Dataskyddsförordningen (GDPR)

Borlänge den 7 december 2016

Martin Brinnen

Datainspektionen

Rätten till privatliv

Datainspektionen

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

Datainspektionen

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?

Datainspektionen

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

Datainspektionen

Personuppgifts-
ansvarig

Dataskydds-
ombud

Personuppgifts-
biträde

Den registrerade

Datainspektionen

När gäller förordningen?

Datainspektionen

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

Datainspektionen

Artikel 2, skäl 15 + Artikel 3, skäl 22-25

När gäller inte förordningen?

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

Datainspektionen

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

Grundläggande principer för behandlingen

Datainspektionen

Principer

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

- **Ansvarsskyldighet**

Datainspektionen

Artikel 5, skäl 39, artikel 6.4, skäl 50

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

Datainspektionen

Hur kan vi visa att vi följer förordningen?

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

Datainspektionen

Artikel 5, 24, 30, 40-42

Rättslig grund för behandlingen

Datainspektionen

Rättslig grund för behandlingen

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

Datainspektionen

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

Datainspektionen

Artikel 7, skäl 42-43, Artikel 8

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

Datainspektionen

Artikel 9, skäl 10 och 51, Artikel 10, Artikel 87

Registrerades rättigheter

Datainspektionen

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

Datainspektionen

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

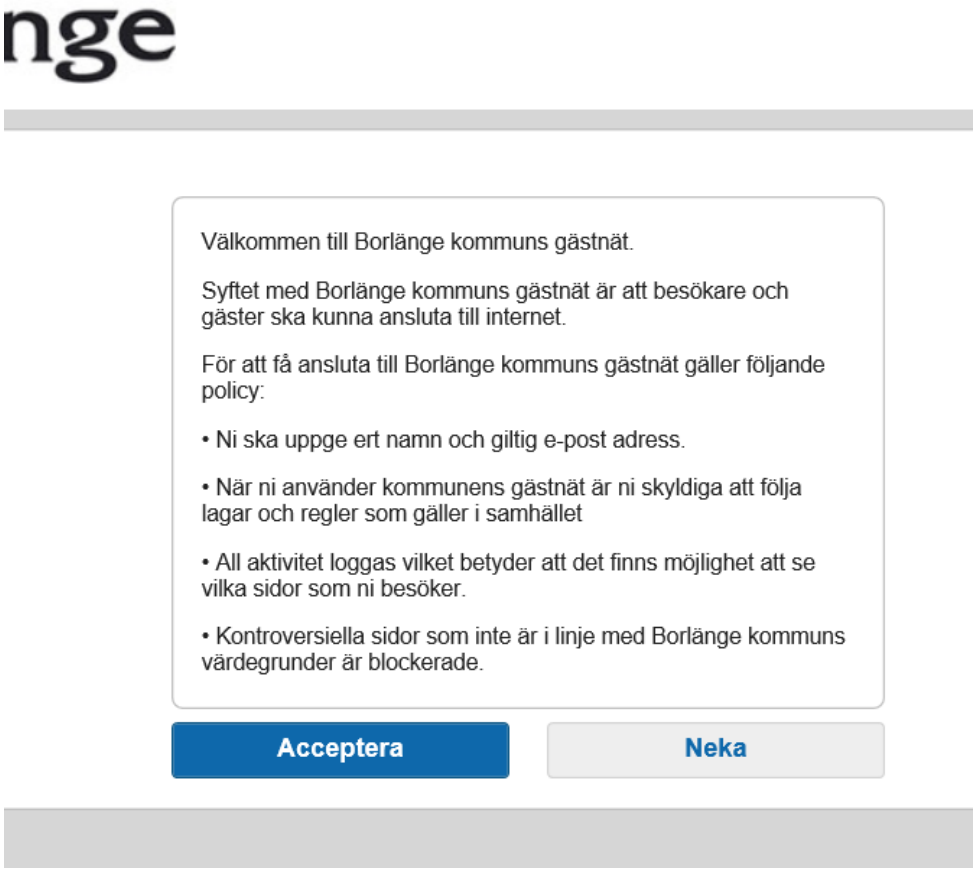
Datainspektionen

Artikel 12, skäl 58-62

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
Rättslig grund	Ja	Ja	Nej	Nej
Kategorier av personuppgifter	Nej	Ja	Ja	Ja
Intresse vid intresseavvägning	Ja	Ja	Nej	Nej
Mottagarna	Ja	Ja	Ja	Ja
Tredjelandsöverföring 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.



