REGION VÄSTERBOTTEN

Personuppgiftslagen - Agenda

08.30 – Kort introduktion
Vad ska vi göra idag?
Vem berörs och varför?
Roller i vår organisation

08.45 – 9.15 PUL / GDPR
Vad innebär begreppen och hur påverkar det oss?
PUL
GDPR
Exempel på personuppgifter

09.15 – 11.45 Introduktion inventering behandling av data
Inventering – Frågebank
Utvärdering - Undantag
Checklista – Utvärdering efter inventering
Åtgärdsplan
Registerförteckning
Förvaltning

Avtal - Personuppgiftsbiträdesavtal
Gemensam tidsplan för genomförande

11.45 – 12.00 Övriga frågor

REGION VÄSTERBOTTEN

Personuppgiftslagen - Agenda

13.00 – Kort introduktion
Vad ska vi göra idag?
Vem berörs och varför?
Roller i vår organisation

13.15 – 13.45 PUL / GDPR
Vad innebär begreppen och hur påverkar det oss?
PUL
GDPR
Exempel på personuppgifter

13.45 – 16.15. Introduktion inventering behandling av data
Inventering – Frågebank
Utvärdering
Checklista - Utvärdering
Åtgärdsplan
Registerförteckning
Förvaltning

Avtal
Personuppgiftsavtal
Gallringsrutiner
Gemensam tidsplan för genomförande

16.15 – 16.30 Övriga frågor

REGION VÄSTERBOTTEN

Personuppgiftslagen - Idag

Vad ska vi göra idag?

- Introduktion till det arbete som ligger framför oss.
- Vem berörs och varför?

Roller i vår organisation

- Ägare av informationen.
- Personal som ansvarar/jobbar med registret eller kan lämna ut information.
- Personal som tar del av data
- Samarbetspartners/leverantörer.
- Dataskyddsombud.

Dataskyddsombud

Dataskyddsombud

- Obligatoriskt om
  - Myndighet eller offentligt organ
  - Storskalig behandling av känsliga personuppgifter
- Rapportera till högsta ledningen
- Sätta sig in i lagstiftning och praxis
- Ej ta emot instruktioner om utförandet av uppdraget
- En eller flera personer beroende på storlek på organisation
- Anställd eller konsult

REGION VÄSTERBOTTEN

Dataskyddsombudets roll

- **Kontrollera att personuppgiftslagen/GDPR följs**
- **Informera personalen**
- **Påpeka brister**
- **Skyldighet att anmäla brister som inte åtgärdas**
- **Samråda med datainspektionen**
- **Hjälpa registrerade**
- **Dokumentera personuppgiftsbehandlingar – förteckningsskyldighet**
- **Föra förteckning över de behandlingar som annars skulle ha anmälts till datainspektionen**

Person-uppgiftslagen

Johnny Lundström

Vad är en personuppgift?

Vad är en personuppgift?

- Om man direkt eller indirekt av den registrerade uppgiften kan förstå vem det handlar om är det fråga om en personuppgift.

REGION VÄSTERBOTTEN

Vad är en personuppgift? Exempel

Exempelområden där behandlingar av personuppgifter kan förekomma

- Kund och prospektregister (kontaktpersoner och enskilda näringsidkare)
- Leverantörsregister (kontaktpersoner och enskilda näringsidkare)
- Elektroniska besöksliggare (i receptionen)
- Filmer/bilder/foton av alla de slag (personal framförallt)
- Reseservice (även om den är outsourcad kan ni vara personuppgiftsansvariga för vissa delar)
- Ekonomisystem (särskilt uppgifter om interna användare)
- Lagerhållning (kan vara på individnivå - vem har plockat vad och till vem?)
- Ruttplanering (utkörningsslingor)
- Passersystem (vem har passerat en dörr och när?)
- Ärendehanteringssystem med fritextfält (fråga alltid efter fritextfält i systemen)
- Pensionslistor (kan finnas på ekonomiavdelningen)
- Medarbetarsamtal/lönesamtal (sparas ofta på IT-medium hos chef)
- Kompetensmatriser (kan vara på individnivå.)
- Kontaktinfo till kollegor (intern telefonkatalog, kontakter i e-postsystemet)
- Utvärderingar av verksamheten (kan vara på individnivå)
- Arkivsystem (till exempel sökregistret kan innehålla personuppgifter)
- Behörighetsadministration (oftast hos IT-avdelningen)
- Behandlingshistorik (loggar)
- Faktainformation till grund för rapporter och statistik (även om själva statistiken är avidentifierad)
- GIS:ar (Geografiska InformationsSystem - kan vara på individnivå)
- Kameraövervakning (även om informationen som regel inte sparas)
- Register över utbildningar
- Rekryteringsdatabaser
- Kompetensdatabaser
- Spontanansökningar
- Chefsutvärderingar
- Personlighetstester/profiler’
- Individuell prestationsmätning
- Beredskaps- och katastrofplanering
- Flextidsystem
- Bemanningsplanering
- Personaltidning (även om den kanske är grundlagsskyddad)
- Intranätet
- Webbplatsen
- Egen registerförteckning - till exempel systemägare och kontaktperson för registerutdrag
- Växelns IT-system (där lagras ofta information om vem som har ringt till vem och när)
- System som inte längre används

