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.

Integritetsskydds myndigheten

Den 10 december 2024

Välkommen till årets DSO-konferens!

Vi sänder live

Konferensen spelas inte in

Tack för era synpunkter och förslag på innehåll!

- Utvärderingar från tidigare konferenser och webbinarier.
- DSO-referensgrupp

Dagens program

- Inledning med Eric Leijonram, IMY:s generaldirektör
- Aktuellt från IMY
- Hänt och på gång inom Europeiska dataskyddsstyrelsen, EDPB
- Erfarenheter från DSO:er
- IMY:s vägledning om konsekvensbedömningar
- AI och GDPR
- Avrundning med Eric Leijonram och moderatorerna

IMY:s generaldirektör

Aktuellt från IMY

Det senaste inom kamerabevakning

2023 års kamerabevakningsutredning

- SOU 2024:27

Två huvudspår

- Myndigheter och andra som utför s.k. uppgift av allmänt intresse
- Brottsbekämpande myndigheter (i brottsbekämpande verksamhet)
- (Glöm inte: övriga)

Kamerabevakningstillstånd – idag

- Myndigheter och andra som utför uppgift av allmänt intresse

- Behöver som huvudregel tillstånd om plats dit allmänheten har tillträde

- (Andra behöver inte tillstånd)

- Polismyndigheten, Säkerhetspolisen, Kustbevakningen, Tullverket

- Behöver inte tillstånd (men dokumenterad intresseavvägning)

Kamerabevakningstillstånd – i framtiden (1 maj 2025)

Ingen behöver tillstånd!

Jag loggades ut från allt för en stund sedan, men det gick att helt enkelt bara ansluta till IMY AOVPN ige

Myndigheter och andra som utför uppgift av allmänt intresse

1. Behöver inte längre tillstånd
2. Dokumenterad intresseavvägning, oavsett om allmänheten har tillträde eller inte
3. Förteckning över bevakning

Vissa undantag från intresseavvägningen och förteckningskravet.

Brottsbekämpande myndigheter i brottsbekämpande verksamhet

1. Dokumenterad särskild intresseavvägning, oavsett om allmänheten har tillträde eller inte

2. Fler punkter ska beaktas särskilt vid bedömningen av bevakningsintresset – fler platser där intresset kan väga tungt

3. Fler undantag från intresseavvägningen (inkl. dokumentation) samt skyldigheten att upplysa och informera om bevakningen

Vad innebär lagändringarna?

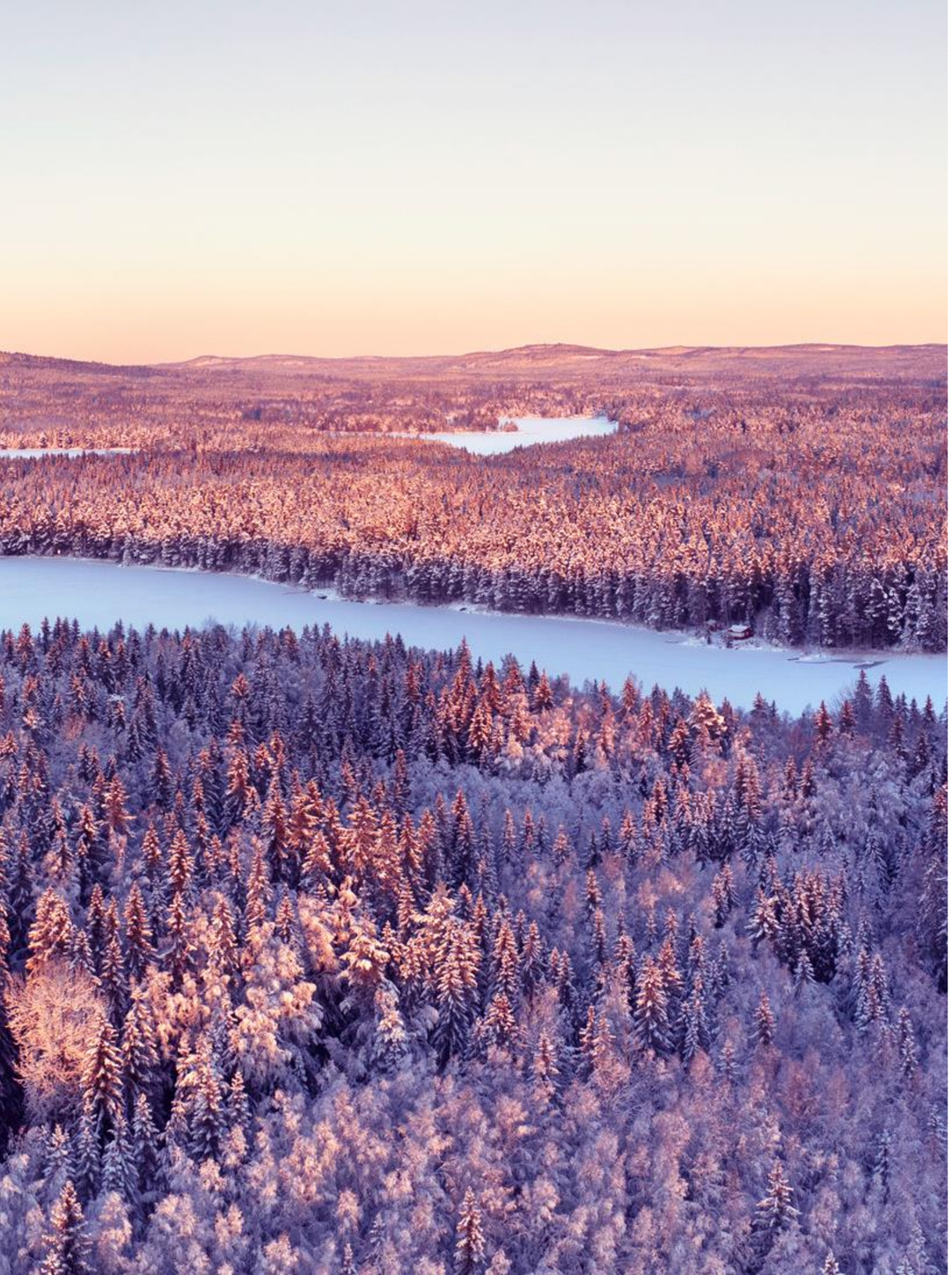
- Brottsbekämpande myndigheter får större möjligheter att bevaka i brottsbekämpande verksamhet

- För andra än brottsbekämpande myndigheter – inte större möjligheter
- Snabbare process för de som behövt söka tillstånd

Den fortsatta processen

- Lagrådsremiss, proposition
- Föreslås träda i kraft 1 maj 2025
- IMY-webbinarium april 2025

DSO-referensgruppen och kunskapsfilmer på IMY play



Referensgrupp Dataskyddsombud

- Stort intresse från DSO:er
- Använt DSO:er som referensgrupp i flera omgångar
  - webbinarium,
  - riktlinjen om konsekvensbedömningar,
  - regulatorisk sandlåda,
  - inför årets DSO-konferens
- Nu söker vi DSO:er för referensgrupper 2025 – håll utkik på hemsidan!
- referensgruppdso@imy.se

