GÄRDE & PARTNERS

SUSEC:s HÖSTMÖTE oktober 2017

- Några juridiska reflektioner kring

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (GDPR)
- Det finns även ett svenskt lagförslag (SOU 2017:39) om anpassningar till GDPR, Dataskyddslagen (DSL)

Connys CV

1989 – Jur. kand. Stockholms Universitet
Verksjurist, Televerket Radio

1992 – Kriminologi, Stockholms Universitet

1993 – Bolagsjurist, Telia-koncernen

1997

2001 – Jur. mag. Law & IT (LLM)

2001 – Bolagsjurist, Flextronics

2004 – Bolagsjurist, TeliaSonera

2008 – Verksjurist, Kronofogdemyndigheten

2009 – Advokatfirman Gärde & Partners
Advokat 2011

(t)

28 år!

IT- rättens affärsrättsliga del
Rådgivning, granskning, tolkning, utformning, förhandling avseende olika slags IT-avtal, upphovsrätt m.m., tvistelösning, rättegång, kurser & utbildning

1997 – 2009 Bisyssla
Juristfirman Conny Larsson

IT- rättens övriga del
Rådgivning/förhandling vid incidenter & utredningar, infohantering, säkerhet, sekretess & tystnadsplikt, IT-brott, rättegång, kurser & utbildning

OCH – styrelseledamot i Svenska Föreningen för IT & Juridik (f.d. ADBJ) och adjungerad i SIG Security

INLEDNING

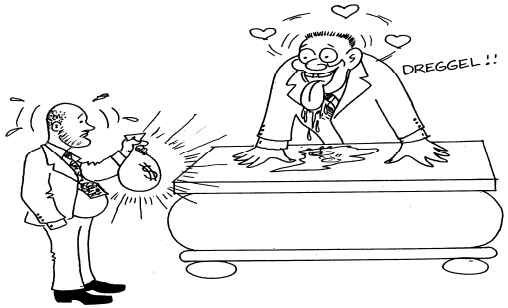
GDPR - Är den endast jämmer & elände eller kan den vara till nytta också?

GDPR – Hot eller möjlighet?

– **+**

RISKER!

- Tillsyn
- Förbud
- Förelägganden
- Vite
- Sanktionsavgift (advokatens favorit)
- Skadestånd
- Bad-will – dålig pressinfo
- Janne Josefsson och UG
- Annat elände …



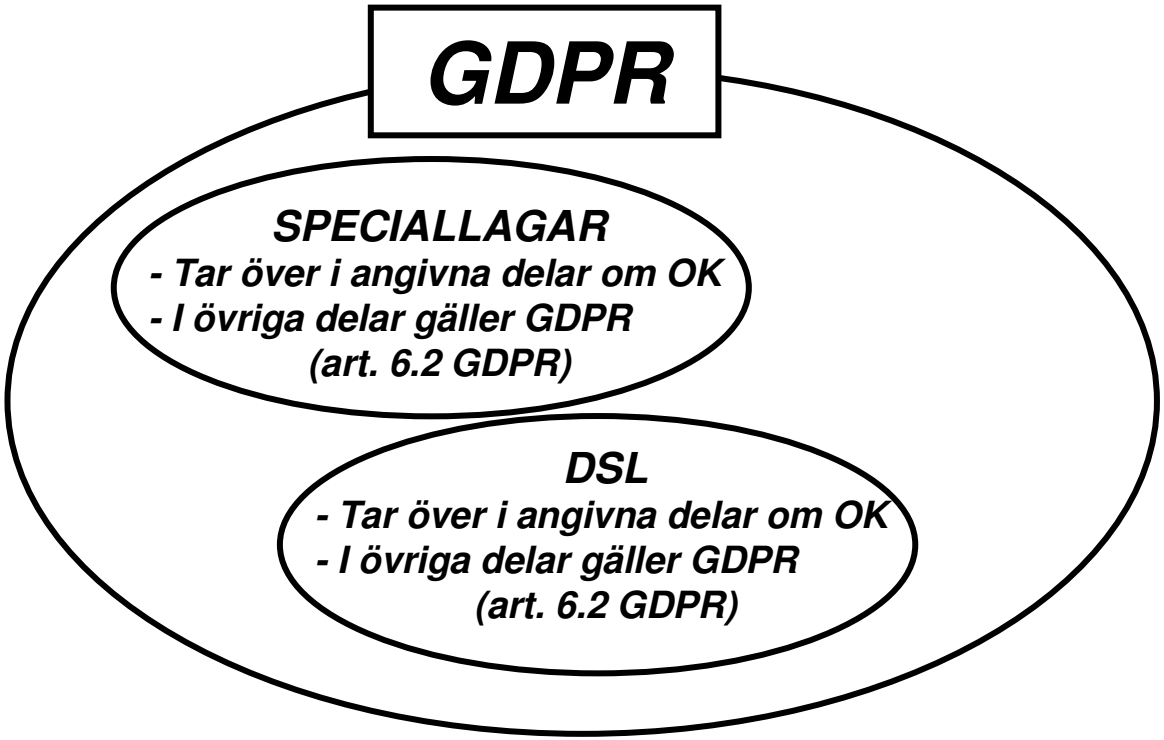
MÖJLIGHETER!