Vad är PUL
- Person och uppgiftslagen?

Vad är PUL?
- Person och uppgiftslagen

- Lagen är till för att skydda människor mot att deras personliga integritet kränks när personuppgifter behandlas. Begreppet "behandlas" är brett, och omfattar insamling, registrering, lagring, bearbetning, spridning, utplåning, med mera.

- I personuppgiftslagen finns regler för hur **personuppgifter** får behandlas. Lagen bygger i hög grad på **samtycke** och **information till de registrerade.**

Vad är en personuppgift?

- Om man direkt eller indirekt av den registrerade uppgiften kan förstå vem det handlar om är det fråga om en personuppgift.

Vad är PUL- Person och uppgiftslagen?

- Lagen är till för att skydda människor mot att deras personliga integritet kränks när personuppgifter behandlas. Begreppet "behandlas" är brett, och omfattar insamling, registrering, lagring, bearbetning, spridning, utplåning, med mera.
- I personuppgiftslagen finns regler för hur **personuppgifter** får behandlas. Lagen bygger i hög grad på samtycke och information till de registrerade

Nya regler om personuppgiftsbehandling från 2018

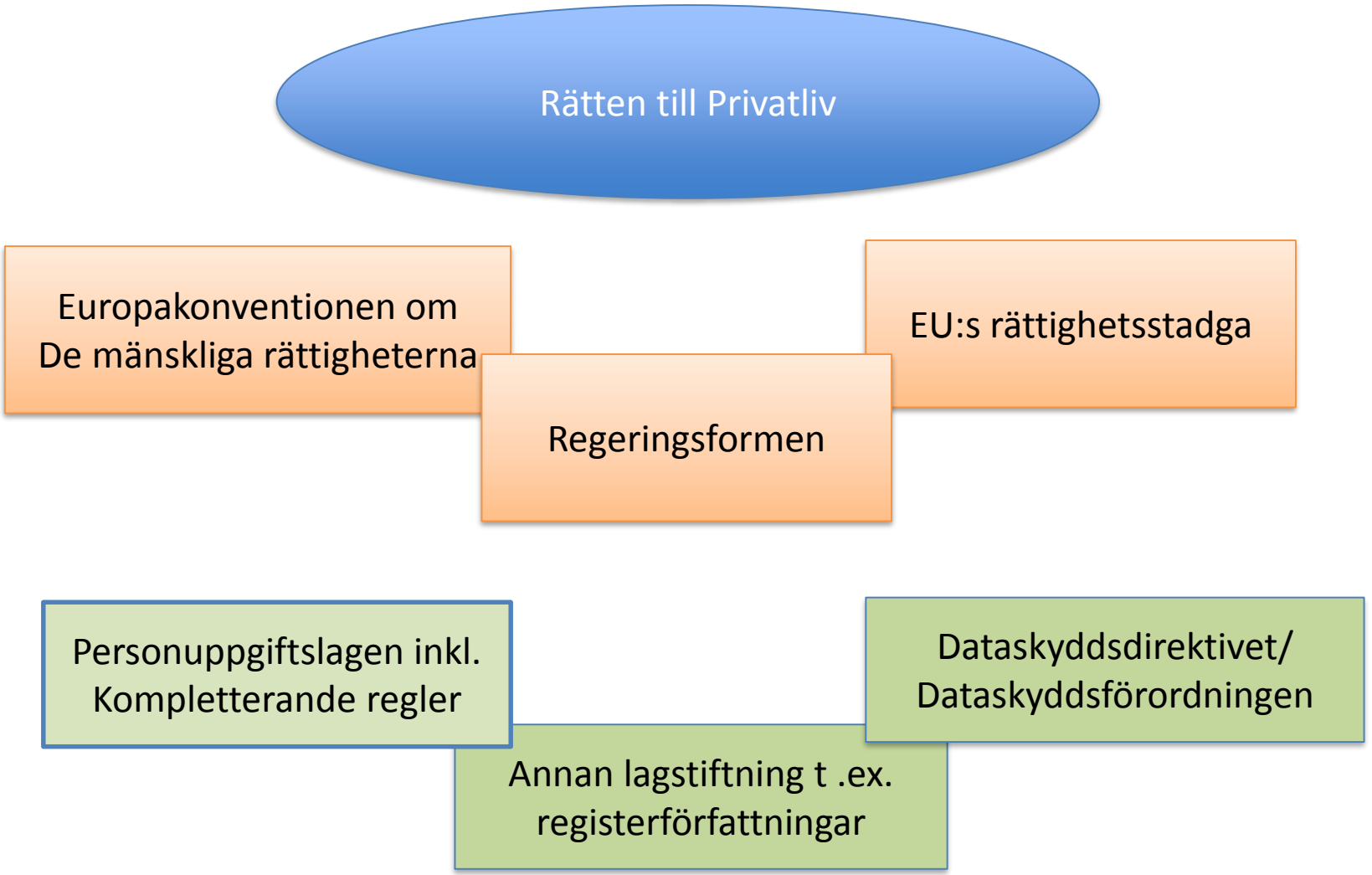
Den 25 maj 2018 kommer en ny EU-förordning om dataskydd att ersätta den svenska personuppgiftslagen.