Filmer om GDPR på IMY play

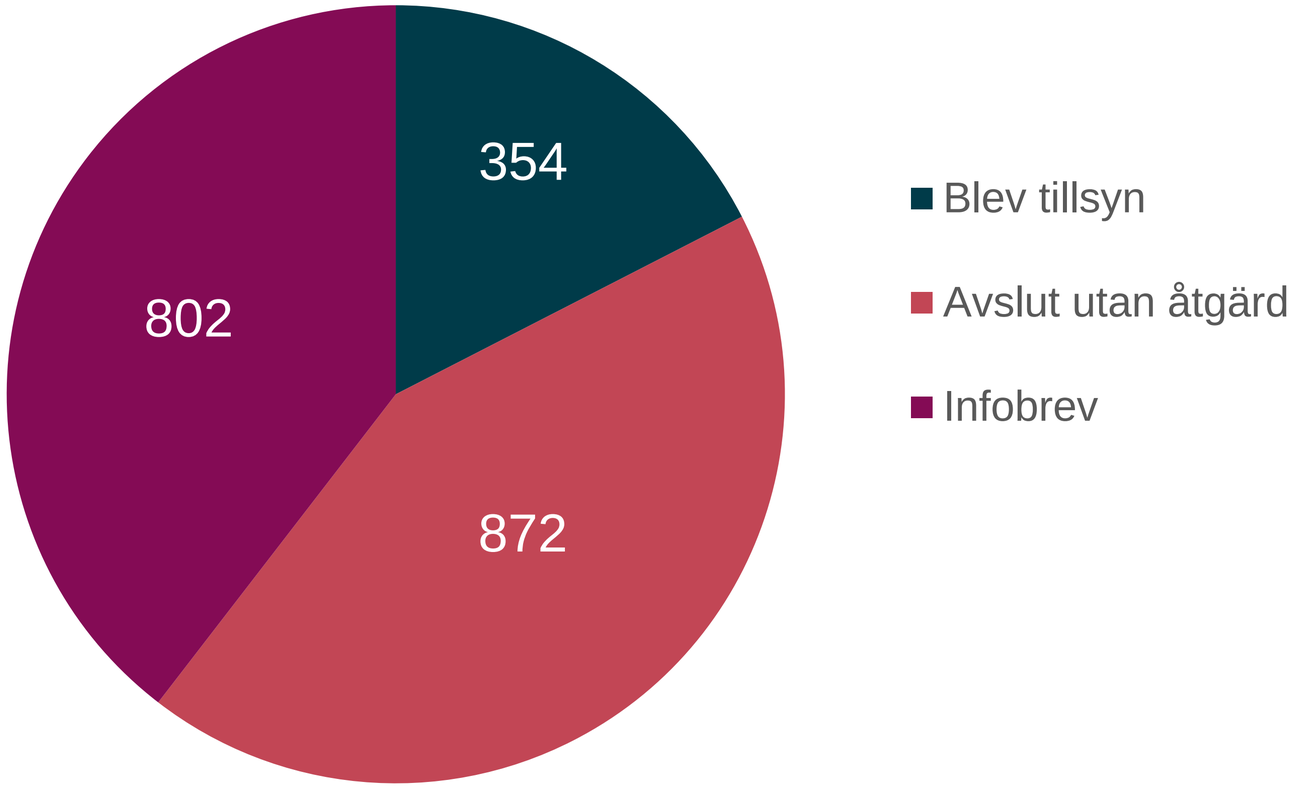
- 6 filmer publicerade hittills 2024
    1. GDPR:s syfte och tillämpningsområde
    2. Grundläggande begrepp
    3. Grundläggande principer
    4. Registrerades rättigheter
    5. Rättsliga grunder
    6. Känsliga personuppgifter
- Över 12 000 visningar
- Ytterligare 5 filmer under 2025
- Se filmerna på IMY play – kunskapsfilmer om GDPR | IMY

IMY:s klagomålshantering

Klagomål

- IMY utreder *alla* klagomål och klaganden är part
- Vad är ett klagomål enligt GDPR?
- Vad innebär det att IMY utreder ett klagomål?

Vad har hänt med de GDPR-klagomål som inkommit till IMY 2024?



- Vissa avslutas direkt utan åtgärd.
- Nästa steg är informationsbrev. PUA informeras om klagomålet och gällande regler.
- Den tredje nivån är att inleda tillsyn.

Tillsynsbeslut mot Apoteket AB och Apohem AB

Tillsynsbeslut mot Apoteket AB och Apohem AB

- Granskning av apotekens användningen av analysverktyget Meta-pixeln på sina webbplatser/nätbutiker.
- Överföring av uppgifter om kunders köp av integritetskänsliga produkter till Meta.
- Hade bolagen vidtagit tillräckliga säkerhetsåtgärder för att skydda kundernas personuppgifter?

Tillsynsbeslut mot Apoteket AB och Apohem AB

Behandlingen har inneburit höga risker med hänsyn till

- karaktären på de uppgifter som behandlats (känsliga personuppgifter* och uppgifter av mer privat natur),
- behandlingens sammanhang (apoteksverksamheter) och
- behandlingens omfattning (många berörda registrerade).

IMY:s granskning visar att apoteken inte vidtagit tillräckliga tekniska och organisatoriska åtgärder i förhållande till den höga risken.

*Jämför med EU-domstolens dom Lindenapotheke, C-21/23, EU:C:2024:846

Tillsynsbeslut mot Apoteket AB och Apohem AB

- Överträdelser av artikel 32 i GDPR (men inte artikel 5.1 f i GDPR jfr IMY:s beslut mot Avanza i DI-2021-5544).
- Sanktionsavgifter om 37 miljoner för Apoteket och 8 miljoner för Apohem.
- Överträdelser av låg allvarlighetsgrad utifrån EDPB:s riktlinjer 04/2022 om beräkning av administrativa sanktionsavgifter med hänsyn till:

➢ Karaktären på uppgifterna som behandlats och överträdelsens omfattning, sammanhang och det faktum att den skett inom bolagens kärnverksamhet.

➢ Vissa vidtagna tekniska och organisatoriska åtgärder och att överföringen skett i skyddad format, till en enda mottagare (inget okontrollerat röjande).

Tillsynsbeslut mot Apoteket AB och Apohem AB

- Ett systematiskt säkerhetsarbete är en grundläggande förutsättning för att skydda personuppgifter.
- Uppföljning av pågående, planerad personuppgiftsbehandling och rutiner för att upptäcka oavsiktliga förändringar.
- Du hittar besluten för Apoteket AB i ärende IMY-2022-3270 och Apohem AB i IMY-2022-3272 (överklagat) här.

Tillsyn mot ett larmbolag

”Ingen ska behöva bli filmad så i sitt eget hem”

Tipsade varandra om larmbilder – om nakna kunder

Tillsyn mot Verisure Sverige AB

- Integritetskänsliga personuppgifter som krävt hög skyddsnivå
- Logguppgifter om bildernas filnamn
- Saknat spårbarhet i behandlingen av bildmaterialet
- Lagringstiden för kort för att skydda personuppgifterna mot obehörigt röjande eller obehörig åtkomst
- Läs beslutet på vår webbplats här

Några medskick

- Att säkerställa lämpliga skyddsåtgärder innebär också att säkerställa tillräcklig spårbarhet i hur personuppgifterna har hanterats.

- Viktigt för att:
  - kunna kontrollera hanteringen av personuppgifter
  - tillgodose registrerades rättigheter

- Principen om lagringsminimering

Hänt och på gång inom Europeiska dataskydds-styrelsen, EDPB

Riktlinje 02/2024 om artikel 48 GDPR

- Antogs den 2 december 2024 – publik konsultation pågår till den 27 januari 2025.

Artikel 48

”Domstolsbeslut eller beslut från myndigheter i tredjeland där det krävs att en personuppgiftsansvarig eller ett personuppgiftsbiträde överför eller lämnar ut personuppgifter får erkännas eller genomföras på något som helst sätt endast om det grundar sig på en internationell överenskommelse, såsom ett avtal om ömsesidig rättslig hjälp, som gäller mellan det begärande tredjelandet och unionen eller en medlemsstat, utan att detta påverkar andra grunder för överföring enligt detta kapitel.”

