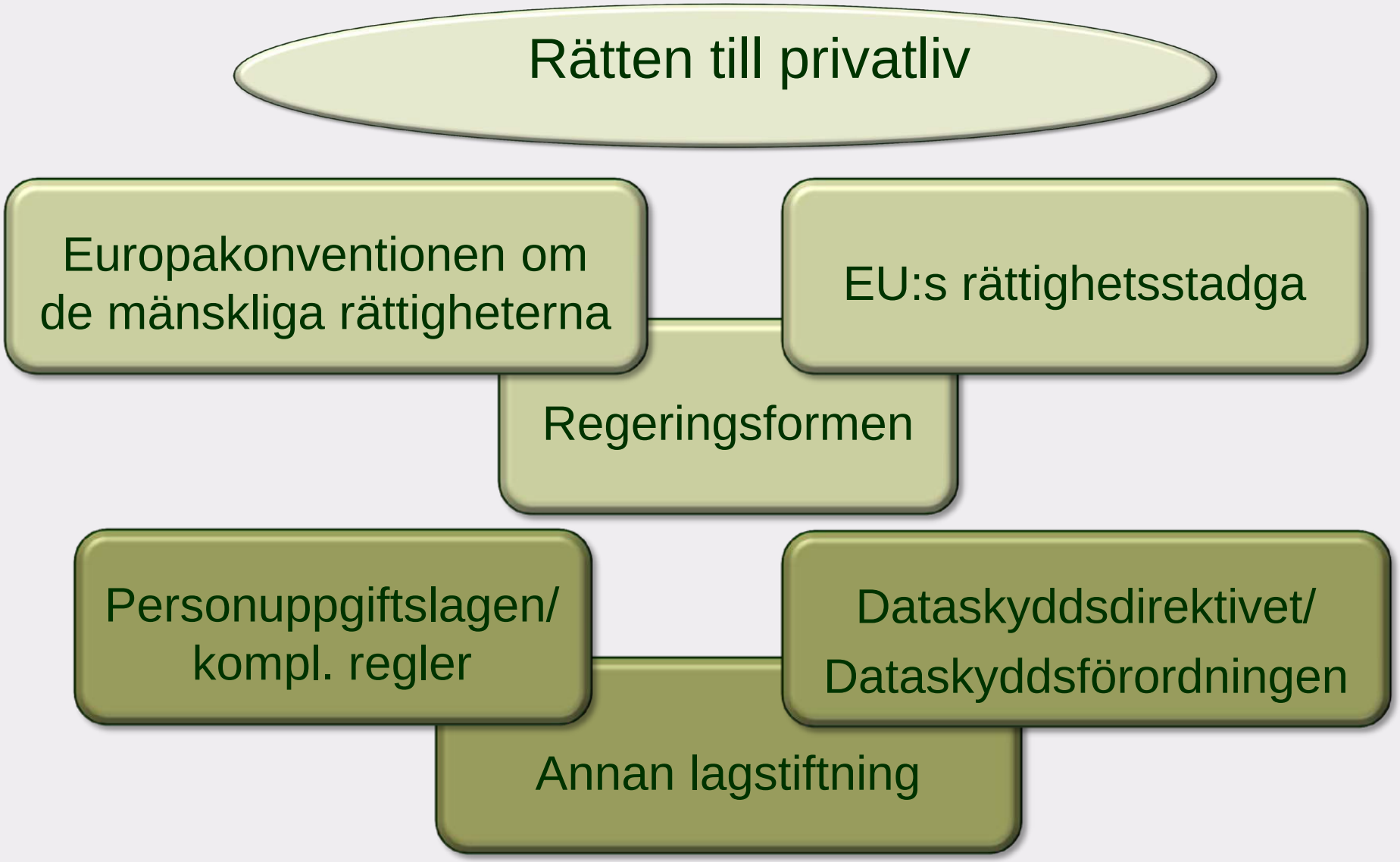
Kort introduktion till EU:s dataskyddsförordningen (GDPR)

