# HENKILÖTIETOJEN KÄSITTELIJÄT JA KANSAINVÄLISET SIIRROT

**Asianajaja, osakas, CIPP/E Ville Vainio**

Asianajotoimisto Applex Oy | 8.12.2021

# GDPR

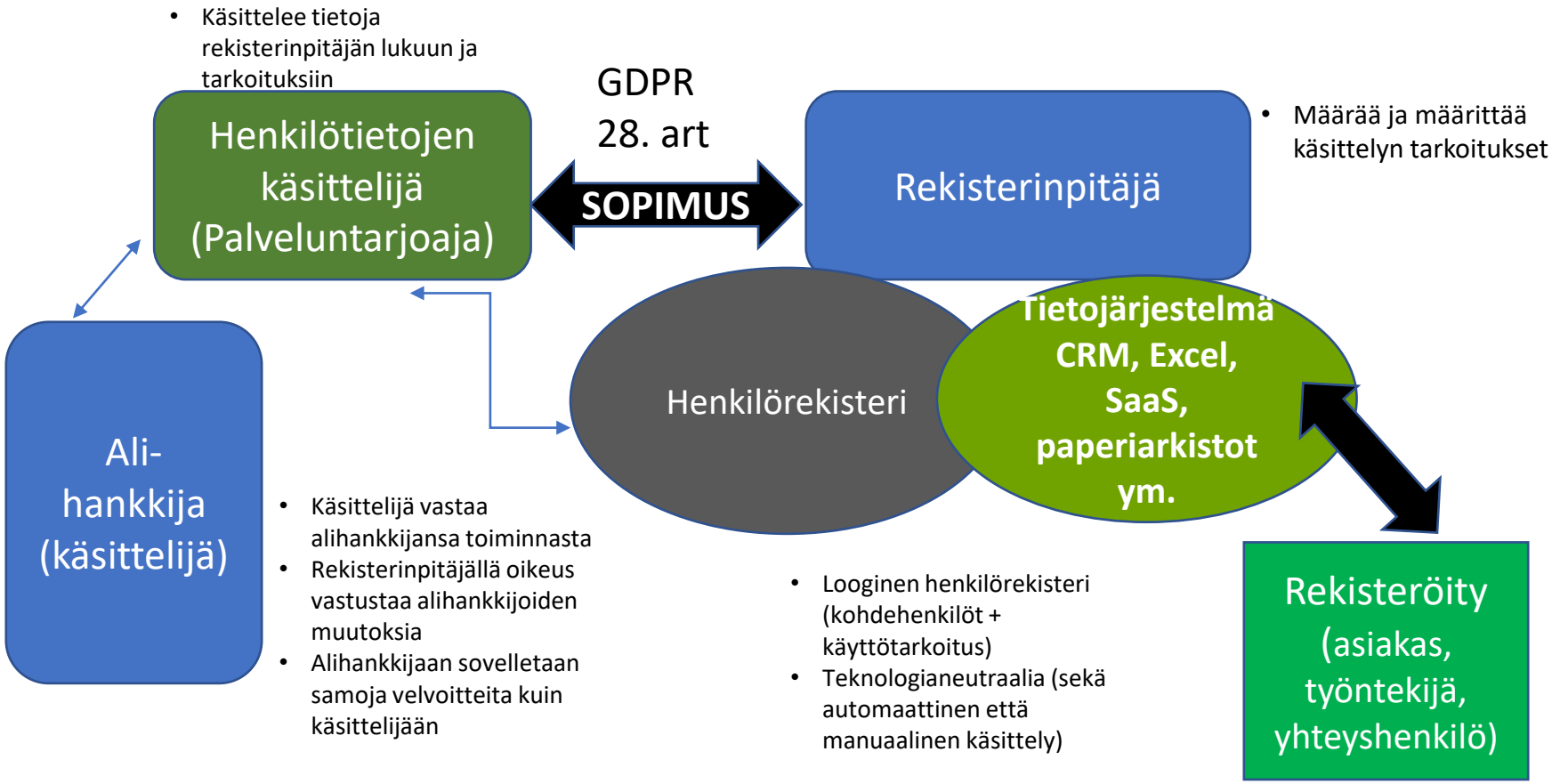
- EU:n yleinen tietosuoja-asetus 679/2016 (General Data Protection Regulation) korvasi EU:n aiemman tietosuojadirektiivin 95/46/EY vuodelta 1995
  - Teknologinen kehitys
  - Yhdet yhteiset tietosuojapelisäännöt
- Asetuksena GDPR on suoraan sovellettavaa EU-lainsäädäntöä (ei siis direktiivi!)
- Soveltaminen alkoi 25.5.2018
- Suomen osalta tietosuoja-asetusta täydentää yleinen tietosuojalaki (1050/2018)



