Svenska kyrkan
KYRKOKANSLIET

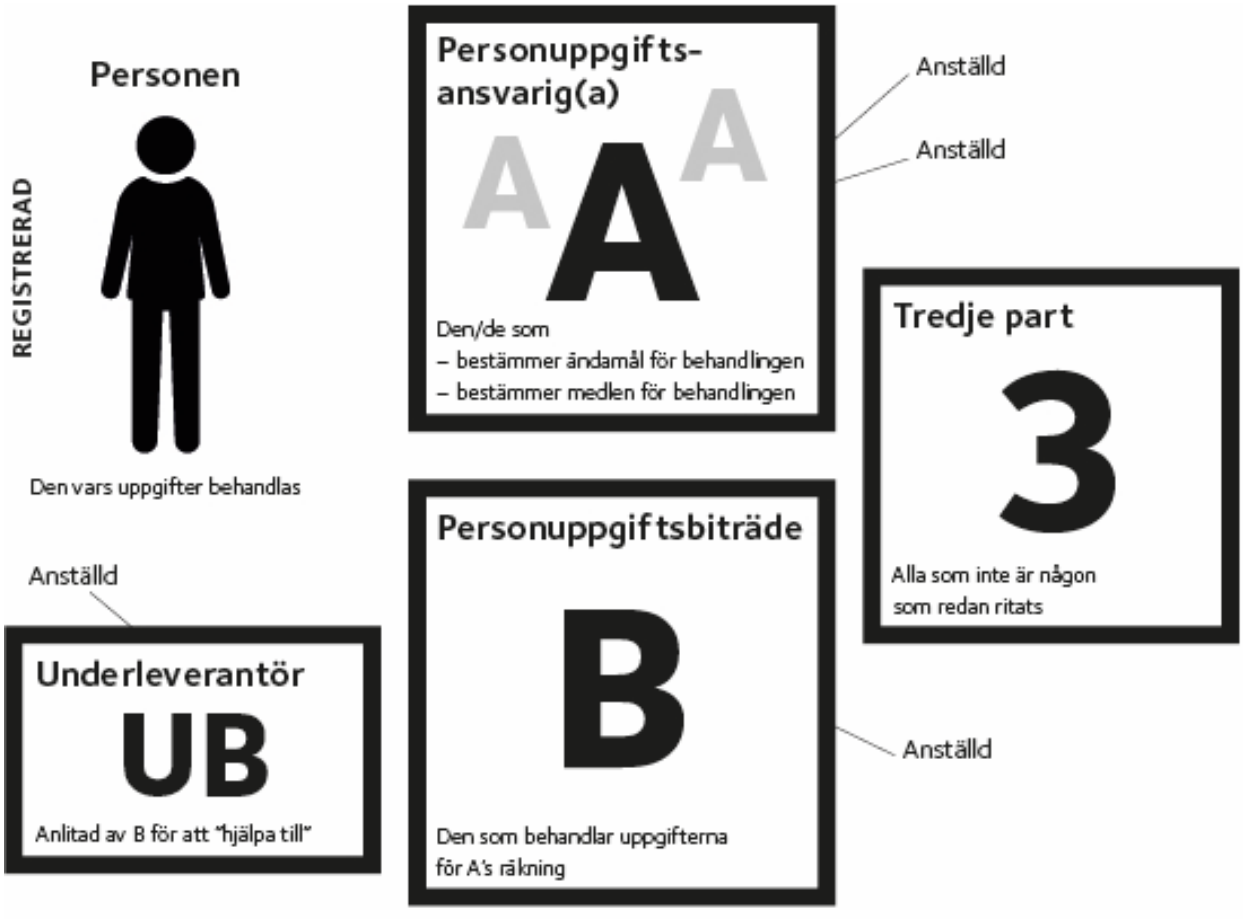
Dataskydd för personuppgifter i fyra steg – lathund om nya dataskyddsförordningen

av rättsavdelningen på kyrkokansliet, oktober 2017

Dataskyddsförordningen[1] börjar gälla i maj 2018. Den är en påbyggnad av personuppgiftslagen (som brukar kallas PUL). Dataskyddsförordningen kommer gälla som lag i hela EU.

Förordningen är strängare än PUL, men många av förordningens grundprinciper är desamma som i PUL. Syftet med reglerna är att skydda information om människor.

