



# Dataskyddsförordningen (GDPR)

Borlänge den 7 december 2016

Martin Brinnen

# Rätten till privatliv



# Vad är nytt?

- Dataskyddsförordning ersätter personuppgiftslagen
  - Ökad harmonisering med EU
  - Missbruksregeln i 5 a § PUL försvinner
- Stärkt ställning för den registrerade
  - "Rätten att bli glömd" (?)
  - Dataportabilitet
- Ökat ansvar för ansvariga och biträden
  - Konsekvensbedömning avseende dataskydd
  - Anmäla personuppgiftsincident
  - Sanktionsavgifter

# Att förstå GDPR

1. Vad står det?
  - a. Läs artikeltext och tillhörande skäl
  - b. Jfr sammanhanget
  - c. Jfr formuleringens användning på annat ställe
  - d. Jfr olika språkversioner (särskilt engelska)
2. Saklig ändring avsedd?
  - a. Jfr direktivet med skäl och språkversioner
  - b. Jfr praxis från EU-domstolen
3. Skillnad i förhållande till personuppgiftslagen?
  - a. Jfr PUL inkl. förarbeten, praxis etc.
4. Oklart? Tidigare oklarhet kvarstår?

# Personuppgiftslagen på två minuter

- Behandling av personuppgifter
- Subsidiär
- Missbruksregeln för löpande text (5 a §)
- Undantag
- Grundläggande krav
- Tillåten behandling
- Känsliga personuppgifter m.m.
- Information till de registrerade
- Rättelse
- Säkerhet
- Tillsyn och skadestånd

Personuppgifts-  
ansvarig

Dataskydds-  
ombud

Personuppgifts-  
biträde

Den registrerade



När gäller förordningen?

# När tillämpas förordningen?

- **Behandling av personuppgifter**
- ... som utförs av personuppgiftsansvariga eller personuppgiftsbiträden som är **etablerade i EU**
- ... som utförs av personuppgiftsansvariga eller personuppgiftsbiträden som är **etablerade utanför EU** och där dessa antingen
  - erbjuder varor och tjänster i EU eller
  - övervakar registrerades beteende i EU



# När gäller inte förordningen?

- Privat behandling
- Tryck- och yttrandefrihet
- Journalistiska ändamål m.m.
- Offentlighetsprincipen
- Nationell säkerhet
- Gemensam utrikes- och säkerhetspolitik
- Brottsbekämpande myndigheter => "polisdirektivet"



# Grundläggande principer för behandlingen

# Principer

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

# Vad innebär principerna i praktiken?

- ✓ identifiera rättslig grund för behandlingen
- ✓ informera de som uppgifterna avser
- ✓ bestäm ändamålet med behandlingen
- ✓ samla endast in uppgifter som behövs för ändamålet
- ✓ samla inte in fler uppgifter än nödvändigt för ändamålet
- ✓ se till att uppgifterna alltid är korrekta och uppdaterade
- ✓ skydda insamlade personuppgifter
- ✓ radera uppgifterna när de inte längre behövs för ändamålet
- ✓ se till att du kan visa att du gör rätt

# Hur kan vi visa att vi följer förordningen?

- Öppenhetsprincipen
- Anta lämpliga strategier för dataskydd
- Dokumentation
- Uppförandekoder
- Certifiering





# Rättslig grund för behandlingen

# Rättslig grund för behandlingen

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

# Samtycke

- varje slag av **frivillig**, specifik, **informerad** och **otvetydig** viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller en **entydig bekräftande handling**, godtar behandling av personuppgifter som rör honom eller henne,
- Samtyckesframställan ska vara **klar och tydlig**
- Mycket begränsat för **myndigheter** att använda
- Samtycke av **barn** (<13/16 år) kräver i vissa fall godkännande av vårdnadshavare



# Känsliga personuppgifter m.m.

- Känsliga personuppgifter
  - bl.a. etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening
  - genetiska och biometriska uppgifter, hälsa och sexualliv
- Uppgifter om lagöverträdelser
- Personnummer
- Överföring till land utanför EU/EES

# Registrerades rättigheter

# Registrerades rättigheter

- **Information** och registerutdrag
  - Rättelse och **radering**
  - Begränsning av behandling
  - **Dataportabilitet**
  - Invändning mot behandling
  - Motsätta sig automatiserad behandling
- 
- Personuppgiftsansvariga har en skyldighet att underlätta utövandet av rättigheterna