Förordningen kallas på svenska ”**Allmän dataskyddsförordning**".
GENERAL DATA PROTECTION REGULATION

Förordningen antogs i april 2016 av Europaparlamentet och EU:s ministerråd efter fyra års förhandlingar. Det ursprungliga förslaget till förordningen lades fram av EU-kommissionen 2012.

REGION VÄSTERBOTTEN

Översikt



GDPR

Nya dataförordningen

Vad är Förordningen?

- Gäller som lag i Sverige
- Ska tillämpas av EU:s medlemsländer från mitten av 2018
- Ersätter Personuppgiftslagen (1998:204)
- Kompletteras med nationella regler
  - Regeringen har tillsatt en utredning (Dir.2016:15)
  http://www.regeringen.se/493ace/contentassets/b16563d102144523a1af80fb44321c43/dir.-201615-dataskyddsforordningen

REGION VÄSTERBOTTEN

Utredning (Dir.2016:15)

Beslutsordning

- 21 dec 2017: beslutade regeringen om en lagrådsremiss till en ny dataskyddslag.
- Q1 2018: Regeringen lämnar förslaget till riksdagen att anta lagen
- 25 maj 2018: Lagen börjar gälla

Den föreslagna lagen innehåller bland annat:

- Dataskyddsförordningen ska med vissa undantag ska gälla även utanför sitt egentliga tillämpningsområde, till exempel i verksamhet som rör nationell säkerhet.
- Lagen subsidiär i förhållande till annan lag eller förordning, vilket möjliggör avvikande bestämmelser i så kallade registerförfattningar.
- Förtydligande under vilka förutsättningar personuppgifter får behandlas med stöd av dataskyddsförordningen.
- Barn minst 13 år ska kunna samtycka till behandling av personuppgifter i samband med användning av informationssamhällets tjänster, till exempel sociala medier.
- Sanktionsavgifter ska kunna tas ut även då en myndighet bryter mot dataskyddsförordningen.
- Vissa bestämmelser om begränsning av de registrerades rättigheter samt om skadestånd och överklagande av bland annat tillsynsmyndighetens beslut.
- Lagen inte ska tillämpas i den utsträckning det strider mot tryckfrihetsförordningen eller yttrandefrihetsgrundlagen.

Länk till lagrådsremiss komplettering till ny dataskyddslag:
http://www.regeringen.se/4b00ca/contentassets/65ecec1e45b34af0bc1c272e40ccf581/ny-dataskyddslag

Varför finns förordningen?

