Dataskyddsförordningen

SVENSKT NÄRINGSLIV

Dataskyddsförordningen

- Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävandet av direktiv 95/46/EG (allmän dataskyddsförordning)
- General Data Protection Regulation, GDPR
- 25 maj 2018
- Ersätter personuppgiftslagen, PUL

Kompletterande dataskyddslag

- Dataskyddsförordningen, DF, direkt tillämplig
- Blir i vissa delar subsidiär: artiklar där nationell reglering tillåts
- Vissa artiklar förutsätter eller tillåter nationella bestämmelser
  - Preciseringar
  - Undantag

½

Normkonflikt

- Grundlag företräde framför vanlig lag
- EU-rätt företräde framför svensk lag
- Speciallag företräde framför generell lag
  – ”Sektorspecifika bestämmelser ska ha företräde framför dataskyddslagen”

  MEN
  – ”…måste vara förenlig med dataskyddsförordningen och avse en fråga som får särregleras genom nationell rätt”

Kompletterande dataskyddslag, DL

- Kompletterande bestämmelser på ett generellt plan

  1 kap, 3 §
  Om en annan lag innehåller bestämmelse som rör behandling av personuppgifter och som avviker från denna lag tillämpas den bestämmelsen

  – Med ”lag” avses både EU-förordningar och svenska lagar antagna av riksdagen
  – Svensk lag eller förordning har endast företräde i den mån dataskyddsförordningen tillåter nationell särreglering

  (Motsvarar 2 § PUL)

Utanför tillämpningsområdet

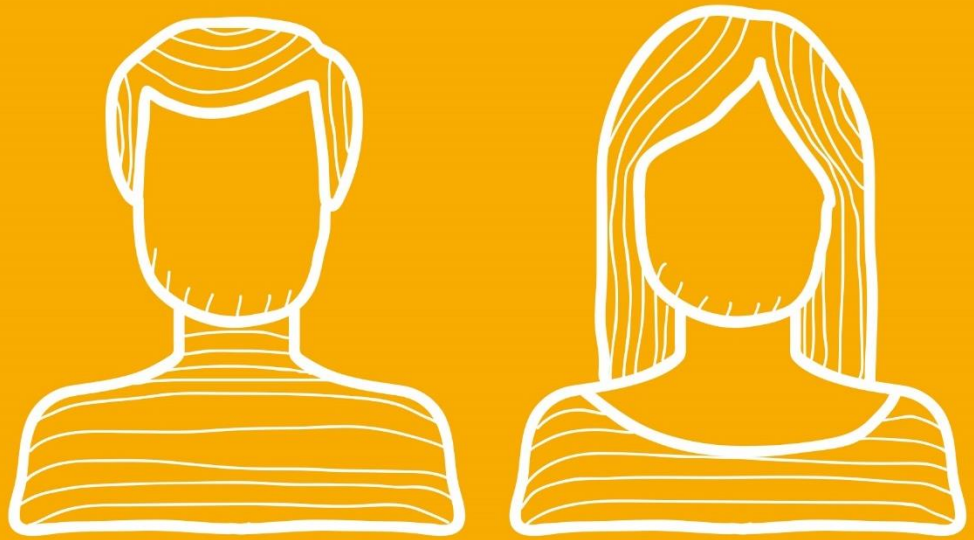
Dataskyddsförordningen och dataskyddslagen gäller inte för behandling;

(artikel 86, 85:2 DF, 1 kap 4 § DL)

- Tryckfrihetsförordningen
- Yttrandefrihetsgrundlagen
- Journalistiskt ändamål
- Akademiskt skapande
- Konstnärligt skapande
- Litterärt skapande
- Privat behandling

Vår rätt till oss själva

SVENSKT NÄRINGSLIV



Integritetsskydd

Skyddet för fysiska personer vid behandling av personuppgifter är en grundläggande rättighet.

Vad skyddar och begränsar integritetsskyddet?

- Lagen om namn och bild i reklam: samtycke krävs (levande personer)
- Dataskyddsregler
- Användarvillkor: företaget/säljaren bestämmer
- Yttrandefrihetsregler: frihet att framföra åsikter och information
- Upphovsrätt: ensamrätt till bild och text

Yttrande- och informationsfrihet

Gammelmedier

- Grundlagsskyddade:
  - Tidningar och tidskrifter: tryckfrihetsförordningen
  - Radio, tv, bio: yttrandefrihetsgrundlagen

- Pressetiska regler

Yttrandefrihet på nätet

- Utgivningsbevis gör att YGL gäller
  - ansök på www.mprt.se

Begreppet personuppgift

Personuppgifter, exempel

- Adress
- Namn
- Personnummer
- Enskilda firmor
- Fotografier
- IP-adresser
- ”Nicks”