# Information och registerutdrag

- Information väsentlig del av integritetsskyddet
- Skyldighet att ge klar och tydlig information
  - Får kombineras med standardiserade symboler
- Kortare tidsfrister
- Kostnadsfritt
- Informationsskyldigheten är mer omfattande än tidigare

# Skyldighet att lämna information

	När personuppgifter samlas in från den registrerade (art. 13)	När personuppgifter samlas in från annan (art. 14)	Den registrerades rätt till tillgång (registerutdrag) (art. 15)	PUA:s register över behandling (art. 30.1)
Personuppgiftsansvarige	Ja	Ja	Nej	Ja
Dataskyddsombudet	Ja	Ja	Nej	Ja
Ändamålen	Ja	Ja	Ja	Ja
<b>Rättslig grund</b>	Ja	Ja	Nej	Nej
Kategorier av personuppgifter	Nej	Ja	Ja	Ja
Intresse vid intresseavvägning	Ja	Ja	Nej	Nej
Mottagarna	Ja	Ja	Ja	Ja
Tredjelandsoverföring m.m.	Ja	Ja	Ja	Ja
Lagringstid	Ja	Ja	Ja	Ja
De registrerades rättigheter	Ja	Ja	Ja	Nej
Rätten att dra tillbaka ett samtycke	Ja	Ja	Nej	Nej
Rätten att lämna klagomål till DPA	Ja	Ja	Ja	Nej
Uppgiftsskyldighet enligt avtal eller lag	Ja	Nej	Nej	Nej
Automatiserat beslutsfattande	Ja	Ja	Ja	Nej
Källa varifrån uppgifterna har hämtats	Nej	Ja	Ja	Nej
Säkerhetsåtgärder	Nej	Nej	Nej	Ja

OBS. Tabellen är förenklad och ej fullständig. Ytterligare skyldigheter att informera finns i andra bestämmelser.

# nge

Välkommen till Borlänge kommuns gästnät.

Syftet med Borlänge kommuns gästnät är att besökare och gäster ska kunna ansluta till internet.

För att få ansluta till Borlänge kommuns gästnät gäller följande policy:

- Ni ska uppge ert namn och giltig e-post adress.
- När ni använder kommunens gästnät är ni skyldiga att följa lagar och regler som gäller i samhället
- All aktivitet loggas vilket betyder att det finns möjlighet att se vilka sidor som ni besöker.
- Kontroversiella sidor som inte är i linje med Borlänge kommuns värdegrunder är blockerade.

**Acceptera**

**Neka**


# Radering – "rätten att bli glömd"

- **Radera** personuppgifter om den registrerade
- **Informera**, i vissa fall, andra personuppgiftsansvariga 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

# 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

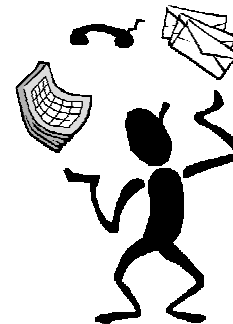




# Skyldigheter för den som behandlar personuppgifter

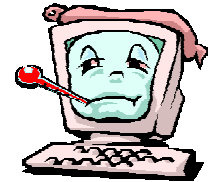
# Skyldigheter för personuppgiftsansvariga

- Ta, och visa, ansvar (ansvarsskyldighet)
- Inbyggt dataskydd och dataskydd som standard
- Register över behandlingar
- Säkerhet
- Anmälan av personuppgiftsincidenter
- Konsekvensbedömningar och förhandssamråd
- Utse dataskyddsombud
- Anlita personuppgiftsbiträde



# Anmälan av personuppgiftsincidenter

- Personuppgiftsincidenter som innebär **risker** för enskildas rättigheter och friheter...
- ...ska anmälas till Datainspektionen inom **72 timmar**
- Personuppgiftsbiträde ska anmäla till personuppgiftsansvarig
- Alla dataskyddsincidenter ska dokumenteras
- Vid hög risk ska, i vissa fall, även registrerade informeras



# Konsekvensbedömningar

- Behandling som kan misstänkas innebära hög risk ska en konsekvensutredning genomföras
- Om hög risk krävs samråd med Datainspektionen

# 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

# Dataskyddssombudets uppgifter

- Ska minst ha följande arbetsuppgifter
  - Informera och ge råd
  - Övervaka efterlevnad
  - Samarbeta med tillsynsmyndigheten
  - Vara tillgänglig för de registrerade
  - Ge råd vid konsekvensbedömning