- Modernisering – Nu gällande regler bygger på ett direktiv från 1995
- Datamängderna växer (mobilt internet. Internet of things)
- Skapa enhetliga dataskyddsregler inom hela EU (Single Digital Market)
  Harmonisering – Samma rättigheter och skyldigheter i hel EU/EES
- Starkare skydd för den personliga integriteten för EU:s medborgare
  Förstärkning av **enskildas rättigheter** och **tydliggörande av ansvar och skyldigheter** för **den** som behandlar personuppgifter

Förordningens grundprinciper

- Ansvar (Accountability)
- Riskhantering (Risk management)
- Äganderätten flyttas tillbaka till individen

Grundläggande principer för **behandling**:

Laglighet och **öppenhet**
Ändamålsbegränsning
Uppgiftsminimering
Korrekthet
Lagringsminiering
Integritet och konfidentialitet

Den personuppgiftsansvarige ska ansvara för och kunna visa att punkterna efterlevs - **Ansvarsskyldighet**

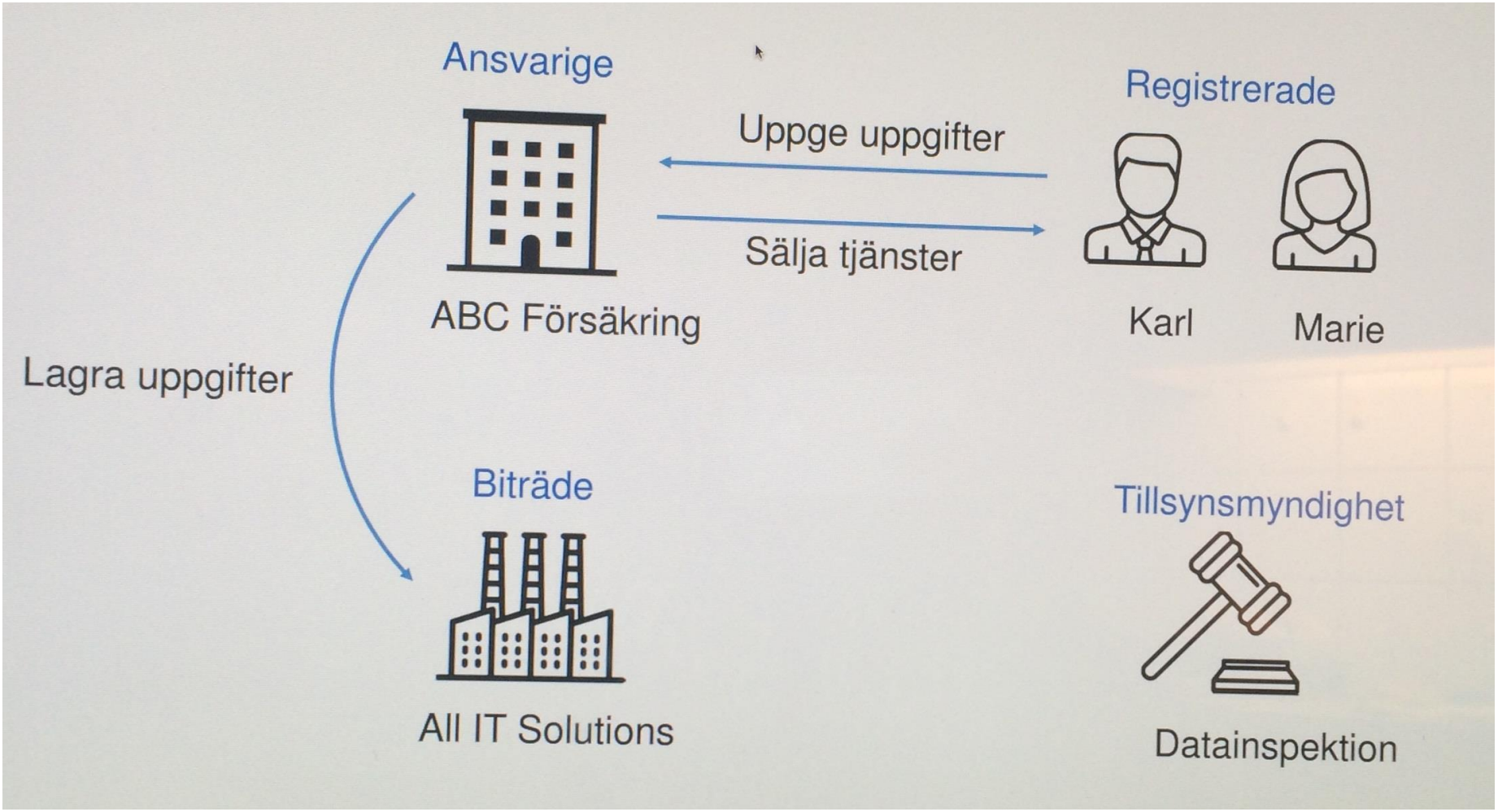
Vad är en personuppgift

Vad är en personuppgift?