Känsliga personuppgifter

- Etniskt ursprung
- Politisk åskådning
- Religion
- Fackligt medlemskap
- Uppgifter om hälsa, sexualliv och sexuell läggning
- Genetiska uppgifter för att identifiera en person
- Biometriska uppgifter för att identifiera en person

Känsliga personuppgifter, undantag

- Samtycke
- Arbetsrätt eller kollektivavtal
- Offentliggjorda uppgifter (av den registrerade)
- Hälso- och sjukvård (tystnadsplikt)
  - Förebyggande hälsovård
  - Bedömning av arbetstagares arbetskapacitet
- Arkiv och statistik

Särskilt känsliga personuppgifter

Fällande domar i brottmål och lagöverträdelser som innefattar brott

” får endast utföras under kontroll av myndighet” (Artikel 10 DF)

- Enstaka uppgifter hos arbetsgivare
- Tillstånd från Datainspektionen
- Ta del av/ läsa

Tillåten behandling av personuppgifter

Principer

- Laglighet
- Korrekthet (uppdaterade, rättade, annars raderade)
- Öppenhet
- Endast för ändamålet
- Uppgiftsminimering
- Lagringsminimering
- Säkerställd integritet och konfidentialitet

Vad gör en behandling tillåten?

Rättslig grund:

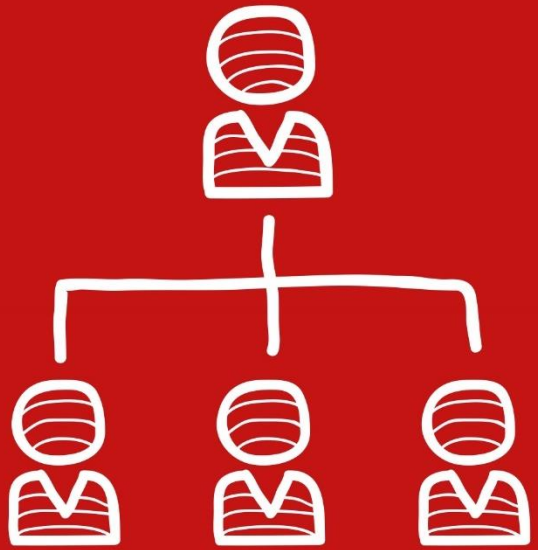
- Samtycke (gäller ej särskilt känsliga personuppgifter)
- Fullgörande av avtal med registrerad
- Rättslig förpliktelse (lag, kollektivavtal, beslut) jmf 2 kap 3 § DL, artikel 6.1c DF
- Skyddande av persons intressen
- Allmänt intresse eller myndighetsutövning
- Intresseavvägning (gäller ej känsliga personuppgifter)
  - Berättigat intresse PUA eller tredje part

Personnummer

- Samtycke
- Intresseavvägning ”klart motiverat” av
  - ändamålet
  - säker identifiering
  - annat beaktansvärt skäl

(3 kap 13 § DL, jmf 22 § PUL)

Ansvarsstruktur



Personuppgiftsansvarig, PUA

Den juridiska personen

Personuppgiftsansvarig har kontrollansvar för personuppgiftsbiträdet

Personuppgiftbiträde, PUB

Behandlar personuppgifter åt personuppgiftsansvarig

Upprätta personuppgiftsbiträdesavtal

Personuppgiftsbiträde står delvis för ansvaret:

- Registerföring
- Tillräckliga säkerhetsåtgärder
- Anlita dataskyddsombud

Dataskyddsombud

- Expert
- Anmälan till datainspektionen
- Inte ha arbetsuppgifter som kan leda till intressekonflikt

Nyheterna i dataskyddsförordningen och dataskyddslagen

SVENSKT NÄRINGSLIV

Samtyckets utformning

Högre krav

- 13-års gräns
- Klart, tydligt
- Samtycke för varje syfte
- Samtycket får inte göras tvingande
- Lika lätt att samtycka som att återkalla samtycke

Tydligare krav på att informera

Kontaktuppgifter för frågor

Vad informationen ska användas till

Varför företaget har rätt att behandla uppgiften

Hur länge informationen sparas

Kontaktuppgifter till Datainspektionen

Begränsning i rätten att få information

Registerutdrag ska tillhandahållas kostnadsfritt, MEN

Om begäran från en registrerad är uppenbart ogrundad eller orimliga får den personuppgiftsansvarige

- ta ut en rimlig avgift
- vägra att tillmötesgå begäran

Radering av uppgifter

- Rensning fortsatt centralt
- Utökade möjligheter för privatpersoner att begära radering av uppgifter,
  ”rätten att bli bortglömd”
- Ska ske ”utan onödigt dröjsmål”

