IMY. Integritetsskydds myndigheten

Vi arbetar för att skydda alla dina personuppgifter, till exempel om hälsa och ekonomi, så att de hanteras korrekt och inte hamnar i orätta händer.

IMY. Integritetsskydds myndigheten

Våren 2022

Grundkurs i dataskyddsförordningen (GDPR) för dig inom offentlig sektor - distans

Introduktion

Den här presentationen bygger på den information som ingår i IMY:s grundkurs i dataskyddsförordningen (GDPR)
.

På flera av sidorna finns en ruta med mer information om ämnet. Det är både hänvisningar till artiklarna i GDPR, länkar till vår webbplats och EDPB:s riktlinjer.

Innehåll

- Viktiga begrepp
- Grundläggande principer
- Syfte och tillämpningsområde
- Rättslig grund
- Känsliga personuppgifter
- De registrerades rättigheter
- Personuppgiftsansvarig och personuppgiftsbiträde
- Personuppgiftsincidenter och tredjelandsöverföringar
- Informationssäkerhet
- Konsekvensbedömningar och förhandssamråd

Viktiga begrepp

Personuppgifter

All slags information som kan knytas till en levande fysisk person.

En personuppgift är en identifierare som direkt eller indirekt kan leda till en fysisk person i livet. Det kan till exempel vara:

- Personnummer
- Namn
- Adress
- Kontaktuppgifter
- Bilder
- Fingeravtryck

Mer information

https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/introduktion-till-gdpr/personuppgifter/

Rättsinformation:
Artikel 4.1, skäl 26-30 GDPR

Känsliga personuppgifter

Behandling som avslöjar:

- Etniskt ursprung
- Politiska åsikter
- Religiös eller filosofisk övertygelse
- Medlemskap i fackförening
- Uppgifter om hälsa
- Sexualliv eller sexuell läggning
- Genetiska uppgifter
- Biometriska uppgifter

➢ För att få behandla känsliga personuppgifter krävs det särskilt stöd.

Mer information

https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/introduktion-till-gdpr/personuppgifter/kansliga-personuppgifter/

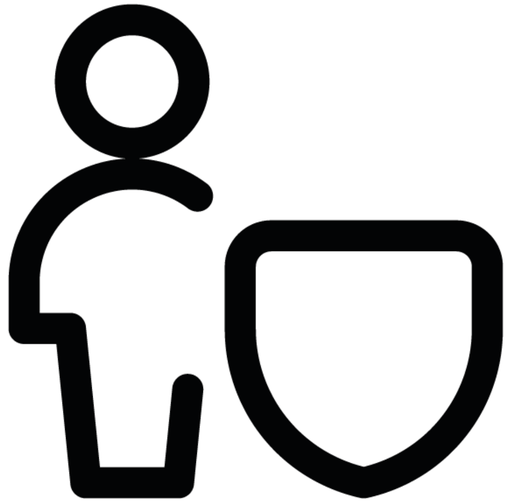
Rättsinformation:

Artikel 9.1, skäl 51 GDPR

3 kap. dataskyddslagen

Den registrerade

- Den fysiska person vars personuppgifter behandlas.



Mer information
Rättsinformation:
Artikel 4.1, skäl 26, 37, 51 GDPR

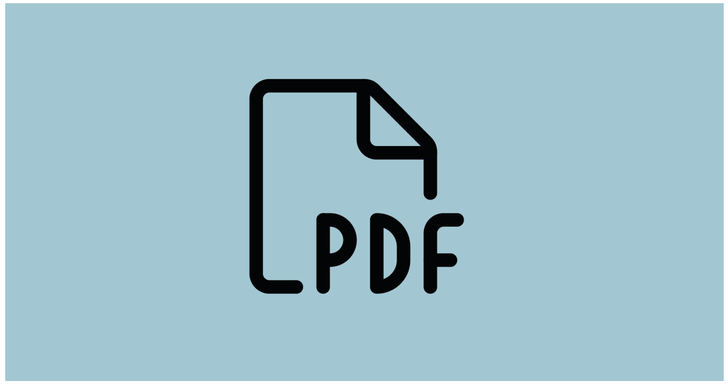
Behandling är en åtgärd som innebär att personuppgifter…

- Samlas in
- Registreras
- Organiseras
- Struktureras
- Lagras
- Bearbetas
- Ändras
- Tas fram
- Läses
- Används
- Lämnas ut
- Överförs
- Sprids
- Justeras
- Sammanförs
- Begränsas
- Raderas
- Förstörs

Mer information
Rättsinformation:
Artikel 4.2, skäl 26, 37, 51 GDPR

Vanliga behandlingar

- Skicka e-post



- Spara en PDF-fil

- Registrerade fyller i online-formulär

Personuppgiftsansvarig

En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter.

Mer information

https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/personuppgiftsansvariga-och-personuppgiftsbitraden/

EDPB:s riktlinjer:

https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf

Rättsinformation:

Artikel 4.7, skäl 26, 37, 51 GDPR

Personuppgiftsbiträde

- Behandlar personuppgifter för den personuppgiftsansvarigas räkning enligt dennes instruktioner.

- Har egna skyldigheter under förordningen
  - Står också under IMY:s tillsyn.

- Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ.

Mer information

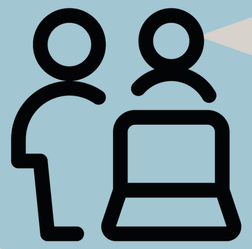
https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/personuppgiftsansvariga-och-personuppgiftsbitraden/att-tanka-pa-som-personuppgiftsbitrade/

EDPB:s riktlinjer:

https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf

Rättsinformation:

Artikel 4.8 och 28, skäl 26, 37, 51 GDPR



Dataskyddsombud

- Dataskyddsombudets uppgifter är bland annat att hjälpa och stötta den personuppgiftsansvariga i att uppfylla GDPR:s regler.
- Om man har skyldighet att utse ett dataskyddsombud, ska det anmälas till IMY. Detta för att vi enkelt ska kunna komma i kontakt med organisationen.
- Både en fysisk person, en grupp eller organisation kan vara dataskyddsombud.

Mer information

https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/dataskyddsombud/

EDPB:s riktlinjer: https://ec.europa.eu/newsroom/article29/items/612048

Rättsinformation:
Artikel 37-39, skäl 97 GDPR

Korrigerande befogenheter

- Vi kan utfärda en skriftlig varning till den som planerar en behandling som sannolikt kommer att bryta mot reglerna.
- Om en verksamhet bryter reglerna kan vi utfärda en reprimand vid mindre allvarliga överträdelser.
- Vi har i vissa situationer möjlighet att förelägga eller förbjuda den som behandlar personuppgifter att vidta olika åtgärder, vi kan också begränsa hur behandlingen får gå till.
- Utöver eller istället för övriga korrigerande åtgärder kan vi besluta om att ta ut en sanktionsavgift på högst 10 miljoner kronor för myndigheter.

Mer information

https://www.imy.se/om-oss/vart-uppdrag/sa-arbetar-vi-med-tillsyn/vad-kan-tillsynen-leda-till/

Rättsinformation:

Artikel 58, 83, skäl 148-152 GDPR

Tredjelandsöverföring

- När personuppgifter överförs från ett land inom EU och EES till ett land utanför detta område.
- Det krävs särskilt stöd i GDPR för att få överföra personuppgifter till ett tredje land.

Mer information

https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/overforing-till-tredje-land/

Rättsinformation:

Artikel 44-50, skäl 101-116 och 169 GDPR

Grundläggande principer

Grundläggande principer

- Genomsyrar all personuppgiftsbehandling.
- De grundläggande principerna är vägen in och vägen ut ur dataskyddsförordningen.
- Den som behandlar personuppgifter bör ha för vana att alltid påbörja och avsluta varje personuppgiftsbehandling med att gå igenom de grundläggande principerna.

De grundläggande principerna

- Laglighet, korrekthet och öppenhet
- Ändamålsbegränsning
- Uppgiftsminimering
- Riktighet
- Lagringsminimering
- Integritet och konfidentialitet
- Ansvarsskyldighet

Mer information

https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/grundlaggande-principer/

Rättsinformation:

Artikel 5, skäl 39, 50, 58 och 60 GDPR

Laglighet, korrekthet och öppenhet

All personuppgiftsbehandling måste:

- Ha lagligt stöd
- Vara korrekt
- Präglas av öppenhet

Mer information

https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/grundlaggande-principer/

Rättsinformation:

Artikel 5.1.a GDPR

Ändamålsbegränsning

Personuppgifter får:

- endast behandlas för särskilda, uttryckligt angivna och berättigade ändamål
- inte behandlas för ändamål som är oförenliga med det ursprungliga

Mer information
https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/grundlaggande-principer/

Rättsinformation:
Artikel 5.1.b och 6.4 GDPR

Uppgiftsminimering

- Utgår från ändamålen med behandlingen.
- Den personuppgiftsansvariga får inte behandla fler personuppgifter än vad som är nödvändigt för att uppnå ändamålen med behandlingen.

Mer information

https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/grundlaggande-principer/

Rättsinformation:

Artikel 5.1.c GDPR

Riktighet

- Personuppgifterna ska vara riktiga och om nödvändigt uppdaterade.

- Oriktiga personuppgifter ska:
  - raderas om inte längre behövs för ändamålet
  - rättas så fort som möjligt

➢ Viktigt att den personuppgiftsansvariga har rutiner för att rätta eller radera oriktiga personuppgifter.

Mer information
https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/grundlaggande-principer/

Rättsinformation:
Artikel 5.1.d GDPR

Lagringsminimering

- Personuppgifter får endast sparas så länge som de behövs för ändamålet med personuppgiftsbehandlingen.
- När personuppgifterna inte längre behövs för ändamålet ska de raderas eller avidentifieras.
- I vissa fall måste den personuppgiftsansvariga spara uppgifterna längre, till exempel genom andra rättslig förpliktelser.
- Den personuppgiftsansvariga bör införa tidsfrister för gallring eller regelbunden kontroll.

Mer information

https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/grundlaggande-principer/

Rättsinformation:

Artikel 5.1.e GDPR

Integritet och konfidentialitet

- Personuppgifterna ska skyddas med lämpliga tekniska och organisatoriska åtgärder så att de inte blir åtkomliga för obehöriga, förstörs eller skadas.