- All slags information som **direkt** eller **indirekt** kan hänföras till en identifierbar fysisk person som är i livet
- **Personuppgifter:** Förnamn, efternamn, födelsedag, bild, IP-nummer …..
- **Känsliga personuppgifter:** Etniskt ursprung, politiska åsikter, hälsa, Sexualliv……

Nya dataförordningen

Exempel



Lagliga grunder för behandling av personuppgifter kommer att krävas

- **Rättslig grund** för personuppgiftsbehandling är:
  - Samtycke
  - Avtal(vid köp, vid reklamationer, etc.)
  - Rättslig förpliktelse
  - Skydd för grundläggande intressen
  - Uppgift av allmänt intresse och myndighetsutövning
  - Efter en intresseavvägning(forskningssyfte, marknadsföring)

Grundläggande principer för behandling:
Laglighet, korrekthet och **öppenhet**
Ändamålsbegränsning
Uppgiftsminimering
Korrekthet
Lagringsminiering
Integritet och konfidentialitet

Den personuppgiftsansvarige ska ansvara för och kunna visa att punkterna efterlevs - **Ansvarsskyldighet**

Missbruksregeln försvinner 25 maj 2018

- IDAG: Personuppgiftslagen (1998:204)
  - Behandling i **ostrukturerat material** tillåten om den inte är kränkande. (missbruksregeln)
    Exempel: Löpande text på webbplats eller i e-post

- FROM MAJ 2018 när Dataförordningen börjar gälla
  - Missbruksregeln försvinner
  - Förordningen ska tillämpas i sin helhet på all automatiserad behandling av personuppgifter
  - Genomför anpassningar för att behandla uppgifterna enligt nya bestämmelser(25 maj 2018)

Ett Samtycke ska vara:

- Individuellt
- Frivilligt
- Särskilt

- Ansvarige måste kunna visa att samtycke har hämtats in
  (Ett ansvar att ha bevis hur samtycket har hämtats in)

- Uttryckligt samtycke

- Aktivt godkännande
  - Inga förkryssade rutor
  - Gäller även cookies

- Rätt att motsätta sig profilering

- Direkt marknadsföring och profilering kräver särskild information

- Samtycke är den starkaste grunden för rätten att behandla personuppgifter

- Fundera över om det verkligen behövs samtycke – granska avtal
  http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/samtycke/

Flera rättigheter för registrerade

- Rätten att bli **bortglömd**
  - Personuppgifter ska raderas
  - Till exempel: Radera information från Google
- Rätten till **dataportabilitet**
  - Överföra personuppgifter till annan tjänsteleverantör
  - Till exempel byta socialt nätverk eller e-posttjänst

72-timmarsregeln för dataintrång

- **Vid intrång i eller kontrollförlust över personuppgifter:**
  - **Anmäla** incidenter inom 72 timmar till tillsynsmyndigheten
  - **Informera** registrerade omgående
  - **Dokumentera** alla incidenter