Applex

# Tietosuojalainsäädännön peruskäsitteet ja toimijat

**Henkilötiedoilla** tarkoitetaan kaikkia tunnistettuun tai (suoraan tai epäsuorasti) tunnistettavissa olevaan luonnolliseen henkilöön (rekisteröity) liittyviä tietoja



# Henkilötietojen siirtoperusteet (GDPR V luku)

- Henkilötietoja saa vapaasti siirtää Euroopan unionin ja Euroopan talousalueen sisällä
- Henkilötietojen siirtoihin EU:n / ETA:n ulkopuolelle on oltava jokin siirtoperuste:
  - Siirto tietosuojan riittävyyttä koskevan päätöksen perusteella
  - Siirto asianmukaisia suojatoimia soveltaen
    - Yritystä koskevat sitovat säännöt (Binding Corporate Rules)
    - Komission hyväksymät vakiolausekkeet
    - Hyväksytyt käytännesäännöt + sitoumukset asianmukaisiksi suojatoimiksi
    - Hyväksytty sertifiointimekanismi + sitoumukset asianmukaisiksi suojatoimiksi
    - Viranomaisten vahvistamat sopimuslausekkeet
- Erityistilanteita koskevat poikkeukset (jos muut perusteet eivät sovellu)
  - Rekisteröidyn nimenomainen suostumus; rekisteröidyn sopimus; rekisteröidyn edun mukainen sopimus; yleinen etu; oikeusvaateet; elintärkeät edut
  - Poikkeussiirroista ilmoitus aina valvontaviranomaiselle!



Applex

# Siirto tietosuojan riittävyyden perusteella

- Komissio todennut riittävän tietosuojan tason: Andorra, Argentiina, Färsaaret, Guernsey, Iso-Britannia, Israel, Mansaari, Japani, Jersey, Uusi-Seelanti, Sveitsi ja Uruguay
- Osittainen komission riittävyyspäätös koskien Kanadaa (kaupalliset organisaatiot)
- Komissio arvioi vähintään neljän vuoden välein ja ottaa huomioon GDPR 45 art. mukaisesti:
  - *a) oikeusvaltioperiaate, ihmisoikeuksien ja perusvapauksien kunnioitus, lainsäädäntö, tietosuojaa koskevat säännöt, ammatilliset säännöt, turvatoimet, oikeuskäytäntö, rekisteröityjen oikeudet, rekisteröityjen muutoksenhakukeinot*
  - *b) tehokkaasti toimiva riippumaton valvontaviranomainen*
  - *c) kansainväliset sitoumukset tai muut oikeudellisesti sitovista yleissopimuksista tai säädöksistä taikka monenvälisiin tai alueellisiin järjestelmiin osallistumisesta johtuvat velvoitteet, jotka koskevat erityisesti henkilötietojen suojaamista*

# EDPB Guidelines 05/2021

- GDPR:ssä ei ole määritelty *”henkilötietojen siirtämistä kolmanteen maahan tai kainsainväliselle järjestölle”*.
- EDPB on määritellyt kolme kumulatiivista kriteeriä, jotka määrittelevät käsittelyn siirroksi:
  - 1) Rekisterinpitäjä tai käsittelijä on GDPR:n alainen kyseisen käsittelyn osalta;
  - 2) Tämä rekisterinpitäjä tai käsittelijä (”tiedon viejä”) luovuttaa kyseisen käsittelyn alaisia henkilötietoja siirtämällä tai muutoin asettamalla ne saataville toiselle rekisterinpitäjälle, yhteisrekisterinpitäjälle tai käsittelijälle (”tiedon tuoja”); ja
  - 3) Tiedon tuoja sijaitsee kolmannessa maassa tai on kansainvälinen järjestö, riippumatta siitä, onko tämä tiedon tuoja GDPR:n alainen 3 artiklan mukaisesti vai ei kyseisen käsittelyn osalta.