Datainspektionen

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

Datainspektionen

Artikel 17 och 19, skäl 65-66

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

Datainspektionen

Artikel 20, skäl 68

Skyldigheter för den som behandlar personuppgifter

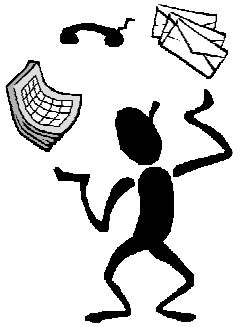
Datainspektionen

Skyldigheter för personuppgiftsansvariga

- Ta, och visa, ansvar (ansvarsskyldighet)

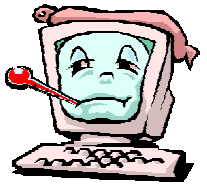
- Inbyggt dataskydd och dataskydd som standard
- Register över behandlingar
- Säkerhet
- Anmälan av personuppgiftsincidenter
- Konsekvensbedömningar och förhandssamråd

- Utse dataskyddsombud
- Anlita personuppgiftsbiträde



Datainspektionen

Anmälan av personuppgiftsincidenter



- Personuppgiftincidenter som innebär risker för enskildas rättigheter och friheter…
- …ska anmälas till Datainspektionen inom 72 timmar
- Personuppgiftsbiträde ska anmäla till personuppgifts-ansvarig
- Alla dataskyddsincidenter ska dokumenteras
- Vid hög risk ska, i vissa fall, även registrerade informeras

Datainspektionen

Konsekvensbedömningar

- Behandling som kan misstänkas innebära hög risk ska en konsekvensutredning genomföras