➢ Det handlar inte bara om teknik. Det omfattar rutiner och instruktioner också.

Mer information

https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/grundlaggande-principer/

Rättsinformation:
Artikel 5.1.f GDPR

Ansvarsskyldighet

Den personuppgiftsansvariga ska:

- ansvara för att de grundläggande principerna följs
- kunna visa att de grundläggande principerna följs

Gentemot vem?

- IMY
- Registrerade personer
- Kanske till och med media?

Mer information

https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/grundlaggande-principer/

Rättsinformation:

Artikel 5.2 GDPR

Mer om personuppgiftsansvarigas skyldigheter: artikel 24.1-3, 25, 26, 30 med flera.

Bra att ta med sig

- Det finns personuppgifter och så finns det känsliga personuppgifter
- En registrerad är den person vars personuppgifter behandlas
- Behandling av personuppgifter innebär att personuppgifter till exempel samlas in, registreras, ändras eller raderas
- Personuppgiftsansvarig är den som bestämmer ändamål och medel för personuppgiftsbehandlingen
- De grundläggande principerna ska genomsyra all behandling av personuppgifter

Syfte och tillämpningsområde

Alla har rätt till skydd av sina personuppgifter

Varför dataskyddsförordningen (GDPR)?

- Gemensamma regler och lika tillämpning i EU
- Regler anpassade för ett digitaliserat samhälle
- Stärkta och tydliga rättigheter och skyldigheter

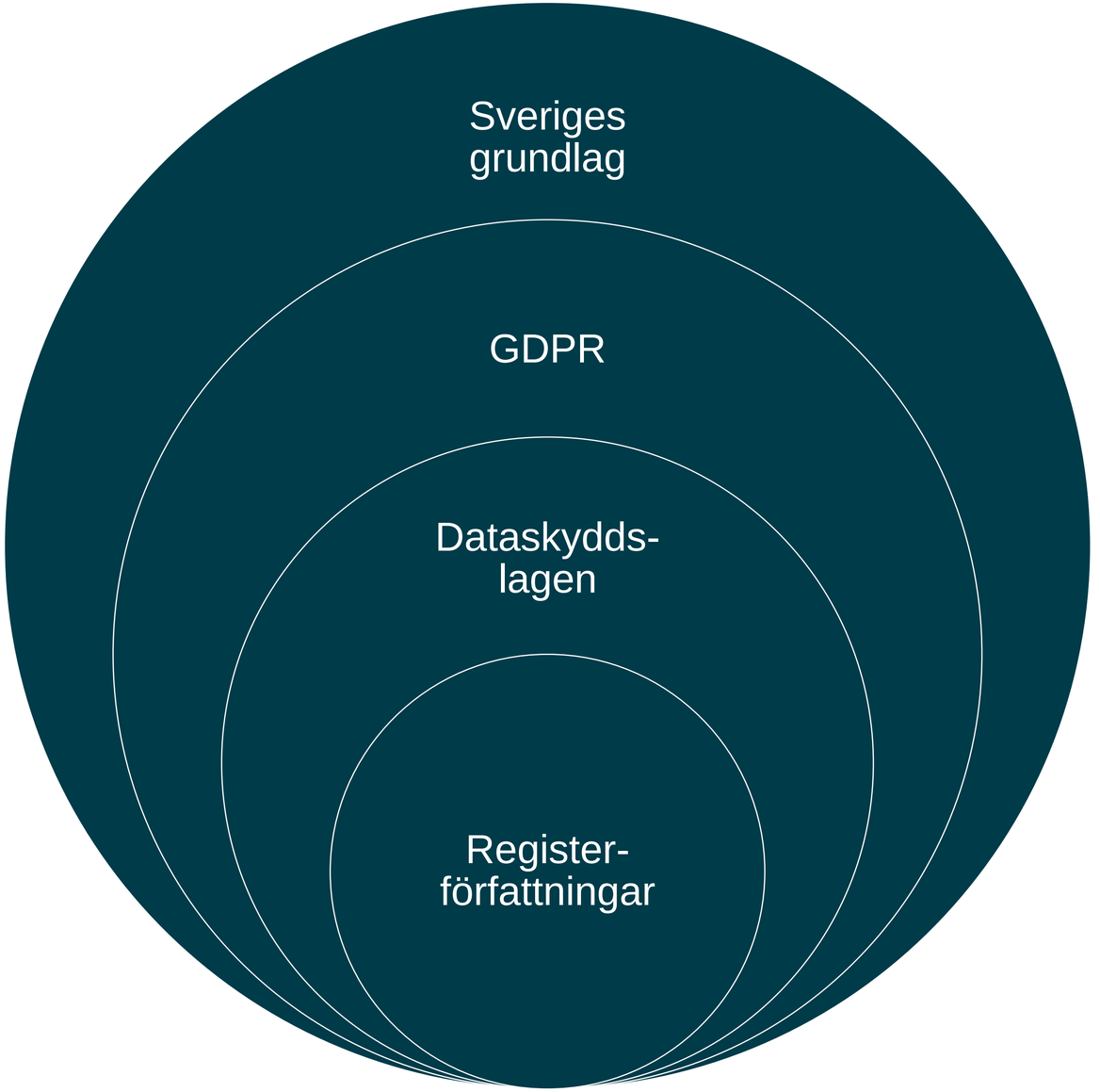
Mer information

https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/introduktion-till-gdpr/syfte-och-tillampningar/

Rättsinformation:

Artikel 3, skäl 22-25 GDPR

Rätten till privatliv



Europakonventionen och EU:s rättighetsstadga

För vilka aktörer gäller GDPR?

- Etablerad inom EU/EES (artikel 3.1)

  - *Har ett verksamhetsställe i EU och behandlar personuppgifter med koppling till verksamheten i EU*

- Etablerad utanför EU/EES men (artikel 3.2)
  - Erbjuder varor och tjänster till EU/EES (se till språk, valuta m.m.)
  - Övervakar beteenden inom EU/EES (spårar och profilerar)

När gäller dataskyddsförordningen (GDPR)?

- Helt eller delvis **automatiserad** behandling av personuppgifter
- *Helt automatiserad – behandling som sker elektroniskt*
  Delvis automatiserad – t.ex. uppgifter som samlas in manuellt och sedan sammanställs elektroniskt

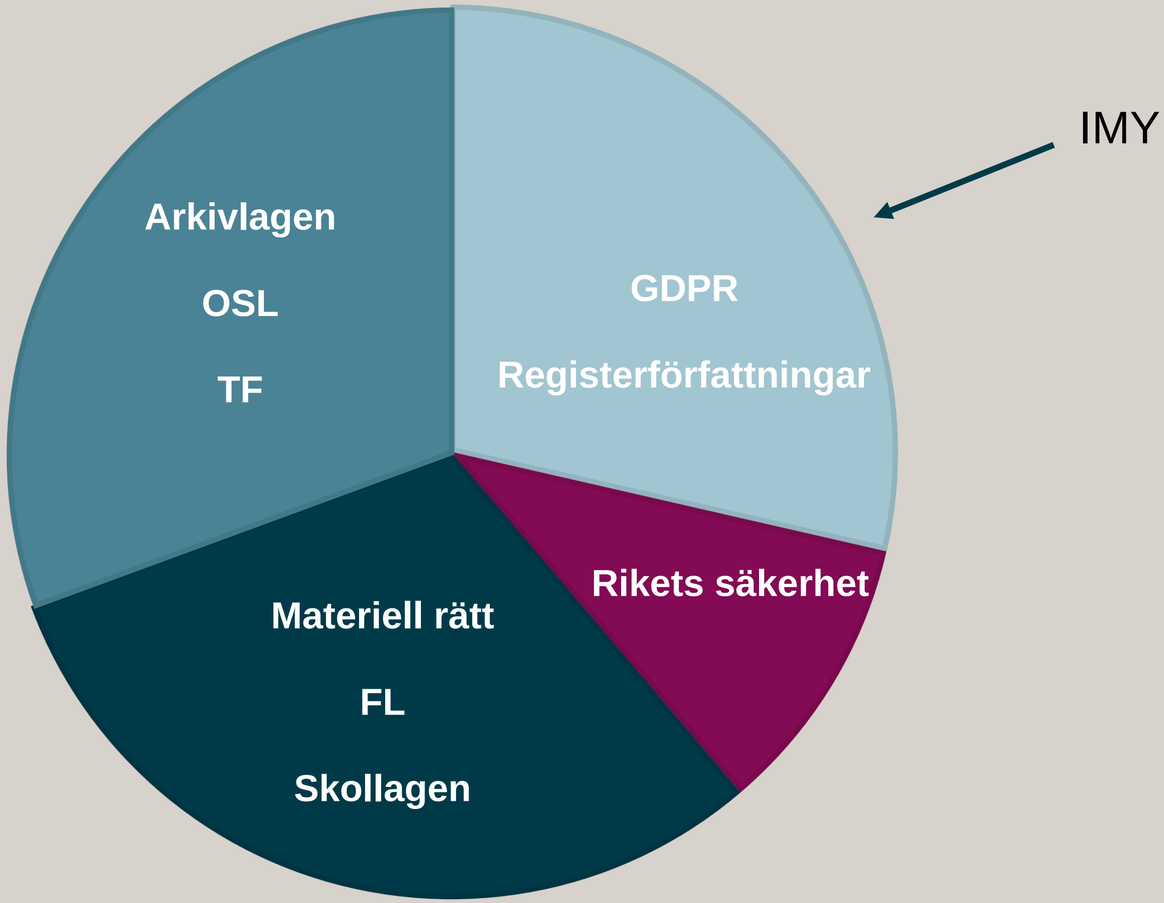
- Manuell behandling (om register)
- *Det avgörande är om information om en person kan erhållas med lätthet.*

- Undantag

För vilka personuppgiftsbehandlingar gäller inte GDPR?

- **Privat behandling**
  (t.ex. semesterfoton)
- **Avlidna personer**
- **Grundlagsskyddad personuppgiftsbehandling**
  (traditionella medier, webbplatser med utgivningsbevis)
- **Allmänna handlingar**
  (offentlighetsprincipen hindras inte)
- **Brottsbekämpande verksamhet**
  (regleras av särskilt EU-direktiv)

Regelverk


Arkivlagen
OSL
TF
GDPR
Registerförfattningar
IMY
Rikets säkerhet
Materiell rätt
FL
Skollagen

Bra att ta med sig

- Syftet med GDPR är att se till att enskildas personuppgifter skyddas.
- Enhetlig tillämpning av GDPR i EU/EES.
- Rätten till privatliv är en grundläggande mänsklig rättighet och följer av Europakonventionen och EU:s rättighetsstadga.
- Flera regelverk ska tillämpas parallellt och får inte stå i strid med varandra.

