GDPR:n tarkastusoikeus käytännössä?

TIETOSUOJAVASTAAVIEN FOORUMI

ASIANTUNTIJAKYSELYN TULOKSET 2019

TIFO

POWERED BY ASML

tifo.fi

TARKASTUSOIKEUS

EU:n tietosuoja-asetuksen ns. tarkastusoikeus (Right of Access) ja sen käytännön soveltaminen ja tulkinnat ovat keskusteluttaneet eri puolella EU:ta ja myös EU:n ulkopuolella.

SELVITYS

Tietosuojavastaavien Foorumi (TIFO) teki TIFO:n tietosuoja-ammattilaisille kyselyn asian tiimoilta. Yli 40 yrityksen edustajat kertoivat kokemuksistaan. Kyselyn tuloksia on kirjattu tähän julkaisuun. Jakaumat on ilmaistu prosentteina. Mukana on myös havaintoja oikeuskäytännöstä EU:sta ja asiaan liittyvästä uutisoinnista.

TIFO

DIALOGILLA ETEENPÄIN

Rekisteröidyn oikeudet ovat tärkeä osa yksityisyyden suojan toteutumista. Modernin tarkastusoikeuden tasapainoinen toteutuminen edellyttää eri tahojen välillä jatkuvaa dialogia, jota tämä selvitys osaltaan haluaa edistää.

Koosteen tekijä: Jari Perko ASML/TIFO, jari@asml.fi, @asiakkuus

GDPR:n tarkastusoikeus-artikla

Article 15 Right of access by the data subject

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:
(a) the purposes of the processing;
(b) the categories of personal data concerned;
(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
(f) the right to lodge a complaint with a supervisory authority;
(g) where the personal data are not collected from the data subject, any available information as to their source;
(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Muita kuin GDPR-prosessin mukaisia rekisteröityjen tarkastusoikeuspyyntöjä kertoi vastaajista saaneensa **48%**

Jäljempänä on avattu kyselyn tuloksia seuraavista tyyppitapauksista

1. Pyydetty tietoja joihin ei oikeutta
2. Pyydetty muulla kuin ohjeistetulla tavalla
3. Pyyntöjä tehty ns. testaustarkoituksessa
4. Pyynnöt aktivismi/häiritsemis/ilkivalta- tms. tarkoituksessa
5. Pyyntö tehty muun kuin rekisteröidyn toimesta

- GDPR:n myötä, ja toki jo ennen sitä, tarkastusoikeuden toteuttamiselle on ollut säännellyt peruskehykset ja rajaukset.
- Käytännön toteutustapoja voi olla erilaisia ja ne vaihtelevatkin usein rekisterinpitäjien välillä.
- On hyvä muistaa että rekisterinpitäjä on vastuussa pyytäjän luotettavasta tunnistamisesta, annettavien tietojen asianmukaisesta rajaamisesta ja kolmansien osapuolten oikeuksien suojaamisesta.

TIFO

PALVELULLISTAMINEN NOUSUSSA - Eräät yritykset ovat kehittäneet asiakkaan omien tietojen pohjalta sähköisiä palvelukokonaisuuksia, jotka tarjoavat erilaisia dataan perustuvia palveluja ja hyötyjä asiakkaille.

1. Onko pyyntö kohdistunut tietoihin joihin tarkastusoikeus ei ulotu?

27%

vastaajista kertoi yrityksen saaneen tällaisia pyyntöjä

POIMINTOJA VASTAAJIEN KOMMENTEISTA

- Pyyntöjä on kohdistunut tietoihin, joiden luovuttamista rajoitetaan muussa laissa.
- On tullut esimerkiksi lehtien juttuihin ja kuviin liittyviä pyyntöjä.
- On pyydetty lokitietoja joita ei voida luovuttaa.
- Tietoja on pyydetty muista henkilöistä.
- Pyyntöjä on kohdistettu salassapidettäviin tietoihin.

TIFO

Case - ”Kaverin tiedoilla kyselen”

James Pavur lähetti tyttöystävänsä suostumuksella tarkastusoikeuspyyntöjä 150 yritykselle.

- Pavur loi testiään varten tyttöystävänsä nimelle uuden käyttämättömän gmail-osoitteen.
- Hän lähetti naisen nimissä tarkastusoikeuspyyntöjä 150 yritykselle USA:ssa ja UK:ssa. 83:llä näistä oli tietoja tyttöystävästä.
- Yli 20 yritystä luovutti tietoja Pavurille tunnistusta tarkemmin tekemättä. Pavur sai mm. passitietoja, tietoja hotelliyöpymisistä, rikosrekisterikyselyn tulokset ja tietoja sukulaisista.
- Testin tulokset esitettiin Black Hat-konferenssissa elokuussa 2019.

Case - UK:n tietosuojaviranomainen

TIFO

Henkilö oli ”pommittanut” UK:n tietosuojaviranomaista vuosien ajan viesteillä ja tarkastusoikeuspyynnöillä. ICO kieltäytyi 2019 enää vastaamasta henkilön pyyntöihin lausuen mm.

