Dataskyddsförordningen

GDPR - General Data Protection Regulation

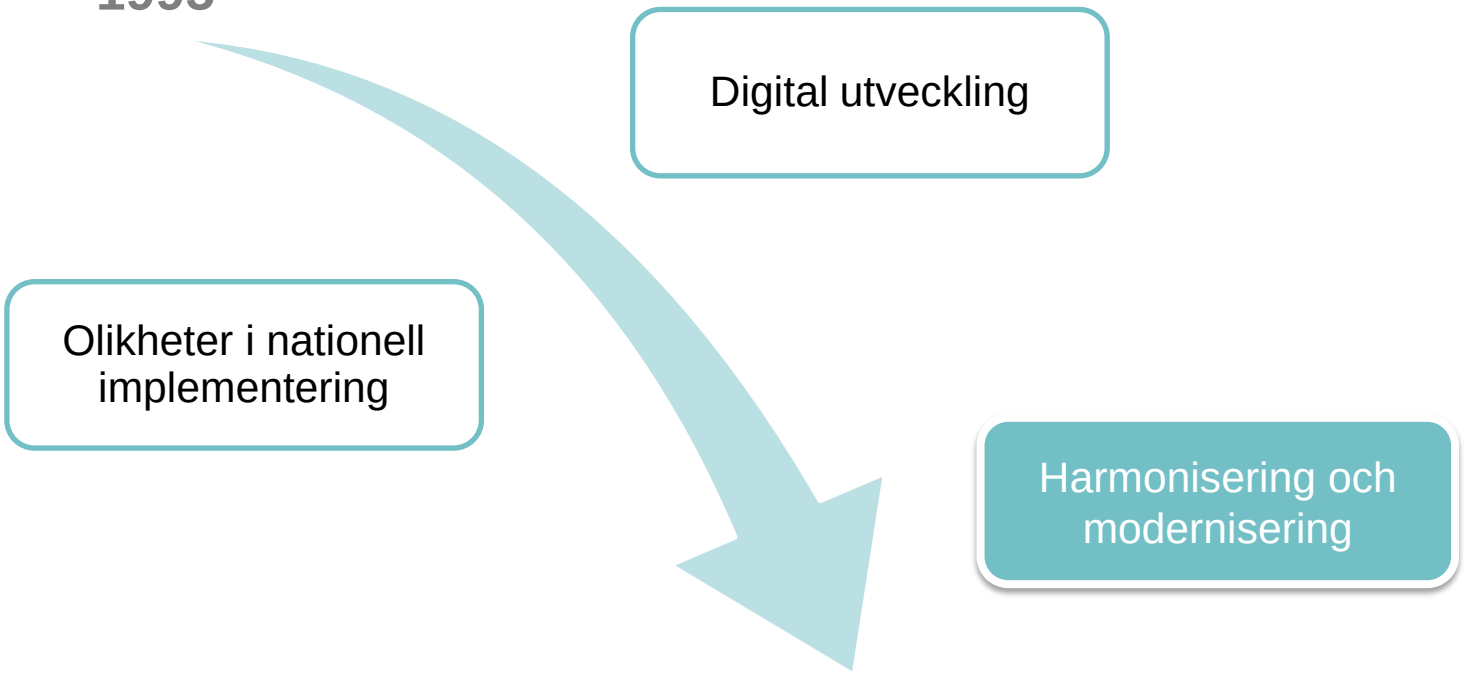
September 2017

Cecilia Frank

IKANO BANK

Bakgrund

Dataskyddsdirektivet (95/46)
1995

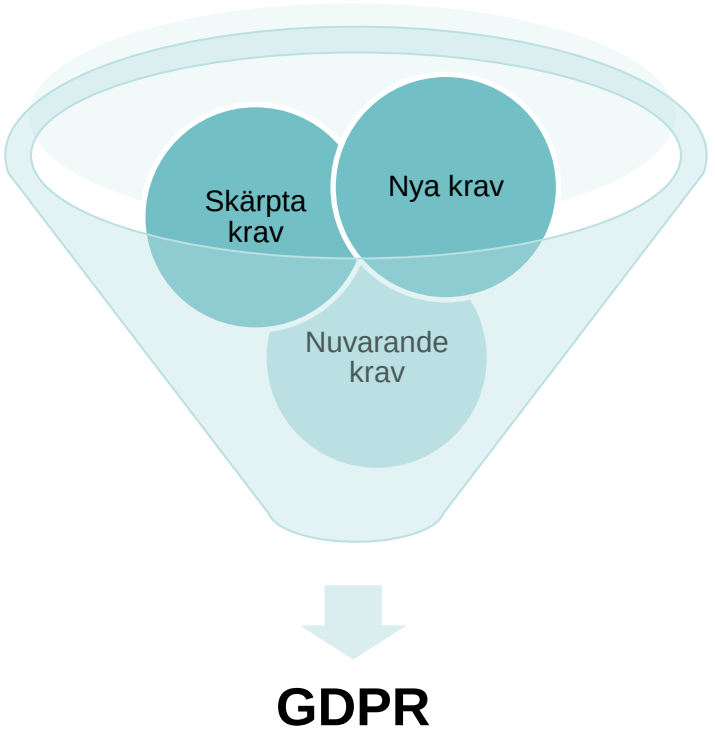


Dataskyddsförordningen (2016/679)
25 maj 2018

Vad innebär GDPR?

- Ökat skydd för individer
- Ökade krav för företag
- Risk för höga sanktionsavgifter (upp till 4 % av årsomsättningen eller 20 000 000 EUR)
- Riskbaserat förhållningssätt

Lokal lagstiftning är fortfarande relevant



Art 4

Definitioner

Personuppgifter = varje upplysning som avser en identifierad eller identifierbar (direkt eller indirekt) fysisk person (t.ex. personnummer, telefonnummer, kontonummer)

Personuppgiftsbehandling = alla åtgärder beträffande personuppgifter, t.ex. insamling, registrering, lagring, bearbetning, framtagning, användning, utlämning, överföring

Registrerad = den identifierade eller identifierbara fysiska personen som behandlingen avser

Personuppgiftsansvarig = den som bestämmer ändamålen och medlen för behandling av av personuppgifter (t.ex. en bank)

Personuppgiftsbiträde = den som behandlar personuppgifter för den personuppgiftsansvariges räkning (t.ex. inkassobolag, tryckeri)

IKANO BANK

Art 2-3

Tillämpningsområde

Materiellt:

- Behandling av personuppgifter som företas på **automatisk väg**
- Annan behandling än automatisk om uppgifterna ingår i eller kommer att ingå i ett **register**

Detta innebär att:

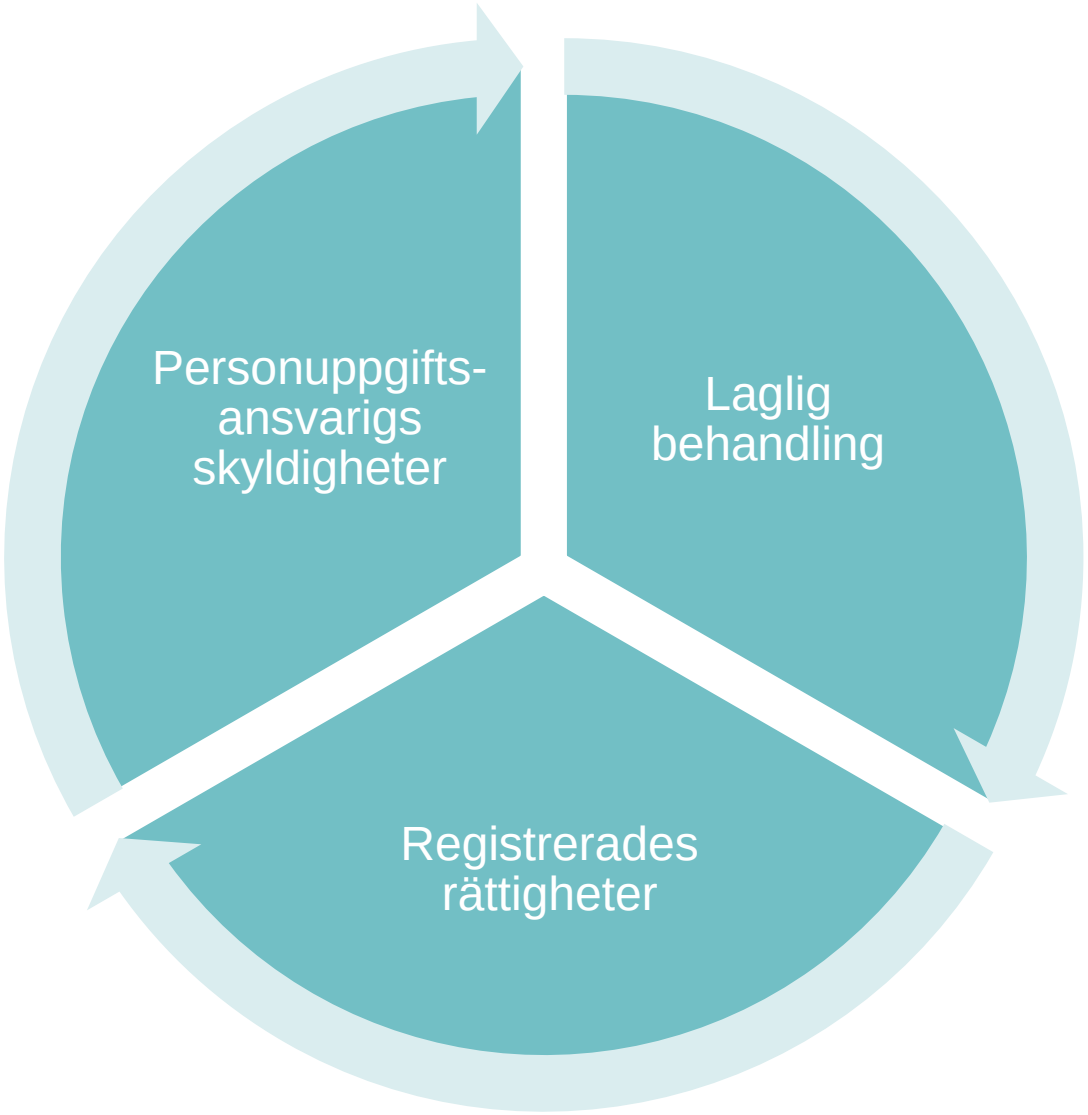
- ➢ det svenska undantaget för ostrukturerade uppgifter försvinner (jfr 5a § PUL)
- ➢ manuell ostrukturerad behandling ligger fortfarande utanför tillämpningsområdet

Territoriellt:

- Företag som är etablerade inom EU
- Företag som är etablerade utanför EU, om de erbjuder varor och tjänster till registrerade inom EU eller övervakar beteenden inom EU