Rättslig grund

Rättslig grund

- Det finns 6 stycken rättsliga grunder.
- Det måste finnas stöd i en rättslig grund för att en personuppgiftsbehandling ska vara tillåten.
- Det är den personuppgiftsansvarige som måste se till att det finns stöd i en rättslig grund.

Mer information
https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/rattslig-grund/

Rättsinformation:
Artikel 6 GDPR

Vilka är de rättsliga grunderna?

- Samtycke

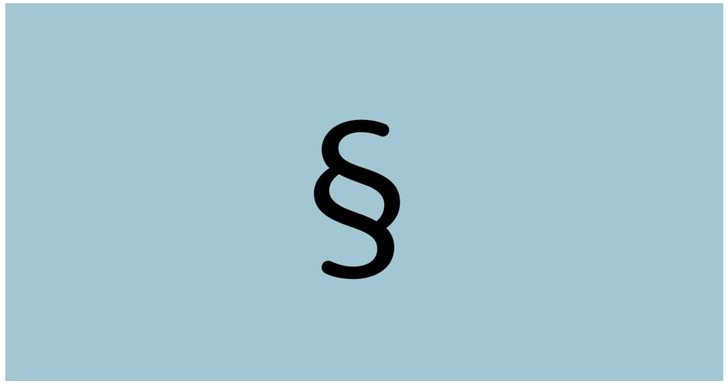
Eller

- Annat

Mer information
https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/rattslig-grund/

Rättsinformation:
Artikel 6 GDPR

Rättsliga grunder – behandlingen är nödvändig för:



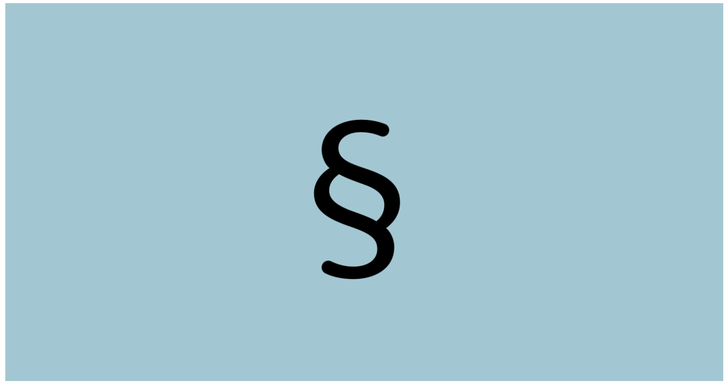
- Avtal (artikel 6.1 b)
- **Rättslig förpliktelse** (artikel 6.1 c)

- Grundläggande intresse (artikel 6.1 d)
- Intresseavvägning (artikel 6.1 f)

- **Uppgift av allmänt intresse** (artikel 6.1 e)
- **Myndighetsutövning** (artikel 6.1 e)

Mer information
Rättsinformation:
Artiklarna 6.1 b-6.1 f GDPR
EU-domstolens domar C-524/06, C-342/12 och C-708/18
Prop. 2017/18:105 s. 46 ff.

Rättsliga grunder – behandlingen är nödvändig för:



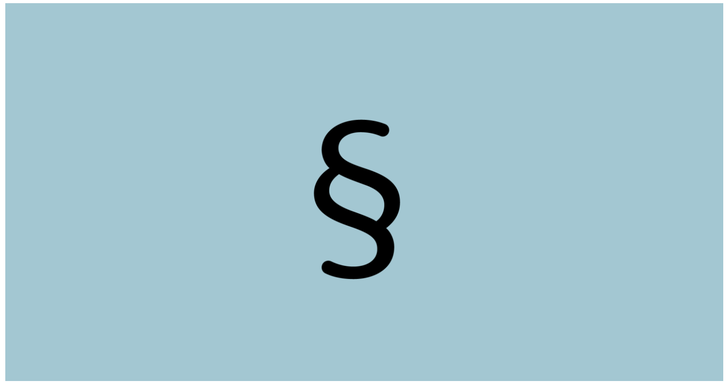
- Rättslig förpliktelse (artikel 6.1 c)

- Uppgift av allmänt intresse (artikel 6.1 e)

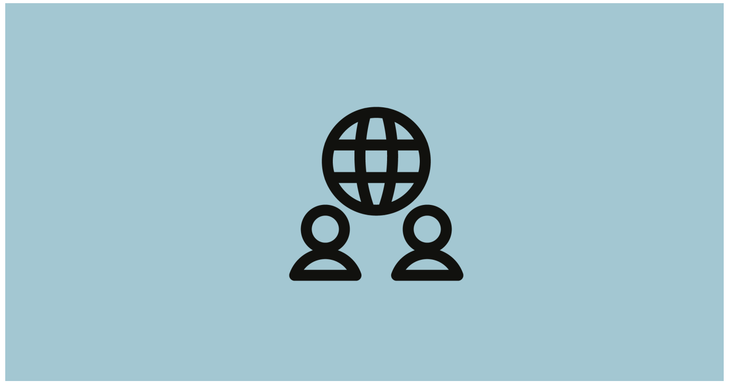
- Myndighetsutövning (artikel 6.1 e)

Mer information
Rättsinformation:
Artiklarna 6.1 c, 6.1 e, skäl 39 GDPR
EU-domstolens domar C-524/06, C-342/12 och C-708/18
Prop. 2017/18:105 s. 46 ff.

Fastställda i unionsrätt eller nationell rätt



- Rättslig förpliktelse



- Uppgift av allmänt intresse

- Myndighetsutövning

- Uppfyller ett mål av allmänt intresse
- Är proportionell

Mer information
Rättsinformation:
Artikel 6.2 och 6.3, skäl 41 GDPR
Prop. 2017/18:105 s. 45 ff.

Rättslig förpliktelse – dataskyddslagen

- Lag
- Annan författning
- Kollektivavtal
- Beslut med stöd av lag eller annan författning

Mer information

https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/rattslig-grund/rattslig-forpliktelse/

Rättsinformation:
Artikel 6.1.c, 6.3 skäl 45 GDPR
2 kap. 1 § dataskyddslagen
Proposition 2017/18:105 s. 52 ff.

Myndighetsutövning – dataskyddslagen

Som ett led myndighetsutövning enligt

- Lag
- Annan författning

Mer information

https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/rattslig-grund/myndighetsutovning-och-uppgifter-av-allmant-intresse/

Rättsinformation:
Artikel 6.1 e GDPR
2 kap. 2 § punkt 2 dataskyddslagen
Prop. 2017/18:105 s. 62 f.

Uppgift av allmänt intresse – dataskyddslagen

Uppgift av allmänt intresse som följer av

- Lag
- Annan författning
- Beslut med stöd av lag eller annan författning

Mer information

https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/rattslig-grund/myndighetsutovning-och-uppgifter-av-allmant-intresse/

Rättsinformation:
Artikel 6.1 e GDPR
2 kap. 2 § punkt 1 dataskyddslagen
Prop. 2017/18:105 s. 55 ff.

Samtycke?

- Frivilligt
- Specifikt
- Informerat
- Otvetydigt

Mer information

https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/rattslig-grund/samtycke/

EDPB:s riktlinjer:
https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_sv.pdf

Rättsinformation:
Artikel 6.1 a, skäl 32, 38, 42-43 GDPR

Bra att ta med sig

- Det ska finnas en tillämplig rättslig grund i artikel 6 GDPR, annars är behandlingen olaglig.
- Behandlingen ska vara nödvändig vid användning av de rättsliga grunderna artikel 6.1 b-6.1 f GDPR.
- De rättsliga grunderna rättslig förpliktelse, allmänt intresse och myndighetsutövning kräver stöd i rättsordningen utöver GDPR.
- Samtycke är oftast en olämplig rättslig grund för myndigheter.
- Myndigheter kan inte använda sig av den rättsliga grunden intresseavvägning när myndigheterna fullgör sina uppgifter.

Känsliga personuppgifter

Känsliga personuppgifter

Mer information
https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/introduktion-till-gdpr/personuppgifter/kansliga-personuppgifter/

Rättsinformation:
Artikel 9.1, skäl 51 GDPR
3 kap. dataskyddslagen
Prop. 2017/18:105 s. 74 ff.

- Hälsa
- Genetiska uppgifter
- Biometriska uppgifter
- Religiös eller filosofisk övertygelse

- Politiska åsikter
- Medlemskap i fackförening
- Sexualliv eller sexuell läggning
- Etniskt ursprung

Undantag

- Uttryckligt samtycke
- Viktigt allmänt intresse
- Hälso- och sjukvård och social omsorg
- Allmänt intresse på folkhälsoområdet
- Organisation med politiskt, filosofiskt, religiöst eller fackligt syfte
- Arbetsrätt
- Tydligt offentliggörande
- Arkiv, forskning, statistik
- Grundläggande intressen
- Rättsliga anspråk

Undantag som kräver unionsrätt eller nationell rätt

- Arbetsrätt
- Viktigt allmänt intresse
- Hälso- och sjukvård och social omsorg
- Allmänt intresse på folkhälsoområdet
- Arkiv, forskning, statistik

Mer information

https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/introduktion-till-gdpr/personuppgifter/kansliga-personuppgifter/myndigheter-och-kansliga-personuppgifter/

Rättsinformation:

3 kap. dataskyddslagen

Prop. 2017/18:105 s. 74 ff.

Viktigt allmänt intresse – dataskyddslagen

Får behandlas av myndighet om

- uppgifterna har lämnats till myndigheten och behandlingen krävs enligt lag
- nödvändigt för handläggning av ett ärende
- nödvändigt med hänsyn till ett viktigt allmänt intresse och inte otillbörligt intrång i personlig integritet

Mer information

https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/introduktion-till-gdpr/personuppgifter/kansliga-personuppgifter/myndigheter-och-kansliga-personuppgifter/

Rättsinformation:

3 kap. 3 § dataskyddslagen

Prop. 2017/18:105 s. 80 ff.

