



 **NU** är det dags för GDPR (25 maj 2018)

Dataskyddsförordningen 25 maj



Dataskyddslag
25 maj

Färdtjänst-
/riksfärdtjänst lag



Arkivlag
Förvaltningslag
Offentlighets- och
sekretesslag

Annan lagstiftning inom
verksamheten



Ex på nationella bestämmelser

Centrala roller

- ❖ **Dataskyddsbud** – Ska vara kunnig och informera vilka skyldigheter som gäller för hantering av personuppgifter samt bevaka att reglerna följs.
Är kontaktperson mot Datainspektionen.
- ❖ **Personuppgiftsansvarig** – den som behandlar personuppgifter i sin verksamhet, nämnden/styrelsen för verksamheten.
- ❖ **Personuppgiftsbiträde** – behandlar uppgifterna verksamhetens räkning (t ex leverantörer av, IT-tjänster eller fotografer som har tillgång till personuppgifter).

Om Dataskyddsbudet citerat från Datainspektionen:

”Ombudets roll är att kontrollera att dataskyddsförordningen (GDPR) följs inom organisationen genom att till exempel utföra kontroller och informationsinsatser.”



Aktuella lagrum handläggning Ftj/Rftj



- **Dataskyddsförordningen (GDPR) Artikel 6 e**
Förordning innehåller regler för hur personuppgifter får hanteras och vilka rättigheter den enskilde har.
- **Förordningen kompletteras med våra nationella lagar**
 - **Dataskyddslagen** (Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning) - reglerar myndigheters arbete med personuppgifter samt Förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning
 - **Lag (1997:736) om Färdtjänst** och **lag (1997:735) om Riksfärdtjänst** - utgör grunden för rätten till Ftj/Rftj och bestämmer villkoren för detta
 - **Förvaltningslagen** (2017:900) träder i kraft 1 juli 2018 - reglerar myndigheternas skyldighet att utreda ärenden och fatta beslut
 - **Offentlighet och sekretesslag** (2009: 400) - reglerar skyddet för olika uppgifter, vem som får ta del av dem och hur de får användas
 - **Arkivlagen** (1990:782) - reglerar hur handlingar från myndigheter ska hanteras när de inte längre är aktuella.

Lag med kompletterande bestämmelser till EU:s dataskyddsförordning (2018:218)

- 2 kap. Rättslig grund för behandling av personuppgifter Rättslig förpliktelse
 - 1 § Personuppgifter får behandlas med stöd av artikel 6.1 c i EU:s dataskyddsförordning, om behandlingen är nödvändig för att den personuppgiftsansvarige **ska kunna fullgöra en rättslig förpliktelse som följer av lag eller annan författning**, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning
- Uppgift av allmänt intresse och myndighetsutövning
 - 2 § Personuppgifter får behandlas med stöd av artikel 6.1 e i EU:s dataskyddsförordning, om behandlingen är nödvändig
 - 1. för att utföra en uppgift av allmänt intresse som följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning, eller
 - 2. som ett **led i den personuppgiftsansvariges myndighetsutövning enligt lag eller annan författning**.

Allmänna villkor för påförande av administrativa sanktionsavgifter – artikel 83

- Böter

- ✓ upp till 10 miljoner euro eller 2 % av globala årsomsättningen (beroende på vad som är högst) bl.a. om

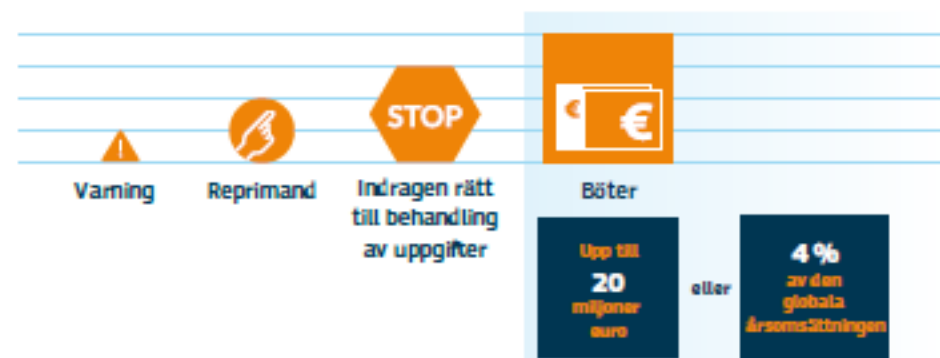
- inget dataskyddsombud
- ingen registerförteckning
- ingen konsekvensbedömning