Materialet

- Materialet kommer från datainspektionens kurs, *Grundkurs i den nya dataskyddsförordningen och personuppgiftslagen*


Rätten till privatliv
Europakonventionen om de mänskliga rättigheterna
EU:s rättighetsstadga
Regeringsformen
Personuppgiftslagen/ kompl. regler
Dataskyddsdirektivet/ Dataskyddsförordningen
Annan lagstiftning

Artikel 8
Skydd av personuppgifter

1. Var och en har rätt till skydd av de personuppgifter som rör honom eller henne.

2. Dessa uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem.

3. En oberoende myndighet ska kontrollera att dessa regler efterlevs.

EU:s rättighetsstadga

Några viktiga definitioner

- Personuppgift enligt **personuppgiftslagen**:
  ”All slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet”

3 § personuppgiftslagen

Några viktiga definitioner

- Personuppgift enligt **dataskyddsförordningen**:
  ”Varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett *namn*, ett identifikationsnummer, *en lokaliseringsuppgift* eller *onlineidentifikatorer* eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, *genetiska*, psykiska, ekonomiska, kulturella eller sociala identitet”

Artikel 4

Allt är inte "klart"

- Många utredningar pågår, beräknas vara klara våren 2017
- Avvakta med utbildningar inom GDPR

Niklas.Nikitin@kau.se
IT-säkerhetssamordnare

Varför nya regler?

- **Modernisering** – nu gällande regler bygger på ett direktiv från 1995
- Förstärkning av **enskildas rättigheter** och tydliggörande av **skyldigheter** för den som behandlar personuppgifter
- **Harmonisering** – samma rättigheter och skyldigheter i hela EU/EES

Niklas.Nikitin@kau.se
IT-säkerhetssamordnare

När gäller dataskyddsförordningen?

- Personuppgiftsansvariga och personuppgiftsbiträden som är etablerade i EU
- Personuppgiftsansvariga och personuppgiftsbiträden som är etablerade utanför EU och
  - erbjuder varor och tjänster i EU eller
  - övervakar registrerades beteende i EU

Artikel 3, skäl 23 och 24

När gäller inte dataskyddsförordningen?

- Undantag för privatpersoners behandling
- Uppgifter om avlidna
- Nationell säkerhet och gemensam utrikes- och säkerhetspolitik
- Brottsbekämpande myndigheter (”polisdirektivet”)
- Tryck- och yttrandefrihet
- Tillgången till allmänna handlingar - offentlighetsprincipen

Artikel 2, skäl 16-21+27, Artikel 85, skäl 153, Artikel 86, skäl 154

Vilka är de största nyheterna?

- En förordning gäller som svensk lag
  - Harmonisering innebär enhetligare tillämpning
  - Missbruksregeln i 5 a § försvinner
- Stärkt ställning för den registrerade
  - Samtycke, information m.m.
- Ökat ansvar för ansvariga och biträden
  - Riskbaserad skyldigheter och ansvar
  - Skyldighet att anmäla dataskyddsincidenter
  - Sanktionsavgifter

Vad är (i princip) oförändrat?

- Strukturen
- Tillämpningsområdet
- Grundläggande krav
- Rättslig grund
- Känsliga personuppgifter
- Överföring till tredje land