- Om hög risk krävs samråd med Datainspektionen

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

Datainspektionen

Artikel 28, 30, 32 och 33

Dataskyddsombudets uppgifter

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

Datainspektionen

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

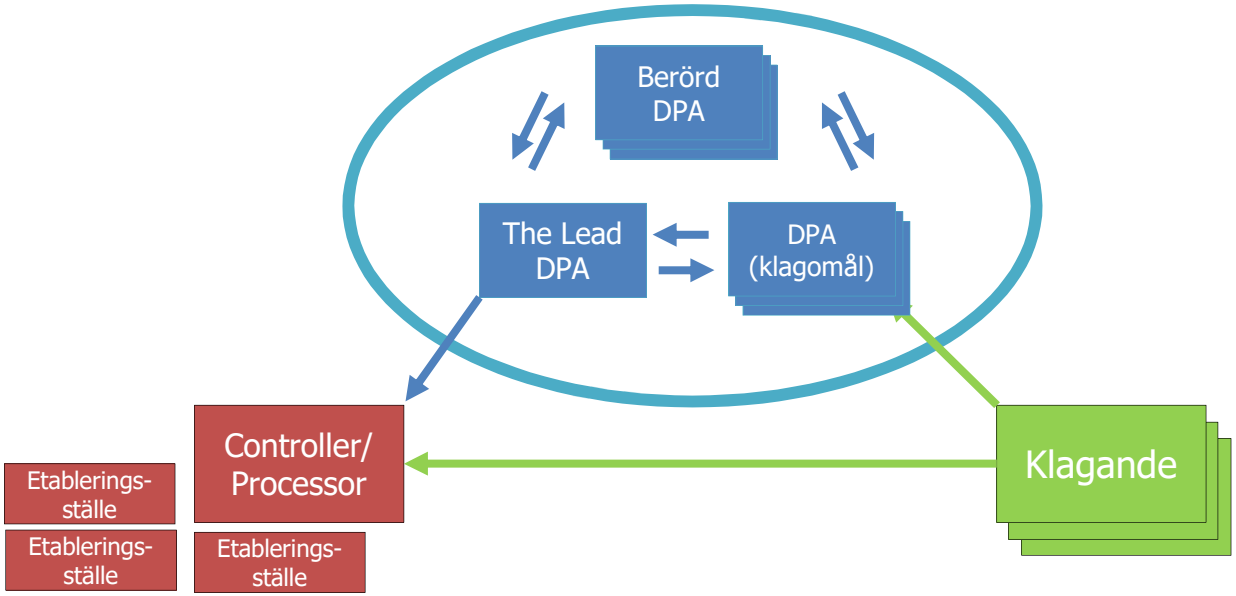
Datainspektionen

Artikel 77, 78, 82 , 83, 84

Gränsöverskridande behandling av personuppgifter inom EU

Datainspektionen

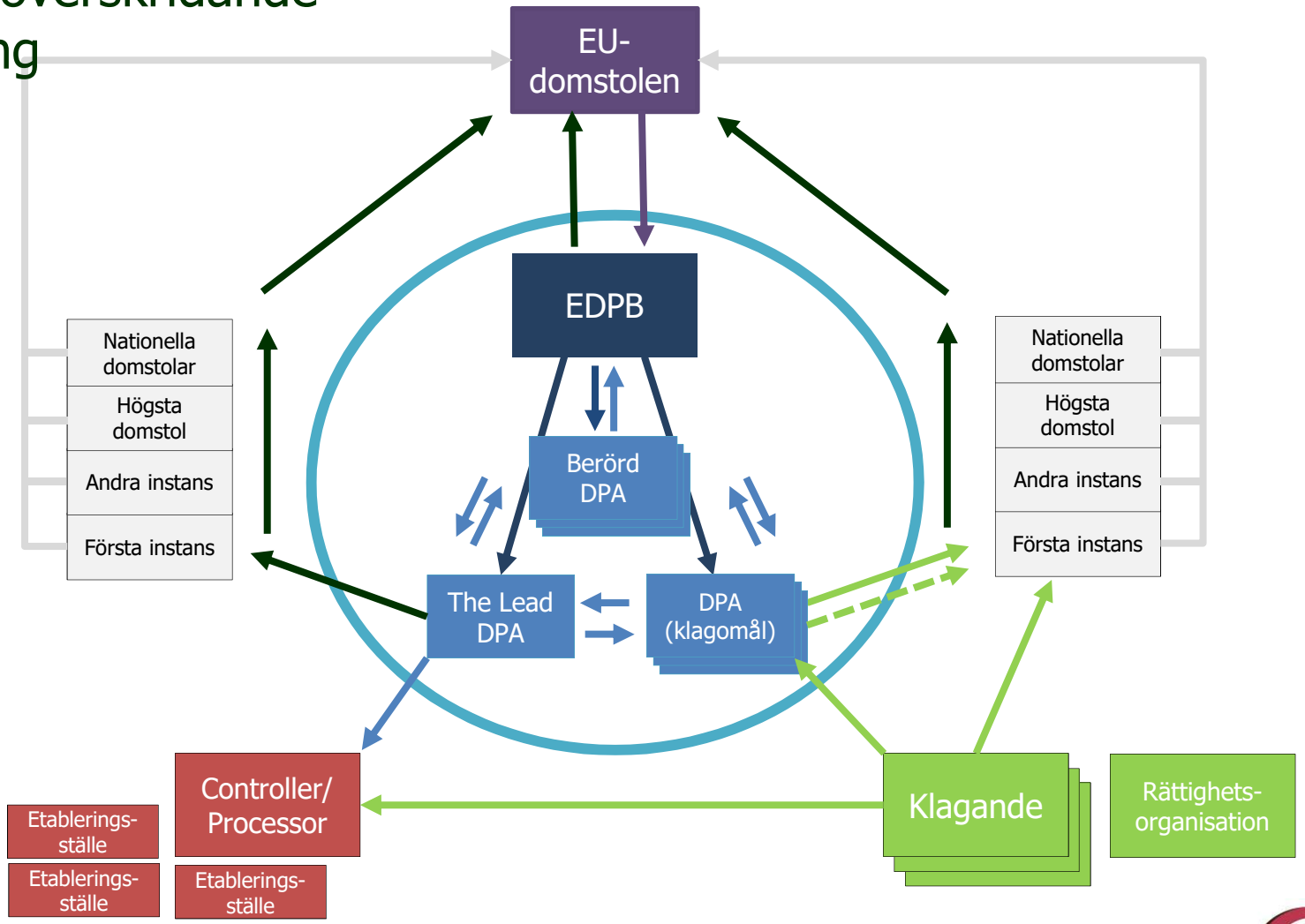
One-stop-shop
vid gränsöverskridande behandling