https://edpb.europa.eu/news/news/2021/edpb-adopts-guidelines-interplay-between-art-3-and-chapter-v-gdpr-statement-digital_en



Applex

# GDPR 3 artikla
# Alueellinen soveltamisala

1. Tätä asetusta sovelletaan henkilötietojen käsittelyyn, jota suoritetaan unionin alueella sijaitsevassa rekisterinpitäjän tai henkilötietojen käsittelijän toimipaikassa toiminnan yhteydessä, riippumatta siitä, suoritetaanko käsittely unionin alueella vai ei.

2. Tätä asetusta sovelletaan unionissa olevia rekisteröityjä koskevien henkilötietojen käsittelyyn, jota suorittava rekisterinpitäjä tai henkilötietojen käsittelijä ei ole sijoittautunut unioniin, jos käsittely liittyy

a) tavaroiden tai palvelujen tarjoamiseen näille rekisteröidyille unionissa riippumatta siitä, edellytetäänkö rekisteröidyltä maksua; tai

b) näiden rekisteröityjen käyttäytymisen seurantaan siltä osin kuin heidän käyttäytymisensä tapahtuu unionissa.

3. Tätä asetusta sovelletaan henkilötietojen käsittelyyn, jota suorittava rekisterinpitäjä ei ole sijoittautunut unioniin vaan toimii paikassa, jossa sovelletaan jonkin jäsenvaltion lakia kansainvälisen julkisoikeuden nojalla.

# Esimerkkejä EDPB:n ohjeistuksen myötä

| Kuvaus | Siirtotilanne |
|---|---|
| Italiassa asuva yksityishenkilö tilaa vaatteita singaporelaisesta verkkokaupasta (jolla ei ole toimintaa EU:ssa). | Kyseessä ei ole henkilötietojen siirto, koska henkilö toimittaa henkilötietonsa omasta aloitteestaan suoraan rekisterinpitäjälle. Singaporelainen yhtiö on mahdollisesti GDPR:n alainen 3(2) artiklan nojalla (jos suuntaa palveluitaan EU-asukkaille). |
| Itävaltalainen yhtiö toimittaa työntekijöidensä tietoja henkilötietojen käsittelijänä toimivalle chileläiselle yhtiölle. | Kyseessä on GDPR V luvun mukainen henkilötietojen siirto rekisterinpitäjältä käsittelijälle (C2P, moduuli 2). |
| EU:n ulkopuolinen rekisterinpitäjä lähettää asiakkaidensa (ei-EU) henkilötietoja Ranskassa sijaitsevalle SaaS-palveluntarjoajalle käsiteltäväksi. | Kyseessä on GDPR V luvun mukainen henkilötietojen siirto käsittelijältä rekisterinpitäjälle (P2C, moduuli 4). |

# Esimerkkejä EDPB:n ohjeistuksen myötä

| Kuvaus | Siirtotilanne |
|---|---|
| Saksalainen rekisterinpitäjä A käyttää ranskalaisen käsittelijän B palveluita. B ulkoistaa palveluita Intiassa sijaitsevalle alikäsittelijä C:lle, ja lähettää A:n henkilötietoja C:lle käsiteltäväksi palveluiden yhteydessä. | Kyseessä on GDPR V luvun mukainen henkilötietojen siirto käsittelijältä alikäsittelijälle (P2P, moduuli 3). |
| Puolalaisen yhtiön (rekisterinpitäjä) työntekijä matkustaa Intiaan työmatkalle. Työntekijä käyttää tietokonettaan ja muodostaa yhteyden yhtiön Puolassa sijaitsevaan tietokantaan. | Kyseessä ei ole GDPR V luvun mukainen henkilötietojen siirto, koska työntekijä ei ole erillinen rekisterinpitäjä vaan erottamaton osa rekisterinpitäjä-yhtiötä. Käsittely tapahtuu yhtiön sisällä GDPR 3(1) artiklan nojalla. |
| Irlantilainen rekisterinpitäjä toimittaa henkilöstönsä tietoja US-emoyhtiölleen (käsittelijä) säilytettäviksi keskitetyssä HR-tietokannassa. | Kyseessä on GDPR V luvun mukainen henkilötietojen siirto rekisterinpitäjältä käsittelijälle (C2P, moduuli 2). |

