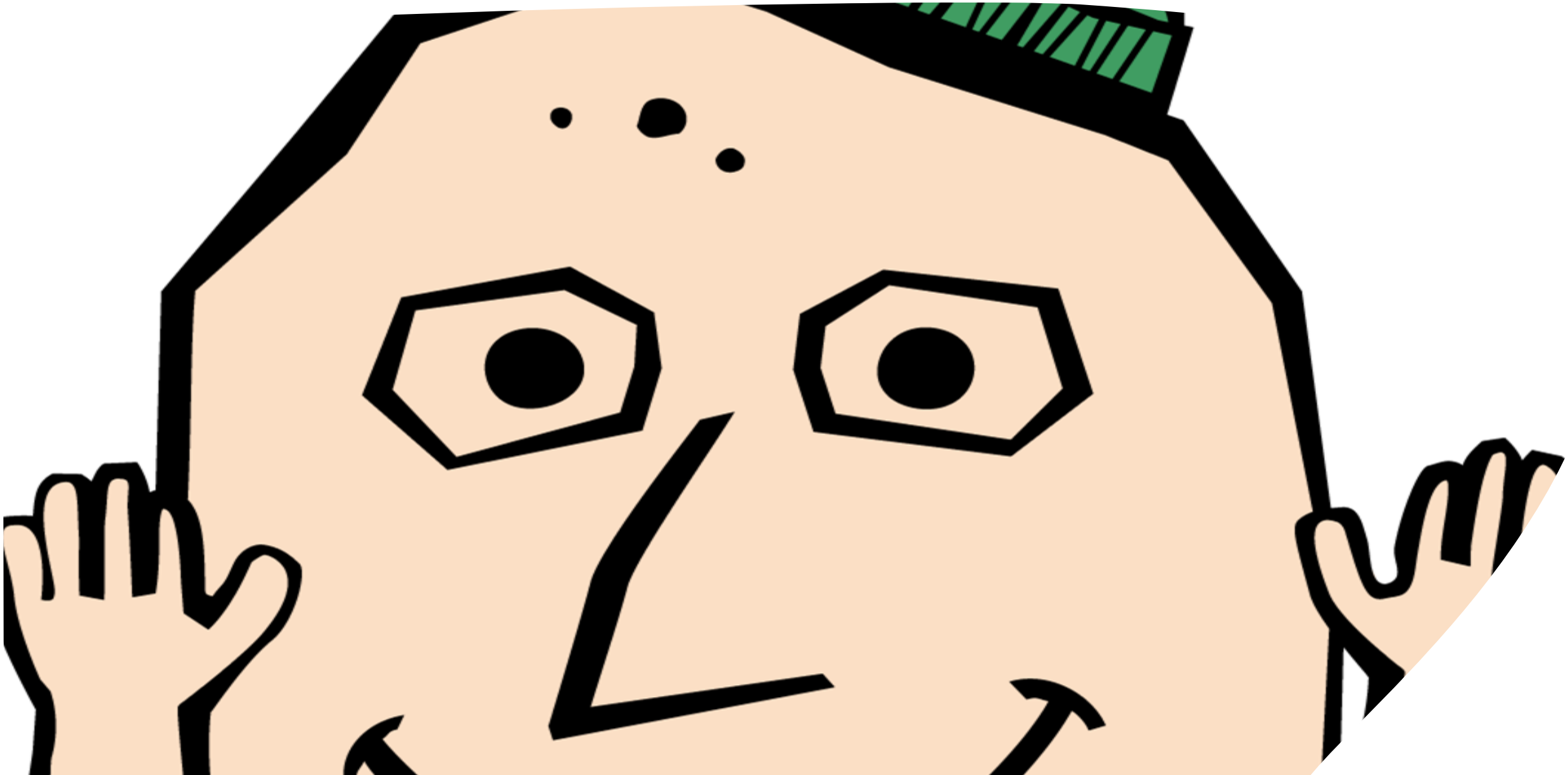
Kokonaiskuva tietosuoja-asetuksesta

General Data Protection Regulation,GDPR

Trafi



EU:n yleinen tietosuoja-asetus

Yleinen tietosuoja-asetus

- Voimaan 24.5.2016
- 2 vuoden siirtymäaika
- 25.5.2018 henkilötietojen käsittelyn on oltava asetuksen mukaista

Mikäli velvoitteita ei ole siirtymäajan päättyessä implementoitu osaksi Trafin toimintaa, on riskinä:

Maineriski tietoviranomaisena

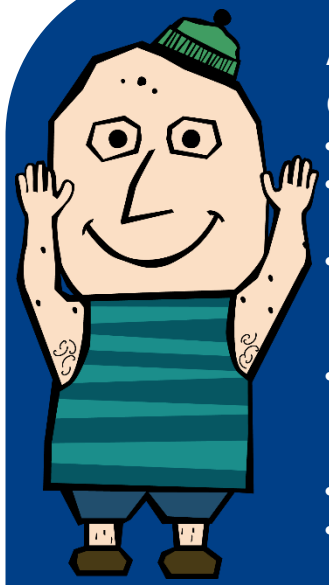
Valvontaviranomaisen sanktiot ja negatiivinen mediajulkisuus

