GDPR- Vad är det?

Råbylunds företagarförening

2017-09-08

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
  - För fulla skadan, även om bara en av flera inblandade
- Omfattande rätt för TSM (=DI) ingripa
  - Tillsynsärenden (gryningsräder)
  - Befogenhet till ”korrigering” (av PuA/PuB)
- Administrativa sanktionsavgifter
  - Största nyheten
  - Alternativt *eller* kumulativt till korrigering
  - Effektiva, proportionerliga och avskräckande – i varje fall
  - Tre grupper och två ”nivåer”
  - Ett antal bedömningsgrunder för *om* påföras och *storleken*
  - Preskription (SE): tillfälle till yttrande inom 5 år från påstådda överträdelsen

PERSONUPPGIFTER - VAD

- Varje upplysning
- Om en fysisk person
  - Viss identifierad person
  - *Eller* person som direkt/indirekt kan identifieras
- Omfattande!
- S.k. ”Särskilda kategorier” av PU – förstärkt skydd

BEHANDLING AV PERSONUPPGIFTER - HUR

- Behandling
  - I princip allt är behandling
- Med ADB eller av analogt register
  - Behandling helt eller delvis på automatisk väg (jfr. ADB)
  - ”Analog” behandling av PU som ingår/kommer ingå i ett register – vissa fall

PERSONUPPGIFTSAKTÖRER – VEM

- Personuppgiftsansvarig (PuA)
  - Fysisk/juridisk person/myndighet etc.
  - Som *bestämmer* ändamål och medel för behandlingen av personuppgifter
  - Kan vara gemensamt personuppgiftsansvarig med annan

- Personuppgiftsbiträde (PuB)
  - Behandlar PU för PuA:s räkning
  - Om PuB fastställer ändamål/medel för behandlingen → ansvar på samma sätt som PuA

Forts. (aktörerna)

- DSO
  - Nyhet
  - Saknas definition. ”Skyddsombud” för PU.
  - Massa regler om kompetens, arbetsuppgifter, sekretess och oavsättlighet
  - Vissa måste utse en DSO (oavsett om är PuA/PuB)
  - Om osäker: Inget fel att utse DSO ”i onödan” (men då gäller reglerna för en DSO fullt ut)
  - 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”
  - Andra smärre begränsningar
- Något om relationen Sv-EU-R
  - EU-förordning; gäller före svensk lag och behöver inte (får inte) ”skrivas in” i svensk lag. PuL ”kilar vidare”
  - Nationell kompletteringslagstiftning (SOU 2017:39), remiss

TILLÅTEN BEHANDLING AV PERSONUPPG.

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

1. Samtycke till behandlingen
   - Nyhet att regleras uttryckligen
   - 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)

- Särskilda krav för barn och ’informationssamhällets tjänster’; under 13 år (SE) ska samtycke ges/godkännas av VH och PuA ska göra rimliga ansträngningar kontrollera, tillgänglig teknik. PuA:s bevisbörda att samtycke lämnats.
- Dokumentera! Börja nu!
- Överväg annan grund!

Forts. (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

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”
  - Genomföra lämpliga åtgärder – inklusive pseudonymisering - för ett effektivt genomförande av *dataskyddsprinciper*, integrerade i behandlingen
  - Både vid fastställandet av medel för genomförandet av behandlingen och vid själva behandlingen
- ”Data protection by default”
  - För att säkerställa att *i standardfallet* endast PU *nödvändiga* för varje specifikt ändamål med behandlingen behandlas
- Datasäkerhet vid behandling
  - Säkerställa en *säkerhetsnivå* som är lämplig ./. risken
  - Olika sorters behandling av samma PU kan kräva olika säkerställande
- PuA:s ansvar. För PuB: datasäkerhet vid behandling

DEN REGISTRERADES RÄTTIGHETER

- Generellt
  - PuA:s ansvar
  - Alltid i koncis, klar, tydlig, begriplig och lätt tillgänglig form samt med klart och tydligt språk.
  - Lämnas skriftligen eller annan form – om lämpligt elektronisk form. Får tillhandahållas muntligen *om den registrerade begär det*, under förutsättning att dennes ID bevisats *på annat sätt*.