# Schrems II -ratkaisu

- EU-tuomioistuin kumosi päätöksellä C-311/18 Euroopan komission tietosuojan tason riittävyyttä koskevan päätöksen EU:n ja Yhdysvaltojen välillä tiedonsiirrot mahdollistaneen Privacy Shield –järjestelyn heinäkuussa 2020
- EU-tuomioistuimen mukaan Yhdysvaltain kansallinen lainsäädäntö ja Privacy Shield-järjestely eivät taanneet olennaisesti vastaavaa tietosuojan tasoa EU-kansalaisten henkilötiedoille eivätkä oikeussuojakeinoja kuin GDPR ja EU:n perusoikeuskirja
- Schrems II –ratkaisu ei kumonnut aiempia Euroopan komission vakiosopimuslausekkeita, mutta EUTI katsoi, että tietojenkäsittelyyn osallistuvien organisaatioiden on sovittava lisäsuojatoimenpiteistä vakiosopimusten käyttämisen lisäksi silloin, kun henkilötietoja siirretään Yhdysvaltoihin
- Lisäsuojatoimenpiteiden tavoite on varmistaa, että kolmansien maiden tiedusteluviranomaiset eivät saisi pääsyä (tai vain rajoitetun pääsyn) EU:sta siirrettyihin henkilötietoihin

# Komission hyväksymät vakiolausekkeet

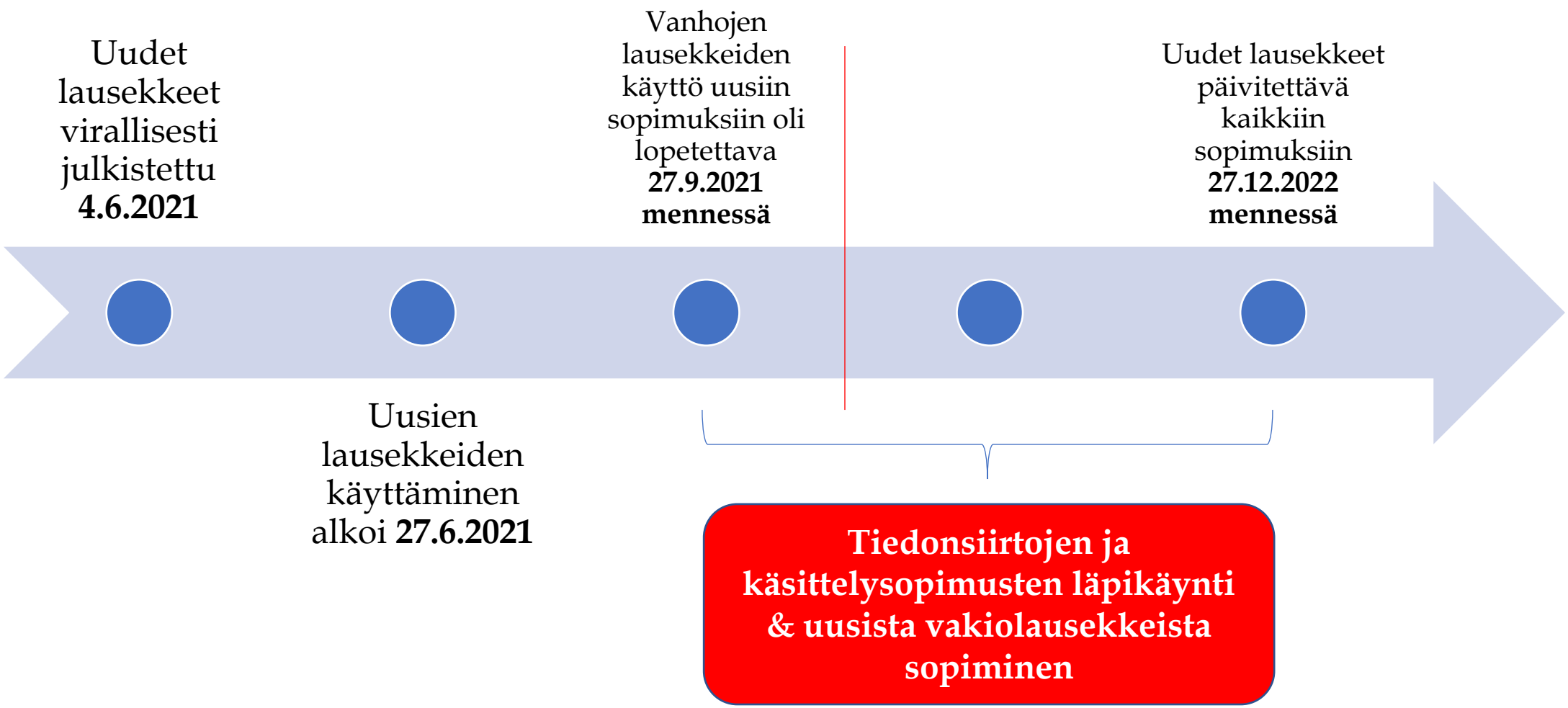
*COMMISSION IMPLEMENTING DECISION (EU) 2021/914*
*of 4 June 2021*
*on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council*