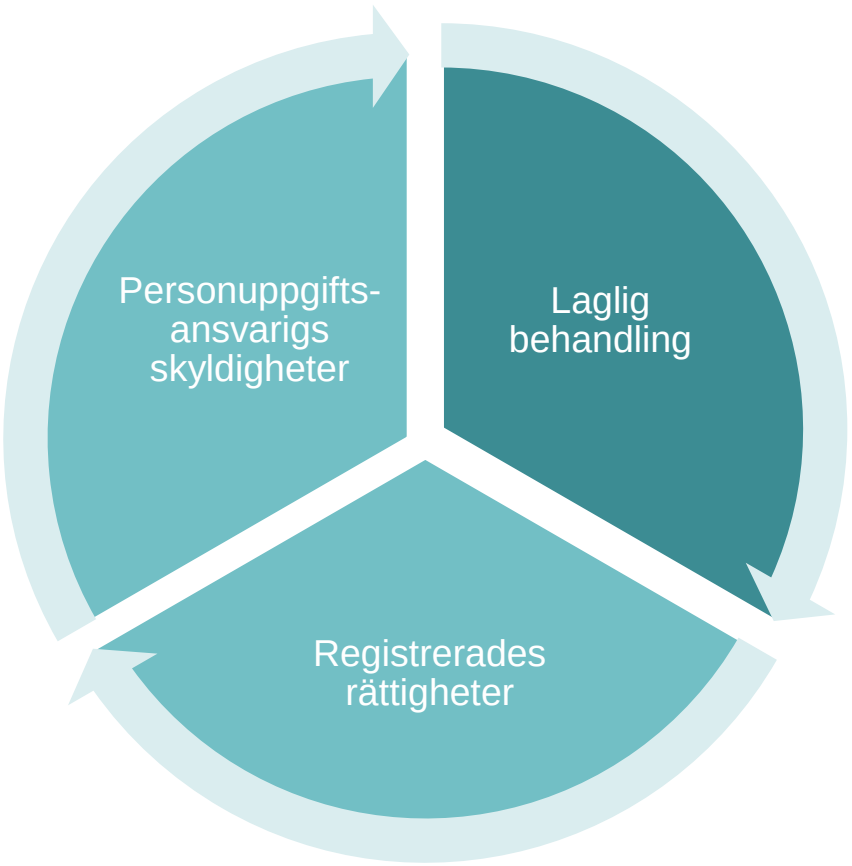
IKANO BANK

GDPR - innehåll



Art 5-6

Laglig behandling



- **Grundläggande principer:**
  - Laglighet och öppenhet
  - Ändamålsbegränsning
  - Uppgiftsminimering
  - Korrekthet
  - Lagringsminimering
  - Integritet och konfidentialitet

- **Laglig grund (ej uttömmande):**
  - Samtycke
  - Avtal
  - Rättslig förpliktelse
  - Berättigat intresse (intresseavvägning)

IKANO BANK

Art 7-10

Laglig behandling (forts)

Mer strikta villkor för giltigt samtycke:

- Klart och tydligt särskiljas från andra frågor - begriplig och lättillgänglig form
- Frivilligt, specifikt, informerat och otvedydigt medgivande
- Lika lätt att återkalla som att ge ett samtycke
- Särskilda krav för samtycke gällande informationstjänster till barn

Särskilt känsliga personuppgifter:

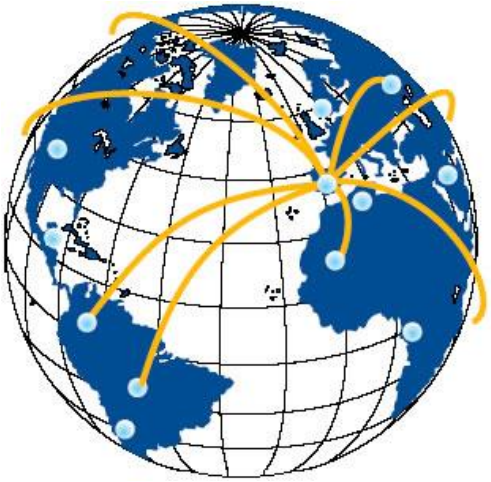
- Särskilda krav för särskilda kategorier av personuppgifter redan i nuvarande lagstiftning (etnicitet, politiska åsikter, religion, fackföreningstillhörighet, hälsa, sexuell läggning)
- Nytt är att även *genetiska och biometriska uppgifter* läggs till de särskilda kategorierna.
- Särskilda krav för uppgifter om fällande domar i brottmål och överträdelser – krävs att behandlingen sker under kontroll av myndighet eller att det finns särskilt lagstöd.

IKANO BANK

Laglig behandling (forts)

Överföring till tredjeland (utanför EU/EES) kräver särskild laglig grund:

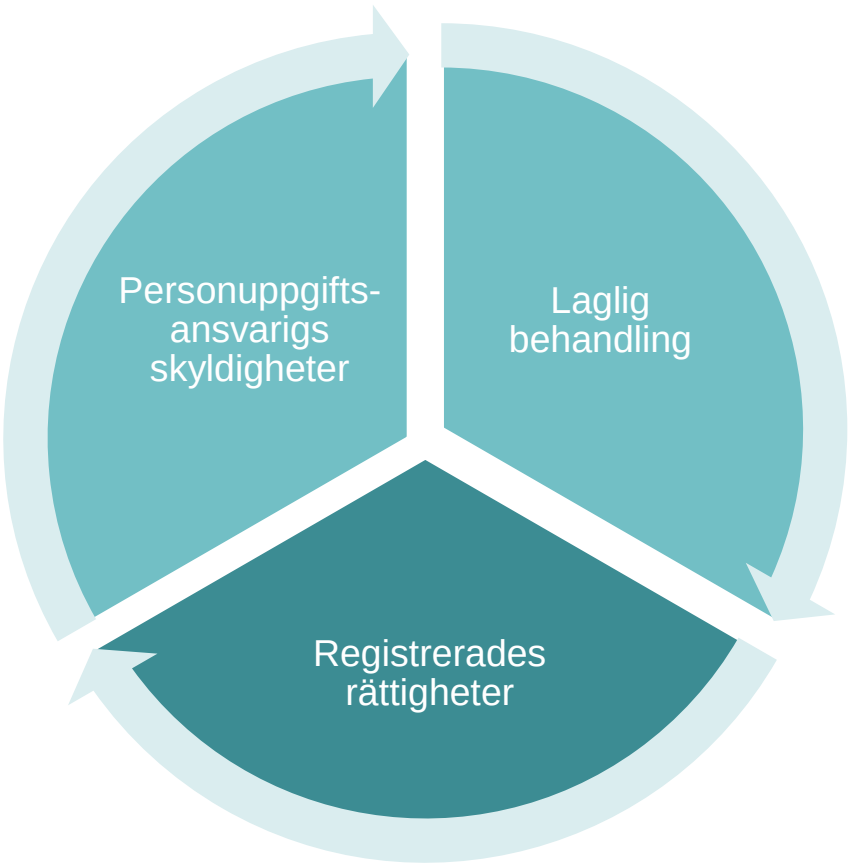
- Landet omfattas av beslut av EU-kommissionen avseende adekvat skyddsnivå (t.ex. Schweiz, Nya Zeeland och USA - om mottagaren är ansluten till *Privacy Shield), eller*
- Överföringen omfattas av specifika skyddsåtgärder, t.ex. bindande företagsbestämmelser eller standardavtalsklausuler
- Undantag för vissa särkilda situationer i art 49



IKANO BANK

Art 12-22

Registrerades rättigheter



- Full transparens – klart och tydligt språk
- Detaljerade krav på information i samband med att uppgifter samlas in
- Rätt till tillgång
- Rätt till rättelse och radering (‘right to be forgotten’)
- Rätt till begränsning av behandling
- Rätt till dataportabilitet
- Rätt att invända mot behandling
- Rätt till icke-automatiserade beslut

IKANO BANK

Registrerades rättigheter (forts)

Möjlighet till nationella begränsningar av rättigheterna - art 23

Rätt till tillgång (jfr registerutdrag enl 26 § PUL) – art 15

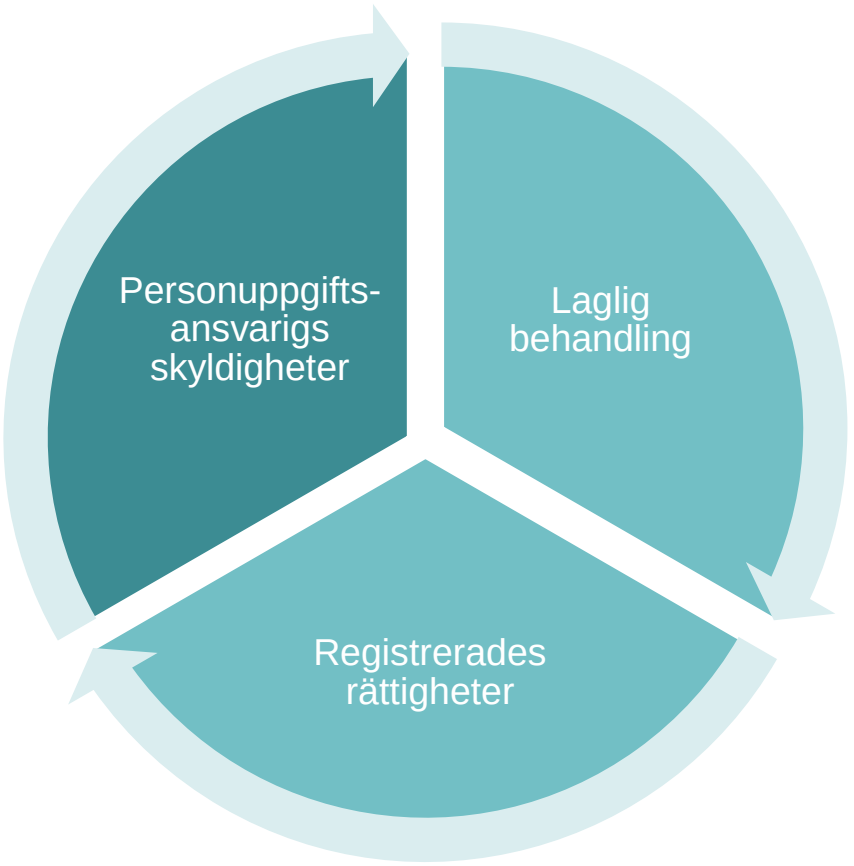
- Mer detaljerade krav på vad som ska ingå i utdraget
- Omfattar all behandling, dock inte uppgifter som inte får lämnas ut enl lag
- Informationen ska kunna lämnas elektroniskt

