GDPR- Vad är det?

Frukostmöte hösten 2017

DATASKYDD?

- Skydd av *fysiska personers* grundläggande rättigheter och friheter, särskilt skydd av PU

- På företagens bekostnad?

DET ALLA PRATAR OM – VAD KOSTAR DET

- Dataskydds- och juristkostnader
- Skadestånd
- Omfattande rätt för TSM (=DI) ingripa
- Administrativa sanktionsavgifter - *nyhet*
  - Förutom korrigering
  - Storleken ”beror på”
  - Preskription (SE)

PERSONUPPGIFTER - VAD

- Varje upplysning
- Om en fysisk person
  - Tillräckligt att kan identifieras indirekt
- S.k. ”Särskilda kategorier” av PU – förstärkt skydd

BEHANDLING AV PERSONUPPGIFTER - HUR

- Behandling
  - I princip allt är behandling
- Med ADB eller av analogt register
  - ”ADB”
  - ”Analoga” register – i vissa fall

PERSONUPPGIFTSAKTÖRER – VEM

- Personuppgiftsansvarig (PuA)
  - Den som *bestämmer* ändamål och medel för behandlingen av personuppgifter
  - Två PuA möjligt
- Personuppgiftsbiträde (PuB)
  - Behandlar PU för PuA:s räkning
  - PuB → PuA

Forts. (aktörerna)

- DSO - *Nyhet*
  - ”Skyddsombud” för PU.
  - Vissa måste utse en DSO (oavsett om är PuA/PuB)
  - Om osäker: Inget fel att utse DSO ”i onödan”
  - DSO:n ej ansvarig mot de registrerade.

TILLÄMPNINGSOMRÅDE GDPR – NÄR & VAR

- I tiden
  - Från den 25 maj 2018
- I rummet
  - Ansvarig person (PuA/PuB) etablerad inom EU;
  - Alternativregeln
- Materiellt
  - Levande personer
  - ”Privatundantaget”
- Något om relationen Sv-EU-R
  - EU-förordning. PuL ”kilar vidare”
  - Nationell kompletteringslagstiftning (SOU 2017:39), remiss

TILLÅTEN BEHANDLING AV PERSONUPPG.

- Utgångspunkten: Förbjudet behandla PU
- Sex undantag för ”vanliga” PU
- ”Missbruksregeln” försvinner

Forts. (tillåten behandling)

1. Samtycke till behandlingen – *nyhet i §-form*
   - För ett/flera specifika ändamål
   - *Frivillig*, specifik, informerad och otvetydig viljeyttring
   - Muntligen/genom en entydig bekräftande handling
   - Inte ”överskjutande” samtycken
   - Särskiljbar, begriplig, begäran (ogiltighet)
   - Rätt att fritt och lätt återkalla. Info därom.

Forts. (samtycke)

- För barn <13 år (SE) och 'informationssamhällets tjänster'; samtycke ges/godkännas av VH.
  PuA kontrollera och bevisa.
- Dokumentera! Börja nu!
- Överväg annan grund!

Forts. (tillåten behandling - 6 grunder)

2. Avtalsundantaget
3. Rättslig förpliktelse → behandlingen nödvändig
4. Påkallat av ett grundläggande enskilt intresse
5. Allmänt intresse/PuA:s myndighetsutövning
6. Intresseavvägning

- 'Särskilda kategorier' av PU

PRINCIPER FÖR BEHANDLING AV PERSONUPPGIFTER

- Tillåtet ändamål *och* i enlighet med de sex principerna.
- Kan *ej* frångå genom samtycke
- PuA ska visa att principerna efterlevs

Forts. (principer för behandlingen)

1. Behandlas lagligt, korrekt och öppet ./. den registrerade
2. Ändamålsbegränsning
3. Uppgiftsminimering
4. Korrekta och (om nödvändigt) uppdaterade uppgifter
5. Lagringsminimering
6. Dataskydd (Integritet och konfidentialitet)

SÄRSKILT OM KRAVET PÅ DATASKYDD

- Lämpliga tekniska *och* organisatoriska åtgärder
- ”Data protection by design”
- ”Data protection by default”
- Datasäkerhet vid behandling

- PuA:s ansvar. För PuB: datasäkerhet vid behandling

DEN REGISTRERADES RÄTTIGHETER

- Generellt
  - Höga krav. PuA:s ansvar
- Information när PU samlats in från den registrerade
  - HR: Vid erhållandet. Kan underlåtas i vissa fall.
  - Säkra bevisning! (Räcker att infon lämnats)
- Information till den registrerade när PU samlats in från annan än den registrerade

Forts. (rättigheter)

- Allmänt om en *begäran* från den registrerade
  - PuA ska *underlätta*. Får säkra ID.
  - Utan dröjsmål (HR) och kostnadsfritt (HR). Undantag.
  - Underrättelseskyldighet

Forts. (rättigheter)

- Rätt till tillgång / registerutdrag
  - Ge liknande info som när fick in PU
  - E-begäran → E-svar
  - Undantag (SE)
- Rätt till rättelse
- Rätt att bli bortglömd
- Rätt till begränsning av behandling
- Rätt att göra invändningar

Forts. (rättigheter)

- Rätt till dataportabilitet - *nyhet*
  - Vissa krav
  - Även rätt till direktöverföring, om tekniskt möjligt
- Rätt att neka automatiserade beslut, inkl. profilering, givet vissa krav
- Rätt att processa

SKYLDIGHETER PUA/PUB

- Register (”record”) över PU-behandling
  - PuA: All behandling under dess ansvar
    - Visst innehåll, jfr informationsskyldigheten
  - PuB: Alla kategorier av behandling utförd för en PuA:s räkning
  - TSM kan begära ut
  - Se upp för undantaget från undantaget

Forts. (skyldigheter)

- PuA:s ansvar
  - Genomföra lämpliga tekniska och organisatoriska åtgärder för att *säkerställa* och *visa* att behandlingen sker enl. GDPR
  - Behörighetsstyrning
  - 3 x Dataskydd
  - Om anlitar PuB
    - Skriftligt **PuB-avtal** med visst innehåll!

Forts. (skyldigheter)

- PuB:s ansvar
  - Underbiträde kräver PuA:s godkännande.
  - Måste följa PuA:s instruktioner (HR).
  - Om anlitar underbiträde
    - **Underbiträdesavtal**, jfr. PuB-avtal
    - Fullt ansvarig mot PuA för underbiträdet
  - Ansvar för datasäkerhet vid behandling

ANMÄLNINGSSKYLDIGHET ”PU-INCIDENT” - *nyhet*

- PU-incident
- Åtgärder
  - Dokumentera (PuA)
  - Anmälan till TSM (PuA)
  - Om PuB: Underrätta PuA utan onödigt dröjsmål
  - Underrätta den registrerade

PRIVACY IMPACT ASSESMENT (”PIA”) - *nyhet*

- Om viss behandlingstyp PU *sannolikt* leder till *hög risk* för fysiska personers rättigheter/friheter
- Krävs alltid i vissa fall
- Bedöma konsekvenserna för PU-skyddet *före* behandlingen
- Konsultera DSO/de registrerade
- Visst innehåll
- Förhandssamråd TSM

ÖVRIGT

- Särskilda regler för överföring av PU till 3:e land/internat. organisation
  - Akta: molntjänster!
  - Mottagande PuA/PuB måste uppfylla vissa särskilda krav

- Börja GDPR:a nu!

FRÅGOR?

Tor Bergkvist

tb@vici.se

010-209 12 65