- Undanröja/minska riskerna
- Få kontroll på hanteringen
- Ordning & reda
- Skydd & säkerhet
- Inte bara personuppgifter
- Minska kostnader
- Good-will – bra pressinfo
- Säljargument – ökade intäkter
- Andra godsaker …

TILLÄMPLIGHET

- **VAD GÄLLER GDPR?**
- **VAR GÄLLER GDPR?**
- **NÄR GÄLLER GDPR?**

VAD gäller GDPR?



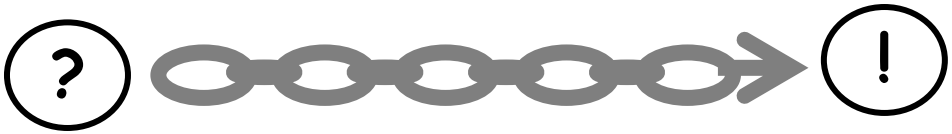
MEN INTE:

- ***Nationell säkerhet!***
- ***Brottsbekämpning!***
- ***EU:s arbetsuppgifter!***
- ***Tryckfrihet & yttrandefrihet***
- ***Privat behandling***
  - *Ej privat på Internet…*

Personuppgifter!

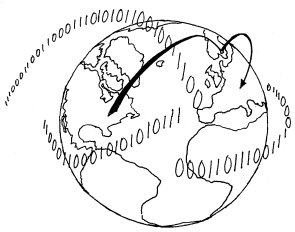
Personuppgift = ***All*** slags information som ***direkt/indirekt*** kan hänföras till en fysisk levande person

- Även om kedjan är lång… (Art. 4 GDPR)



- Krypterade uppgifter, om de kan göras läsbara
- Anonyma uppgifter som kan identifieras ”bakvägen”, såsom
  - Telefonnummer mm, där enskilda personer finns registrerade som ägare, abonnenter etc. (jfr dock LR Ö 14897-97)
- Enskild firma (registreras på personen/personnr)
- IP-adress (RegR mål nr 3978-07 – fastställde KR i Stockholms dom i mål nr 285-07, Antipiratbyrån)

VAR gäller GDPR?



Stor risk/chans att PuA/PuB anses vara inom EU/EES

1. Personuppgiftsansvarig/personuppgiftsbiträde inom EU/EES

- Etablerad inom EU/EES (verksamhetsställe här)
- Faktiska/reella utförandet av verksamheten här
- Oberoende av vem uppgiften gäller

2. Personuppgiftsansvarig/personuppgiftsbiträde utanför EU/EES och det gäller

a) utbjudande av varor eller tjänster till personer inom EU/EES
- språk, valuta, omnämnande m.m

b) övervakning/profilering av sådana personer
- spårning och teknisk kartläggning

3. Behandlingen sker på ett ställe där EU/EES-medlems nationella rätt gäller enligt folkrätten

- Ambassad, konsulat, fartyg m.m.

(Art.4, skäl 22-25)

NÄR gäller GDPR?

25 maj 2018
GDPR börjar tillämpas
(Art. 99 GDPR)

BEHANDLING AVSLUTAD
INNAN 25 MAJ 2018
- PuL gäller!
- Inte GDPR!

BEHANDLING PÅBÖRJAD
INNAN 25 MAJ 2018 OCH
FORTSÄTTER DÄREFTER
- GDPR gäller!
- Inte PuL!

BEHANDLING PÅBÖRJAD
EFTER 25 MAJ 2018
- GDPR gäller!
- Inte PuL!

NU – Lite eftertanke . . .

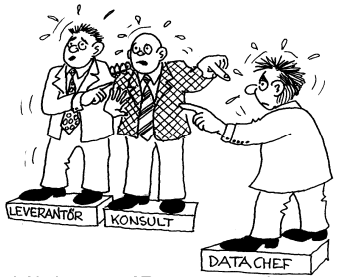
Skulle registreringsnumret på en personbil kunna vara en personuppgift?
Är det någon skillnad om det är fråga om en förmånsbil eller hyrbil?
(Några minuters individuell eftertanke och efterföljande diskussion)

ÅTGÄRDER

1) **FÖRBEREDELSE – Utse ansvarig + lägg upp en plan!**
2) **INVENTERING – Vilken info behandlar vi?**
3) **KONSEKVENSBEDÖMNING – Gör en SBA!**
4) **ÅTGÄRDANDET – Rätta till fel & brister!**
5) **UPPFÖLJNINGEN – Kolla hur bra vi lyckats! (Se'n börjar allt egentligen om igen…)**

FÖRBEREDELSEN – Utse ansvarig!

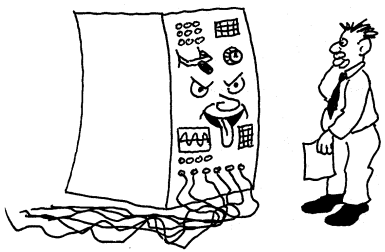
VILKA ROLLER HAR VI FÖR VÅR INFORMATIONSHANTERING?	
Roll?	**Ansvar?**
Systemägare	Internt definierat ……..?
Systemansvarig	Internt definierat ……..?
Systemförvaltare	Internt definierat ……..?
Informationsägare	Internt definierat ……..?
Informationsansvarig	Internt definierat ……..?
Informationsförvaltare	Internt definierat ……..?
Personuppgiftsansvarig	Legalt definierat! – Den som ensam eller tillsammans med andra bestämmer över behandlingen! **= *VI KOMMER INTE UNDAN!!!***



En vanlig mänsklig egenskap:
- ANSVAR är något vi vill ska finnas hos någon annan!