Personnummer och samordningsnummer – dataskyddslagen

Får behandlas

- med stöd av samtycke
- när det är **klart motiverat** med hänsyn till
  - ändamålet med behandlingen,
  - vikten av säker identifiering, eller
  - något annat beaktansvärt skäl

Mer information
https://www.imy.se/privatperson/dataskydd/introduktion-till-gdpr/vad-ar-personuppgifter/personnummer/

Rättsinformation:
3 kap. 10 § dataskyddslagen
Prop. 2017/18:105 s. 101 ff.

Kom ihåg!

Rättslig grund

- GDPR
- Unionsrätt/nationell rätt
- Dataskyddslagen

Känsliga personuppgifter

- GDPR
- Unionsrätt/nationell rätt
- Dataskyddslagen

Bra att ta med sig

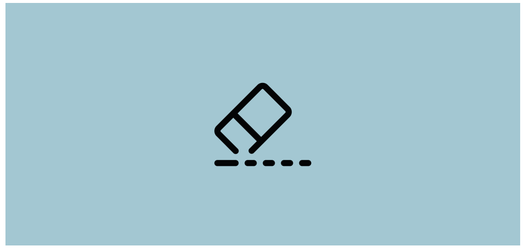
- Uttryckligt förbud mot behandling av känsliga personuppgifter.
- Omfattar samtliga uppgifter som faller inom begreppet, oavsett bedömning i det enskilda fallet.
- Den personuppgiftsansvariga måste kunna stödja sig på ett av undantagen för att en behandling av känsliga personuppgifter ska vara laglig.
- Undantag finns både i GDPR, unionsrätt och nationell rätt.

De registrerades rättigheter

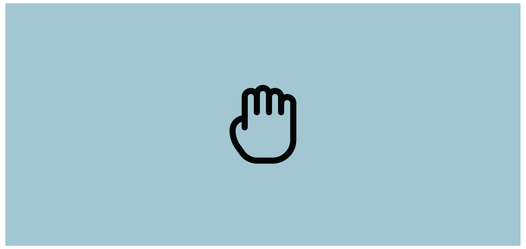
De viktigaste rättigheterna

Rätt till information (artikel 12-14)

Rätt till tillgång (registerutdrag) (artikel 15)



Rätt till rättelse (artikel 16)



Rätt att göra invändningar (artikel 21)

Rätt till radering (art. 17)

Mer information:
https://www.imy.se/privatperson/dataskydd/dina-rattigheter/

Rättsinformation:
Artikel 12-21, skäl 58-73 GDPR

Information och kommunikation

- Klar och tydlig
- Lätt att hitta och förstå
- Tillhandahålla information
- Tidsfrister
- Kostnadsfritt – undantag finns!

Mer information

https://www.imy.se/privatperson/dataskydd/dina-rattigheter/ratt-till-information/

EDPB:s riktlinjer: https://www.imy.se/globalassets/dokument/riktlinjer-om-oppenhet-och-information-till-registrerade.pdf

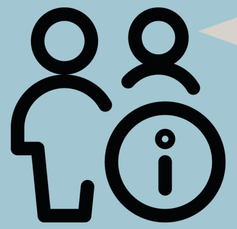
Rättsinformation:

Artikel 12, skäl 39, 58, 59, 60, 64 GDPR

Rätt till information

Vilken information ska ges?

- Vem som är personuppgiftsansvarig
- Kontaktuppgifter till den personuppgiftsansvariga
- Kontaktuppgifter till dataskyddsombudet
- Vilka personuppgifter som behandlas
- Varför personuppgifterna behandlas (ändamålen)
- Hur länge personuppgifterna behandlas
- Kategorier av mottagare av personuppgifterna
- I tillämpliga fall om överföring av personuppgifter till mottagare i ett tredjeland eller internationell organisation kommer ske
- Information om den registrerades rättigheter och möjligheten att inkomma med klagomål till IMY



Rätt till information

Hur ska informationen ges?

- ✓ Begriplig och lättillgänglig form
- ✓ Klart och tydligt språk

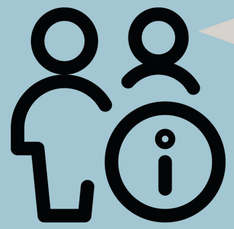
Mer information

https://www.imy.se/privatperson/dataskydd/dina-rattigheter/ratt-till-information/

EDPB:s riktlinjer: https://www.imy.se/globalassets/dokument/riktlinjer-om-oppenhet-och-information-till-registrerade.pdf

Rättsinformation:

Artikel 13-14, skäl 58-62 GDPR



Rätt till information

När ska informationen ges?

- Om personuppgifterna samlats in från den registrerade själv:
  - när uppgifterna samlas in
- Om personuppgifterna samlats in från någon annan:
  - inom en rimlig period,
  - vid första den första kontakten med den registrerade, eller
  - vid utlämnande till annan, men alltid
  - senast inom 1 månad
- Därutöver ska information alltid lämnas på begäran av den registrerade

Mer information

https://www.imy.se/privatperson/dataskydd/dina-rattigheter/ratt-till-information/

EDPB:s riktlinjer: https://www.imy.se/globalassets/dokument/riktlinjer-om-oppenhet-och-information-till-registrerade.pdf

Rättsinformation:

Artikel 13-14, skäl 58-62 GDPR

Rätt till tillgång (registerutdrag)

- Rätt att få kopia av personuppgifterna och information om behandlingen
- Elektronisk begäran
- Kostnadsfritt
- Identifiering

Begränsningar

- Får inte ha negativ inverkan på *andras* rättigheter och friheter
- Andra regelverk, t.ex. offentlighets- och sekretesslagen

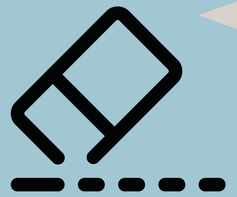
Mer information

https://www.imy.se/privatperson/dataskydd/dina-rattigheter/ta-del-av-dina-personuppgifter/

Rättsinformation:

Artikel 15, skäl 58-62 GDPR

Praxis från EU-domstolen: C-141/12 & C-372/12



Rätt till rättelse

- Rätta felaktiga personuppgifter
- Komplettera ofullständiga personuppgifter
- Se till den sektorsspecifika lagstiftningen

Mer information
https://www.imy.se/privatperson/dataskydd/dina-rattigheter/rattelse/

Rättsinformation:
Artikel 16 och 19, skäl 65 GDPR

Invändning och radering

- Beror på vilken rättslig grund
- Rätten till radering är inte ovillkorlig
- Se till de specifika omständigheterna

Mer information:
https://www.imy.se/privatperson/dataskydd/dina-rattigheter/att-gora-invandningar/

Rättsinformation:
Artikel 21, skäl 69-70 GDPR

https://www.imy.se/privatperson/dataskydd/dina-rattigheter/radering/

Rättsinformation:
Artikel 17 och 19, skäl 65-66 GDPR

Personuppgiftsansvarig och personuppgiftsbiträde

Personuppgiftsansvarig

- Bestämmer
  - Vilka personuppgifter som ska behandlas
  - Varför de ska behandlas (ändamål)
  - Hur de ska behandlas (medel)

- Personuppgiftsansvaret kan i vissa fall bestämmas genom lagstiftning.

Mer information

https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/personuppgiftsansvariga-och-personuppgiftsbitraden/

EDPB:s riktlinjer:
https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf

Artikel 4.7, skäl 26, 37, 51 GDPR

Gemensamt personuppgiftsansvar

- Två eller fler personuppgiftsansvariga som gemensamt fastställer ändamålen med och medlen för behandlingen
- Fastställ i ett gemensamt arrangemang vilken aktör som ansvarar för vad

Mer information

EDPB:s riktlinjer:
https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf

Artikel 26, skäl 79 GDPR
EU-domstolens domar C-210/16, C-25/17, C-40/17

Personuppgiftsbiträde

- En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvarigas räkning
- Får bara behandla personuppgifter på instruktion från den personuppgiftsansvariga.
- Upprätta personuppgiftsbiträdesavtal!

Mer information

https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/personuppgiftsansvariga-och-personuppgiftsbitraden/

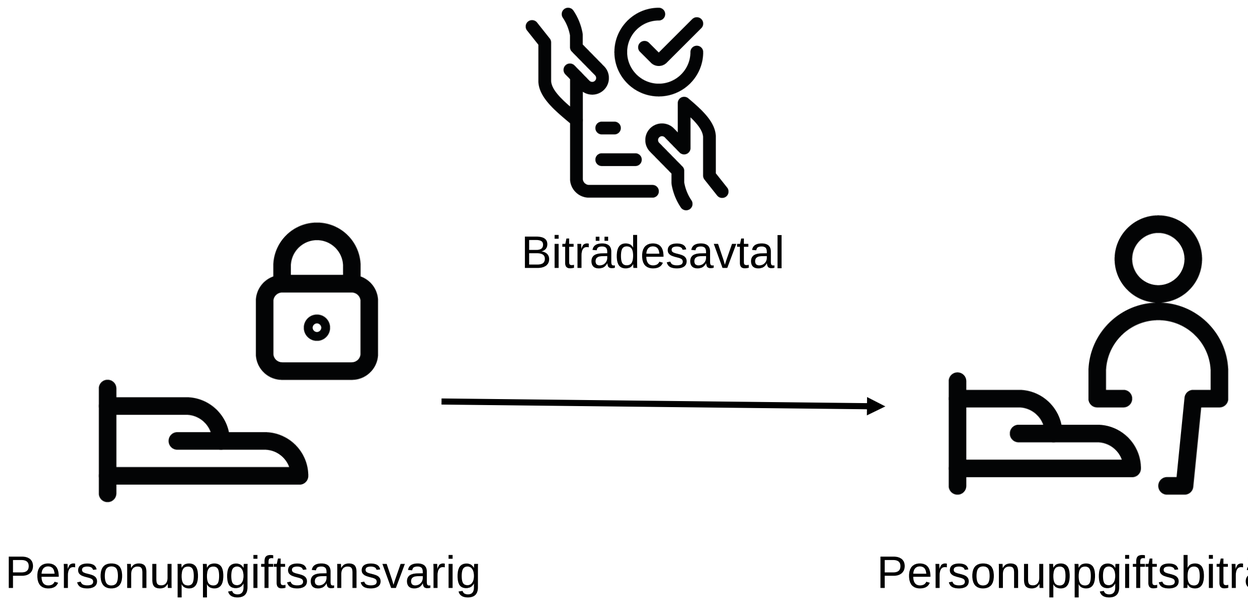
EDPB:s riktlinjer:

https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf

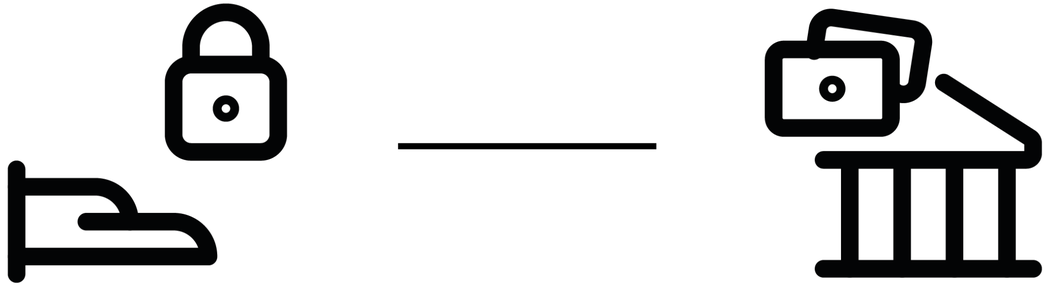
Rättsinformation:

Artikel 4.8 och 28, skäl 26, 37, 51 GDPR

Exempel: IT-support



Exempel: Bank



Personuppgiftsansvarig

Personuppgiftsansvarig

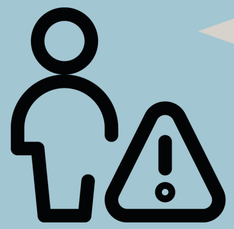
Exempel på arbetsmetod

1. Kartlägg personuppgiftsbehandlingen
2. Fastställ ansvarsfördelningen
3. Reglera och dokumentera förhållandet mellan inblandade aktörer

Bra att ta med sig

- Ha rutiner för hantering av registrerades rättigheter
- Tänk på tidsfristerna för hantering av rättigheterna
- Undersök vad den enskilde vill om det är oklart
- Personuppgiftsansvarig är den som bestämmer ändamål och medel för behandlingen av personuppgifter
- Reglera och dokumentera förhållandena mellan aktörerna

Personuppgiftsincidenter



En personuppgiftsincident är en säkerhetshändelse som leder till:

- Oavsiktlig eller olaglig förstöring, förlust eller ändring av personuppgifter
- Obehörigt röjande eller obehörig åtkomst till personuppgifter

➢ Av misstag eller medveten handling

Mer information

https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/personuppgiftsincidenter/

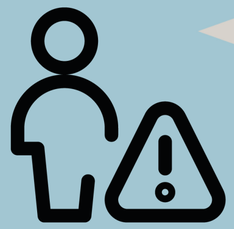
EDPB:s riktlinjer: https://www.imy.se/globalassets/dokument/anmalan-av-personuppgiftsincidenter-enligt-forordning-eu-2016_679.pdf

Rättsinformation:

Artikel 33-34, 58, 83, skäl 75, 85-88 GDPR

Anmäla till IMY?

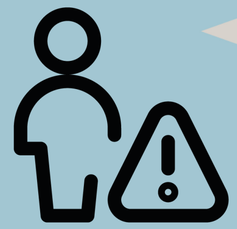
- Om risken är sannolik
- Inom 72 timmar från upptäckt
- E-tjänst på IMY.se
- Kan kompletteras



Begränsa och återställ

När en incident inträffat ska den personuppgiftsansvariga vidta åtgärder för att:

- Stoppa incidenten
- Minimera konsekvenserna

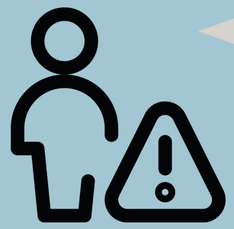


Bedöm riskerna

- Dokumentera alla incidenter internt!

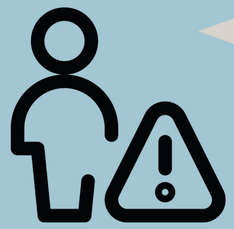
Utgå ifrån de unika parametrarna för den inträffade incidenten

- Typ av incident?
- Hur många påverkas?
- Hur lätt att identifiera?
- Typ av personuppgifter?
- Kategorier av registrerade?
- Vilka negativa konsekvenser kan det bli?
- Hur sannolika är de potentiella negativa konsekvenserna?



Exempel på risker

- Bedrägerier
- ID-kapning
- Ekonomisk förlust
- Förnedring
- Anseendeskada
- Psykiskt lidande

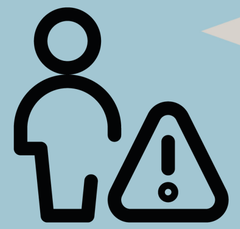


Informera de registrerade?

- Om hög risk
- Utan onödigt dröjsmål
- Vad ska informationen innehålla?
- Undantag

Omständigheter att ta hänsyn till vid en riskbedömning

- Typ av incident?
- Hur många påverkas? Hur lätta är de att identifiera?
- Kategorier av registrerade? Exempelvis barn eller andra särskilt utsatta?
- Typer av personuppgifter? Känsliga personuppgifter eller mer harmlösa?
- Vad kan uppgifterna användas till? Exempelvis ID-kapning.
- Vilka negativa konsekvenserna kan det bli? Exempelvis ekonomisk skada.
- Hur sannolika är de potentiella konsekvenserna och hur allvarliga kan de bli?



Dokumentera – ta ställning

- Alla personuppgiftsincidenter ska dokumenteras
- Vad som ska dokumenteras följer av artikel 33.5 i GDPR
  - De inträffade omständigheterna
  - Incidentens effekter
  - Vidtagna åtgärder
  - Om den personuppgiftsansvariga bedömer att en incident inte ska anmälas till IMY ska det motiveras varför

Information till de registrerade

- Om personuppgiftsincidenten sannolikt leder till en hög risk för de registrerades fri- och rättigheter ska de registrerade informeras enligt artikel 34 i GDPR.
- När ska informationen lämnas? – Så snart som möjligt.
- Vad ska informationen innehålla? – Inträffade omständigheter samt eventuella åtgärder som den registrerade behöver vidta. Se artikel 34.2 i GDPR.
- Hur ska informationen lämnas? – Det kommunikationsmedlet som vanligtvis används eller det som bäst kommer att nå de drabbade.
- Information behöver inte lämnas om:
  - Den personuppgiftsansvariga vidtagit lämpliga tekniska och organisatoriska åtgärder så att det inte längre finns någon sannolik risk för de registrerades fri- och rättigheter,
  - Vidtagit ytterligare åtgärder som har minskat risken,
  - Om det skulle innebära en oproportionerlig ansträngning att göra det

Bra att ta med sig

- Det är viktigt att din organisation har rutiner för personuppgiftsincidenter.
- En personuppgiftsincident ska anmälas till IMY inom 72 timmar om risken för de registrerade är sannolik.
- Gör en riskbedömning!
- Ni ska dokumentera alla personuppgiftsincidenter internt.

Tredjelandsöverföringar

Tredjelandsöverföringar

- Personuppgifter blir tillgängliga för någon utanför EU/EES
- Exempel: molntjänstleverantör utanför EU och e-post till mottagare utanför EU.
- Särskilt stöd i GDPR krävs
- Syfte
- Informera alltid de registrerade

Mer information

https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/overforing-till-tredje-land/

Europeiska dataskyddsstyrelsens riktlinjer om definition av begreppet tredjeland:

https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en

Rättsinformation:
Kapitel V GDPR
EU-domstolens dom C-311/18

När får man föra över uppgifter till tredje land?

- Adekvat skyddsnivå
- Lämpliga säkerhetsåtgärder
- Särskilda situationer och enstaka fall

Adekvat skyddsnivå

- Bedömning av EU-kommissionen
  - Länder
  - Internationella organisationer
  - Sektorer
- Utifrån ett antal aspekter
  - Mänskliga rättigheter,
  - Övrig lagstiftning
  - Tillsynsmyndighet
- Kräver inget särskilt tillstånd

Mer information

https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/overforing-till-tredje-land/adekvat-skyddsniva/

Rättsinformation:

EU-domstolens dom C-311/18

Länder med adekvat skyddsnivå

- Andorra
- Argentina
- Bailiwick of Guernsey
- Färöarna
- Isle of Man
- Israel
- Japan
- Jersey
- Nya Zeeland
- Schweiz
- Uruguay
- Storbritannien
- Kanada (i vissa fall)

Lämpliga skyddsåtgärder: Bindande företagsbestämmelser

- Internationell koncern
- Företagsinterna regler

- Ska godkännas av tillsynsmyndighet
- Yttrande av Europeiska dataskyddsstyrelsen

Lämpliga skyddsåtgärder: Standardavtalsklausuler

- Godkända av EU-kommissionen
- Skyldigheter för överförande och mottagande part
- Får ej ändras
- Finns tre alternativ

Mer information

https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/overforing-till-tredje-land/lampliga-skyddsatgarder/

Rättsinformation:

Artikel 46.2 GDPR

EU-domstolens dom C-311/18

Andra lämpliga skyddsåtgärder

- Rättsligt bindande instrument mellan myndigheter
- Godkända uppförandekoder och certifieringar
- Särskilt tillstånd från IMY

Särskilda situationer och enskilda fall

Några exempel

- Samtycke
- Avtal
- Allmänintresse
- Rättsliga anspråk
- Tvingande berättigade intressen

➢ Endast i undantagsfall

➢ Informera de registrerade

➢ Informera IMY

Mer information

https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/overforing-till-tredje-land/sarskilda-situationer-och-enstaka-overforingar/

EDPB:s riktlinjer:
https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_sv.pdf

Föra över uppgifter till USA

- Privacy Shield
- Schrems II-domen
- Oklart läge
- Ny principöverenskommelse
- Rekommendationer från Europeiska dataskyddsstyrelsen

Bra att ta med sig

- En tredjelandsöverföring är när personuppgifter görs tillgängliga för någon utanför EU/EES.
- En tredjelandsöverföring ska ha stöd i GDPR för att vara laglig.
- Det är ett fortsatt oklart läge rörande överföringar till USA.
- Överföringen ska följa alla andra regler i GDPR också.