Niklas.Nikitin@kau.se
IT-säkerhetssamordnare

”Navet” – grundläggande principer

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

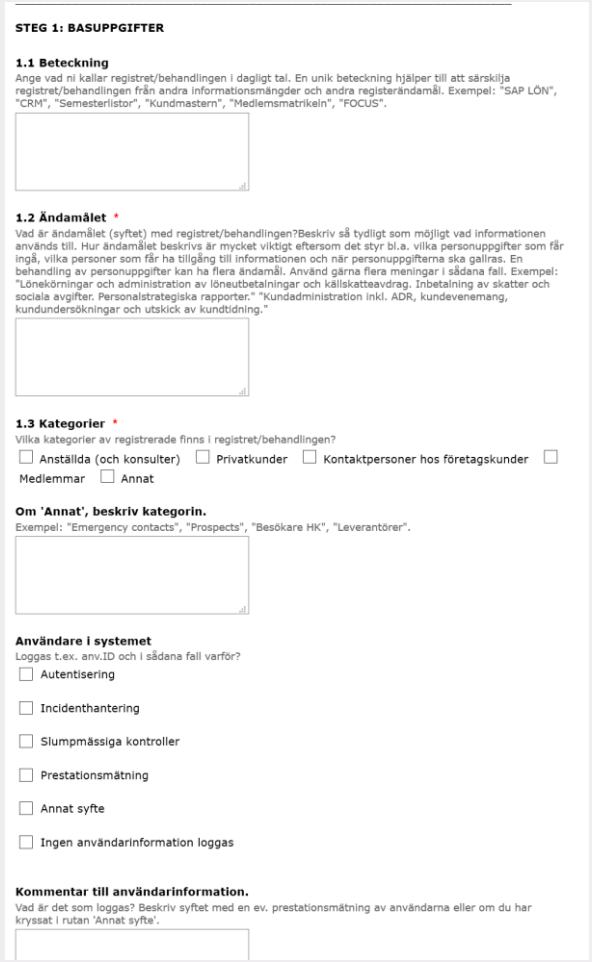
Art. 5, skäl 39, art. 6.4, skäl 50

Hur kan vi visa att vi följer förordningen?

- Certifiering och uppförandekoder
- Anta interna strategier för dataskydd
- Dokumentation
- Konsekvensbedömning
- Öppenhetsprincipen

Niklas.Nikitin@kau.se
IT-säkerhetssamordnare

Kau ska använda Draftit för dokumentera personuppgiftsanvändandet



STEG 1: BASUPPGIFTER

1.1 Beteckning

Ange vad ni kallar registret/behandlingen i dagligt tal. En unik beteckning hjälper till att särskilja registret/behandlingen från andra informationsmängder och andra registerändamål. Exempel: "SAP LÖN", "CRM", "Semesterlistor", "Kundmastern", "Medlemsmatrikeln", "FOCUS".

1.2 Ändamålet *

Vad är ändamålet (syftet) med registret/behandlingen?Beskriv så tydligt som möjligt vad informationen används till. Hur ändamålet beskrivs är mycket viktigt eftersom det styr bl.a. vilka personuppgifter som får ingå, vilka personer som får ha tillgång till informationen och när personuppgifterna ska gallras. En behandling av personuppgifter kan ha flera ändamål. Använd gärna flera meningar i sådana fall. Exempel: "Lönekörningar och administration av löneutbetalningar och källskatteavdrag. Inbetalning av skatter och sociala avgifter. Personalstrategiska rapporter." "Kundadministration inkl. ADR, kundevenemang, kundundersökningar och utskick av kundtidning."

1.3 Kategorier *

Vilka kategorier av registrerade finns i registret/behandlingen?

☐ Anställda (och konsulter) ☐ Privatkunder ☐ Kontaktpersoner hos företagskunder ☐ Medlemmar ☐ Annat

Om 'Annat', beskriv kategorin.

Exempel: "Emergency contacts", "Prospects", "Besökare HK", "Leverantörer".

Användare i systemet

Loggas t.ex. anv.ID och i sådana fall varför?

☐ Autentisering

☐ Incidenthantering

☐ Slumpmässiga kontroller

☐ Prestationsmätning

☐ Annat syfte

☐ Ingen användarinformation loggas

Kommentar till användarinformation.

Vad är det som loggas? Beskriv syftet med en ev. prestationsmätning av användarna eller om du har kryssat i rutan 'Annat syfte'.

Niklas.Nikitin@kau.se
IT-säkerhetssamordnare

När får ni behandla personuppgifter?

