien ilmoitusvaatimuksissa olisi kunnioitettava niiden luottamuksellisuusvelvoitteita asiakkaitaan eli keskeisten palvelujen tarjoajia kohtaan, eikä digitaalisen palvelun tarjoajia pitäisi pyytää jakamaan luottamuksellisia liiketoimintatietoja.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Bryssel [Belgia]
Puh.: +32 (0) 2 609 53 10 Faksi: +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Komission avoimen datan portaalin jäsen: 64270747023-20

TIETOJA DIGITALEUROPESTA

DIGITALEUROPE edustaa digitaaliteknologia-alaa Euroopassa. Jäseniimme kuuluu joitakin maailman suurimpia IT-alan sekä televiestintä- ja kuluttajaelektroniikan yhtiöitä ja kansallisia yhdistyksiä kaikkialta Euroopasta. DIGITALEUROPEn tavoitteena on, että eurooppalaiset yritykset ja kansalaiset voivat hyötyä täysimittaisesti digitaaliteknologioista. Se pyrkii myös Euroopan kasvuun ja siihen, että Eurooppa houkuttelee puoleensa pysyvästi maailman parhaimpia digitaaliteknologia-alan yrityksiä.

DIGITALEUROPE varmistaa alan osallistumisen EU:n käytäntöjen kehittämiseen ja täytäntöönpanoon. DIGITALEUROPEssa on 62 yritysjäsentä ja 37 kansallista teollisuusyhdistystä eri puolilta Eurooppaa. Verkkosivustollamme on lisätietoja DIGITALEUROPEn viimeaikaisista uutisista ja toiminnasta: http://www.digitaleurope.org

DIGITALEUROPEN JÄSENYYS

Yritysjäsenet

Airbus, Amazon Web Services, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cisco, Dell, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Ingram Micro, Intel, iQor, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric IT Corporation, Sharp Electronics, Siemens, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies, ZTE Corporation.

Kansalliset toimialayhdistykset

Alankomaat: Nederland ICT, FIAR
Belgia: AGORIA
Bulgaria: BAIT
Espanja: AMETIC
Irlanti: ICT IRELAND
Iso-Britannia: techUK
Italia: ANITEC
Itävalta: IOÖ
Kreikka: SEPE
Kypros: CITEA
Liettua: INFOBALT
Portugali: AGEFE
Puola: KIGEIT, PIIT, ZIPSEE
Ranska: AFNUM, Force Numérique, Tech in France
Romania: ANIS, APDETIC
Ruotsi: Föreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Saksa: BITKOM, ZVEI
Slovakia: ITAS
Slovenia: GZS
Sveitsi: SWICO
Suomi: Teknologiateollisuus ry
Tanska: DI Digital, IT-BRANCHEN
Turkki: Digital Turkey Platform, ECID
Ukraina: IT UKRAINE
Unkari: IVSZ
Valko-Venäjä: INFOPARK
Viro: ITL