INVENTERA – Vad behandlar vi?

PÅGÅENDE BEHANDLINGAR AV PERSONUPPGIFTER			
System, tjänst, annat	**Personuppgiftsslag**	**Ändamål & laglig grund**	**Ansvarig**
Personal- och löneregister	Namn, adress, personnummer, kontaktuppgifter, fackligt medlemskap, hälsa & sjukdom	Uppfylla anställnings-avtal, utöva rättigheter & skyldigheter	Personal/HR-avdelningen
Telefoni-, e-post passagekoll	Anslutningsuppgifter (tfnnr, IP-adress mm)	Kommunikation, användning och tillträde	IT-avdelningen
Kundregister	Kundinfo (privatpersoner & företag mm)	Uppfylla & adm. avtal	Marknads- & sälj-avdelningen
Leverantörer	Leverantörsinfo (företag mm)	Uppfylla & adm. avtal	Inköpsavdelningen
Annat ….. ?	…….	…….	…….



GÖR ETT REGISTER!
- Ska finnas tillgängligT t.ex. vid tillsyn!
- Ta kontroll över vilka som får anskaffa!
(Art. 30 GDPR)

Känslig personuppgift?

”KÄNSLIG” PERSONUPPGIFT!

- ras & etniskt ursprung
- politiska åsikter
- religiös eller filosofisk övertygelse
- medlemskap i fackförening!!!
- hälsa & sexualliv
- genetiska/biometriska uppgifter

(Art. 9 GDPR)

- Även uppgifter om brott och lagöverträdelser

(Art. 10 GDPR)

- Även personnummer

(Art. 87 GDPR)

UNDVIK sådana uppgifter om ni inte absolut måste ha dem!

551332-0055

Interna ”brottsregister”?

Uppgift om brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden

- Får endast behandlas av ***myndigheter***!
- Regeringen eller DI kan meddela ytterligare undantag
  - T.ex. Antipiratbyrån (numera Rättighetsalliansen), enligt beslut av DI
  - Oftast med starkt inskränkande villkor
  - Ibland tidsbegränsade och måste återkommande omprövas

Utesluter inte att arbetsgivare i samband med incidentutredning behandlar personuppgift som behövs för utredningen och för anspråk mot personen.

- Måste vara tillfälligt och begränsas:
  - Åtkomligt för särskilt behöriga (några få)!
  - Pågå bara tills ärendet är klart!
  - Uppgifterna ska bort därefter!

INTE LÄGGA UPP EGNA KRIMINALREGISTER!!!

KONSEKVENSBEDÖMNING – Gör!

VILKA TÄNKBARA HOT FINNS? (Hotlista)	***HUR STOR ÄR RISKEN (. . .%)?***	***VAD KAN SKADAN BLI (Konsekvensen)***	***RISKVÄRDE (sannolikheten x skadan)***
1) Externa intrång			
2) Interna läckor			
3) Intern obehörig användning			
4) Tekniska fel/ brister (buggar)			
5) Avbrott			
6) Oönskad förändring/radering mm			
7) Virusangrepp/annan skadlig kod			
8) Spioneri/företagsspioneri			
9) Oönskat utlämnande enligt lag			
10)			

DOKUMENTERA!
- Ska finnas tillgänglig t.ex. vid tillsyn!
- Ta kontroll över vilka som får anskaffa!
(Art. 35 GDPR)

ÅTGÄRDANDET

1) **ÄNDAMÅL – Ange *varför* vi behandlar personuppgifterna!**
2) **LAGLIG GRUND – Ange vilken *laglig grund* i GDPR som behandlingen avser!**
3) **SÄKERHETEN – ”Lämpliga” åtgärder!**
4) **ÅTGÄRDANDET – Kolla överensstämmelse med GDPR + rätta till fel & brister!**
5) **UPPFÖLJNINGEN – Kolla hur bra vi lyckats! (Se’n börjar allt egentligen om igen…)**

ÄNDAMÅL för behandlingen!