Informationssäkerhet

Innehåll

- Informationssäkerhet och dataskydd
- Informationssäkerhet och dataskyddsförordningen
  - Säkerhet i samband med behandlingen, artikel 32
  - Säkerhetsåtgärder enligt dataskyddsförordningen
  - Tillämpning av säkerhetskraven

Informationssäkerhet och dataskydd

Vården varnas för cyberattacker: "Ökad aktivitet"

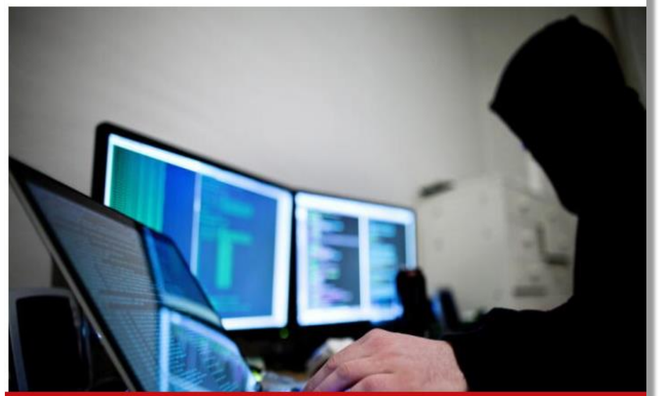
UPPDATERAD 2 NOVEMBER 2020 PUBLICERAD 2 NOVEMBER 2020

Bedragare fortsätter utnyttja coronaviruset för nätfiske

Försöker efterlikna myndigheter och kända organisationers hemsidor för att lura besökare att lämna över sina person- och bankuppgifter.

Utpressningsvirus mot svenska storföretag

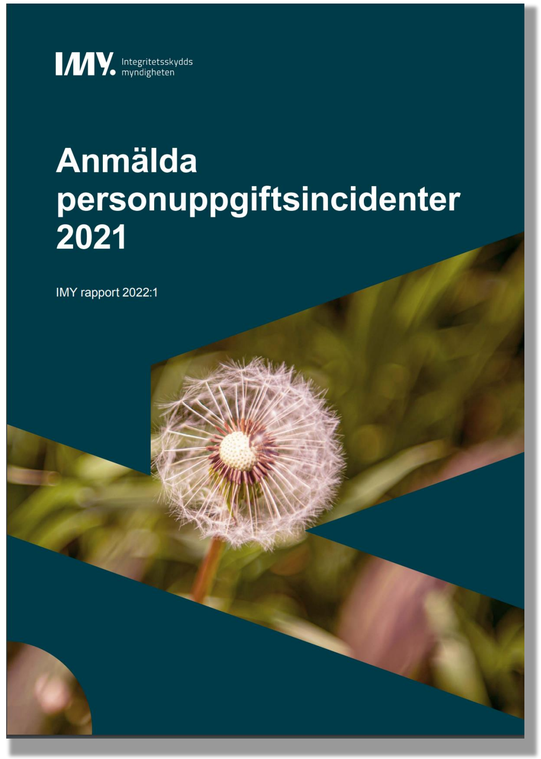
PUBLICERAD: 2020-11-12 12:20



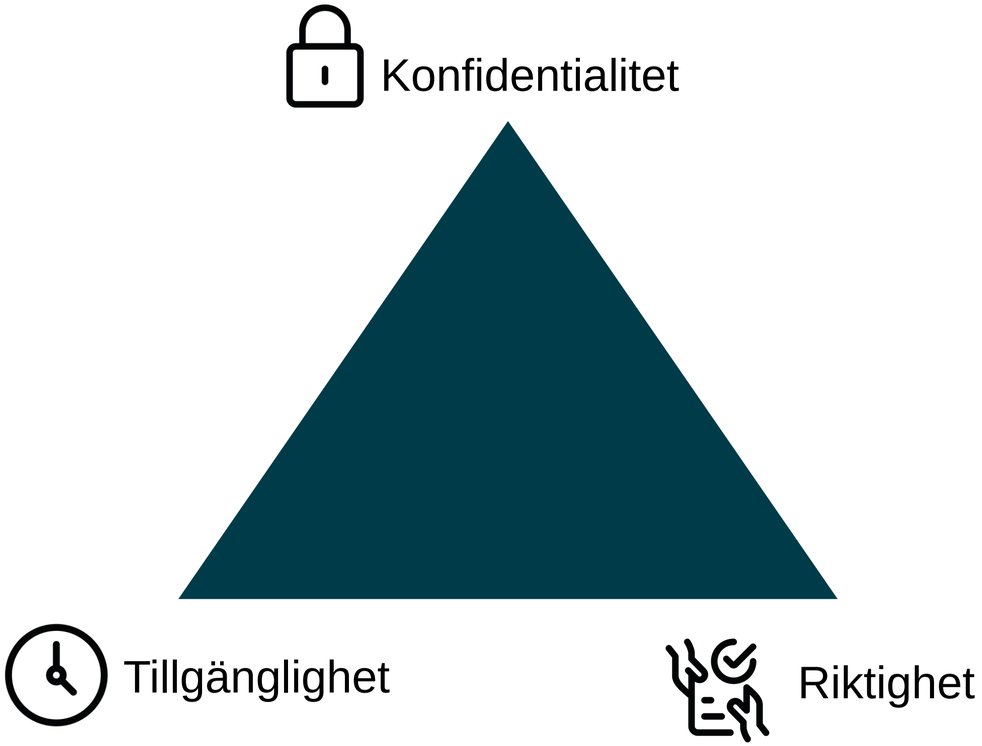
Digitala stöd ska stärka smittskyddsarbetet

Publicerad 05 november 2020

Regeringen ger E-hälsomyndigheten samt Folkhälsomyndigheten i uppdrag att genomföra kartläggningar av hur digitala stöd kan stärka och förenkla smittskyddsarbetet i Sverige och Europa.