Forts. (rättigheter)

- Information när PU samlats in från den registrerade
  - Vid erhållandet
  - Dock ej i den mån den registrerade redan förfogar över informationen
  - Säkra bevisning! (Räcker att infon lämnats)
  - Ytterligare info före ytterligare behandling för ett nytt, angivet, ändamål
- Information till den registrerade när PU samlats in från annan än den registrerade
  - Tidpunkt
  - 4 undantag
  - Ytterligare info före ytterligare behandling för ett nytt, angivet, ändamål

Forts. (rättigheter)

- Allmänt om en *begäran* från den registrerade
  - PuA ska *underlätta* utövandet av den registrerades rättigheter
  - Får (HR) vid rimligt tvivel om ID hos den som *begär* begära ytterligare nödvändig info för att ID:a.
  - En *begäran* ska som utgångspunkt tillgodoses utan dröjsmål
  - Informationen ska lämnas kostnadsfritt. Undantag: uppenbart ogrundad/orimlig *begäran*, särskilt pga. repetitiv
  - PuA ska underrätta varje mottagare till vilka PU lämnats ut om gjorda rättelser/begränsningar/om den registrerade ”glömts bort”

Forts. (rättigheter)

- Rätt till tillgång
  - Rätt till ”registerutdrag”
  - Dessutom: Ge liknande info som när fick in PU
  - E-begäran → E-svar
  - Förslag till undantag (SE) för PU i *löpande text* som inte fått sin *slutliga utformning* när begäran gjordes / minnesanteckningar
- Rätt till rättelse på begäran
  - Rätt att få felaktiga (egna) PU rättade
  - Rätt att komplettera ofullständiga PU
- Rätt att bli bortglömd på begäran
  - Rätt att under vissa omständigheter få sina PU raderade. Finns undantag.
  - Om uppgifterna offentliggjorts ska PuA vidta rimliga åtgärder för att underrätta andra PuA:a som behandlar PU:a.

Forts. (rättigheter)

- Rätt till begränsning av behandling på begäran
  - Rätt att under vissa omständigheter kräva att PuA begränsar behandlingen
  - Medför att PU endast får behandlas i viss utsträckning
  - Måste underrätta den registrerade innan begränsningen upphör
- Rätt att göra invändningar
  - Rätt att invända mot PuA:s åberopade allmänna intresse/ intresseavvägning som grund för behandlingen – även mot profilering grundad härpå
  - PuA:s rätt behandla upphör. Finns undantag.
  - Behandling för direkt marknadsföring, inkl. profilering (om direkt MF), rätt att när som invända, varvid behandlingen ska upphöra.
  - Den registrerade ska informeras om invändningsrätten senast vid första kommunikationen med denne.

Forts. (rättigheter)

- Rätt till dataportabilitet
  - Nyhet
  - Rätt för en registrerad att få ut (egna) PU *som själv tillhandahållit,* digitalt
  - Vissa krav
  - Rätt till överföring direkt till annan PuA, om tekniskt möjligt
  - Gäller ej behandling nödvändig för uppgift av allmänt intresse/som är led i PuA:s myndighetsutövning
- Rätt att neka automatiserade beslut, inkl. profilering, som har *rättsliga följder* för personen eller på liknande sätt påverkar denne/a i betydande grad
  - Undantag
- Rätt att processa

SKYLDIGHETER PUA/PUB

- Register (”record”) över PU-behandling
  - Skriftligt/elektroniskt
  - PuA: All behandling under dess ansvar
    - Visst innehåll, jfr informationsskyldigheten
  - PuB: Alla kategorier av behandling utförd för en PuA:s räkning
    - Visst innehåll
  - TSM kan begära ut
  - U-tag för företag/organisationer sysselsätter färre än 250 personer
    - Undantag

Forts. (skyldigheter)

- PuA:s ansvar
  - Genomföra lämpliga tekniska och organisatoriska åtgärder för att *säkerställa* och *visa* att behandlingen sker enl. GDPR
  - Behörighetsstyrning
  - Om anlitar PuB
    - Enbart PuB som ger tillräckliga garantier för att behandlingen uppfyller GDPR
    - **PuB-avtal!** (I den utsträckning PuB inte binds i de oblig. frågorna av unionsrätten/nat. rätt)
  - PuB-avtal
    - Ska vara skriftligt, elektroniskt ok
    - Ska reglera/föreskriva vissa saker
  - PuA: Ansvar bl.a. för "Data protection by design/default" samt datasäkerhet vid behandling

Forts. (skyldigheter)

- PuB:s ansvar
  - PuB får inte anlita annan PuB utan PuA:s skriftliga förhandsgodkännande.
  - PuB/PuB:s AT får bara utföra behandling av PU på PuA:s instruktioner/enligt tvingande rätt.
  - Om PuB1 anlitar PuB2
    - **Underbiträdesavtal**
    - PuB1 fullt ansvarig mot PuA om PuB2 inte sköter
  - Underbiträdesavtal
    - Ska vara skriftligt, elektroniskt ok
    - Ska ålägga PuB2 samma skyldigheter som gäller för PuB mot PuA
  - PuB: 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
  - En bedömning kan inkl. liknande behandlingar
- Konsultera ev. DSO
- Konsultera de registrerade/företrädare, om lämpligt
- 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