ÄNDAMÅL / PRINCIPER	
(9 § PuL)	(art. 5 GDPR)
1. Lagligt! **2. Korrekt och enligt god sed!** - DI och branschpraxis avgör vad som är ”god sed” **3. Bestämt ändamål!** - särskilda, uttryckligt angivna och berättigade **4. Följ ändamålet!** **5. Endast adekvata och relevanta** uppgifter! **6. Inte fler uppgifter än nödvändigt** mht ändamålet! **7. Riktiga och aktuella** uppgifter! **8. Åtgärda** felaktiga och ofullständiga uppgifter! **9. Spara inga uppgifter längre än nödvändigt** mht ändamålet!	**a) Laglighet, korrekthet och öppenhet** – gentemot den registrerade **b) Ändamålsbegränsning** – särskilda, uttryckligt angivna och berättigade ändamål + inte senare behandlas på oförenligt sätt därmed **c) Uppgiftsminimering** – adekvata, relevanta och inte alltför omfattande **d) Korrekthet** – uppgifterna ska vara korrekta och vid behov uppdaterade + raderas/rättas om de är felaktiga **e) Lagringsminimering** – Inte förvara i en form som möjliggör identifiering längre än nödvändigt m h t ändamålen **f) Integritet & konfidentialitet** – Lämplig säkerhet, bl.a. skydd mot intrång och obehörig användning + förlust, förstöring, skada ***= Huvudsakligen överensstämmelse GDPR och PuL (har vi gjort rätt tidigare betr. ändamålen, gör vi det sannolikt enligt GDPR också)***

NU – Lite mer eftertanke . . .

Någon har stulit datorer och annan utrustning i våra lokaler
- Får vi använda info i vårt passagekontrollsystem för att kolla vem som varit närvarande?
- Hur kan vi motivera det utifrån PuL?
- Vad är det normala ändamålet med ett passagekontrollsystem?

(3 minuters individuell eftertanke)

LAGLIG GRUND för behandlingen!

”NORMALA” PERSONUPPGIFTER	OCH OM DET ÄVEN ÄR ”KÄNSLIGA” PERSONUPPGIFTER
(10 § PuL, art. 6.1 GDPR)	• ras & etniskt ursprung • politiska åsikter • religiös eller filosofisk övertygelse • medlemskap i fackförening!!! • hälsa & sexualliv (13 § PuL, art. 9.1 GDPR)
1. *Samtycke* (3 § PuL, art. 7 GDPR) (kan när som helst återkallas!) ***2. Nödvändigt*** a) uppfylla *avtal* b) fullgöra *rättslig skyldighet* c) skydda den *registrerades vitala intressen* d) utföra arbetsuppgift av *allmänt intresse* e) fullgörande av *myndighetsutövning* f) *intresseavvägning*	**1. S*amtycket ska <u>även</u> vara*** (kan när som helst återkallas!) a) Uttryckligt, eller genom b) tydligt offentliggörande (15 § PuL, art. 9.2 GDPR) **2. *Behandlingen <u>även</u> nödvändig för att*** (16 § PuL, art. 9.2 GDPR) a) fullgöra skyldigheter/utöva rättigheter inom arbetsrätten b) skydda vitala intressen (liv & hälsa) + samtycke kan ej inhämtas c) fastställa, göra gällande eller försvara rättsliga anspråk **3. *Särskilda undantag*** (17-20 §§ PuL, art. 9.2 GDPR) - Ideella organisationer - Hälso- & sjukvård - Forskning & statistik,

NU – Åter lite eftertanke . . .

Vad gäller om jag t.ex. anlitar en blomsterbutik för att leverera blommor till mamma när hon fyller år?

- Blomsterbutiken vill kunna fakturera mig och behöver då mitt namn eller adress

- Samtidigt vill blomsterbutiken kunna bära ut blommorna och behöver därför mammas' namn och adress

- Är det tillåtet att behandla uppgifterna???

(3 minuters individuell eftertanke)

SÄKERHETEN!

SÄKERHETEN VID BEHANDLING AV PERSONUPPGIFT

"Lämplig" säkerhetsnivå m.h.t.

1) den tekniska miljön
2) kostnaderna
3) ev. särskilda risker
4) uppgifternas känslighet

Såväl tekniska som organisatoriska åtgärder
(31 § PuL, art. 32 GDPR)

Säkerhetskraven är inte konkreta - d.v.s. svårt förutse vad som rent faktiskt krävs! - Duger t.ex. ISO 27001?

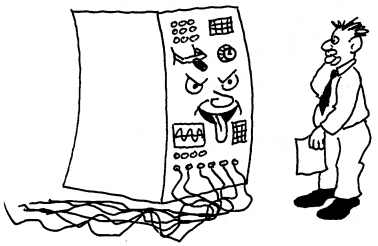
DI kan meddela säkerhetsföreskrifter enligt PuL, andra åtgärder enligt GDPR!
(32 § PuL, jfr. art. 42 GDPR (certifiering), art. 58 åtgärder mot PuA/PuB)

Dataloggar ***rekommenderas av Datainspektionen*** som exempel på säkerhetsåtgärder för att skydda personuppgifter mot otillåten behandling
(Datainspektionens Allmänna råd - Säkerhet för personuppgifter)
- Därmed har vi stöd för att det är tillåtet och t.o.m. ett krav att vi ska föra loggar

SÄRSKILT OM PuB-AVTALEN

- **VILKA EXTERNA PARTER SKÖTER VÅR INFORMATIONSHANTERING?**
- **OUTSOURCAT, MOLNTJÄNSTER?**
- **HUR SER PuB-AVTALEN UT?**
- **VAD BEHÖVER JUSTERAS FÖR ATT UPPFYLLA GDPR?**

NÄR KRÄVS PuB-AVTAL?



NÄR NÅGON ANNAN ANLITAS FÖR VÅR BEHANDLING AV PERSONUPPGIFTER!