# Vad händer om ni bryter mot reglerna?

- Datainspektionen
  - Tillsyn och föreläggande
  - **Administrativa sanktionsavgifter**; upp till 20 milj Euro eller 4 % av globala omsättningen
  - Medlemsstaterna kan besluta om avgifter för myndigheter
  
- Den registrerade
  - Klagomål
  - Skadestånd

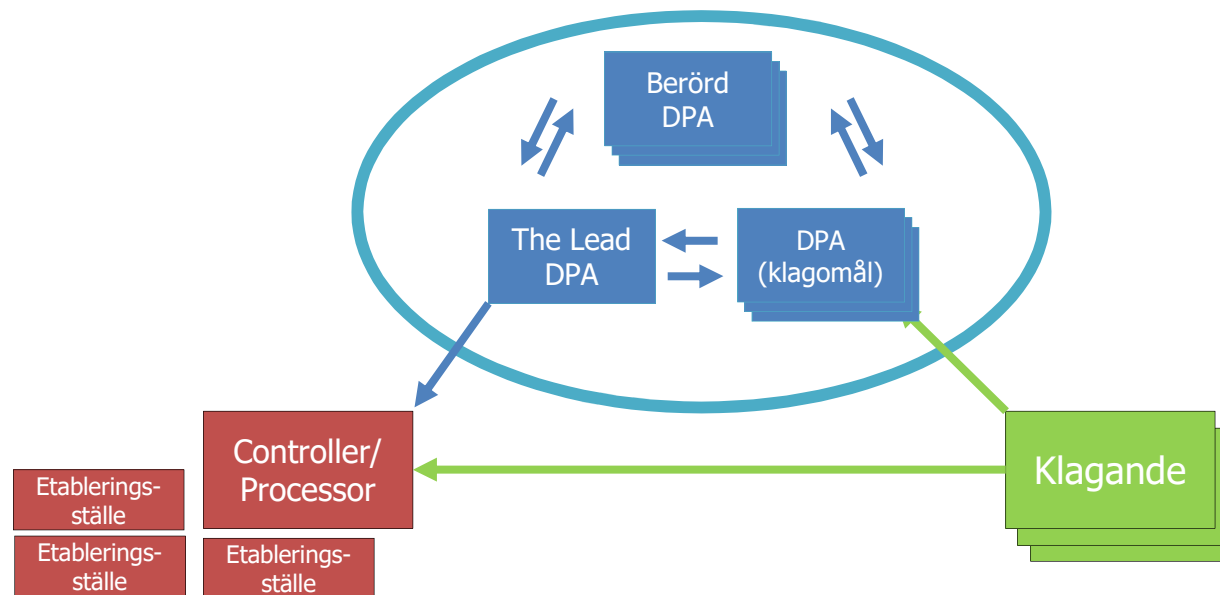


# Gränsöverskridande behandling av personuppgifter inom EU



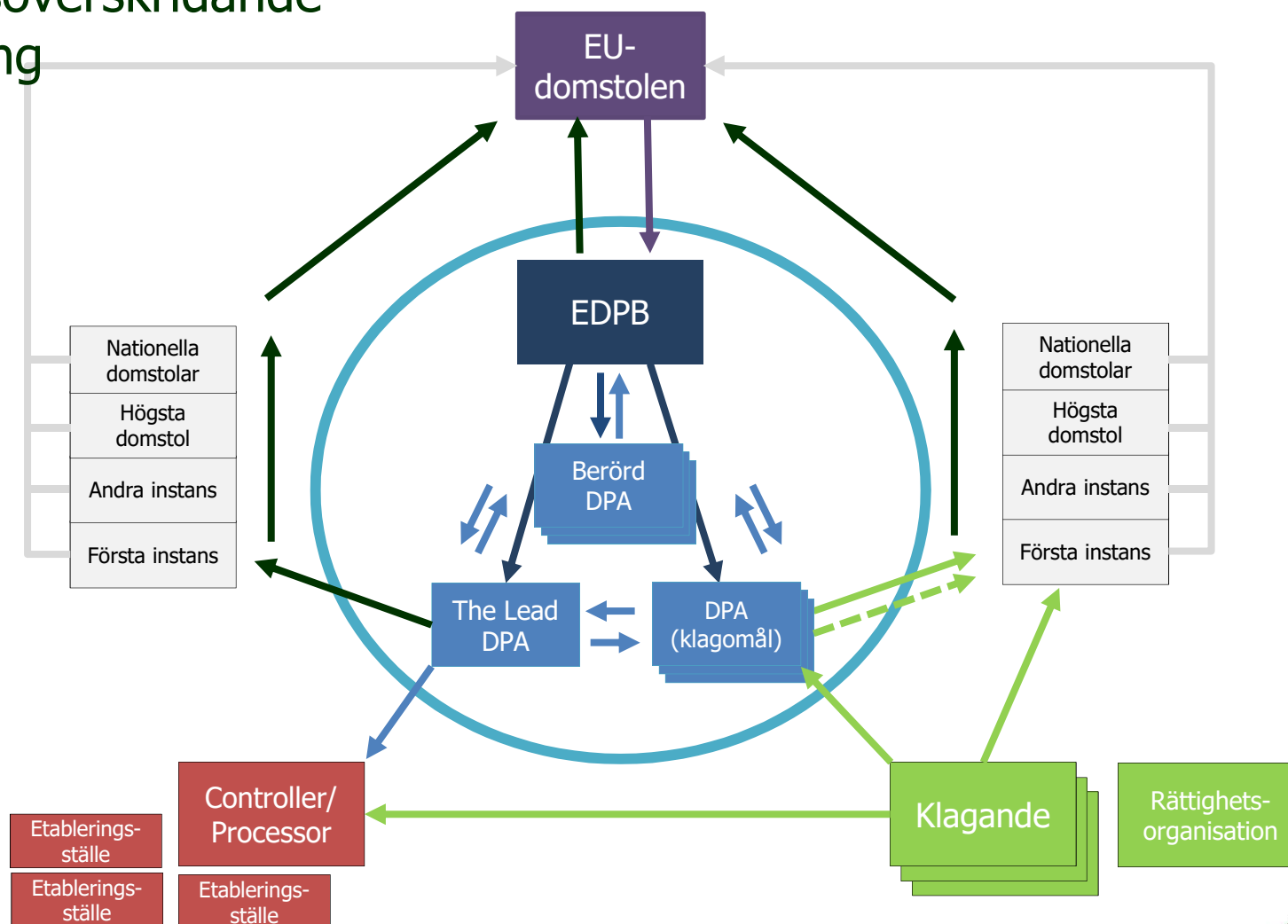
# One-stop-shop

vid gränsöverskridande behandling



DPA = Data Protection Authority  
EDPB = European Data Protection Board

# Överklaganden vid gränsöverskridande behandling



DPA = Data Protection Authority  
EDPB = European Data Protection Board

Förbered er



EU:s dataskyddsförordning

25 maj 2018

533 dagar kvar

# Förberedelser för GDPR - Checklista

- Skapa medvetenhet inom organisationen
  - Är ledningen insatt?
  - Finns det resurser för arbetet?
  - Utse dataskyddsombud?
- Inventera personuppgiftsbehandlingar
  - Vilka kategorier av personuppgifter behandlas?
  - Känsliga personuppgifter? Uppgifter om barn?
  - Hur samlas uppgifterna in och till vem lämnas de ut?
  - Upprätta ett register över personuppgiftsbehandlingar
  - Särskilda integritetsrisker ("hög risk")

# Förberedelser för GDPR - Checklista

- Se över vilken rättslig grund för behandlingen
  - Missbruksregeln försvinner, alternativ?
  - Hur inhämtas samtycke?
  - Myndigheter kan i princip inte använda samtycke eller intresseavvägning
- Se över vilken information som lämnas till de registrerade
  - Uppfyller ni informationskraven?
  - Lättillgänglig form samt klart och tydligt språk

# Förberedelser för GDPR - Checklista

- Ta fram rutiner för de registrerades rättigheter
  - Registerutdrag, rättelse, radering, begränsning, dataportabilitet, invändning, automatiserade beslut
- Verksamhet i flera länder?
  - Vilken dataskyddsmyndighet inom EU blir ansvarig myndighet för personuppgiftsbehandlingen?
  - Överförs personuppgifter till tredje land?
- Se över säkerheten för behandlade personuppgifter
  - Ta fram rutiner för incidentrapportering
  - Inbyggt dataskydd och dataskydd som standard