Ostrukturerad information

- I 5a § PUL finns ett undantag för personuppgifter som finns i ostrukturerad form, t ex i löpande text

- Motsvarande undantag saknas i förordningen

Begränsningar för ostrukturerat material

- 5 kap 2 § DSL undantar registrerades rätt till tillgång (artikel 15 DF)
  - Personuppgifter i löpande text, tex minnesanteckningar eller PM som;
    - Inte lämnats till tredje part
    - Inte enbart statistik eller arkivändamål
    - Inte behandlats längre än ett år

Inbyggt dataskydd

IT-struktur viktig

Hantera krav genom system som möjliggör efterlevnad

Kryptering

Anmälningsplikt om dataincident

- Personuppgiftsincidenter ska anmälas till tillsynsmyndigheten
- Dataintrång
- Oavsiktlig förlust av uppgifter
- Ska ske utan onödigt dröjsmål – inte senare än 72 timmar efter vetskap

- Det vill säga: Ställer krav på att organisation finns som kan hantera sådan rapportering

Information om dataincident

- Personuppgiftsincident ska anmälas till den registrerade OM incidenten leder till hög risk för fysiska personers rättigheter och friheter.

- OBS! Inte krav på inom 72 timmar.

- Behöver inte ske om det skulle inbegripa en oproportionell ansträngning. I så fall ska allmänheten informeras.

Krav på dataskyddsombud

Krav om kärnverksamhet

- Behandla personuppgifter som medför regelbunden och systematisk övervakning i stor omfattning
- Stor omfattning av känsliga personuppgifter
- Kartläggning av enskildas beteenden

Krav på konsekvensbedömning

- Om behandlingen hög risk för de registrerades rättigheter
- Kartlägg vilka åtgärder som behövs för riskminimering
- Personuppgiftsansvarige ska rådfråga dataskyddsombudet
- Tillsynsmyndigheten ska upprätthålla en förteckning av det slags behandlingsverksamheter som omfattas av kravet

Möjlighet till dataportabilitet

- OM behandlingen bygger på samtycke och behandlingen sker automatiserat

- De registrerade ska ha rätt att få ut sina personuppgifter som lämnats till och genererats hos en personuppgiftsansvarig

- Ha rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig
  – Företaget ska föra över om tekniskt möjligt till annan leverantör

Uppförandekoder

- Tillämpning av godkända uppförandekoder för att visa att den personuppgiftsansvarige fullgör sina skyldigheter

- IT-system kan/bör/ska designas för att uppfylla kraven
  - Se Datainspektionen

Datainspektionens befogenheter

Tillsynsmyndigheternas befogenheter ökar

- Förhandskontroller som rör riskfylld behandling
- Kan utdöma ”administrativ sanktionsavgift”
- Enskilda ska kunna vända sig till ”sin” tillsynsmyndighet, även om klagomålet gäller ett företag i ett annat EU-land

Sanktionerna

Kan dömas ut tex om företaget inte lämnar information till den registrerade eller inte rapporterar intrång i tid.

Den administrativa avgiften kan högst uppgå till
- 20 miljoner euro, eller
- 4 % av den globala årsomsättningen (koncernnivå)

Hur allvarlig?
Medveten eller oavsiktlig?
Åtgärder för att minska skadan?
Ekonomisk vinning?

Preskriptionstid fem år

Export av uppgifter (utanför EU)

- Adekvatsbeslut
  - Av EU-kommissionen godkända länder
- Godkända standardavtalsklausuler
- Avtal för koncern (artikel 47 DF)
- Tillstånd av datainspektionen

Åtgärder att vidta inför de nya reglerna

SVENSKT NÄRINGSLIV

Åtgärder att vidta

- Se till att organisationen blir medveten om förändringarna
- Utred vilka personuppgifter ni behandlar och hur
  - Ostrukturerad information?
  - Känsliga uppgifter?
- Vilket stöd har ni för er behandling av personuppgifter?
  - Lagstöd
  - Avtal
  - Samtycke
  - Intresseavvägning

Åtgärder att vidta, forts.

- Bygg upp kapacitet för att lämna information mm
- Bygg upp kapacitet för att hantera intrång
- Bygg in skydd för personuppgifter i IT-systemen
  – ”privacy by design”
- Byt ut system/ kontroller att de är anpassade
- Utse dataskyddsombud, om så krävs
- Har ni verksamhet i flera länder – gör en bedömning av vilken tillsynsmyndighet som kommer bedriva tillsynen

Glöm inte

Utbilda personalen

Skapa rutiner

Bevaka nya riktlinjer från Datainspektionen