(GDPR, art. 28.3)

Typiska situationer:

- Outsourcing av vår IT-drift
- Multisourcing av driften
- Molntjänster av olika slag

(OBS JO 2011-3032: - sekretessregler i t.ex. OSL kan betyda att vi inte kan låta någon annan (PuB) sköta vår informationshantering, om detta kan anses innebära att vi egentligen lämnar ut sekretessbelagd info till denne)

INNEHÅLLET I PuB-AVTALET

ÖVERGRIPANDE KRAV PÅ PuB-AVTALET:

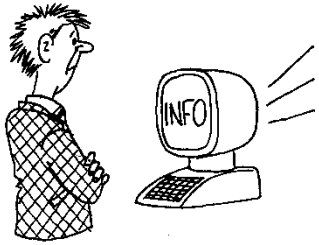
- *Personuppgifter får endast behandlas enligt **PuAs instruktioner***
- *PuB måste ålägga personalen tystnadsplikt, om de inte omfattas av tystnadsplikt enligt lag*
- *PuB **måste vidta säkerhetsåtgärder enligt art 32***
- *PuB får inte anlita annat PuB (UB) utan PuAs skriftliga OK*
- *Om PuB anlitar annat PuB ska motsvarande avtal ordnas även där*
- *PuB ska tekniskt och organisatoriskt bistå PuA att fullgöra sin infoplikt mot de registrerade*
- *PuB ska **tekniskt och organisatoriskt uppfylla säkerhetskraven** enligt GDPR (art 32-36)*
- *Vid avtalets upphörande enligt PuAs önskemål radera eller återlämna personuppgifterna*
- *PuB ska ge PuA tillgång till info + tillfälle inspektera att PuB fullgör sina skyldigheter*
- *Regressanspråk om den ene parten orsakar att den andre parten drabbas av skadeståndsansvar eller sanktionsavgift?*
- *Kan även räcka med att PuB anslutit sig till EU-godkänd uppförandekod eller certifierats (art 40 och 42 GDPR och skäl 81)*
- *EU-kommissionen eller tillsynsmyndigheten (DI) kan bestämma standardavtalsvillkor för PuB-avtalen*

(Art. 28 GDPR)

SÄRSKILT OM INFOPLIKT

- INTERNT – EXTERNT?
- ÄR VI SKYLDIGA ATT INFORMERA?
- VAD OMFATTAR INFORMATIONSPLIKTEN?
- NÄR SKA INFORMATION LÄMNAS?
- HUR SKA INFORMATIONEN SKE?
- REGISTERUTDRAG?

INTERNT - Policy!



VÅRT AB:s HEMSIDA

Välkommen!
Bla-bla-bla
- vi är bäst!
- Chefen är vackrast!
- konkurrenten är fet, ful o dum!

X

Våra policies;
- Säkerhetspolicy.....
- Infopolicy.....
- IT-policy.....
- IT-säkerhetspolicy.....
- Förmånsbilspolicy.....
- Policy distansarbete.....
- Resepolicy.....

ANGER UTTRYCKLIGEN VAD VI FÅR GÖRA!

- **Klar & tydlig!**
- **Lätt att tillgå!**
- **Förhandlad med facket (se 11 § MBL)!**
- **Beslutad i viss formell ordning!**
- **Viss formell ordning för ändringar!**
- **Bestämd tid och bestämt sätt för meddelande om införande!**
- **Varning för konflikt mellan olika policies!**

Utan policy blir det svårt att hävda brott mot anställningsavtalet - och därmed även svårt att sätta dit personalen…

Policyn blir därför ett viktigt instrument, dels för *ATT* informera personalen, dels för att bevisa att vi *HAR* informerat personalen!

Att vi har informerat är på detta sätt inte bara en del av *informationsplikten*, utan även en del av *säkerhetskraven*!

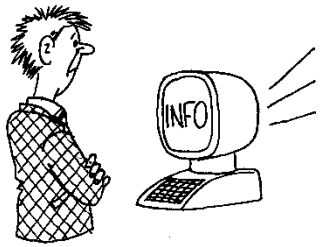
EXTERNT – Självmant & på begäran

SJÄLVMANT

Informera i förväg **om behandlingen!**

- vad, hur & varför
- vid insamling/registrering
- Vanligt att vi missar!

(Art. 12-14 GDPR)



REGISTERUTDRAG

På begäran **från den registrerade!**

- vad, hur & varför
- gratis, en gång per kalenderår

(Art. 15 GDPR)

Självmant

PuA ska *SJÄLVMANT* informera registrerad!
(vanligt att DI kritiserar för brister i informationen!!!)
(Art. 13-14 GDPR)

OM VAD?
- Identitet (vem du är) & kontaktinfo
- Ändamål & rättslig grund (varför uppgiften behandlas och varför det är tillåtet)
- Säkerhetsåtgärder, registrerads olika rättigheter (rättelse mm), ev. mottagare, lagringstid m.m.