- ✓ upp till 20 miljoner euro eller 4 % av globala årsomsättningen (beroende på vad som är högst) bl.a. om

- behandlar personuppgifter fast det inte är tillåtet
- man behandlar särskilda kategorier av personuppgifter fast man inte får
- inte lämnar information som krävs

Kostnaden om du inte följer reglerna

Din lokala dataskyddsmyndighet övervakar efterlevnaden; deras arbete samordnas på EU-nivå. Kostnaden för att inte följa reglerna naturligtvis kan bli hög.



Dataskyddslag (Sverige) Avgiften blir högst fem miljoner kronor vid mindre allvarliga överträdelser och högst tio miljoner kronor vid de allvarligare överträdelser som avses i artikel 83.5 och 83.6 i GDPR

Vanliga grunder för myndigheter

För att behandlingen av personuppgifterna ska vara laglig måste det finnas en **rättslig grund**. Myndigheter använder främst de rättsliga grunderna

- rättslig förpliktelse
- uppgift av allmänt intresse eller myndighetsutövning
- avtal

Myndigheter har **begränsade möjligheter** att använda sig av:

- samtycke
- intresseavvägninghär

Mer information hittar du [här](#)

Klar och tydlig information och kommunikation samt klara och tydliga villkor för utövandet av den registrerades rättigheter – artikel 12

- All information ska vara begriplig och lämnas i en lätt tillgänglig form
 - ✓ ett klart och tydligt språk
 - ✓ skriftligt
 - ✓ elektroniskt
 - ✓ även muntligt (identitetskontroll krävs)
 - ✓ vid begäran om åtgärd (utdrag, rättelse, radering, begränsning, portabilitet, invändningar) ska information lämnas inom en månad

Information som ska tillhandahållas om personuppgifterna samlas in från den registrerade – artikel 13

- När uppgifterna erhålls ska information lämnas till den registrerade om bl.a.:
 - ✓ vem som är personuppgiftsansvarig och ev. dataskyddsombud
 - ✓ syftet med och den rättsliga grunden för behandlingen
 - ✓ eventuella mottagare av uppgifterna
 - ✓ överföring till tredjeland
 - ✓ lagringsperioden och kriterier för fastställande av perioden
 - ✓ rätt till registerutdrag, rättelse, radering, begränsning, uppgiftsportabilitet och att invända mot behandlingen
 - ✓ rätt att återkalla samtycke
 - ✓ att man kan ge in klagomål till tillsynsmyndigheten
 - ✓ varifrån uppgifterna kommer
 - ✓ förekomst av profilering (bl.a. förutsedda följder)
- Behöver ej informera i den mån den registrerade redan förfogar över informationen

Register över behandlingar – artikel 30

- **Personuppgiftsansvarig** och eventuella företrädare ska föra ett register över behandlingar av personuppgifter
- Följande uppgifter ska dokumenteras
 - a) namn och kontaktuppgifter för personuppgiftsansvarig, ev. företrädare och ev. dataskyddsombud
 - b) ändamålen med behandlingen
 - c) kategorier av registrerade och kategorier av personuppgifter
 - d) kategorier av mottagare
 - e) ev. överföring till tredjeland
 - f) tidsfrist för radering (om möjligt)
 - g) tekniska och organisatoriska säkerhetsåtgärder

Enkla grunder i dataskydd

Den 25 maj 2018 får Sverige och övriga EU en ny gemensam lagstiftning som reglerar hur bland annat företag får behandla personuppgifter. En nyhet i denna dataskyddsförordning är kännbara sanktionsavgifter om man bryter mot reglerna, något som har fått många företag att fundera över hur de hanterar och skyddar personuppgifter. Här följer en grundkurs i dataskydd med fokus på mindre företag.