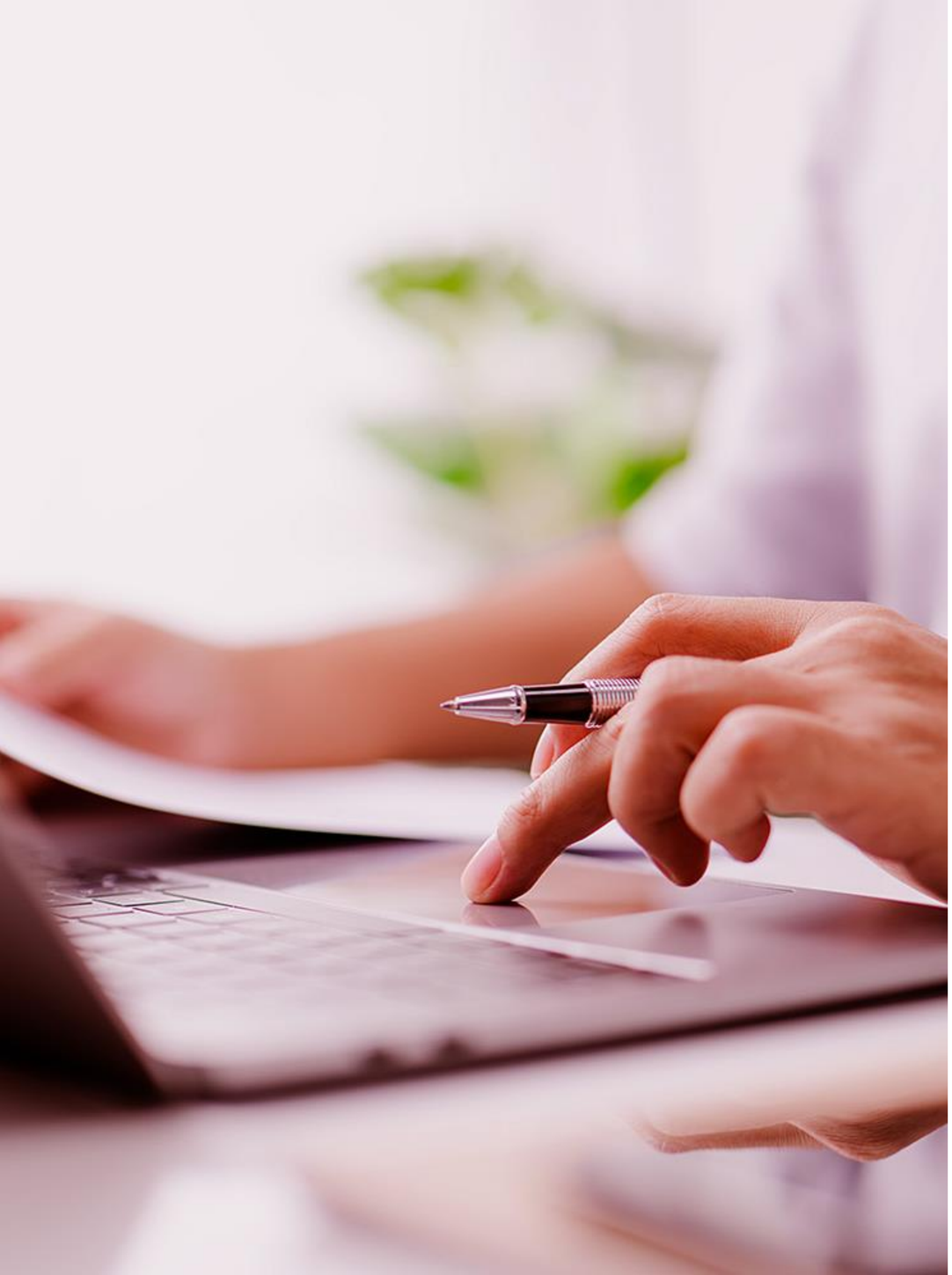
Riktlinje 02/2024 om artikel 48 GDPR

- Utlämnande av personuppgifter som svar på begäran från myndighet i tredjeland utgör ”överföring”
- Krav på rättslig grund (artikel 6) och stöd för överföringen (kapitel V)
- Internationell överenskommelse kan utgöra rättslig grund (artikel 6.1 c/e) och/eller stöd för överföringen (artikel 46.2 a)
- Men! Inte uteslutet att använda annan rättslig grund (artikel 6) och/eller stöd för överföringen (kapitel V) om tillämpligt

Riktlinje 1/2024 om behandling med stöd av intresseavvägning

- Antogs den 8 oktober 2024 – publik konsultation avslutad

- Riktlinjen består av fyra delar:
  - **Del 1**: Generell introduktion
  - **Del 2**: Analys av de tre kriterier som ska vara uppfyllda för att använda artikel 6.1 f som rättslig grund
  - **Del 3**: Förhållandet mellan artikel 6.1 f och de registrerades rättigheter
  - **Del 4**: Specifika kontexter där artikel 6.1 f kan bli aktuell som rättslig grund



Tre kriterier för att använda artikel 6.1 f som rättslig grund

1. Det ska finnas ett berättigat intresse
   - (i) Lagligt, (ii) klart och precist angivet, (iii) faktiskt och inte hypotetiskt
   - Kommersiellt intresse kan utgöra berättigat intresse (C-621/22)

2. Behandlingen ska vara nödvändig (för att tillgodose intresset)
   - Möjligt att uppnå med mindre ingripande åtgärder?

3. Intresseavvägning mellan det berättigade intresset och de registrerades intressen
   - Vilka rimliga förväntningar har de registrerade?
   - Skyddsåtgärder (*eng.* ”mitigating measures”)

Förhållandet mellan artikel 6.1 f och de registrerades rättigheter

- Rätten till information
- Rätten till tillgång
- Rätten att invända
- Rätten till radering
- Rätten till rättelse
- Rätten till begränsning av behandling
- Automatiserat individuellt beslutsfattande

Specifika kontexter där artikel 6.1 f kan aktualiseras

- Behandling av barns personuppgifter
- Myndigheters behandling
- Behandling för att förhindra bedrägerier
- Behandling för direktmarknadsföring
- Behandling för administrativa ändamål inom en koncern
- Behandling för att säkerställa nätverks- och informationssäkerhet
- Utlämnande till behöriga myndigheter

På gång inom EDPB

- Riktlinje om behandling för forskningsändamål
- GDPR och AI – Artikel 64.2-yttrande, stakeholder event, riktlinjer om webbskrapning och om samspelet AI-GDPR…
- EDPB:s samordnade åtgärd 2023 avs. dataskyddsombud: uppföljning
- CEF 2025 – rätt till radering
- Utvärdering av Data Privacy Framework – EDPB:s rapport