Aktörer (artikel 4)



[1] Europaparlamentets och rådets förordning 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän dataskyddsförordning)

Personuppgift och behandling (artikel 4)

Personuppgift = varje **upplysning** som **avser** en identifierad eller identifierbar **fysisk person**

Identifierbar = direkt eller indirekt kan identifieras genom t.ex. namn, nummer, lokaliseringsuppgift, onlineidentifikator, faktor/er specifika för personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet

Behandling = **åtgärd/er** beträffande **personuppgifter**

t.ex. insamling, registrering, organisering, strukturering, lagring, bearbetning, ändring, framtagning, läsning, användning, utlämning (genom överföring, spridning eller tillhandahållande på annat sätt), justering, sammanförande, begränsning, radering, förstöring

Teknikneutrala regler (artikel 2)

Förordningen gäller för

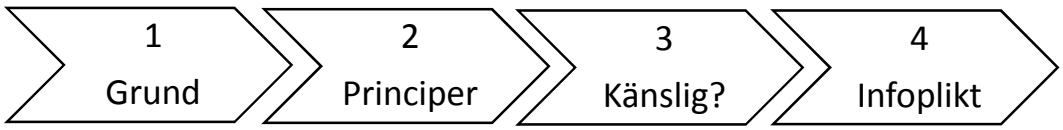
- personuppgiftsbehandling som görs delvis eller helt automatiskt, t.ex. i ett datasystem (motsats till manuell behandling) **och**
- icke-automatisk personuppgiftsbehandling när personuppgifterna ingår eller kommer ingå i ett register. Förordningen gäller t.ex. inte en pärm med papper bakom särskilda flikar

Nyhet: det finns inte längre någon regel som säger att behandling av personuppgifter i ostrukturerat material är undantaget från de flesta reglerna.

Detta innebär att förordningen sannolikt gäller för t.ex. enkla Excel- och Wordlistor och Outlook.

Svenska kyrkan
KYRKOKANSLIET

GRUNDLÄGGANDE ”TÄNK” i fyra steg



STEG 1 och 1b – *sid 4-5 i denna lathund*

Har vi **grund** (anledning) för behandlingen enligt artikel 6?

Är samtycke möjlig grund? Är samtycke lämplig grund?

STEG 2 – *sid 6*

Uppfyller vi **principerna** i artikel 5? Främst:

- Har vi tydliga och definierade ändamål? Ändamålen blir ramen (cirkeln i illustrationen) som påverkar nästan ALLT.
- Kan vi avstå från att behandla vissa uppgifter och ändå uppnå ändamålet? Uppgifterna ska vara tillräckliga men inte ”kan-vara-bra-att-ha-i-framtiden”. Vi får inte behandla fler uppgifter än vad som är nödvändigt för de beskrivna ändamålen.
- Hur länge behöver vi behandla uppgifterna i detta system för ändamålen? Hur flyttar vi bort (till t.ex. arkiv) eller raderar/anonymiserar uppgifterna när tiden ”gått ut”?
- Hur säkerställer vi att hålla uppgifter aktuella, om det ingår i ändamålet?
- Hur säkerställer vi säkerhet för uppgifterna?

Hur kan vi visa att vi följer dessa principer?

illustration av principerna

STEG 3 – *sid 7*

Är uppgiften **känslig**?
Har vi grund för behandling av den känsliga uppgiften enligt artikel 9?

STEG 4 – *sid 8*

Vilken **information** måste vi ge personen och när? (artikel 13 och 14)

Svenska kyrkan
KYRKOKANSLIET

STEG 1

Har vi GRUND för behandling? (artikel 6)

En av situationerna (a–f) nedan måste vara uppfylld för att vi ska kunna gå vidare till ”steg 2”. Det är nämligen detaljerat reglerat i vilka situationer behandling av personuppgifter är tillåten.

Den första situationen, när behandling är tillåten, är att personen har samtyckt. De övriga situationerna handlar om att personuppgiftsbehandlingen behövs (är nödvändig) för ett visst syfte.

a) Personen har **samtyckt** till att personuppgifterna behandlas för ett eller flera **specifika ändamål**.

   – Samtycket måste omfatta de specifika ändamålen. Därför måste personen få *veta* ändamålen, och vi behöver dessförinnan ha *formulerat* ändamålen.

b) Behandlingen är nödvändig för att fullgöra ett **avtal där personen är part** eller för att vidta åtgärder på begäran av personen innan ett sådant avtal ingås.

   – Gäller oavsett om personen har avtalat med oss eller med någon annan.

c) Behandlingen är nödvändig för att fullgöra **personuppgiftsansvariges rättsliga förpliktelse**.
   Ny föreslagen begränsning[2]: ”rättslig förpliktelse” bestäms av riksdag/regering/myndighet eller följer av kollektivavtal!

   – Gäller om *kyrkan* har den rättsliga förpliktelsen

   – **Nyhet om begränsningen blir verklighet:** Kyrkan kommer *inte* kunna stödja sig på en ”förpliktelse” i kyrkoordningen eller bestämmelse från kyrkostyrelsen!

d) Behandlingen är nödvändig för att skydda **intressen** som är av **grundläggande** betydelse **för personen/**annan person.