Klicka på bilden så kommer du
direkt till aktuell websida,



Checklista för hemmaplan

- Uppdatera alla blanketter och hemsidor dvs. ta bort info om PuL
- Komplettera ansökningsblanketter och hemsida med information om vilka uppgifter som hanteras mm
- Ha koll på vem som utsetts till Dataskyddsombud (DSO)
- Inventera era register dvs. verksamhetsprogram, filer etc.
- När det är aktuellt biträdesavtal

Frågor?



Konsult, Dataskyddsombud mm

- Anders Göranson
- AnGöra AB
- Anders.goranson@angoraab.se

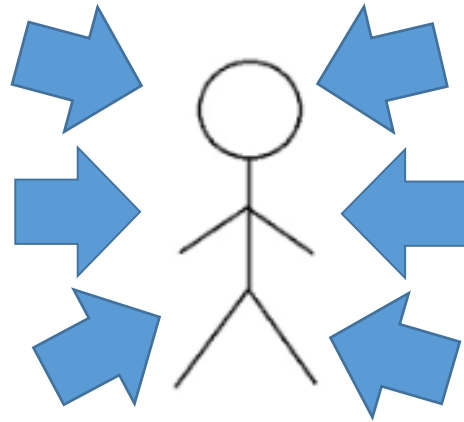
Några exempel på definitioner - artikel 4

Personuppgifter, vad avses?

Personuppgift:

Är en uppgift som direkt eller indirekt kan användas för att identifiera en person som är i livet.

- För- och efternamn
- Personnummer
- Smeknamn
- Adress
- Fastighetsbeteckning
- Bild
- Film, ljudupptagning
- Etc.



Särskilda personuppgifter:

Kallas ofta "känslig" personuppgift. Kännetecknas av information som visar på:

- Ras eller etniskt ursprung
- Politiska åsikter
- Religiös eller filosofisk övertygelse
- Medlemskap i fackförening
- Hälsa eller sjukdom
- Sexualliv eller sexuell läggning
- Genetisk eller biometrisk information

- **Behandling** – **ungefär som idag**
- **Begränsning av behandling**
 - ✓ markering av lagrade personuppgifter med syftet att begränsa behandlingen av dessa i framtiden
- **Profilering** – **nytt**
- **Pseudonymisering** – **nytt**
- **Personuppgiftsansvarig**
- **Personuppgiftsbiträde**
- **Mottagare** – den till vilken uppgifter lämnas ut

- **Personuppgiftsincident – nytt**
 - en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.
- **Genetiska uppgifter – nytt**
 - ✓ som rör genetiska kännetecken
- **Biometrisk uppgifter – nytt**
 - ✓ fysiska , fysiologiska eller beteendemässiga kännetecken t.ex. fingeravtryck och ansiktsbilder
- **Uppgifter om hälsa – nytt**
 - ✓ även uppgifter om tillhandahållande av hälsovård
- **Informationssamhällets tjänster**
 - tjänster som vanligtvis utförs mot ersättning på distans, på elektronisk väg och på individuell begäran av en tjänstemottagare



Principer om behandling av personuppgifter – artikel 5

- Motsvarar 9 § PuL – **inga större förändringar**
 - ✓ a) **laglighet, korrekthet och öppenhet**
 - ✓ b) **ändamålsbegränsning** (särskilda, uttryckligt angivna och berättigade ändamål, ej behandla för oförenliga ändamål)
 - ✓ c) **uppgiftsminimering** (adekvata, relevanta, ej för många)
 - ✓ d) **korrekthet** (korrekta, uppdaterade, rättas utan dröjsmål)
 - ✓ e) **lagringsminimering** (ej spara längre än nödvändigt)
 - ✓ f) **integritet och konfidentialitet** (uppgifterna ska skyddas mot obehörig eller otillåten behandling m.m.)
 - ✓ **Ansvarsskyldighet** (den personuppgiftsansvarige ska kunna ansvara för och kunna visa att punkterna ovan efterlevs)