NÄR?
1. När uppgifterna insamlas ***från registrerad***
2. Uppgifter insamlade ***från annan***
   a) Inom rimlig tid, max 1 månad
   b) Senast vid första kontakten med den registrerade
   c) Senast första gången uppgifterna lämnas ut

UNDANTAG:
a) Sån't den registrerade redan vet
b) Omöjligt eller orimligt
c) PuA är skyldig att behandla + lämpliga säkerhetsåtgärder finns
d) Tystnadsplikt/sekretess hindrar

På begäran

SKYLDIGHET ATT INFORMERA *EFTER ANSÖKAN* från den registrerade!
(Art. 15 GDPR)

OM VAD?
- Om & vilka personuppgifter om personen behandlas
- Ändamål & rättslig grund (varför uppgiften behandlas och varför det är tillåtet)
- Den registrerades olika rättigheter (rättelse, klagorätt mm), ev. mottagare, lagringstid m.m.
- Varifrån uppgifterna kommer och till vilka de ev. ska utlämnas
- Ev. automatiskt förfarande och vad som gäller för detta

NÄR?
1. En gång/kalenderår - gratis
2. Ytterligare utdrag – ”skälig” avgift

UNDANTAG:
a) Om det kränker andras rättigheter
b) Lagförslag: Ej färdiga uppgifter eller endast minnesanteckning (5:2 DSL, jfr 5 a § PuL)

NU – Ännu mera eftertanke . . .

ATT DISKUTERA:

Hur lämnar vi information om vår personuppgiftsbehandling?

- På vår externwebb?
- I dokument som vi skickar eller mejlar till alla registrerade, t.ex. avtal?
- Kommer vi att behöva ändra på vårt sätt att informera?

(någon minuts individuellt funderande…)

DATASKYDDSOMBUD

OBLIGATORISKT:

- *Hos **myndigheter** eller andra **offentliga organ** (utom i domstolars dömande verksamhet)*
- *När verksamheten innebär **regelbunden, systematisk och omfattande övervakning***
- *När verksamheten innebär **omfattande behandling av särskilda kategorier** av personuppgifter, inkl. uppgifter om fällande domar i brottmål/överträdelser*

(art. 37.1 a-c GDPR)

SÄRSKILDA FÖRUTSÄTTNINGAR:

- *OK med **ett enda DSO inom koncern** om DSO lätt kan nås*
- *OK med **ett enda DSO för flera myndigheter** om det är lämpligt mht storlek, organisation m.m.*

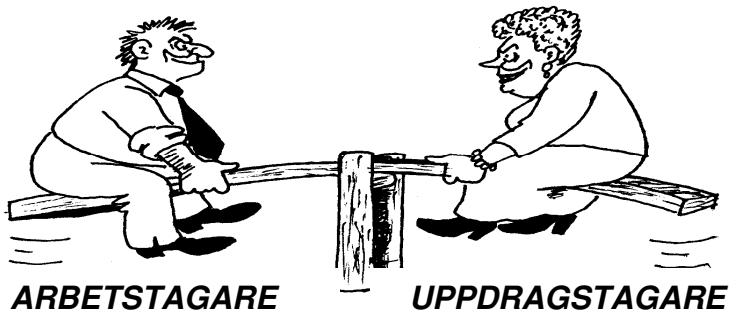
(art. 37.2-3 GDPR)

ANDRA FALL:

- *OK att ha ett DSO även i andra fall (d.v.s. frivilligt)*
- *EU och medlemsländerna kan föreskriva om DSO även i andra fall*

(art 37.4 GDPR)

Lämpligt DSO?



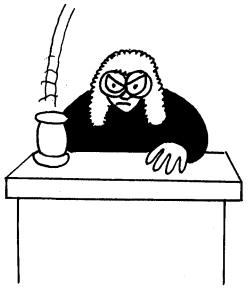
ATT FUNDERA ÖVER

- **Vad är bäst – arbetstagare (internt PuO/DSO) eller uppdragstagare (externt PuO/DSO)?**
  - Ingående kännedom om verksamheten – specialistkunskap inom PuL/GDPR?
  - Kan ett internt PuO/DSO verkligen hävda sitt oberoende?
  - Hur bra går löneförhandlingen för ett duktigt internt PuO/DSO?
- **Måste det ena utesluta det andra?**
  - D.v.s. varför inte ha båda?
  - Internt PuO/DSO vet hur organisationen ser ut, vilka system som finns och vem man ska prata med, medan externt PuO/DSO kan fylla på med specialistkompetens
- **Glöm inte den tekniska kunskapen!**
  - Det behövs kännedom om hur systemen är utformade och vad som kan göras

SANKTIONER

- VAD KAN HÄNDA OM VI INTE SKÖTER OSS?
- ÄR SANKTIONSAVGIFTERNA ETT SÅ ALLVARLIGT HOT SOM DE FRAMSTÄLLS?
- BEHÖVER VI BEKYMRA OSS FÖR SKADESTÅND?

SANKTIONER - Allmänt



FÖRELÄGGANDEN, FÖRBUD M.M. BESLUT MEDDELADE AV DATAINSPEKTIONEN
(Art. 58.2)

SKADESTÅND
- Ersättning till den registrerade för sådan materiell/immateriell skada som uppkommit
(Art. 82)

ADMINISTRATIV SANKTIONSAVGIFT
- Vid brott mot GDPR
- Mellan 2 – 4 % av global årsomsättning
(Art. 83)

POLISANMÄLAN
- Tjänstefel (BrB 20:1)

JO-/JKANMÄLAN
- Tjänstefel (BrB 20:1)

FÖRELÄGGANDEN M.M.