”…since May 2018 we have received in excess of 290 items of correspondence from you. Many of these communications have included unsubstantiated accusations of the ICO’s complicity in various crimes and have targeted members of ICO staff with the intention of causing distress…Your requests for information under Article 15 of the GDPR appear to be similarly motivated. We consider that these requests are not made to legitimately establish what information we hold and how we are handling your personal data, but part of a campaign to challenge the decisions that have already been concluded within due process…”

[lähde: 2040infolawblog.com]

2. Onko pyyntö tehty muulla tavalla kuin olette rekisterinpitäjänä ohjeistaneet ?

Kolmannes vastaajista kertoi yrityksen saaneen tällaisia pyyntöjä

POIMINTOJA VASTAAJIEN KOMMENTEISTA

- Tullut soittoja vaihteeseen ja sekä sähköpostipyyntöjä – ”haluan tietoni heti”
- Pyyntöjä tullut Facebookin privaviestillä
- Tullut myös pyyntöjä joissa asiakas ei halua tunnistautua riittävästi
- Pyyntöjä tullut kolmannen osapuolen kautta
- Yrityksen johdolle osoitetun reklamaatiosähköpostin osana

TIFO

3. Onko pyyntöjä tehty ns. testaus-tarkoituksessa?

Pyyntöjä testaustarkoituksessa arvioi saaneensa

20%

POIMINTOJA VASTAAJIEN KOMMENTEISTA

- Tällaisia pyyntöjä on tullut kilpailijoilta, toimittajilta, lakiopiskelijoilta ja ns. ammattivalittajilta.
- Tällaisia tehtiin lähinnä heti GDPR:n jälkeen jolloin haastettiin yrityksen toimintamallia ja tapaa tunnistaa henkilö.
- Jutun tekotarkoituksessa journalisteilta, jotka ovat itse olleet myös asiakkaita.

TIFO

PYYNTÖÖN VASTAAMISEN LAAJUUDESTA

Digitaalisten palveluiden jokapäiväisen käytön ja sitä myöten alati kertyvän ”datajalanjäljen” myötä on eri puolella EU:ta keskusteltu tarkastusoikeuden käytännön laajuudesta. On keskusteltu esimerkiksi sitä mitä vanhasta tietosuojadirektiivistä GDPR:ään siirtynyt 15 artiklan ”copy”-termi käytännössä oikein tarkoittaa?

Tulkintaa Saksasta

Baijerin tietosuojaviranomainen on GDPR:ää koskevassa ohjeistuksessaan (Datenschutzreform 2018) linjannut, että tarkastusoikeudesta kyseessä on enemmänkin strukturoitu yhteenveto käsiteltävistä tiedoista kuin jokaisen yksittäisen tiedon saamisesta, ”im Sinne einer sinn voll strukturierten Zusammenfassung”.

Kölninissä oli tuomioistuimessa (LG Köln 26 O 25/18) puolestaan taannoin tapaus, jossa laajuuden problematiikka oli esillä. Henkilö oli pyytänyt vakuutusyhtiöltä hyvin yksityiskohtaisia tietoja esim. puhelumuistiinpanoja ja yksittäisiä viestejä. Vaikka tuomioistuin lausui yleisesti päätöksessään yllä selostetun Baijerin viranomaisen ohjauksen suuntaisesti niin se kuitenkin katsoi, että henkilöllä tulisi olla pääsy tällaiseenkin tietoon. Toisaalta lausuttiin myös, että tietyntyyppiset sisäiset arvioinnit ja analyysit eivät olisi olisi kokonaisuutena tarkastusoikeuden tarkoittamaa henkilötietoa. Tulkinnat ja keskustelut jatkuvat.

TIFO

4. Onko pyyntöjä tehty aktivismi/häiritsemis/ilkivalta- tai muussa vastaavassa tarkoituksessa?

18%

on saanut tällaisia pyyntöjä

POIMINTOJA VASTAAJIEN KOMMENTEISTA

- Rekisteröity ilmoitti että aikoo jatkossa tehdä tarkastuspyynnön säännöllisesti puolen vuoden välein.
- Pyytäjien itse keksimiä aikarajoitteita ja jopa rahallisia kiristystyyppisiä vaatimuksia.
- Protestityyppisiä pyyntöjä reaktiona johonkin asiakkaan tilanteeseen esim. epätyydyttävä ratkaisu reklamaatioprosessissa.
- Eräät ovat jopa myöntäneet, että haluavat aiheuttaa pyynnöllä mahdollisimman paljon haittaa, koska eivät ole olleet tyytyväisiä johonkin palveluun.
- Tietoisesti tehtyjä aivan ylimitoitettuja tietopyyntöjä.

TIFO

5. Onko pyyntöjä on tehty muun kuin rekisteröidyn toimesta?

Tällaisia oli saanut **viidennes (20%)** vastaajista

POIMINTOJA VASTAAJIEN KOMMENTEISTA

- Henkilö on pyytänyt saada puolisonsa tietoja.
- Yritetty saada sukulaisten tietoja näiden yhteystiedoilla.
- Edunvalvojan valvottavaansa koskeva pyyntö (sisältyykö valvontamääräykseen?).
- Pyyntöjä henkilön edustamalta palveluntarjoajalta esimerkiksi yleisluonteisella sähköpostilla.

TIFO

Koosteen tekijä: Jari Perko ASML/TIFO, jari@asml.fi, @asiakkuus

tifo.fi