Erfarenheter från dataskyddsombud

TRAFIKVERKET

TRAFIKVERKET

Dataskyddsombud

Praktiskt arbete och metodik

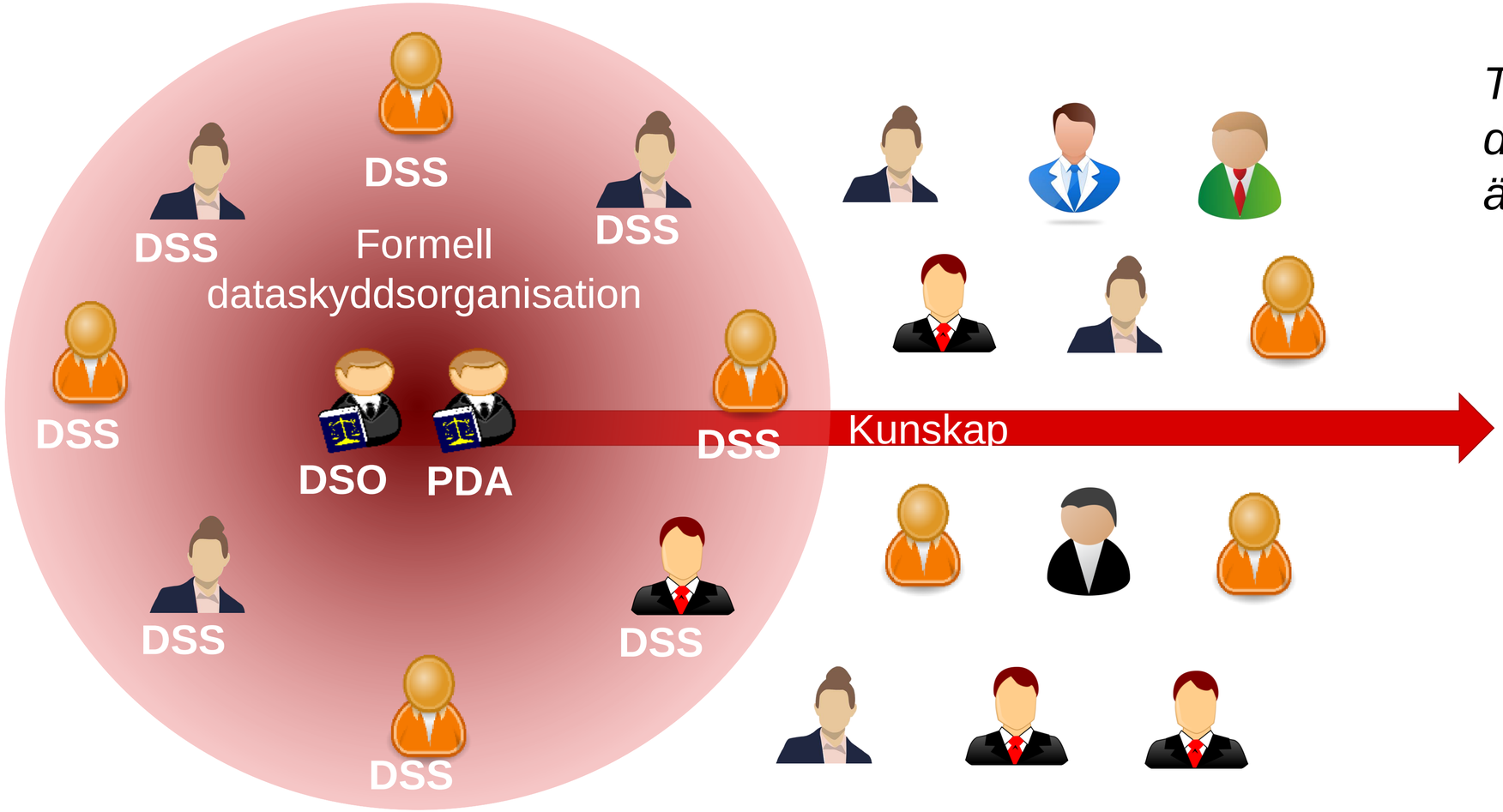
Statens järnvägsnät, 1400 mil

Statens vägnät, 10000 mil

Anläggningens värde:	500 miljarder
Årlig budget:	85 miljarder
Anställda:	10000

DSO	Dataskyddsombud
PDA	Persondataanalytiker
DSS	Dataskyddssamordnare

Säkerhetsspecialister, IT-tekniker, projektledare, verksamhetsspecialister, jurister, arkivarier, chefer, etc



Trafikverkets dataskyddsorganisation är ett kompetensnätverk

Primär strategi

- Förbättra efterlevnaden av dataskyddet
  - Rådgivning
  - Integrerad granskning
- Integrera och förenkla efterlevnaden i styrning, it-lösningar och processer
  - Styrande dokument
  - FAQ
- Proaktivt säkra efterlevnaden
  - Utbildning

Skriftliga råd i dataskyddsfrågor

”Om organisationen gör XXXX, är det min bedömning att Trafikverket efterlever GDPR.”

”Bedömningen är baserad på … (faktaunderlag)”

Detta är ett råd från dataskyddsombudet

Dataskyddsombudet roll är att informera och ge råd och rekommendationer om hur den personuppgiftsansvarige, dvs Trafikverkets verksamhet, kan agera för att efterleva dataskyddsförordningen. Verksamheten fattar beslut om hur man väljer att agera, har det fulla ansvaret för efterlevnaden och ansvarar för att dokumentera sina ställningstaganden. Man kan välja att inte följa dataskyddsombudets råd, men genom att agera i linje med dataskyddsombudets råd och dokumentera detta så har man med hög sannolikhet efterlevt dataskyddsförordningen.

Ställningstaganden och beslut rörande personuppgifter skall dokumenteras genom att skicka ett mail som beskriver beslutet till gdpr@trafikverket.se.

Skriftliga råd i dataskyddsfrågor

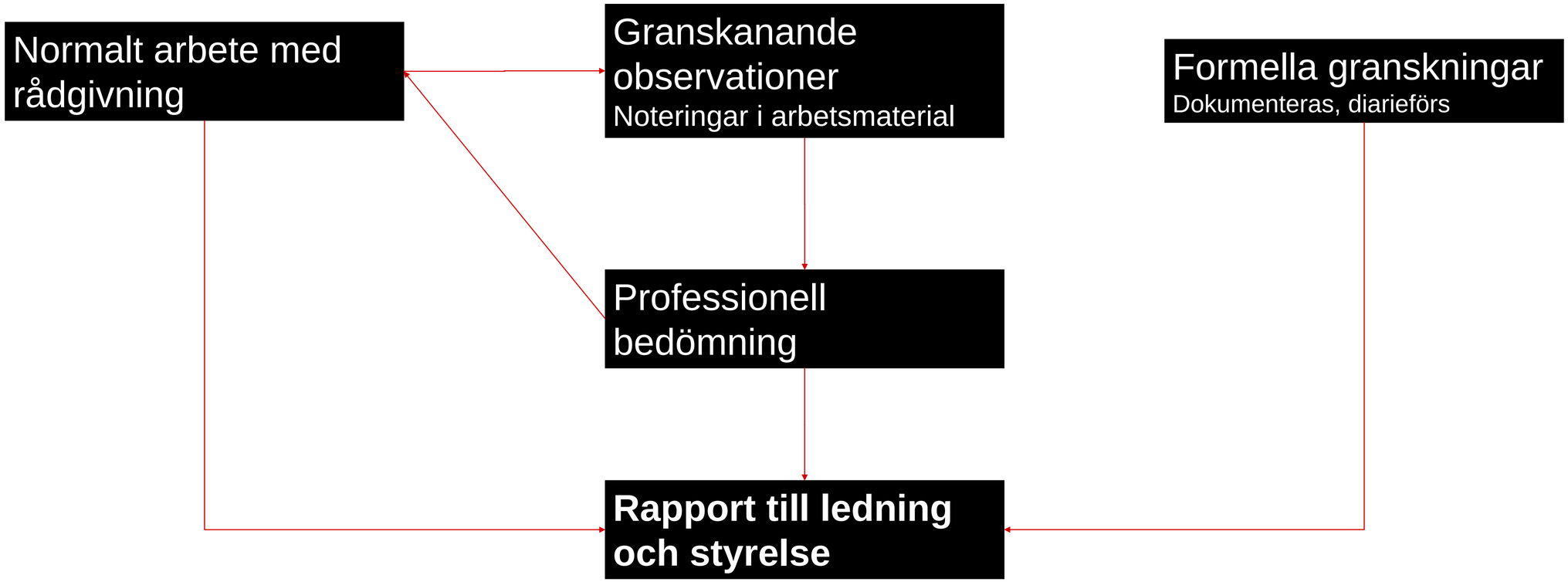
”Om organisationen gör XXXX, är det min bedömning att Trafikverket inte efterlever GDPR. Jag rekommenderar [åtgärder]”