DPA = Data Protection Authority
EDPB = European Data Protection Board

Datainspektionen

Överklaganden
vid gränsöverskridande behandling



DPA = Data Protection Authority
EDPB = European Data Protection Board

Datainspektionen

Förbered er

Datainspektionen

EU:s dataskyddsförordning

25 maj 2018

533 dagar kvar

Datainspektionen

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”)

Datainspektionen

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

Datainspektionen

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

Datainspektionen

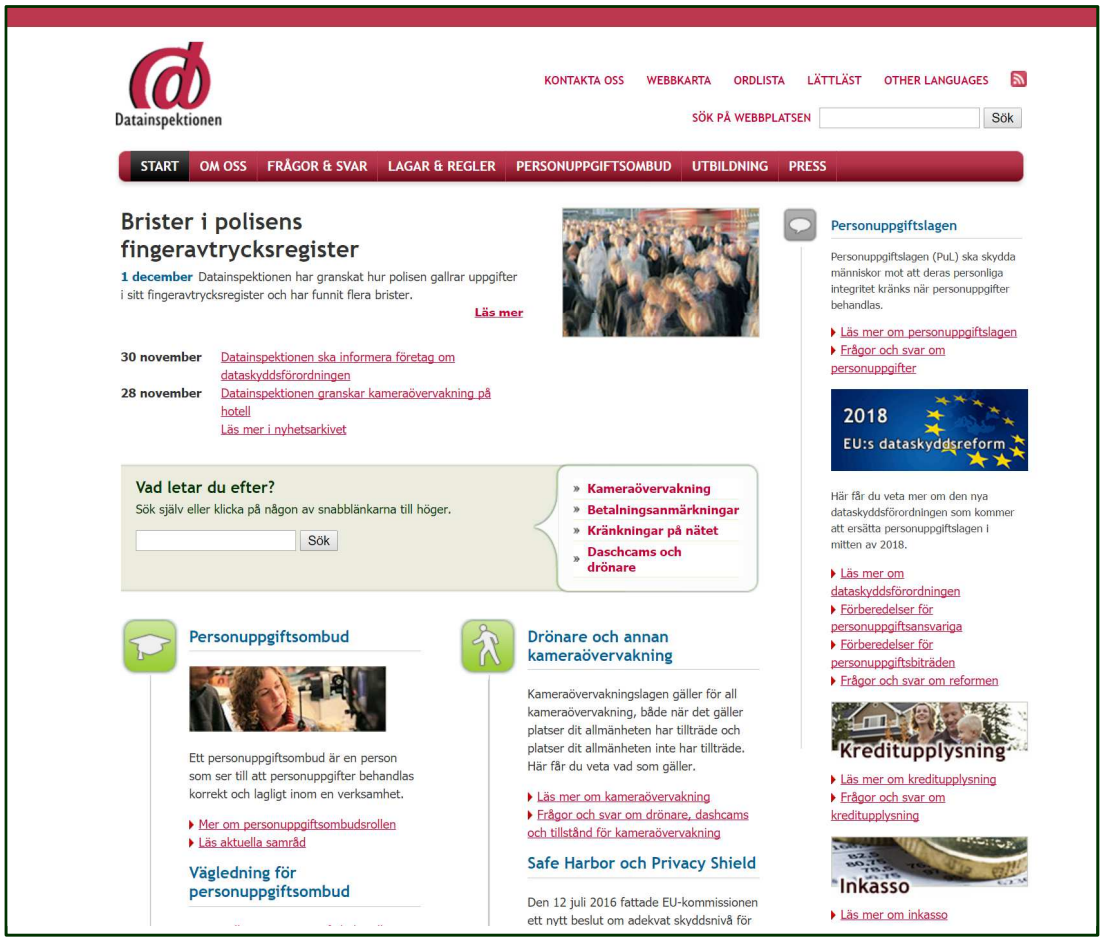
Förberedelser för GDPR - Checklista

- 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

Datainspektionen

Datainspektionen

www.datainspektionen.se



Datainspektionen

Frågor?

Datainspektionen