Trafi

Tunnista, määritä ja dokumentoi henkilötietojen käsittelytoimet ja opi niistä uutta sekä täytä samalla asetuksen vaatimukset

Tietosuoja-asetusta **EI** tule lähestyä hallinnollisten seuraamusten näkökulmasta

Trafin tietosuojatyöryhmä



Asiakkaalla oikeus

- läpinäkyvyyteen
- saada pääsy omiin tietoihin
- tietojen oikaisemiseen ja poistamiseen
- käsittelyn rajoittamiseen ja vastustamiseen
- estää profilointi
- siirtää tiedot järjestelmästä toiseen

3 4

Asiakkaan henkilötiedot

Sopimus

Rekisteri

Rekisteri

2 Tietoturva-poikkeamien havaitseminen / reagointikyvyk-kyys

Trafi

1 **Sopimuskumppanit**

Vastuut

Sopimuk-sen sisältö

Toiminnan ohjaus

Laadun hallinta

Kehittä-misen hallinta

- **Lupien hallintaprosessit**
- **Tarkastusprosessit**
- **Vaikuttamisprosessit**
- **Verotusprosessit**
- **Tietopalveluprosessit**

- **Sisäänrakennettu ja oletusarvoinen tietosuoja**
- **Tietosuojavastaava**
- **Riskipohjainen lähestymistapa**
- **Osoitusvelvollisuus**

5 6 7 8

1 Työpaketti: Sopimustyöpaketti

Sopimustyöpaketti koskee henkilötietojen käsittelyyn liittyviä toimeksiantosopimuksia

Toimeksianto-sopimusten on täytettävä tietosuoja-asetuksen vaatimukset viimeistään 25.5.2018

Toimialojen selvitettävä, mitkä henkilötietojen käsittelyä sisältävät tehtävät on ulkoistettu.

Jokaisen sopimuksen liitteenä on oltava Trafin tietoturvaliite.

Liitteen päivitys Tietohallintopal-veluissa työn alla.

Trafin lukuun tehtävää henkilötietojen käsittelyä

Tietosuoja-työryhmä tunnistanut jo joitakin sopimuksia

2 Työpaketti: Tietoturvaloukkaukset

Trafi

- Selvitettävä, miten tietoturvaloukkaus havainnoidaan/reagointikyvykkyys
- Luotava tehokas ja kattava kriisi- ja häiriötilanneviestintä
- Määriteltävä tietoturvaloukkauksien dokumentointitapa
- Luotava määrämuotoinen ilmoitusprosessi ja toimintaohjeet

Edellyttää, että on olemassa riski rekisteröidyn oikeuksille ja vapauksille

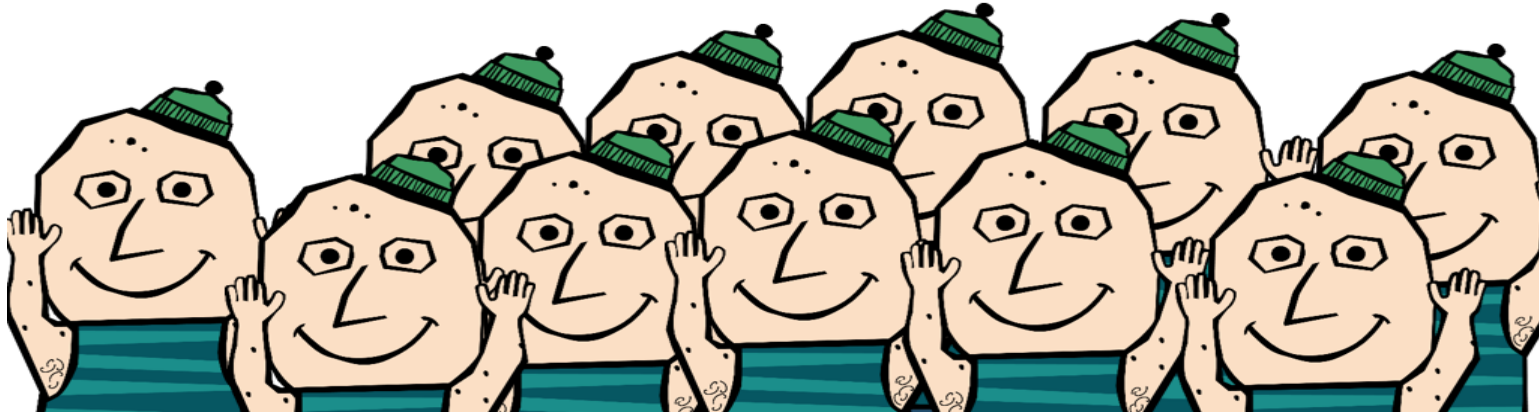
Ilmoitus valvontaviran-omaiselle

Ei tarvitse tehdä, jos esim. vuotaneet henkilötiedot on salattu ja salausavaimet eivät ole vaarantuneet