- Samtycke
- Behandling är nödvändig för
  - avtal
  - rättslig förpliktelse
  - grundläggande intressen
  - arbetsuppgift av allmänt intresse och myndighetsutövning
  - intresseavvägning (ej för myndigheter)

Niklas.Nikitin@kau.se
IT-säkerhetssamordnare

Samtycke

- Samtyckesframställan ska presenteras på **ett klart och tydligt sätt** och ni ska **kunna visa** att den registrerade har samtyckt
- Den registrerade ska informeras om rätten att återkalla ett samtycke
- Mycket begränsat för **myndigheter** att använda
- Om villkoret för att få tillgång till en vara och tjänst är ett samtycke till onödig behandling (utöver) kan det innebära att samtycket inte kan anses frivilligt
- Samtycke av **barn** under 16 år (13 år) kräver godkännande av vårdnadshavare för ”informationssamhällets tjänster”

Artikel 6-8, skäl 42-43

När får ni behandla personuppgifter?

- Samtycke
- Behandling är nödvändig för
  - avtal
  - rättslig förpliktelse
  - grundläggande intressen
  - arbetsuppgift av allmänt intresse
  - myndighetsutövning
  - intresseavvägning (**ej för myndigheter**)

Artikel 6, skäl 44-50

När får ni föra över personuppgifter till tredje land?

- En överföring kräver **stöd i dataskyddsförordningen**!
- Gäller även för **personuppgiftsbiträdet**.
- Beslut av Kommissionen om att landet har en adekvat skyddsnivå
- Lämpliga skyddsåtgärder har vidtagits
- Särskilda undantag t.ex. samtycke, fullgöra ett avtal, allmänintresset, rättsliga anspråk, skydda grundläggande intressen

Artikel 45, skäl 103-107, Artikel 46, skäl 108-109, Artikel 47, skäl 110, Artikel 49, skäl 111

Registrerades rättigheter

- **Information** och registerutdrag
- Rättelse och radering
- Begränsning av behandling
- **Dataportabilitet**
- Invändning mot behandling
- Motsätta sig automatiserad behandling

Artiklarna 12-23

Radering – ”rätten att bli glömd”

- **Radera** personuppgifter om den registrerade
- **Informera**, i vissa fall, andra personuppgifts- ansvariga och mottagare
- **Förutsättningar**, bl.a.
  - om uppgifter inte längre behövs för ändamålen
  - återkallat samtycke
- **Undantag**, bl.a.
  - Nödvändig för yttrande- och informationsfriheten
  - Nödvändig för rättslig förpliktelse, allmänt intresse och myndighetsutövning, rättsliga anspråk

Artikel 17 och 19, skäl 65-66

Invända mot behandling

- Den registrerade har rätt att invända mot (**motsätta sig**) behandling av sina personuppgifter som grundas på allmänt intresse, myndighetsutövning eller intresseavvägning
- Den personuppgiftsansvarige måste göra en **ny prövning** (intresseavvägning) utifrån den registrerades situation och eventuellt **upphöra** med behandling
- Vid **direkt marknadsföring** måste behandling upphöra
- Särskilt om **forskning och statistik** och bevakning av **rättsliga anspråk, allmänt intresse** m.m.

Artikel 21, skäl 69-70

Dataportabilitet

- Rätt att **få ut** och **överföra** egna personuppgifter till annan personuppgiftsansvarig i ett strukturerat, allmänt använt och maskinläsbart format, **om**
  - uppgifter har tillhandahållits av den registrerade,
  - behandling sker med stöd av samtycke eller avtal,
  - behandling sker automatiserat
  - inte påverkar andra rättigheter och friheter

Artikel 20, skäl 68

Skyldigheter för personuppgiftsansvariga

- Ansvarsskyldighet
- Den personuppgiftsansvarige ska **vidta åtgärder** för att säkerställa att förordningen följs, och för att kunna visa att förordningen följs
- Inbyggt dataskydd och dataskydd som standard
- Krav på biträdesavtalet
- Register över behandlingar
- Säkerhet
- Anmälan av personuppgiftsincidenter
- Konsekvensbedömningar och förhandssamråd
- Utse dataskyddsombud