Rätt till dataportabilitet – art 20:

- Rätt att få uppgifterna i strukturerat, allmänt använt och maskinläsbart format
- Omfattar endast sådana uppgifter som den registrerade har tillhandahållit
- Omfattar endast automatiserad behandling som grundar sig på samtycke eller avtal.

IKANO BANK

Personuppgiftsansvarigs skyldigheter



- Ansvarsskyldighet - art 24, art 5 p. 2
- Anmälningsskyldighet avseende rättelse, radering, begränsning - art 19
- Inbyggt dataskydd och dataskydd som standard, t.ex. pseudonymisering - art 25
- Biträdesavtal - art 28
- Register över behandling - art 30
- Samarbeta med tillsynsmyndighet - art 31
- Säkerhet - art 32
- Anmäla personuppgiftsincident - art 33-34
- Konsekvensbedömning - art 35
- Dataskyddsombud - art 37-39

IKANO BANK

Personuppgiftsansvarigs skyldigheter (forts)

Säkerhet – art 32:

- *Lämpliga* tekniska och organisatoriska säkerhetsåtgärder ska vidtas för att uppnå *lämplig* säkerhetsnivå
- Beakta risken utifrån typ av uppgifter och behandlingens art, omfattning etc.
- Beakta standarder, tillgänglig teknik och kostnader

Kontroll över personuppgiftsbiträden – art 24, 28:

- Säkerställa att biträden implementerar lämpliga tekniska och organisatoriska skyddsåtgärder (biträden har även självständigt ansvar)
- Bedömning innan avtalet ingås och löpande, kontroll på underleverantörer
- Särskilda krav vid överföring utanför EU/EES (tredjelandsöverföring) - art 44-49

IKANO BANK

Personuppgiftsansvarigs skyldigheter (forts)

Personuppgiftsincident – art 33-34:

- Ska anmälas till Datainspektionen inom 72 timmar , såvida inte osannolikt att det inneburit en risk för den registrerades rättigheter och friheter.
- Ska även anmälas till den registrerade utan onödigt dröjsmål, om det är sannolikt att incidenten leder till hög risk för den registrerades rättigheter och friheter.

Konsekvensbedömning – art 35

- Ska göras om en ny typ av behandling sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. Finns vägledning för vilka faktorer som ska beaktas.

Dataskyddsombud – art 37-39:

- Obligatoriskt för företag där kärnverksamheten består av
  a) behandling som kräver regelbunden och systematisk övervakning av registrerade i stor omfattning, *eller*
  b) behandling i stor omfattning av särskilt känsliga personuppgifter