”Om organisationen gör XXXX, är det min bedömning att det är oklart om Trafikverket efterlever GDPR. Jag rekommenderar [åtgärder]”

”Om organisationen gör YYYY, är det min bedömning att efterlevnaden av GDPR förbättras i relation till nuläget. Vidare åtgärder ZZZZZ rekommenderas”

”Bedömningen är baserad på … (faktaunderlag)”

Integrerad granskning



Styrande dokument

Personuppgiftsbehandling i Trafikverket
2017:0761

Personuppgiftsbiträdesavtal
2018:0474
TMALL 0975 (*SKR:s mall för PUB-avtal*)

Rollbeskrivningar

- Dataskyddsombud 2018-0512
- Dataskyddssamordnare 2018-0513
- Persondataanalytiker 2018-0514

FAQ

TRAFIKVERKET

Alla objekt Databladsvyn ... Sök efter ett objekt...

Rubrik	Ändrat
Leverantören vill inte föra över avtalade uppgifter till Trafikverket och hänvisar till GDPR	2024-08-26 13:49
Får jag radera personuppgifter?	2024-07-02 13:42
Personuppgiftsincidenter - hur ska de hanteras?	2024-06-10 15:26
Får man lämna ut allmän handling som innehåller personuppgifter?	2023-12-20 10:34
Personuppgiftsbiträdesavtal - Mini-FAQ	2023-12-04 19:55
Får man använda sin @trafikverket-mail för att registrera sig på olika tjänster på internet?	2023-10-16 17:36
Vilken informationsklass gäller för personuppgifter, och hur får de hanteras	2023-10-10 10:06
Får man publicera fastighetslistor, samrådshandlingar och liknande på webben.	2023-09-28 08:18

Stort fokus på internutbildning

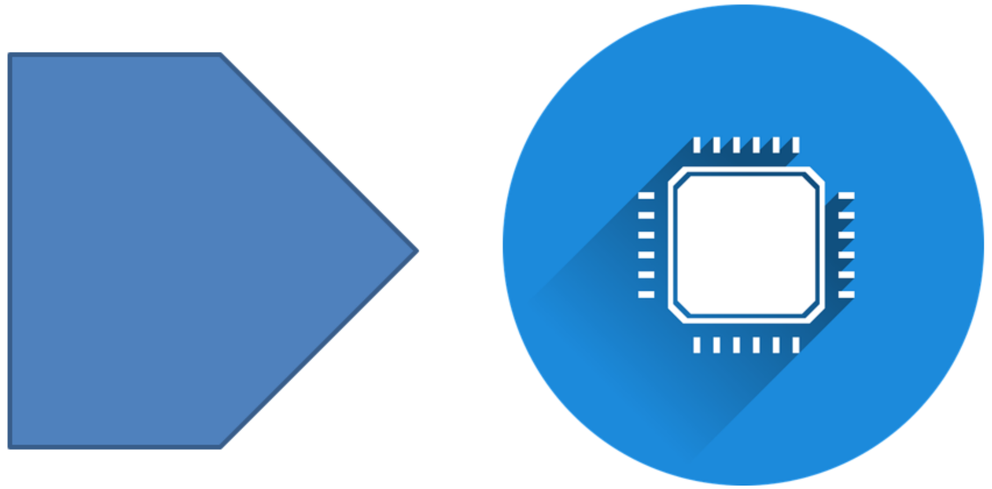
Molntjänster

AI-regler

Inbyggt dataskydd

Dataskydd i testning

Både affärsprocesser och tekniska system skall **designas** med inbyggt dataskydd och dataskydd som standard (DPbDD)

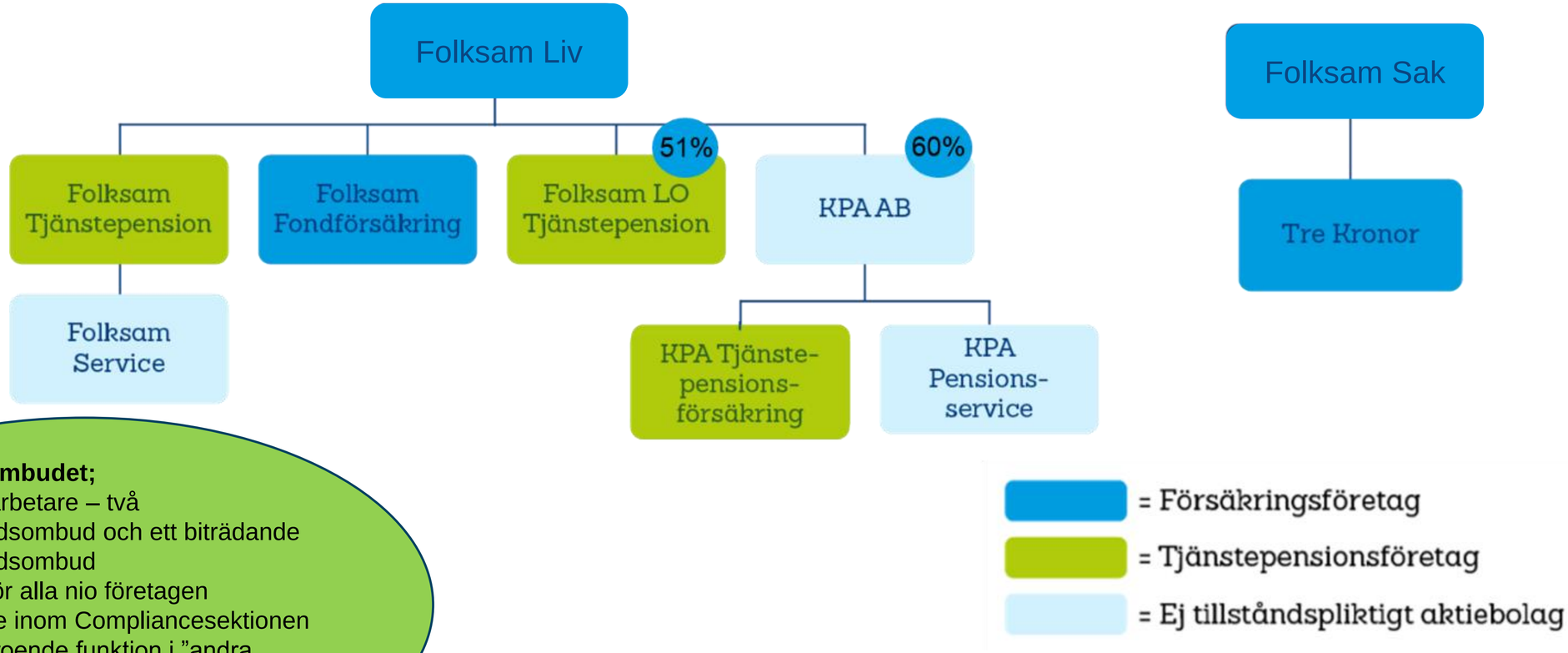


Ett år hos dataskyddsombudet – med fokus på riskbedömningen

Agenda

- DSO och Folksamgruppen
- Årsplanen
- Dataskyddsombudets riskbedömning
- Hur prioritera?