Registerhantering

- Skyldiga att föra register över behandling av personuppgifter som lagras digitalt men även utskrivna ex i pärm.
- Kan gälla olika datasystem, Exel-listor, samtycken, avtal m fotografer, e-postlistor mm.
- Ska innehålla bland annat:
 - Ändamål med behandlingen
 - Beskrivning av kategorier av registrerade
 - Om uppgifterna skickas vidare
 - Om uppgifterna förs över till tredje land



Laglig behandling av personuppgifter – artikel 6

- Motsvarar 10 § PuL
 - a) samtycke, eller nödvändig behandling för
 - b) fullgöra avtal
 - c) **rättslig förpliktelse för den personuppgiftsansvarige**
 - d) skydda intressen som är av grundläggande betydelse för den registrerade (tidigare vitala intressen)
 - e) arbetsuppgift av allmänt intresse eller **led i myndighetsutövning**
 - f) intresseavvägning
- Lagstiftaren får precisera tillämpningen

Villkor för samtycke – artikel 7

- I princip allt som görs inom färdtjänst- och riksfärdtjänstområdet sker med stöd av **rättslig förpliktelse för den personuppgiftsansvarige eller myndighetsutövning**
- Viljeyttring som ska vara
 - ✓ frivillig
 - ✓ specifik
 - ✓ informerad
 - ✓ otvetydig
- Som ges genom
 - ✓ uttalande eller
 - ✓ entydig bekräftande handling
- Personuppgiftsansvarig har bevisbördan
- Ska vara lika lätt att återkallas som att ges

Den registrerades rätt till tillgång – artikel 15 (och 12)

- "Registerutdrag" (**rätt till tillgång**)
 - ✓ ungefär samma regler som idag, **dessutom** gäller
 - ✓ möjlighet till elektroniska registerutdrag
 - ✓ art. 15.3: "Om den registrerade gör begäran i elektronisk form ska informationen tillhandahållas i ett elektroniskt format som är allmänt använt om den registrerade inte begär något annat."
 - ✓ begriplig och lättfattlig form, även muntligt efter id-koll
 - ✓ ska lämna en kopia av de uppgifter som håller på att behandlas
 - ✓ **gratis** (för ytterligare kopior får man ta ut en administrativ avgift – om begäran är oskälig p.g.a. dess repetitiva karaktär art. 12.5)

Exempel på tuffare krav för de personuppgiftsansvariga

- ❖ Rapportering av personuppgiftsincidenter
- ❖ Registerförteckningar
- ❖ Konsekvensbedömning
- ❖ Utnämning av dataskyddsombud (tidigare lika med personuppgiftsombud men nu större ansvar)
- ❖ Sanktioner

Utnämning av dataskyddsombudet – artikel 37

- Gäller både för personuppgiftsansvariga och personuppgiftsbiträden
- **Dataskyddsombud är obligatoriskt om:**
 - ✓ myndighet eller offentligt organ behandlar personuppgifter eller om
 - ✓ den personuppgiftsansvariges eller personuppgiftsbiträdets kärnverksamhet kräver regelbunden och systematisk övervakning av enskilda i stor omfattning eller om
 - ✓ den personuppgiftsansvariges eller personuppgiftsbiträdets kärnverksamhet består av behandling i stor omfattning av särskilda kategorier av uppgifter eller personuppgifter som rör fällande domar i brottmål och överträdelser

Dataskyddsbudets uppgifter – artikel 39

- Dataskyddsbudet ska ha åtminstone följande uppgifter
 - ✓ informera och ge råd till den personuppgiftsansvarige, personuppgiftsbiträdet och anställda som behandlar personuppgifter
 - ✓ övervaka efterlevnaden av förordningen, inbegripet bl.a. ansvarstilldelning och utbildning av personal som deltar i behandling av personuppgifter
 - ✓ ge råd vad gäller konsekvensbedömning
 - ✓ samarbeta med och vara kontaktpunkt för tillsynsmyndigheten