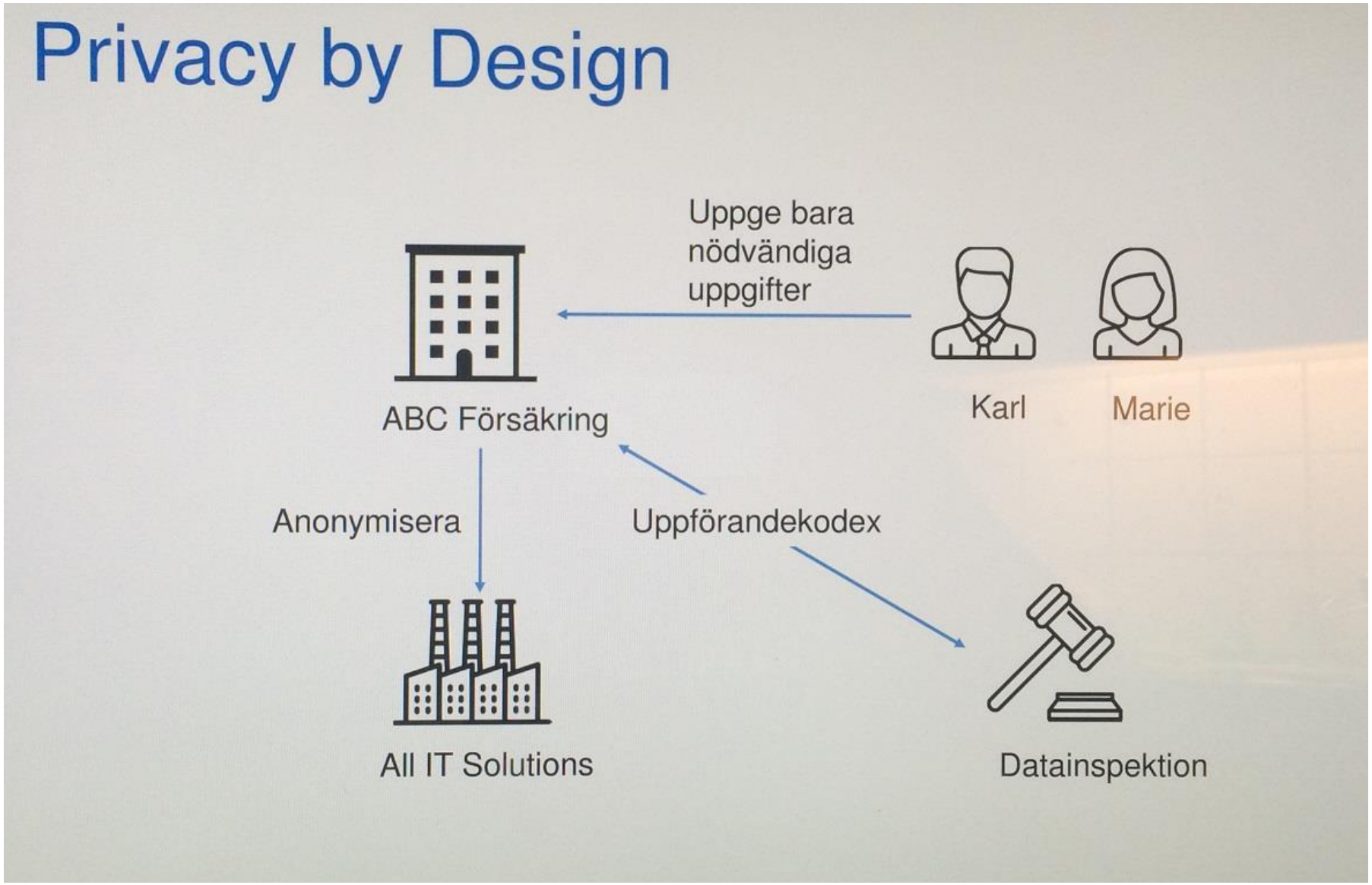
Konsekvensbeskrivning

Man bedömer och värderar risker och inverkan på dataskydd.

- Krävs för behandlingar med **höga integritetsrisker**
- Måste genomföras **innan** behandlingen påbörjas
- Hög risk: Dataskyddsombudet ska samråda med Datainsektionen

Registerförteckning över behandling av data

- Skyldighet att föra förteckning över vilken behandling som sker
- Gäller både ansvarig och biträde
- Gäller företag/organisationer/kommuner/myndigheter som
  - Hanterar personliga uppgifter
  - Hanterar uppgifter om lagöverträdelser
  - Behandlar personuppgifter på en stor skala
  - Direktrapportering till DI om fler än 250 anställda
  - Under 250 anställda - **dataskyddsombud**


Privacy by Design
Uppge bara nödvändiga uppgifter
ABC Försäkring
Karl
Marie
Anonymisera
Uppförandekodex
All IT Solutions
Datainspektion

Privacy by Design

- Högt focus på data- och integritetsskydd redan från projektets början
- Spara bara de uppgifter som behövs
- Anonymisera och pseudonymisera uppgifterna
- Uppförandekodex

Utökat ansvar

- Ansvarig och biträde är **båda** ansvariga för behandlingen
  - Ansvarig har huvudansvaret
  - Om biträde går utöver avtalsbestämmelse
    - biträde blir ansvarig
  - Även företag med säte i tredje land omfattas
  - Anpassa avtal med leverantör utifrån nya GDPR

Starkare sanktioner

- 10 millioner euro eller 2 % av årsomsättningen
    - Ingen registerförteckning
    - Ingen konsekvensbedömning (DPIA)
    - Inget dataskyddsombud (DPO)

- 20 millioner euro eller 4 % av årsomsättningen
    - Otillåten behandling
    - Otillåten behandling av känsliga uppgifter
    - Inte lämnar information som krävs
    - Felaktigt samtycke
    - Otillåten överföring från tredje land

Hur kommer du och jag, vi att påverkas?