https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en

# Vakiolausekkeet

- Vakiolausekkeet uusittiin kesällä 2021 vastaamaan GDPR:n ja EU-tuomioistuimen ns. Schrems II –ratkaisun vaatimuksia
  - Aiemmat vakiolausekkeet vuosilta 2001, 2004 ja 2010 henkilötietodirektiiviin perustuen
- Yleinen osio + erityisehdot (moduulit) eri siirtotilanteita varten
- Joustavampia käyttää kuin aiemmin, mutta vaativat yksityiskohtaisia kuvauksia
- Mahdollistavat useamman osapuolen mukana olon sekä myöhemmän liittymisen
- Vakiolausekkeita ei saa muuttaa, mutta niihin liittyen saa sopia muita ehtoja, kunhan ne eivät ole ristiriidassa vakiolausekkeiden kanssa
  - Ristiriitatilanteissa vakiolausekkeita sovelletaan ensisijaisesti muihin ehtoihin nähden

# Vakiolausekkeiden aikajana



# Vakiolausekkeet / Moduulit

| | Moduuli | Tiedon viejä (GDPR:n alainen) | | Tiedon tuoja | |
|---|---|---|---|---|---|
| C2C | Moduuli 1 | Rekisterinpitäjä | → | Rekisterinpitäjä | |
| C2P | Moduuli 2 | Rekisterinpitäjä | → | Käsittelijä | |
| P2P | Moduuli 3 | Käsittelijä | → | Käsittelijä/alikäsittelijä | UUSI |
| P2C | Moduuli 4 | Käsittelijä | → | Rekisterinpitäjä | |

# Vakiolausekkeiden rakenne

**II, III, IV Modulaarisuus**

| Osio | Pääkohdat |
|---|---|
| Osio I | Tarkoitus ja soveltamisala, edunsaajat, tulkinta, soveltamisjärjestys, siirron kuvaus, liittymislauseke |
| Osio II – Osapuolten velvollisuudet | Tietosuoja- ja tietoturvaperiaatteet, alikäsittelijät, rekisteröityjen oikeudet, osapuolen vastuu, valvontaviranomainen |
| Osio III – Paikallinen lainsäädäntö | Vakuutukset ja velvollisuudet vieraiden viranomaisten pyyntöjen ja pääsyn varalta (***Schrems II -ehdot***) |
| Osio IV - Loppusäännökset | Irtisanominen (rikkomuksen perusteella), sovellettava laki, riidanratkaisupaikka |

# Osio III – Paikallinen lainsäädäntö (Schrems II-ehdot)

- Tietojen viejä ja tuoja molemmat vakuuttavat:
  - Ettei niillä ole syytä uskoa, että kolmannen maan lait ja käytännöt estäisivät tietojen tuojaa täyttämästä vakiolausekkeiden mukaisia velvollisuuksiaan, ottaen huomioon
    - Siirron olosuhteet
    - Kolmannen maan lait ja käytännöt
    - Relevantit sopimukselliset, tekniset ja organisatoriset suojatoimet
- Riskiperusteinen lähestymistapa
  - Arvioinnissa vaikuttavat esim. aiemmat käytännön kokemukset, kuten viranomaisten esittämät pyynnöt tai se, että viranomainen ei ole aiemmin esittänyt pyyntöjä