# Förberedelser för GDPR - Checklista

- Det räcker inte bara att göra rätt utan ni ska kunna visa att ni gör rätt!
- Utarbeta lämpliga strategier för dataskydd
- Följ utvecklingen (nationell lagstiftning)
- Tänk på att skyddet för personuppgifter inte bara är en grundläggande rättighet utan även en fråga om de registrerades förtroende
- Att inte förbereda sig för dataskyddsförordningen kan bli dyrt





## Förberedelser inför EU:s dataskyddsförordning

### Vägledning till personuppgiftsansvariga

Hur kan ni som hanterar personuppgifter förbereda er inför EU:s nya dataskyddsförordning?  
13 frågor att besvara redan idag



Dataskyddens

## Förberedelser inför den nya dataskyddsförordningen 2018



## Vägledning för personuppgiftsbiträden

I mitten av 2018 ska den nya dataskyddsförordningen börja tillämpas. Dataskyddsförordningen kommer att gälla som lag i Sverige och ersätta personuppgiftslagen. Syftet med förordningen är att skapa enhetliga dataskyddsregler inom hela EU vilket underlättar för företag att verka på hela unionens inre marknad. Dataskyddsförordningen kommer att medföra stora förändringar för de som behandlar personuppgifter.

Dataskyddens har tidigare tagit fram en vägledning för hur **personuppgiftsansvariga** redan idag ska kunna förbereda sig inför de nya reglerna. Vägledningen hittar du på vår webbplats: [www.dataskyddens.se/dataskydd-pua](http://www.dataskyddens.se/dataskydd-pua)

Dataskyddsförordningen kommer dessutom att medföra stora förändringar för er som behandlar personuppgifter för annans räkning. Den här informationen riktar sig därför särskilt till er som är **personuppgiftsbiträden**.

### Samma definition men en förändrad roll

Den som behandlar personuppgifter för den personuppgiftsansvariges räkning kommer, i likhet med vad som gäller idag, att vara personuppgiftsbiträde. I den nya dataskyddsförordningen förändras dock denna roll. Personuppgiftsbiträdet kommer att få nya skyldigheter och ett betydligt utökat eget ansvar för personuppgiftsbehandlingen. I ett flertal situationer kommer även personuppgiftsbiträden att omfattas av samma skyldigheter som gäller för personuppgiftsansvariga.

Juni 2016



# www.datainspektionen.se

The screenshot shows the homepage of the Swedish Data Inspection Board (Datainspektionen). At the top left is the logo, a stylized '@' symbol. To its right are navigation links: KONTAKTA OSS, WEBBKARTA, ORDLISTA, LÄTTLÄST, and OTHER LANGUAGES. Below these is a search bar labeled 'SÖK PÅ WEBBPLATSEN' with a 'Sök' button. A dark red navigation bar contains the following menu items: START, OM OSS, FRÅGOR & SVAR, LAGAR & REGLER, PERSONUPPGIFTSOMBUD, UTBILDNING, and PRESS.

The main content area features a large article titled 'Brister i polisens fingeravtrycksregister' with a sub-headline '1 december Datainspektionen har granskat hur polisen gallrar uppgifter i sitt fingeravtrycksregister och har funnit flera brister.' To the right of the article is a photograph of a group of people. Below the main article are two smaller news items: '30 november Datainspektionen ska informera företag om dataskyddsförordningen' and '28 november Datainspektionen granskar kameraövervakning på hotell'. A search box with the text 'Vad letar du efter?' and a 'Sök' button is located below these items. To the right of the search box is a list of categories: Kameraövervakning, Betalningsanmärkningar, Kränkningar på nätet, and Dashcams och drönare.

On the right side of the page, there is a section titled 'Personuppgiftslagen' with a sub-headline 'Personuppgiftslagen (PUL) ska skydda människor mot att deras personliga integritet kränks när personuppgifter behandlas.' Below this are links for 'Läs mer om personuppgiftslagen', 'Frågor och svar om personuppgifter', and a graphic for '2018 EU:s dataskyddsreform'. Further down is a section for 'Kreditupplysning' with links for 'Läs mer om kreditupplysning', 'Frågor och svar om kreditupplysning', and 'Inkasso'.

At the bottom of the page, there are two more sections: 'Personuppgiftsombud' with a sub-headline 'Vägledning för personuppgiftsombud' and 'Drönare och annan kameraövervakning' with a sub-headline 'Safe Harbor och Privacy Shield'.

Frågor?