   – Gäller om en *person* har detta intresse, inte om kyrkan har intresse. Hög tröskel, t.ex. medvetslös och behöver vård.

[2] Förslaget har getts av en statlig utredning (se SOU 2017:39 s 41) och behandlas av regeringen, som kommer med ett slutligt förslag under hösten 2017. Vi vet ännu inte om regeringen kommer att föreslå samma sak och om riksdagen därefter kommer att besluta som regeringen föreslår.

e) Behandlingen är nödvändig för att utföra en uppgift av **allmänt intresse** eller som ett led i personuppgiftsansvariges myndighetsutövning. **Ny föreslagen begränsning [2]:** ”uppgift av allmänt intresse” kan bara bestämmas av riksdag/regering/ myndighet eller följa av kollektivavtal!

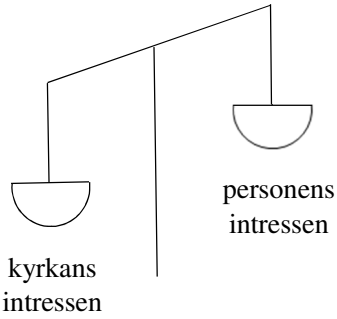
– **Obs:** om vi baserar behandling på allmänt intresse så har personen stora möjligheter att bli raderad om personen begär det av personliga skäl (artikel 21).

– **Nyhet om begränsningen blir verklighet:** Kyrkan kommer inte kunna stödja sig på om ett intresse står i kyrkoordningen eller bestämmelse från kyrkostyrelsen!

f) Behandlingen är nödvändig för personuppgiftsansvariges/ tredje parts **berättigade intressen** som **väger tyngre** än personens intressen/grundläggande rättigheter och friheter.

– Alltså intresseavvägning mellan kyrkan och personen.

– **Obs** om vi baserar behandling på intresseavvägningen, har personen stora möjligheter att bli raderad om personen begär det av personliga skäl (artikel 21).



STEG 1b Är SAMTYCKE lämpligt och möjligt?

Samtycke är en **grund** för att behandla både ”vanliga” och känsliga personuppgifter. Samtycket måste avse specifikt/specifika ändamål. Samtycke medför inte att vi slipper kravet på att följa principerna i ”steg 2”.

Osäkerhet för framtiden – personen kan återkalla samtycket och då får vi inte längre behandla uppgifterna. Klarar systemet detta?

Dokumentation och administration – Vi bör ha bevis på att personen samtyckt och vad personen samtyckt till, så att vi kan visa i efterhand att samtycke gavs.

Teknik – Vi måste **göra det lika lätt att återkalla** samtycke som att ge samtycke.

Samtycke får inte missbrukas till att be om ”bra-att-ha” uppgifter

Samtycke bör **inte användas av arbetsgivare** mot anställda när det finns beroendeförhållande (kan känna sig tvingad = inget verkligt samtycke).

Ett samtycke **måste vara** frivilligt, specifikt och informerat. Det ska vara en otvetydig viljeyttring som kan vara ett uttalande eller en ”entydig bekräftande handling” som innebär att personen godtar att personens uppgifter behandlas. Samtycke måste inte vara skriftligt, men vi ska kunna bevisa att samtycket finns.

STEG 2

PRINCIPER att följa (artikel 5)

a) Behandla personuppgifterna **lagligt, korrekt** och **med öppenhet** gentemot personen.

b) Ändamål

1. När man samlar in personuppgifter måste man ha **särskilda, uttryckligt angivna och berättigade ändamål** för behandlingen.

2. Om man sedan vill behandla personuppgifterna för ett nytt ändamål (utan att behöva gå genom stegen igen) så får **det nya ändamålet inte vara oförenligt** med de tidigare ändamålen. Följande är *alltid förenligt* med tidigare ändamål: arkiv av allmänt intresse, vetenskaplig forskning, historisk forskning, statistik.

c) Minimera uppgifterna

Personuppgifterna ska vara **adekvata, relevanta och inte för omfattande** i förhållande till ändamålen. Inga ”bra-att-ha” uppgifter tillåts, bara nödvändiga uppgifter för ändamålen.

d) Korrekthet utifrån ändamålet

Personuppgifterna ska vara **korrekta** och, om nödvändigt, **uppdaterade**. Säkerställ att personuppgifter som är felaktiga, i förhållande till ändamål, snabbt raderas eller rättas.

e) Minimera lagring

Personerna ska **inte kunna identifieras under längre tid än vad som är nödvändigt** utifrån ändamålen (t.ex. att man anonymiserar uppgifter efter en tid eller helt tar bort dem).