**SIIRRON OLOSUHTEET**

**Käsittelyketjun pituus**
**Osapuolten määrä**
**Käytetty siirtokanava**
**Aiotut eteenpäinsiirrot**
**Vastaanottajan tyyppi**
**Käsittelyn tarkoitus**
**Henkilötietojen ryhmät ja muoto**
**Liiketoimintasektori**
**Säilyttämisen sijainti**

# Osio III – Paikallinen lainsäädäntö (Schrems II-ehdot)

- <u>Tietojen tuoja sitoutuu:</u>
  - Tekemään parhaansa (*best efforts*) tarjotakseen olennaista tietoa viejälle siirron olosuhteista
  - Ilmoittamaan viejälle viivytyksettä, mikäli lainsäädännön muutos vaikuttaa sen sitoumuksiin
  - Ilmoittamaan tietojen viejälle viranomaisten pyynnöistä saada pääsy sekä toteutuneista pääsyistä henkilötietoihin
    - Mikäli ilmoittaminen on kiellettyä (tietojen tuojaan sovellettavan lainsäädännön nojalla), tietojen tuojan on tehtävä parhaansa (*best efforts*) saadakseen kiellon kumottua + dokumentoitava tämä ja annettava tiedot viejälle pyynnöstä
    - Tietojen määrä, mitä tietoja pyydetty, mikä viranomainen on pyytänyt, onko pyyntöjä haastettu ja mikä on haastamisen lopputulos, jne.

# Osio III – Paikallinen lainsäädäntö (Schrems II-ehdot)

- Tietojen tuoja sitoutuu:
  - Arvioimaan viranomaisen pyynnön lainmukaisuuden
  - Haastamaan pyynnön mikäli, sitä harkitusti arvioituaan, toteaa haastamiselle olevan järkevät perustelut olemassa + muutoksenhaun tekeminen
  - Haastamisen jälkeen ryhtymään toimenpiteisiin, jotta pyyntöä ei tarvitse toteuttaa, ennen kuin toimivaltainen viranomainen (kuten tuomioistuin) on ratkaissut asian
  - Olemaan paljastamatta pyydettyjä henkilötietoja viranomaiselle paitsi milloin sovellettavat prosessisäännöt niin vaativat
  - Paljastamaan henkilötietoja vain niin vähän kuin vaaditaan
  - Ilmoittamaan tietojen viejälle, mikäli se ei kykene noudattamaan vakiolausekkeita

# Vakiolausekkeet ja lisäsopiminen

- Isommat palveluntarjoaja-käsittelijät oletettavasti tekevät sopimukset vain omille sopimuspohjilleen; muutoksista vaikeaa (ellei mahdotonta) neuvotella – ”ota tai jätä”
  - *Schrems II* –asiat paketoituna käsittelijän standardidokumenttiin valmiiksi rekisterinpitäjä-asiakkaille?
  - Toisaalta isommalla rekisterinpitäjä-asiakkaalla voi olla hyvä neuvottelutilanne pienempään palveluntarjoajaan nähden
  - Tietojen viejä joka tapauksessa vakuuttaa, että se on tehnyt kohtuulliset toimenpiteet varmistaakseen, että tietojen tuoja noudattaa lausekkeita
- Mistä osapuolet mahdollisesti haluavat poiketa: vastuunrajoitukset, auditointiehdot jne.
  - Lähtökohtaisesti kukin osapuoli vastaa täysimääräisesti aiheuttamistaan vahingoista
  - Toisin kuin tietojenkäsittelysopimuksia koskevassa GDPR 28(3) artiklassa, vakiolausekkeissa nimenomaisesti mainitaan, että tarkastuksia voidaan tehdä tietojen tuojan toimitiloissa tai fyysisessä toimipaikassa!