Ilmoitus rekisteröidylle

Ilmoitus Trafille

Sopimus-kumppanilla tietoturva-loukkaus



3 Työpaketti: Rekisteröidyn oikeudet 1 (läpinäkyvyys)

Trafi

Selosteet käsittely-toimista

Visuaalinen informaatio rekisteröi-dyille

Trafi

Asiakkaiden infopaketit

- Mitä tietoa Yrmystä on rekistereissä?
- Mistä Yrmyn tiedot saadaan Trafin rekistereihin?
- Mihin Yrmyn tietoja käytetään?
- Miten Yrmy voi tarkistaa tietonsa?
- Miten Yrmy saa tietonsa oikaistua?

Trafi.fi

Asiakas keskiössä

Informaatiotarpeiden selvittäminen suoraan asiakkailta

- Miten asiakas haluaa tulla informoiduksi?
- Osallistetaan asiakas (kysely tms.)

4 Työpaketti: Rekisteröidyn oikeudet 2

Trafi

Trafi

Rekisteröidyn oikeuksiin liittyvien prosessien tarkastaminen/ luominen

- Rekisteröidyn oikeudet korostuvat osana rekisterinpitäjän velvollisuuksia
- Rekisteröidyn oikeuksilla osallistetaan rekisteröity tietojensa käsittelyyn, luodaan läpinäkyvyttä rekisterinpitäjän toimintaan henkilötietojen käsittelyssä ja tuetaan rekisteröidyn tiedollista itsemääräämisoikeutta
- Oikeudet vaihtelevat riippuen siitä mikä on henkilötietojen käsittelyn oikeusperuste

5 Työpaketti: Sisäänrakennettu ja oletusarvoinen tietosuoja

Mitä tarkoittaa?

- Tietosuoja-asetuksen 5 artiklan mukaiset tietosuojaperiaatteet otetaan huomioon jo henkilötietojen käsittelyä suunniteltaessa
- Henkilötietojen tekniset ja organisatoriset suojatoimet ovat osa henkilötietojen käsittelyä

Miten toteutetaan?

- Tietosuojan ja tietoturvan huomioiminen kehittämistoiminnan yhteydessä
- Sisäiset ohjeet ja menettelyt (esim. turvasähköpostin käyttö)
- Tiedonhallinnan prosessi ja tiedonhallinnan hyvät käytänteet
- Rekisterien hallinta
- Käytönvalvonta (esim. lokitiedot)
- Tietojen anonymisointi ja pseudonymisointi
- Auditoinnit

Oletusarvo tietosuojan huomioimiselle koko tiedon elinkaaren ajan

6 Työpaketti: Tietosuojavastaava

Tietosuoja tiimi

- Dokumentoidaan tietosuojavastaavan tehtävät
  - läpinäkyvyys organisaatiolle
- Perustetaan Trafin sisäinen tietosuojatiimi johdon tueksi
  - raportointi määrävälein ajankohtaisista tietosuojaan liittyvistä asioista ja Trafin tietosuojan tilasta

7 Työpaketti: Riskipohjainen lähestymistapa

Trafi

PIA ja DPIA

Art. WP 29 ohje vaikutustenar-vioinnista

PIA
= riskiarviointi

DPIA
= vaikutusten arviointi, jos riskit arvioitu suuriksi , eikä rekisterinpitäjä ole toteuttanut toimenpiteitä niiden pienentämiseksi -> ennakkokuuleminen

- Riskinarviointi tehdään kehittämisen toimintamallin edellyttämien tietosuoja- ja tietoturva- lausuntojen yhteydessä
- Henkilörekisteri-, tietovirta- ja tietoarkkitehtuurikuvaukset tukevat riskinarviointia
- Toteutuvat jo esim. tiedon avaamisen yhteydessä
- Käsitteet ja toimintamallit

8 Työpaketti: Osoitusvelvollisuus

Osoita olevasi tilinteko-kykyinen

Suunnittele & dokumentoi henkilötietojen käsittely

- Tietotilinpäätös vuosittain
- Tietosuojasertifikaatti jatkossa ?
- Selosteet käsittelytoimista
- PIA & DIA-menettelyt ja niistä syntyvät dokumentit
- Tietosuojaperiaatteiden noudattamisen osoittaminen
- Tietosuojakäytännöt

Kiitos!

Trafi Liikenteen turvallisuusvirasto

Liikenteen turvallisuusvirasto

Kumpulantie 9, 00520 Helsinki

PL 320, 00101 Helsinki

Puhelin 029 534 5000

www.trafi.fi