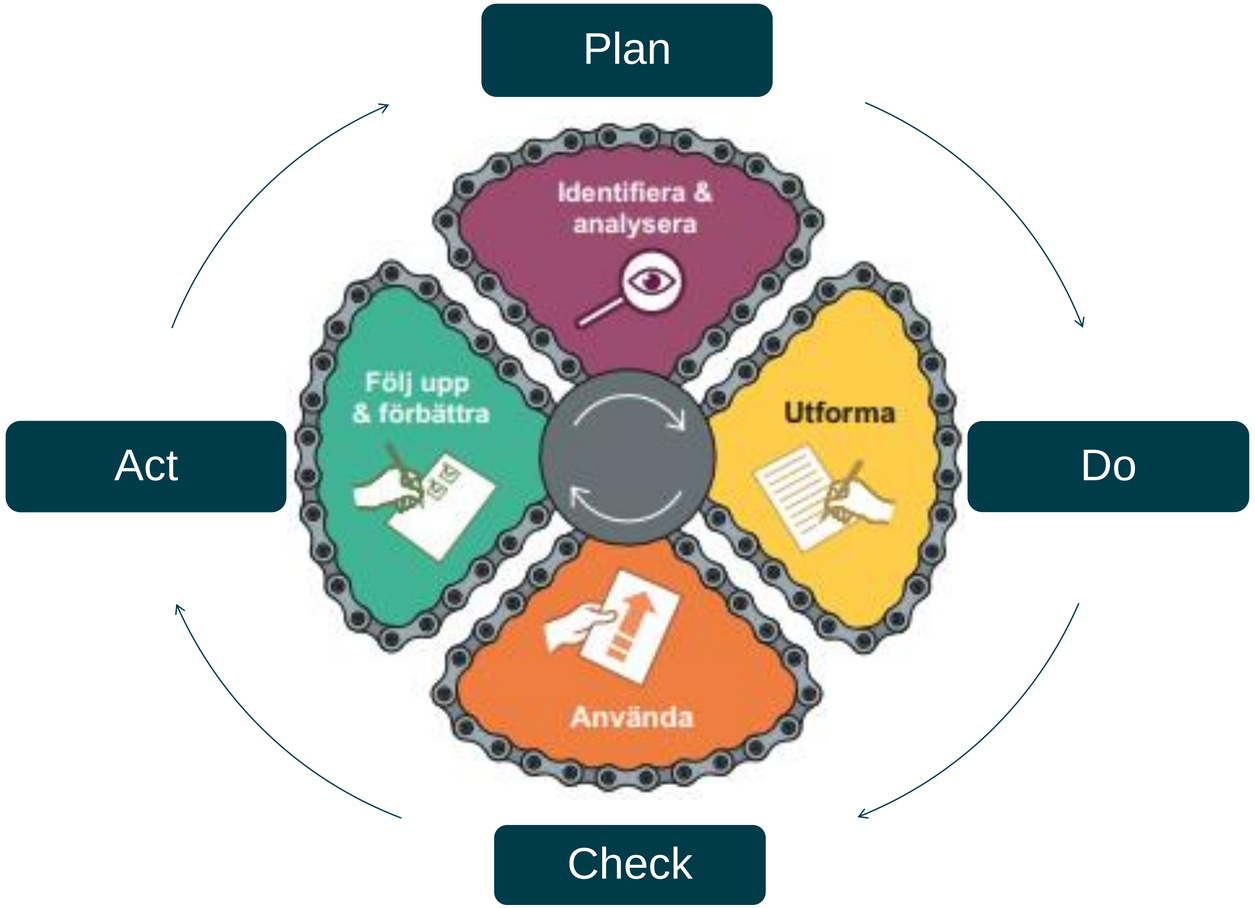


Informationssäkerhet handlar om att ge informationen rätt skydd

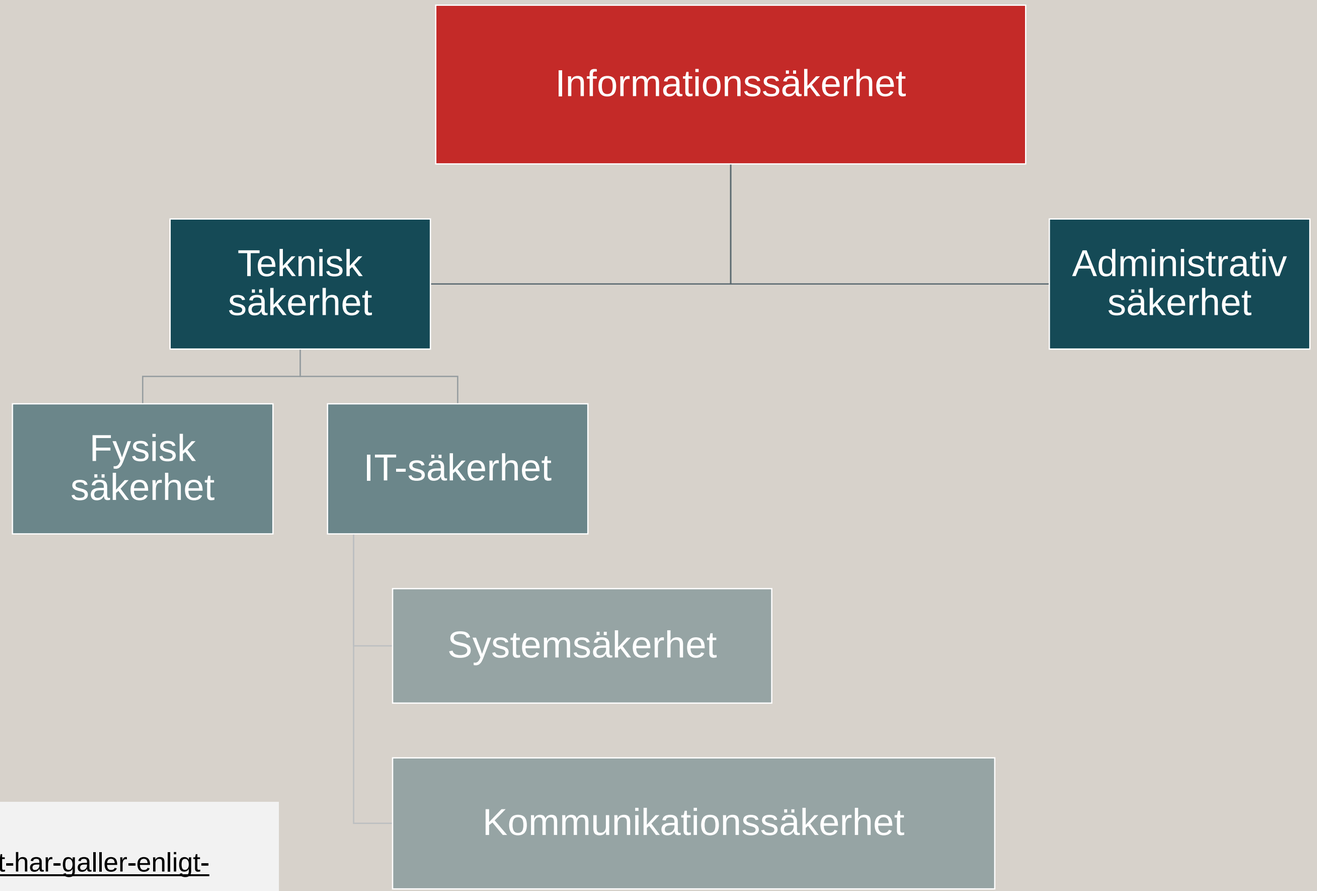


- **Konfidentialitet:** Att informationen skyddas mot obehörig insyn
- **Riktighet:** Att informationen skyddas mot oönskad förändring
- **Tillgänglighet:** Att information görs åtkomlig för behörig person vid rätt tillfälle

Systematiskt och riskbaserat informationssäkerhetsarbete



Struktur informationssäkerhet



Mer information

https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/informationssakerhet/

Skyddsobjekt för informationssäkerhet

- Organisationens mest värdefulla tillgångar
- Informationstillgångarna och informationsklassning
- Det överordnade syftet är ofta att säkra *verksamhetens* fortgående.

Var kommer **dataskyddet** in i det sammanhanget?

- Skydd för registrerades fri och rättigheter.

Risker för den registrerades fri- och rättigheter

Riskanalys

En central del av informationssäkerhet- och dataskyddsarbetet

- Vad kan hända?
- Hur sannolikt är det?
- Vad blir konsekvenserna?

Standarder och vägledning

- EDPB:s vägledningar, www.edpb.europa.eu
- SS-ISO/IEC 27000-serien, www.sis.se
- NIST, www.nist.gov/cyberframework
- MSB och www.informationssäkerhet.se
- CIS Critical Security Controls, www.cisecurity.org
- ENISA, www.enisa.europa.eu
- OWASP Top 10, www.owasp.org

Säkerhet i samband med behandlingen

Säkerhet i samband med behandlingen, artikel 32

Med beaktande av den senaste utvecklingen, genomförandekostnader

- behandlingens **art, omfattning, sammanhang och ändamål**
- samt **riskerna**, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter
- …ska den personuppgiftsansvarige *och* personuppgiftsbiträdet vidta **lämpliga tekniska och organisatoriska åtgärde**r för att säkerställa…

Forts. Säkerhet i samband med behandlingen, artikel 32

… en **säkerhetsnivå som är lämplig i förhållande till risken**… t.ex.

- pseudonymisering (kodning) och kryptering
- kontinuitetsplanering
- incidenthantering
- testa, undersöka, utvärdera åtgärderna

- Särskild hänsyn ska tas till **risken** för
  - förstöring, förlust eller ändring
  - obehörigt röjande eller obehörig åtkomst

Behandlingens art

- Vilka slags uppgifter är det fråga om?
  - Integritetskänsliga uppgifter?
  - Uppgifter om en särskilt utsatt grupp?
  - Betydande maktobalans mellan PUA och den registrerade?

- Är behandlingen
  - systematisk och strukturerad?
  - tillfällig och oplanerad?
  - långvarig eller momentan?
  - förutsägbar för den registrerade?

Behandlingens omfattning

- Antal registrerade
- Antal uppgifter om varje registrerad
- Antal personer som har åtkomst till uppgifterna
- Behandlingens geografiska omfattning

Behandlingens sammanhang

Behandlingens tekniska och organisatoriska kontext

Exempelvis:

- Hur är behandlande parter organiserade?
- Finns en eller flera personuppgiftsansvariga?
- Ett eller flera biträden?
- Särskilt förtroligt sammanhang?

Behandlingens ändamål

Varför behandlar vi personuppgifterna? Vad är syftet med behandlingen?

- Säkerhetsövervakning?
- Tillhandahålla tjänster?
- Kontrollera den registrerade?
- M.m.

Ett riskbaserat arbetssätt

- Beroende av de risker som personuppgiftsbehandlingen innebär.
- Hög risk kräver starka skyddsåtgärder.
- Riskbedömning ersätter inte krav på rättslig grund eller annan regelefterlevnad!
- Kvarvarande högrisk resulterar i konsekvensbedömning.

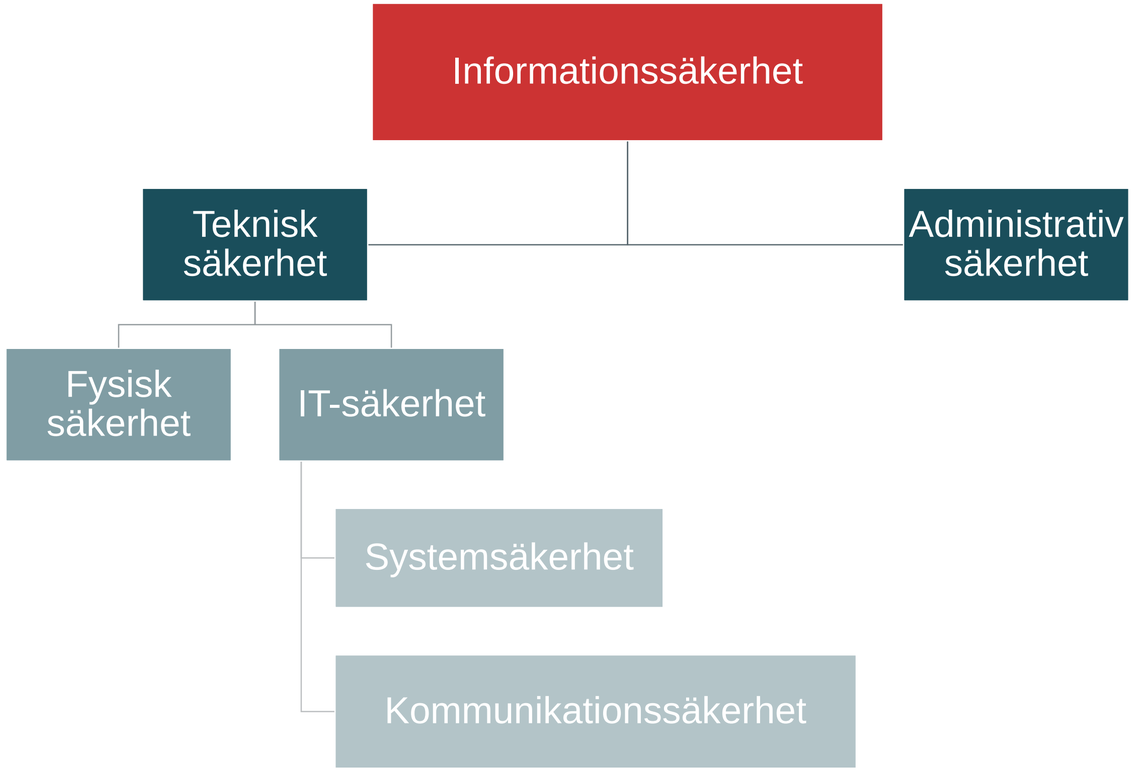
Vad innebär lämplig säkerhetsnivå?

- Anpassade säkerhetsåtgärder för att finna balans mellan behandlingens
  - Säkerhetsbehov
  - Säkerhetsåtgärd

Säkerhetsåtgärder

Administrativa (organisatoriska) och tekniska åtgärder

- Datakommunikation
- Åtgärder till skydd mot skadlig kod
- Fysisk säkerhet
- Incidenthantering
- Kontinuitetsplanering
- Mobilt arbete
- Inventarier och licenser
- Autentisering och behörighetsadministration
- Loggning



Säkerhet handlar om förmågor

- Riskhantering
- Kontinuitetsplanering
- Incidenthantering
- Ett ständigt förbättringsarbete!