Applex

# Liite 1 – Kuvaus siirroista

**SOVELLETTAVAT MODUULIT**

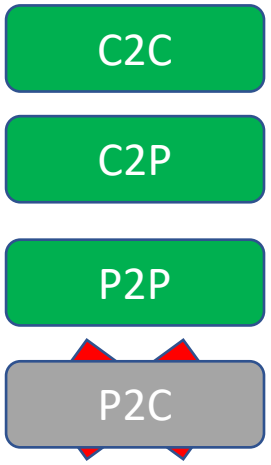
- C2C
- C2P
- P2P
- P2C

- Kuvaus osapuolista, siirroista, toimivaltaisesta valvontaviranomaisesta
  - Tiedon viejä ja tiedon tuoja yhteystietoineen
  - Rekisteröityjen ryhmät, käsiteltävät henkilötiedot
  - Arkaluontoiset tiedot + suojatoimet
  - Siirtojen toistuvuus, luonne, tarkoitukset, säilytysajat
- Mikäli tiedon tuoja siirtää tietoja eteenpäin, silloin myös alikäsittelijäsiirtojen kohde, luonne ja kesto on kuvattava
  - Kenelle tietoja siirretään, miksi, ja kuinka kauan?

➢ Läpinäkyvyyden lisääminen koko tiedonkäsittelyketjussa

# Liite 2 - Tietoturvatoimet

**SOVELLETTAVAT MODUULIT**




- Yksityiskohtainen (ei yleinen!) kuvaus asianmukaisista teknisistä ja organisatorisista tietoturvatoimista
- Kuvattava myös alikäsittelijän tietoturvatoimet
- Liitteessä on kattava listaus esimerkkitoimenpiteistä
  - IT-/tietoturva-asiantuntijoiden apua tarvittaneen kuvausten tekemiseksi!

*Measures for user identification and authorisation*

*Measures for the protection of data during transmission*

*Measures for the protection of data during storage*

*Measures for ensuring physical security of locations at which personal data are processed*

*Measures for ensuring events logging*

*Measures for ensuring system configuration, including default configuration*

*Measures for internal IT and IT security governance and management*

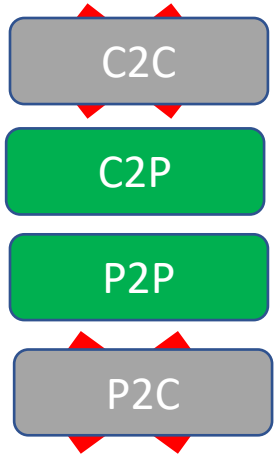
*Measures for certification/assurance of processes and products*



Applex

# Liite 3 - Alikäsittelijät

**SOVELLETTAVAT MODUULIT**




- Tehdään moduulien 2 ja 3 alla ainoastaan, jos alikäsittelijän käyttäminen edellyttää erityistä kirjallista ennakkolupaa
- Mikäli tiedon tuojalle sen sijaan on annettu yleinen kirjallinen ennakkolupa alikäsittelijöiden käyttämiselle, liitettä 3 ei sovelleta

The controller has authorised the use of the following sub-processors:

1. Name: .....

   Address: .....

   Contact person's name, position and contact details: .....

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): .....

2. .....

# Euroopan tietosuojaneuvoston suositukset henkilötietojen siirtämiseksi

*Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, Adopted on 18 June 2021*

https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

# EDPB:n suositukset

1. Tunnista siirrot
2. Varmista tiedonsiirtomekanismi
3. Arvioi vastaanottajamaan lait ja käytännöt
4. Tunnista ja ota käyttöön lisäsuojatoimet
5. Virallista lisäsuojatoimenpiteiden käyttöönotto
6. Arvioi uudelleen siirtojen suojan taso

# Vinkkejä

- 1. Tunnista roolisi rekisterinpitäjä, käsittelijänä tai alikäsittelijänä
- 2. Tunnista kaikki osapuolet ja tiedonsiirtotilanteet
- 3. Tarkista ja päivitä sopimukset tilanteen mukaan
- 4. Tee(tä) arvio henkilötietojen vastaanottajamaan paikallisista laeista ja olosuhteista
- 5. Ota lisäsuojatoimenpiteitä käyttöön tilanteen mukaan
- 6. Suorita ja dokumentoi siirtoja koskevat vaikutustenarvioinnit
- 7. Uudelleenarvioi säännöllisesti

**Asianajotoimisto Applex Oy**

Puh. 010 2999 471
info@applex.fi

**www.applex.fi**