Dataskyddsombudet övervakar personuppgiftsbehandlingen hos företagen i Folksamgruppen



Dataskyddsombudet;

- Tre medarbetare – två dataskyddsombud och ett biträdande dataskyddsombud
- Arbetar för alla nio företagen
- Placerade inom Compliancesektionen – en oberoende funktion i ”andra linjen”
- Arbetar riskbaserat – utifrån risker för registrerade

Årsplanen - plan för arbetet och grund för uppföljning

Beslutas av dataskyddsombudet utifrån riskbedömningen. Tar även avstamp i dataskyddsombudets vision och mål (baserat på motsvarande för Folksamföretagen och IMY)

a) Råd och stöd enligt GDPR så som konsekvensbedömningar (regelbaserat)

b) Granskningar (riskbaserat)

c) Uppföljning av iakttagelser i granskningar (intern rutin)

d) Råd och stöd vid årlig genomgång av interna regelverk (intern rutin)

e) Riskbedömning två gånger per år (regelbaserat och interna rutiner)

f) Utbildningar (riskbaserat)

g) Omvärldsbevakning (regelbaserat)

Dataskyddsombudet riskbedömning

- Löpande och sammanställs två gånger per år.
- Rapporteras till vd och styrelser i årsrapport. Utifrån vad riskbilden visar - rapportering till halvåret.
- Görs enligt beslutad metodik för företagens kontrollfunktioner - rapporteringen är likartad och sker samtidigt. Lättare för ledningen att förstå.
- Försäkrings- och tjänstepensionsföretag har lagreglerade krav på riskbedömning och riskrapportering. Avser då *företagets risker* i försäkrings- och tjänstepensionsrörelsen (risker enligt GDPR ingår).
- Dataskyddsombudets bedömning och rapportering avser *risker för registrerade* enligt GDPR – viktigt att framhålla skillnaderna i rapporteringen. Riskerna för de registrerade driver det strategiska dataskyddsarbetet.

Dataskyddsombudets riskbedömning – regulatoriska områden per företag

- Riskerna bedöms inom olika områden i GDPR (regulatoriska områden), exempelvis säkerhet, registrerades rättigheter, personuppgiftsincidenter mfl
- Riskstatus och vad vi baserat riskbedömningen på inom varje regulatoriskt område dokumenteras per företag.
- Vi inhämtar information om risker utifrån bland annat

- företagens konsekvensbedömningar,
- företagens egna dokumenterade sk operativa risker för halvåret
- information från dataskyddsorganisationen om risker de identifierat, arbete som gjorts av dem under halvåret och som behöver göras under nästkommande period
- information om risker baserat på iakttagelser och åtgärder i våra och andra kontrollfunktioners granskningar

Exempel på presentation – risker per regulatoriskt område (alltså inte representativ riskbild för Folksamgruppen)

Regulatoriskt område	Nivå helår (ange aktuellt år)	Nivå helår (ange föregående år)
	Hög risk	Mycket hög risk
	Förhöjd risk	Låg risk
	Förhöjd risk	Hög risk
	Förhöjd risk	Hög risk
	Låg risk	Förhöjd risk
	Hög risk	Hög risk
	Låg risk	Hög risk
	Låg risk	Förhöjd risk
	Låg risk	Låg risk

Parametrar för sannolikhet och konsekvens (exempel på nyckelriskindikatorer - KRI)

- Sannolikhet

a) Finns interna regelverk, b) dokumenterade processer, c) manuella rutiner, d) är dataskyddet inbyggt i system, e) genomförs internkontroller och konsekvensbedömningar på området (vad utvisar de), f) vad utvisar granskningar, g) pågår arbete i verksamheten och hur mycket återstår, h) har verksamheten rapporterat risker/brister/incidenter på området, i) är ansvar tydlig utpekat i verksamheten, j) hur ser det ut beträffande incidenter k) har området fokus i IMY:s tillsynsplaner, l) vad visar omvärldsbevakningen på området?

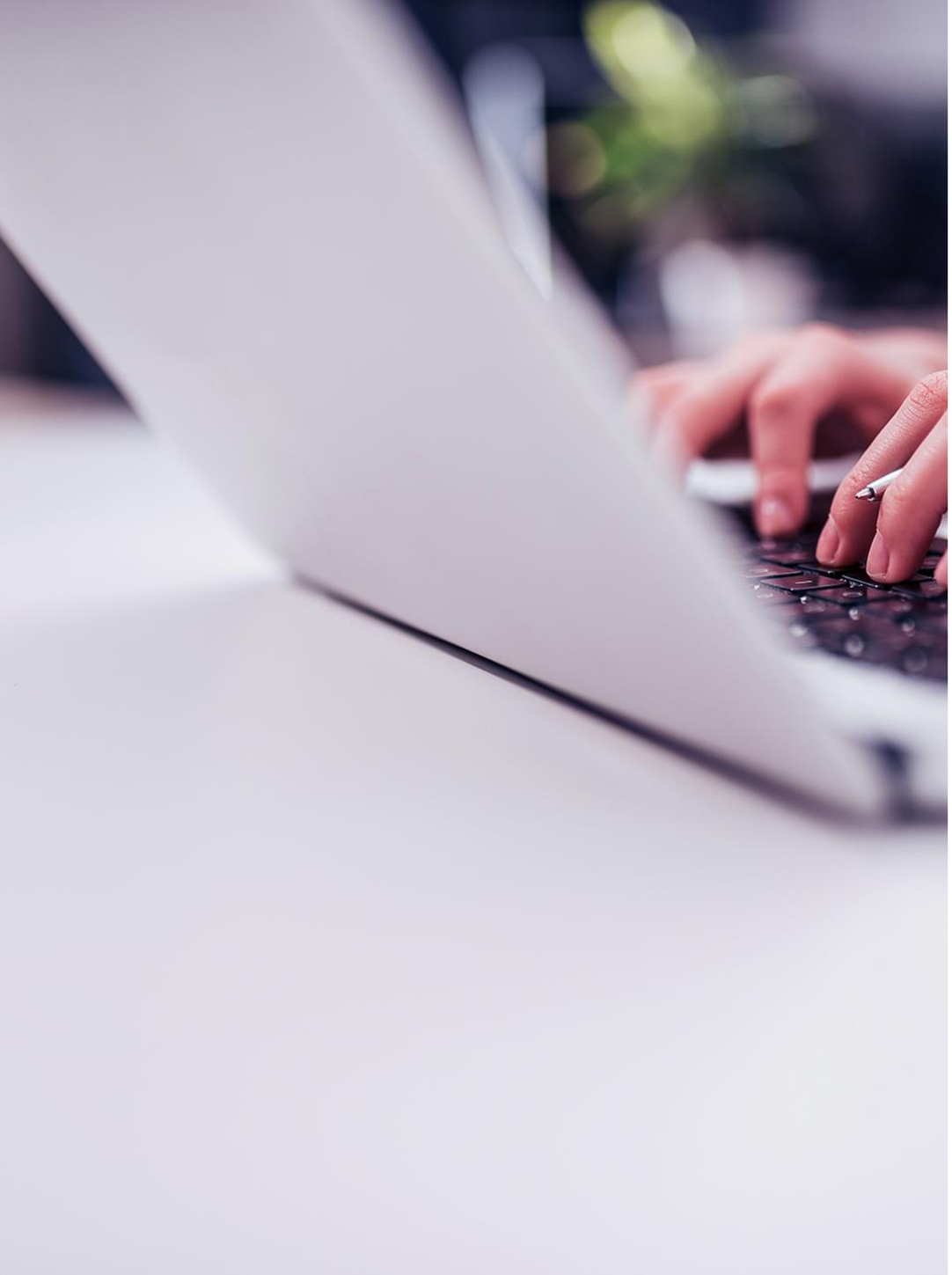
- Konsekvens

a) Hur påverkas registrerades rättigheter och friheter, b) omfattas området av den högsta sanktionsskalan i dataskyddsförordningen, c) hur kan tillsynsmyndigheten förväntas bedöma eventuella överträdelser, vad visar praxis.