- Alla som behandlar personuppgifter påverkas

- Omfattande anpassningar

  - Organisatoriska
  - Administrativa
  - Tekniska

Tack för medverkan

REGION VÄSTERBOTTEN

GDPR – Samtycke och gallring

För att underlätta framtida hantering av samtycke och gallring kan några enkla regler införas:

- Använd email enbart som transportör av information, dvs ej för t.ex. lagring eller process (eg. ”huvudbärare”) av vital information (på detta sätt kan mail gallras utan att vital information går förlorad)

- Se till att ha endast ett ärende per email-konversation

- Undvik massutskick och att skicka listor/personuppgifter i innehållet i ett email.

- Skapa effektiva och säkra rutiner för att löpande gallra email och säkerställa att det finns mekanismer för att hitta och processa personuppgifter, både i adressfält och/eller innehåll

Hur kan man förbereda sig?

- Kartläggning
- Riskanalys
- Tekniska och organisatoriska åtgärder/riktlinjer
- Utse en PUL-ansvarig/ Dataskyddsombud(om man inte har sedan tidigare)
- Gallringsplan
- Implementering
- Uppföljning

Innebörd nya DSF?

Dataskyddsförordningen ersätter Personuppgiftslagen och träder i kraft i maj 2018.
Här är de sex största förändringarna:

1. Strängare krav på företag och myndigheter att informera om varför de behandlar personuppgifter, vilka de uppgifterna är och hur de hanteras.

2. Behandlingen får bara ske i samtycke och uppgifterna får inte användas för något annat är vad individen gett sitt samtycke till.

3. Företag och myndigheter måste kunna visa hur de hanterar uppgifterna på ett säkert och korrekt sätt. Det räcker inte att säga att de har rutiner, de måste kunna visa att de följs – till exempel kan det betyda att de snabbt måste kunna lämna ut registerutdrag. Företagen måste kunna göra en integritetsanalys.

Innebörd nya DSF?

4. Varje företag/myndighet måste ha ett dataskyddsombud. Personen har större ansvar och fler skyldigheter än tidigare. Vissa företag behöver dataskyddsombud, när det handlar om särskilt riskfylld personuppgiftshantering. Det är fortfarande oklart vilka som omfattas av det kravet.

5. Dataskydd som standard – känsliga data ska alltid krypteras. Detta kallas också privacy by default.

6. Datainspektionen kan utfärda böter, administrativa sanktioner, till företag och myndigheter som inte sköter sig. Det kan bli dyrt, upp till fyra procent av organisationens omsättning. Eller 20 miljoner euro om organisationen inte är ett företag

REGION VÄSTERBOTTEN

Vad är ett dataskyddsombud

- **Enligt definitionen (paragraf § 13 personuppgiftslagen)**
- **En fysisk person**
- **Utsedd av den personalansvarige**
- **Självständigt kontrollera att personuppgifter behandlas korrekt**
- **”Internrevisor”**

REGION VÄSTERBOTTEN

Förteckningens innehåll

- **Personuppgiftsansvariges namn, adress, telefonnummer o org.nummer**
- **Ändamålet med behandlingen**
- **Registrerade som berörs**
- **Uppgifter som ska behandlas**
- **Mottagare av uppgifterna**
- **Överföring till tredje land**
- **Säkerhetsåtgärder som vidtagits**