(Art. 58.2 GDPR)

OLIKA REAKTIONER FRÅN DATAINSPEKTIONEN

a) **VARNING**

b) **REPRIMAND**

c) **FÖRELÄGGA ATT TILLMÖTESGÅ BEGÄRAN FRÅN EN REGISTRERAD**

d) **FÖRELÄGGA ATT BEHANDLA ENLIGT GDPR**

e) **FÖRELÄGGA ATT MEDDELA REGISTRERAD OM PERSONUPPGIFTSINCIDENT**

f) **BEGRÄNSA ELLER FÖRBJUDA BEHANDLING**

g) **FÖRELÄGGA OM RÄTTELSE, RADERING, BEGRÄNSING ELLER INFO HÄROM TILL SÅDANA SOM FÅTT PERSONUPPGIFTERNA**

h) **ÅTERKALLA CERTIFIERING**

i) **PÅFÖRA SANKTIONSAVGIFT**

j) **FÖRELÄGGA OM AVBRYTANDE AV BEHANDLING UTANFÖR EU/EES**

SKADESTÅND

(Art. 82 GDPR)

1) Allmänt: - *Skadeståndsberättigad* = Den registrerade

- *Skadeståndsansvarig* = PuA eller PuB (den registrerade väljer)
- *Omfattning:* Materiell/immateriell skada

2) Ansvarsfördelning: - Varje PuA som medverkat vid behandlingen

- PuB endast för sitt brott mot uttryckliga skyldigheter enligt GDPR eller PUA:s instruktioner

3) PuA/PuB har bevisbördan: - PuA/PuB har bevisbördan för att denne INTE orsakat den skada som den registrerade påstår

4) Solidariskt ansvar: - Den registrerade har rätt till HELA ersättningen från PuA/PuB som denne vänt sig till

5) Regressrätt - PuA och PuB får sedan göra upp om fördelningen regressvis med proportionerlig fördelning utifrån delaktighet

6) Behörig domstol: - I det land där PuA/PuB är etablerad, eller där den registrerade har sitt hemvist (om inte PuA är en myndighet för då ska talan väckas där denna är etablerad)

- Nationellt i Sverige: 1) Där PuA/PuB har sitt säte (RB 10:1 st.3), men även 2) där skadan uppstått (RB 10:8, jfr RH 2007:54 och 2010:21)

Skadeståndsbelopp

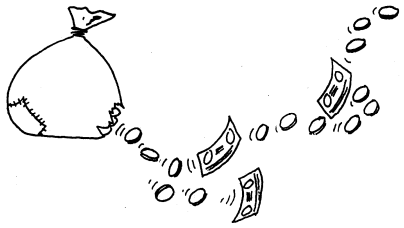
BELOPPSSCHABLONER HAR UPPKOMMIT GENOM RÄTTSPRAXIS

- 3 000 SEK – 5 000 SEK (Jfr HD:s dom 2013-12-06, T 2807-12)
- Högre belopp i några enstaka fall (Svea hovrätts dom den 28 pril 2017, mål nr T 6161-16, ”Romregistret”, 30 000 SEK per person)
- Ersättning för ombudskostnader endast om tvistens värde överstiger ½ prisbasbelopp (RB 18:8a)
- Rättsskyddet i hemförsäkringen täcker vanligen inte tvister där värdet understiger ½ prisbasbelopp

= ***Är det över huvud taget någon mening med att föra en process om skadestånd p.g.a. behandling av personuppgifter?***

- Som registrerad bör du tänka dig för innan du drar igång!

- Som PuA är det kanske inte så farligt att bli skadeståndsskyldig (men många bäckar små blir en stor å)...

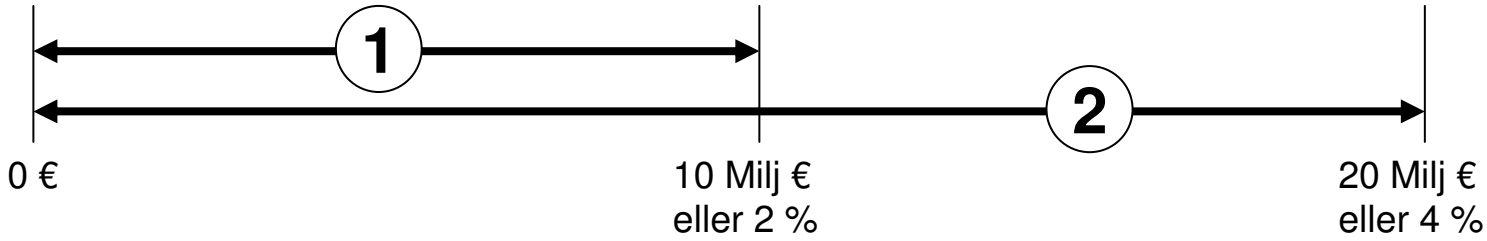


ADMINISTRATIV SANKTIONSAVGIFT

(Art. 83 GDPR)