Hur prioritera - att planera efter riskbedömningen

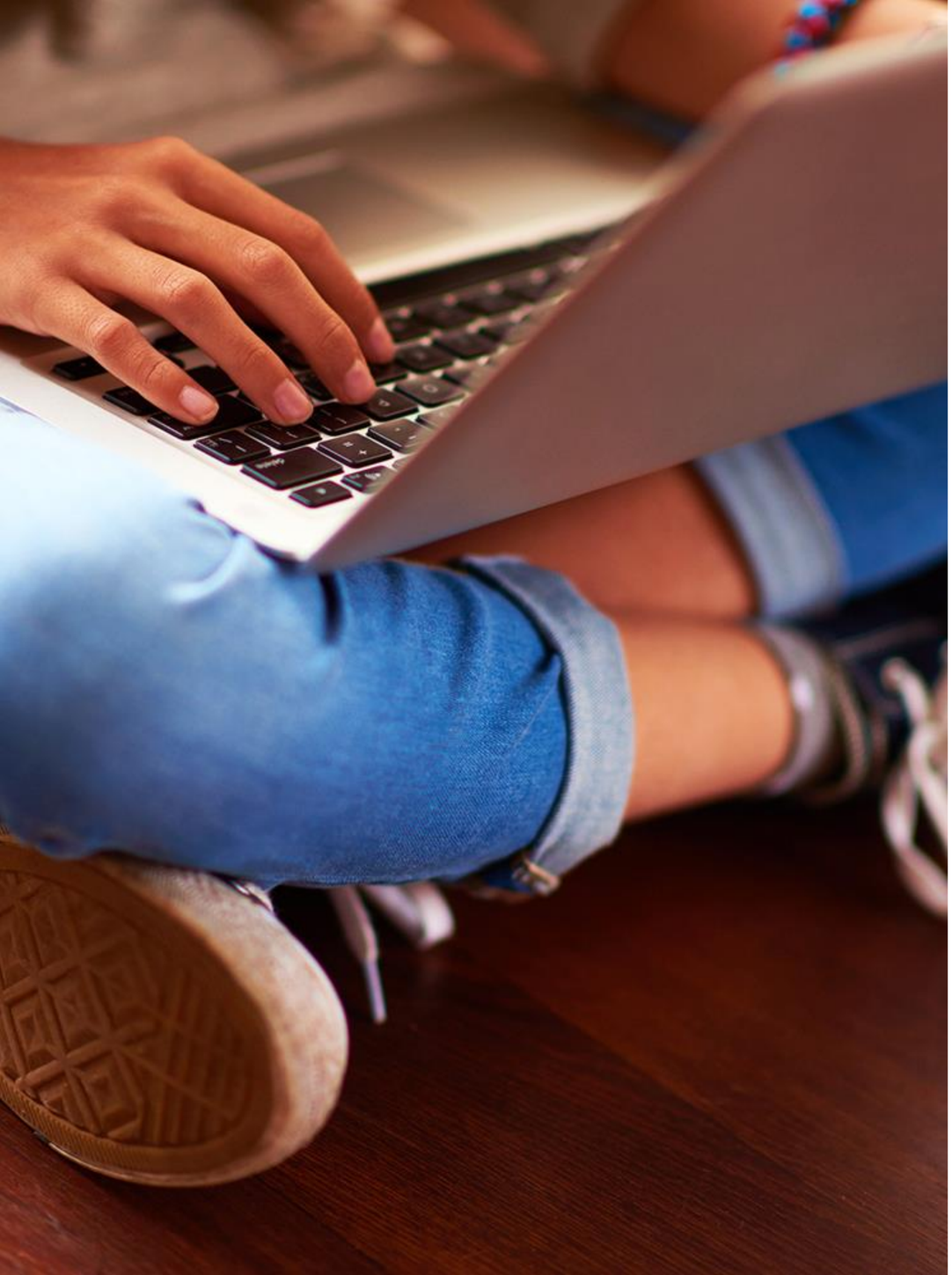
- Fokus förstås på regulatoriska områden som har högst risk
- Tar hänsyn till arbete som planeras i verksamheten – vad gör dataskyddsorganisationen, internrevisionen?
- Kan göra en granskning, bevakning eller kartläggning av ett område som dataskyddsbudet saknar närmare kunskap om