Dokumentera!

Bra att ta med sig

- Informationssäkerhet stödjer ert dataskyddsarbete och ert dataskyddsarbete stödjer ert informationssäkerhetsarbete.
- Prata med era kollegor som jobbar med informationssäkerhet.
- Gör inte dataskyddsarbete frikopplat från övrigt säkerhetsarbete.
- Ta inspiration från standarder och vägledningar.

Konsekvensbedömning och förhandssamråd

Det är nu det gäller!

- Konsekvensbedömning är en viktig del i efterlevnaden av dataskyddsförordningen, och särskilt viktig att göra för de personuppgiftsbehandlingar som leder till sannolik hög risk för registrerades fri- och rättigheter.

Vad är en konsekvensbedömning?

- En konsekvensbedömning är avsedd att vara en oavbruten process för att identifiera och hantera risker.
  - Bidrar till inbyggt dataskydd och dataskydd som standard
  - Leder till bedömning om behovet av behandlingen står i proportion till syftet
  - Identifierar risker och lämpliga åtgärder
  - Skapar och påvisar efterlevnad av dataskyddsförordningen

När ska arbetet påbörjas?

- I samband med ny eller förändrad personuppgiftsbehandling, vilket kan ske i samband med:
  - Behov av förändring av arbetssätt/process
  - Behov av organisatorisk förändring
  - Behov av nya verktyg/hjälpmedel
  - Behov av ny tjänst/produkt
  - etc
- Regelbundet för befintliga personuppgiftsbehandlingar
  - I samband med förändringar i omvärld
  - Ändringar i behandlingens sammanhang, mottagarna, sammanslagning i åtgärder m.m.
  - Förändringar i behandlingens omvärld
  - etc

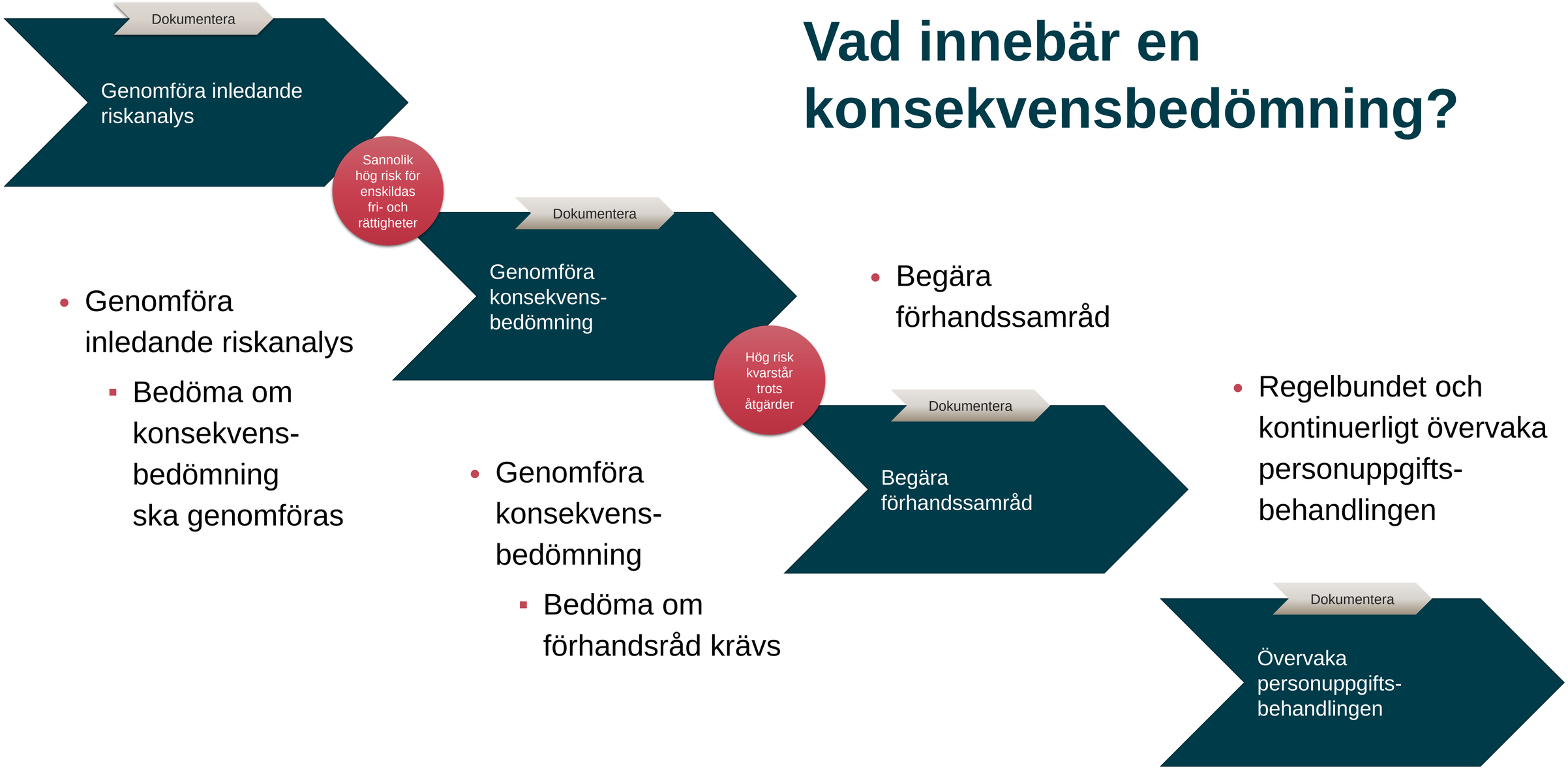
Varför konsekvensbedömning?

- Förebygga risker innan de uppkommer och därmed skydda människors fri- och rättigheter.

Vem ansvarar?

- Det är personuppgiftsansvarig som ansvarar för att konsekvensbedömning görs.

Vad innebär en konsekvensbedömning?



- Genomföra inledande riskanalys
  - Bedöma om konsekvens-bedömning ska genomföras
- Genomföra konsekvens-bedömning
  - Bedöma om förhandsråd krävs
- Begära förhandssamråd
- Regelbundet och kontinuerligt övervaka personuppgifts-behandlingen

Genomför inledande riskanalys

- Skyddsobjekt: Fysisk levande person
- Identifiera risker utifrån
  - Dataskydd och integritet
  - Grundläggande mänskliga rättigheter
  - Dataskyddsförordningens principer

Bedöm om konsekvensbedömning ska genomföras

- Behandlingen medför sannolikt hög risk för registrerades fri- och rättigheter.
- Om behandlingen innefattar flera av de nio kriterier som EDPB tagit fram, är det sannolikt att behandlingen innebär hög risk.
- I vissa situationer/behandlingar är ni *alltid* skyldiga att genomföra en konsekvensbedömning.
- Tveksam? Gör då konsekvensbedömning.

Genomför konsekvensbedömning

- **Ta fram en systematisk beskrivning** av den planerade behandlingen och **behandlingens syfte**.
- **Göra en bedömning** av om behandlingen är **nödvändig och proportionerlig** i förhållande till syftet med den.
- **Iterativ process**
  - **Göra en bedömning av riskerna** för de registrerades rättigheter och friheter.
  - **Identifiera och ta fram de åtgärder** som ni planerar för att hantera riskerna och för att visa att dataskyddsförordningen efterlevs.
- **Planera genomförandet** av översyn och hantering av identifierade förändringar

Begär förhandssamråd!

- Gedigen dokumenterad konsekvensbedömning
  - Personuppgiftsbehandlingen är beskriven
  - Ändamålet för behandlingen framgår
  - Vilket lagligt stöd som finns personuppgiftsbehandlingen
  - Etc.
- Åtgärder och garantier för att skydda registrerades rättigheter och friheter ska framgå
- Vilka risker som kvarstår och varför de kvarstår
- Tydlighet i vem/vilka som är personuppgiftsansvarig/a
- IMY ska lämna ett yttrande inom 8 veckor, men tiden kan komma att förlängas.

Övervaka personuppgiftsbehandlingen

- Kom ihåg att övervaka personuppgiftsbehandlingen och de faktorer som kan påverka dess behandling.

- Om något förändras => börja om och titta över om nya risker har tillkommit eller förändrats på grund av förändringen och om nya åtgärder måste göras, eller befintliga förändras.

Här finns dataskyddsförordningens artiklar om konsekvensbedömning och förhandssamråd, tillsammans med IMY:s kommentarer. Kommentarerna är tänkta att fungera som hjälp och stöd i ert arbete med konsekvensbedömningar och förhandssamråd.

Artikel 35: Konsekvensbedömning avseende dataskydd

Artikel 35.1

Om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter. En enda bedömning kan omfatta en serie liknande behandlingar som medför liknande höga risker.

Länkar

Kriterier för godkänd konsekvensbedömning

- www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/konsekvensbedomningar-och-forhandssamrad/kriterier-for-en-godtagbar-konsekvensbedomning/

Blanketten för begäran

- www.imy.se/verksamhet/utfora-arenden/begar-forhandssamrad/

EDPB:s riktlinjer om konsekvensbedömning

- www.imy.se/globalassets/dokument/riktlinjer-om-konsekvensbedomning-avseende-dataskydd.pdf

IMY:s förteckning och information

- www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/konsekvensbedomningar-och-forhandssamrad/forteckning-over-nar-en-konsekvensbedomning-ska-goras/

Bra att ta med sig

- Arbeta systematiskt med verksamhetens övergripande informationssäkerhet
- Samverka inom den egna verksamheten
- Verktyg i säkerhetsarbetet
  - Informationsklassning
  - Kravställning av säkerhetsåtgärder
  - Riskanalys
  - Konsekvensbedömning
  - Förhandssamråd

Följande fyra punkter hjälper verksamheten att arbeta strukturerat och därmed att uppfylla kraven i dataskyddsförordningen.

1. Utgå från grundläggande principer och rättslig grund
2. Analysera skyddsobjekt, omfattning och risker
3. Analysera åtgärder och lämplighet
4. Motivera era beslut och dokumentera kontinuerligt

Konsekvensbedömning – en oavbruten process för att identifiera och hantera risker

- Ett **verktyg**
- En **process**
- Ger stöd till att skapa **förmågan** att skydda enskildas fri- och rättigheter

Tack!