IKANO BANK

Art 58,83

Tillsynsmyndighetens befogenheter

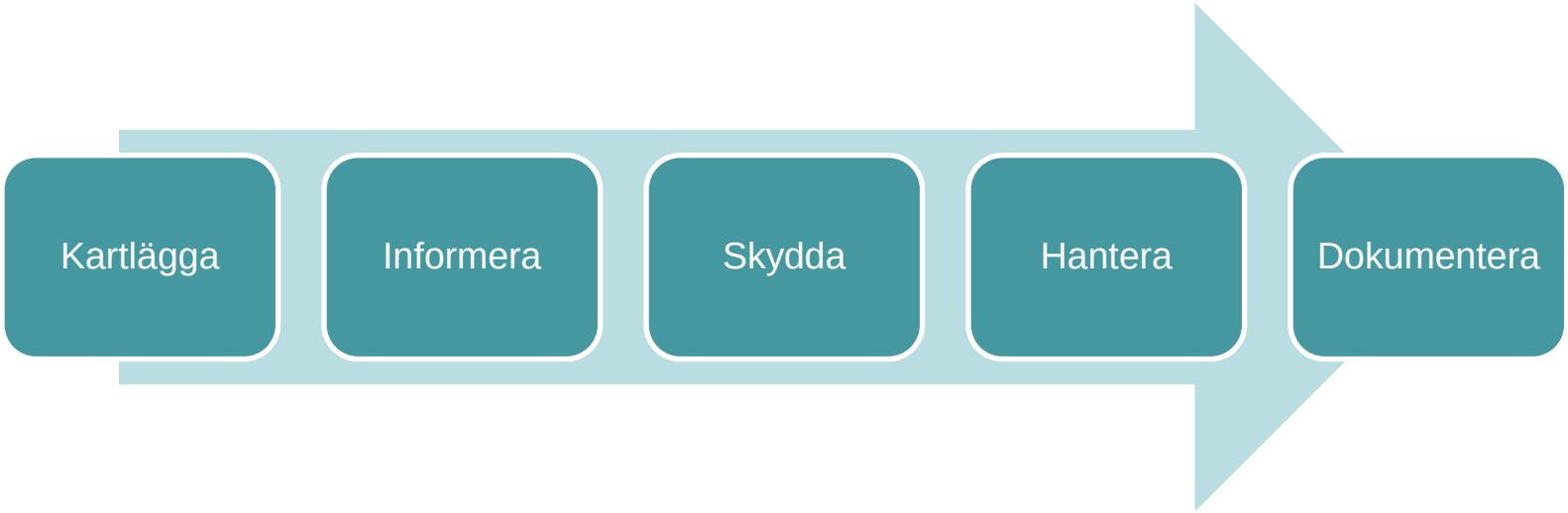
Både personuppgiftsansvarig och personuppgiftsbiträde kan bli föremål för:

- Varning/reprimand
- Föreläggande
- Begränsning av behandling
- Förbud mot behandling
- Administrativa sanktionsavgifter
  - Max 4 % av globala årsomsättningen eller 20 000 000 EUR (max 20 000 000 *SEK* för myndigheter)
  - Nivån bestäms av omständigheterna i det enskilda fallet (karaktär, omfattning, varaktighet, antal berörda, faktisk skada etc) med beaktande av förmildrande och försvårande omständigheter såsom tidigare överträdelser, graden av samarbete med myndigheten, ekonomisk vinst/undvikande av förlust pga överträdelsen.

IKANO BANK

GDPR - vad behöver göras?

- Kartlägga och bedöma all personuppgiftsbehandling
- Säkerställa tillräcklig information till registrerade
- Säkerställa tillräckligt skydd för personuppgifter – tekniska och organisatoriska åtgärder
- Säkerställa möjlighet att hantera begäran från registrerade, t.ex. begäran om tillgång (registerutdrag), portabilitet, rättelse, radering
- Dokumentera – för att påvisa regelefterlevnad



IKANO BANK

Publicerade vägledningar (EU)

- Guidelines on the right to data portability, WP 242 rev.01
- Guidelines on Data Protection Officers (‘DPOs’), WP 243
- Guidelines for identifying a controller or processor’s lead supervisory authority, WP 244
- Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, WP 248

Kommande vägledningar…

- Samtycke – oktober
- Profilering – december
- Rapportering av personuppgiftsincident - december

Kompletterande reglering

Sverige:

SOU 2017:39

- Ny dataskyddslag - ny lag och förordning med kompletterande bestämmelser till EU:s dataskyddsförordning

Ds 2017:26

- En anpassning till dataskyddsförordningen – kreditupplysningslagen och några andra författningar

SOU 2016:65

- Ett samlat ansvar för tillsyn över den personliga integriteten

EU:

Direktiv (EU) 2016/680

- personuppgiftsbehandling som utförs av brottsbekämpande verksamheter

Ny e-Privacy-förordning

- ny förordning om integritet och elektronisk kommunikation föreslås träda i kraft samtidigt som GDPR. Kommer att ersätta nuvarande e-Privacy-direktiv (2002/58) och innebära ändringar i lagen (2003:389) om elektronisk kommunikation.

IKANO BANK