IMY:s vägledning om konsekvensbedömningar



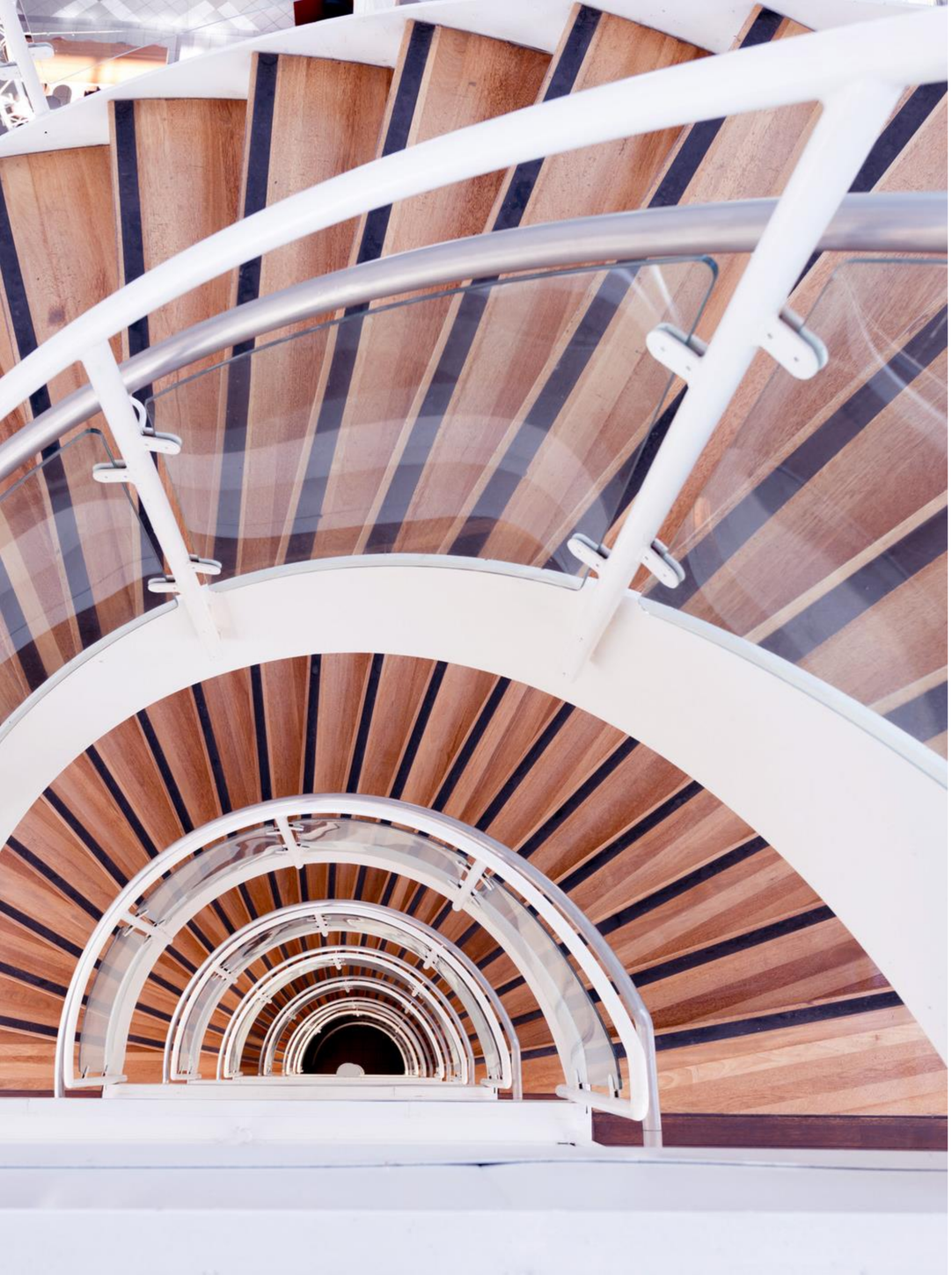
En vägledning i två delar

- En guide till regelverk och riktlinjer
- En guide till det praktiska arbetet med tillhörande mallar



Guide till regelverk och riktlinjer

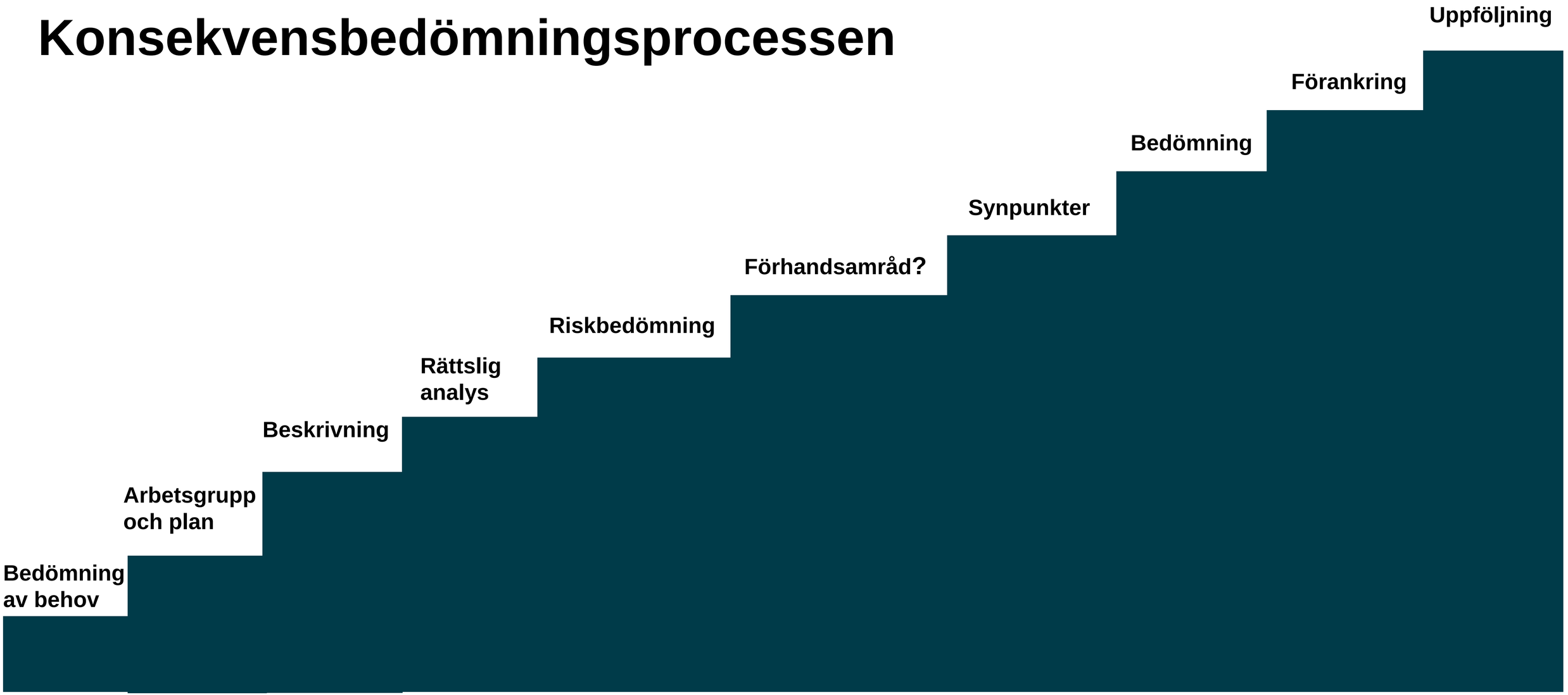
- Vad?
- När?
- Hur?



Den praktiska guiden

- En metod i 10 steg

Konsekvensbedömningsprocessen



Dataskyddsombudets roll i konsekvensbedömningsarbetet

- Ge råd inför en konsekvensbedömning
- Ge råd kring metod
- Ge råd vid riskbedömningen
- Övervaka genomförandet
- Utvärdera resultatet

Vad händer framåt?

- Finslipning och formgivning december–februari
- Framtagande av nytt material till IMY.se
- Publicering i februari
- Webbinarium i februari

AI och GDPR

AI-vägledningen

- Vägledning om AI och GDPR publiceras på IMY:s innovationsportal
- Publicering av ett antal delar om särskilt utmanande frågor
- En teknisk och en juridisk del

Dataskyddsfrågor

- Grundläggande principer: ändamålsbegränsning och uppgiftsminimering
- Rättslig grund: allmänt intresse och intresseavvägning
- Personuppgiftsansvar
- Svarta lådan och rätten till information
- Diskriminerande algoritmer

Grundläggande principer

Ändamålsbegränsning

- Personuppgifter får endast samlas in för särskilda, uttryckligt angivna och berättigade ändamål
- Får inte behandlas på ett sätt som är oförenligt med dessa ändamål.

Uppgiftsminimering

- Personuppgifter får inte behandlas i större omfattning än vad som är nödvändigt

Uppgiftsminimering vid utveckling av AI

- Noggrant analysera vilka uppgifter som är relevanta
- Välja ut en mindre mängd data med hög relevans och kvalitet
- Börja i en mindre omfattning och öka succesivt
- Följa hur AI-modellen utvecklas och gör regelbundna utvärderingar

Rättslig grund: intresseavvägning

- Finns det ett berättigat intresse hos den personuppgiftsansvarige?

- Är behandlingen av personuppgifter nödvändig för det berättigade intresset?

- **Avvägning**: väger den registrerades intresse tyngre än den personuppgiftsansvariges berättigade intresse?

Rättslig grund: uppgift av allmänt intresse

- Uppgift av allmänt intresse

- Kompletterande bestämmelser som fastställer uppgiften

- Den kompletterande bestämmelsen måste vara precis och förutsebar

Black box, transparens och tillgång

Är det fråga om automatiserat individuellt beslutsfattande?

- Huvudregel: registrerade har rätt att inte bli föremål för ett sådant beslut
- Registrerade har rätt till ytterligare information om behandlingen

Korrekthet och diskriminerande algoritmer

- Snedvriden data > diskriminerande algoritmer
- Kan strida mot principen om korrekthet

Avrundning

Vi är nyfikna på vad du tycker!

- Svara gärna på vår utvärdering!

- Presentationen som visats skickas till dig efter konferensen

Stort tack för idag!

IMY. Integritetsskydds myndigheten

www.imy.se