REGION VÄSTERBOTTEN

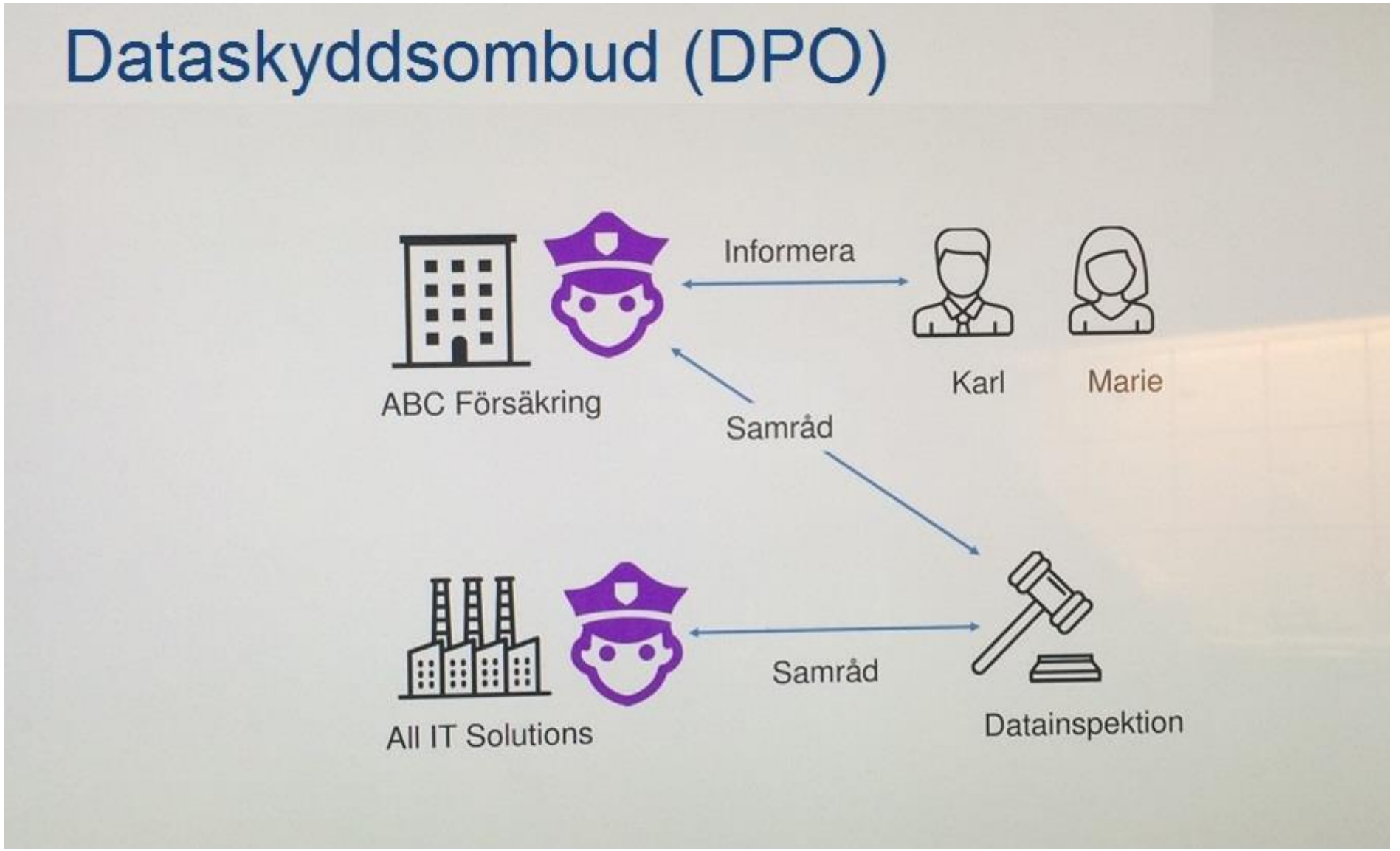
Personuppgiftsombudets Uppgift

- **God informationssäkerhetshantering räddar organisationen**
- **Omfattar både hårdvara, mjukvara och medarbetare**
- **Risker**
  - Ekonomiska
  - Förtroendemässiga
  - Interna
  - Externa
- **Legala skyldigheter**
- **PuO/DPO ser till att personuppgifter behandlas på ett korrekt sätt och lagligt inom den egna organisationen, en garanti för integritetsskyddet**

REGION VÄSTERBOTTEN

Att starta

- **Visa organisationen att jag är PoU/DPO**
- **Vad vill jag? Vad vill organisationen?**
- **Bygg intern organisation och utbilda berörda personer som kan tänkas möta/arbeta med frågorna.**
- **Inventering**
- **Sätta upp rutiner, ex. för begäran om registerutdrag, klagomål**
- **Rapport och ”Actionplan”**


Dataskyddsombud (DPO)
Informera
Karl
Marie
ABC Försäkring
Samråd
All IT Solutions
Samråd
Datainspektion