Artikel 24, 25, 28, 30 och 32-35

Skyldigheter för personuppgiftsbiträden

- Lämna garantier för att förordningen följs
- Krav på biträdesavtalet
- Bistå den personuppgiftsansvarige
- Register över behandling
- Eget ansvar för säkerhet
- Anmälan av personuppgiftsincidenter – till den personuppgiftsansvarige
- Utse dataskyddsombud

Artikel 28, 30, 32 och 33

Vad händer om ni bryter mot reglerna?

- Datainspektionen
  - Tillsyn och föreläggande
  - Administrativa sanktionsavgifter
- Den registrerade
  - Klagomål
  - Skadestånd

Artikel 77, 78, 82 , 83, 84

Vad händer 2018?

- Dataskyddsförordningen ersätter dataskyddsdirektivet från 1995 och personuppgiftslagen upphör att gälla
- All svensk lagstiftning inom förordningens tillämpningsområde måste ses över (påbörjat)
- Europeiska dataskyddsstyrelsen ersätter den s.k. 29-gruppen
- Datainspektionen får nya arbetsuppgifter
- Personuppgiftsansvariga och personuppgiftsbiträden ska vara förberedda och följa dataskyddsförordningen

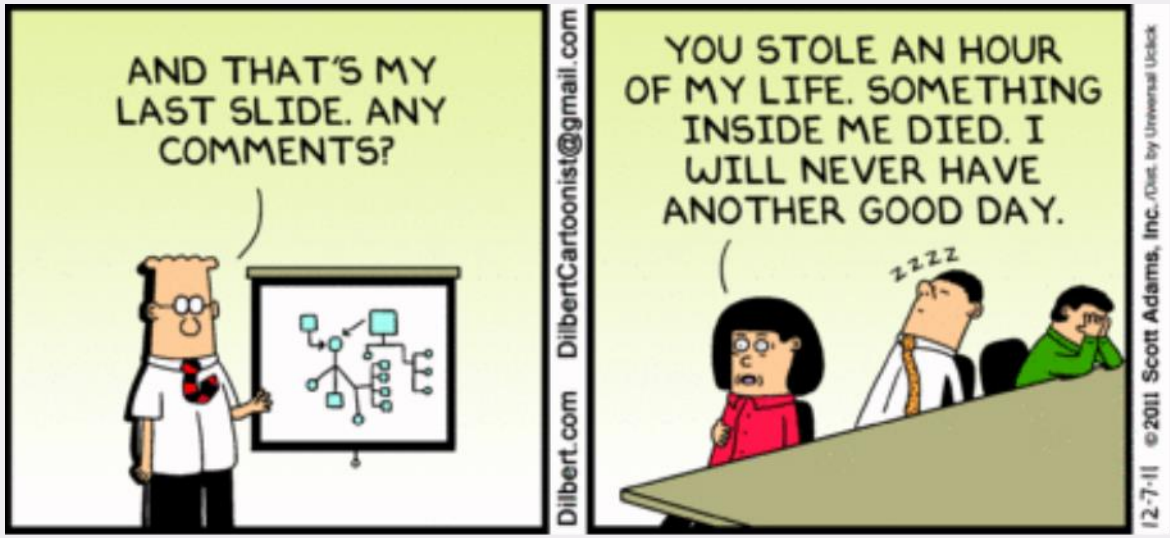
Niklas.Nikitin@kau.se
IT-säkerhetssamordnare

Vad gör Kau inför GDPR?

- Startat en dataskyddsgrupp för att bl.a. arbeta med detta
- Vill samarbeta!

Niklas.Nikitin@kau.se
IT-säkerhetssamordnare

Frågor?



Niklas.Nikitin@kau.se
IT-säkerhetssamordnare