Men om man *enbart* behandlar för syftena arkiv av allmänt intresse, vetenskaplig forskning, historisk forskning eller statistik får man lagra personuppgifterna under längre tid.

f) Integritet och konfidentialitet

Man måste använda lämpliga tekniska eller organisatoriska åtgärder för att **säkerställa lämplig säkerhet**, t.ex. skydd mot obehörig/otillåten behandling, skydd mot förlust/förstöring/ skada genom olyckshändelse.

Ansvar – Personuppgiftsansvarige ansvarar för och ska **kunna visa** att ovanstående punkter efterlevs.

Svenska kyrkan
KYRKOKANSLIET

STEG 3

Är det en KÄNSLIG personuppgift? (artikel 9)

Det finns extra regler för personuppgifter som avslöjar t.ex. religiös övertygelse, medlemskap i fackförening, etniskt ursprung och hälsa. Dessa är känsliga personuppgifter.

För att behandla känslig personuppgift krävs – förutom att man klarat steg 1 och 2 – en av följande:

a) Personen har **uttryckligen samtyckt** till att de känsliga personuppgifterna behandlas för det **specifika ändamålet**

b) Nödvändig behandling pga. skyldigheter/rättigheter inom **arbetsrätt** och social trygghet (t.ex. för att följa kollektivavtal). Svenskt förslag: Uppgifterna får endast ges vidare till tredje part med samtycke eller pga. skyldighet inom arbetsrätten.

c) *Personen kan inte samtycka och det gäller egna grundläggande intressen (t.ex. medvetslös, behöver sjukvård)*

d) Icke vinstdrivande organ med t.ex. **religiöst syfte** får behandla uppgifterna inom ramen för berättigad verksamhet med lämpliga skyddsåtgärder. Det gäller bara medlemmar, tidigare medlemmar och personer som har regelbunden kontakt. **DOCK får uppgifterna inte lämnas ut utanför organet om inte personen har samtyckt till det.***

e) Personen har tydligt **offentliggjort uppgifterna** (t.ex. kandiderat i kyrkoval, deltagit i TV-soffa)

f) **Rättsliga anspråk** eller domstolars dömande

g) Viktigt allmänt intresse som svensk lag bestämmer

h) *Förebyggande hälso- och sjukvård*

i) *Folkhälsa*

j) **Arkiv av allmänt intresse, vetenskaplig forskning, historisk forskning, statistik**

*** Hur gäller d) i förhållande till kyrkans lagstadgade handlingsoffentlighet?**

Det är än så länge osäkert. Vi har i augusti 2017 skrivit till regeringen och informerat om att utifrån förslagen i SOU 2017:39 så kommer kyrkan inte kunna följa handlingsoffentligheten när det gäller känsliga uppgifter om personer. Regeringen/riksdagen är de enda som kan göra så att vi får fortsätta lämna ut.

Svenska kyrkan
KYRKOKANSLIET

STEG 4

INFORMATIONSPLIKT till personen (artikel 13 och 14)

Omfattning av informationen?

Oavsett om uppgifterna samlas in *från personen* eller *från annat håll* finns detaljerade krav i artikel 13 och 14 på vilken slags information den personuppgiftsansvarige måste ge till den registrerade personen. Observera att också när behandlingen baseras på samtycke måste vi ge informationen!

Viss information vi ska ge är generell, t.ex. vem som är personuppgiftsansvarig och om uppgifterna kan hamna utanför EU (=tredje land). Annan information handlar specifikt om behandlingen/behandlingarna, t.ex. ändamålet/ändamålen, vilken grund vi använder, hur länge uppgifterna sparas i systemet och vilka som har eller kan få tillgång till uppgifterna.

När måste vi ge informationen?

- Om vi samlar in uppgifterna från personen: samtidigt som vi får uppgifterna från personen.

  MEN vi *behöver inte ge* information som personen redan förfogar över (artikel 13.4)

- I alla andra fall:
  - om uppgifterna används för kommunikation med personen
    – när den första kommunikationen görs till personen
  - om uppgifterna tros eller planeras lämnas ut
    – när uppgifterna lämnas ut första gången
  - övriga fall
    – senast en månad efter vi fick uppgifterna

  MEN vi *behöver inte ge* information (art 14.5)

  – som personen redan förfogar över

  – som skulle innebära oproportionerlig ansträngning, MEN då får vi se till att internetpublicera informationen istället eller på annat sätt informera generellt

  – om erhållande/utlämnande av uppgifter står i svensk lag

  – om uppgifter som inte får röjas pga. tystnadsplikt/sekretess