TVÅ ALTERNATIV
1. Max 10 000 000 €, eller max 2 % av global årsomsättning för företagskoncern (art. 83.4 GDPR)
2. Max 20 000 000 €, eller max 4 % av global årsomsättning för företagskoncern (art. 83.5 GDPR)
- För myndigheter max 10 000 000 SEK resp. 20 000 000 SEK (SOU 2017:39, förslag till DSL)

- **Beroende på vilka artiklar i GDPR som överträtts** (art. 83.4-5 GDPR)
- **Och beroende på vissa omständigheter som föreligger i det aktuella fallet** (art. 83.2 GDPR)



Regelbrott som avgör beloppet

1) Upp till 10 000 000 €, eller om PuA är ett företag 2 % av totala globala årsomsättningen om detta är mer

a) PuA:s och PuB:s skyldigheter enligt art. 8 (barns samtycke), 11 (identifiering av den registrerade, 25–39 (krav på PuA/PuB, register, konsekvensbedömning, säkerhet m.m.), 42 och 43 (i samband med certifiering) har åsidosatts.
b) Certifieringsorgan som åsidosatt skyldigheter enligt art. 42 och 43.
c) Ett särskilt övervakningsorgan som åsidosatt skyldigheter enligt art. 41.4.

2) Upp till 20 000 000 €, eller om PuA är ett företag 4 % av totala globala årsomsättningen om detta är mer

a) *Grundläggande principer* för behandling, inklusive villkor för samtycke, har åsidosatts (art. 5, 6, 7 och 9).
b) *Registrerades rättigheter* (info, rättelse, radering m.m.) har åsidosatts (art. 12–22).
c) *Otillåten överföring utanför EU/EES* (art. 44–49).
d) Åsidosättanden av *skyldigheter enligt nationell lagstiftning* som antagits på grundval av kapitel IX (offentlighetsprincipen, sekretess, anställningsförhållanden, personnummer m.m.).
e) *Underlåtenhet att rätta sig efter DI:s föreläggande*, begränsning av behandling av uppgifter eller beslut om att avbryta uppgiftsflödena enlighet med artikel 58.2 eller underlåtelse att ge tillgång till uppgifter i strid med artikel 58.1.

(Art. 83.4-5 GDPR)

Omständigheter som avgör beloppet

(Art. 83.2 GDPR)

a) Överträdelsens karaktär:
- typ av överträdelse, omfattning, konsekvenser m.m.

b) Uppsåt eller oaktsamhet

c) PuA:s/PuB:s agerande för att åtgärda

d) Graden av ansvar hos PuA/PuB:
- m.h.t tekniska och organisatoriska åtgärder enligt art 25 och 32.

e) Tidigare överträdelser

f) Samarbete med tillsynsmyndigheten

g) Kategorier av personuppgifter
- värre ju känsligare de är

h) Om PuA/PuB själv anmält

i) Tidigare förelägganden m.m.
- inte bra om det är återfall

j) Uppförandekoder/certifiering:
- Hur PuA/PuB tillämpat uppförandekoder/certifiering (art. 40 och 42)

k) Annan försvårande eller förmildrande faktor:
- ekonomisk vinst som uppnås, förlust som undviks, (direkt eller indirekt)

AVSLUTNING

Sammanfattning av allt vi nu pratat om . . .

GDPR – LATHUND

GRUNDLÄGGANDE FRÅGOR

1. Behandlar vi personuppgifter?
- Direkt/indirekt, d.v.s. i princip allt…

2. Vilket ändamål har vi?
- D.v.s. varför behöver vi uppgifterna

3. Vilken är vår lagliga grund?
a) samtycke, b) nödvändigt för att …

4. Om uppgifterna är känsliga?
- även personnummer, info om brott
- då måste vi ha särskild anledning

5. Vilka säkerhetsåtgärder behövs?
- Många uppgifter, känsliga, spridas, kan bli stor skada = Större krav!

6. Anlitar vi någon? – PuB, PuB-avtal

7. Har vi informerat?
- Externt/internt? Hemsidan …

8. Ska uppgifterna utomlands?
- Försiktigt utanför EU/EES

ÅTGÄRDER INFÖR GDPR

1. INVENTERA!
- Vilka slags personuppgifter har vi?

2. Gör en FÖRTECKNING!
- Register över behandlingen (vad/ varför/hur/av vem (PuB) m.m.)

3. KONSEKVENSBEDÖM!
- Gör GAP/SBA (hot, risk, skada)

4. Se över PUB-AVTALEN!
- Justera enligt GDPR! Snarast!

5. SÄKERHETSÅTGÄRDER!
- Automatiseras (privacy by design)?

6. Utse DSO?
- P.g.a. att det krävs enligt GDPR
- Annars p.g.a. lämpligt (extern/intern)

7. KORRIGERA behandlingen!
- Så att den är OK enligt GDPR
- Jfr. DI:s 13-punktsmodell

KONTAKTINFO

SLUT!!!

Tack för mig!

Conny Larsson
conny.larsson@gardepartners.se

Advokatfirman Gärde & Partners AB

Danderydsgatan 14
SE-114 26 Stockholm
Tel: 08-660 00 41/Fax: 08-660 00 51