GDPR och molnet

Konferens SUNET Inkubator den 16 maj 2017

GDPR - Dataskyddsförordningen

- EU:s allmänna dataskyddsförordning ska börja tillämpas den 25 maj 2018.
- GDPR kommer att kompletteras av en nationell dataskyddslag och tillhörande förordning. (SOU 2017:39)
- Vissa myndigheter lyder dessutom under s.k. registerförfattningar. Dessa är fortfarande gällande och kan komma att justeras innehållsmässigt.

Varför integritetsskydd?

Bland annat för att:

- De registrerade, dvs. du och jag och alla andra vars uppgifter behandlas, ska veta vem som behandlar våra uppgifter, var de behandlas och för vilka syften.
- Vi ska kunna få upprättelse om våra personuppgifter behandlas på ett otillåtet sätt.
- Vi ska i regel inte behöva utsättas för kartläggning och övervakning.

Vad vill vi uppnå?

- Ansvarsskyldighet – den som ansvarar för en personuppgifts-behandling följer regelverket och kan visa att så sker.
- Säkerhet - den som ansvarar för en personuppgiftsbehandling ser till att tillräckliga tekniska och organisatoriska säkerhetsåtgärder vidtas för att skydda uppgifterna som behandlas.
- Transparens – den som ansvarar för en behandling, och den vars uppgifter behandlas, ska ha tillräcklig insyn i behandlingen för att kunna avgöra om den är tillåten eller inte.

ANSVARSSKYLDIGHET

Personuppgiftsansvarig

- Bestämmer *ändamål* och *medel*.
- Den som är personuppgiftsansvarig ska bl.a. se till att behandlingen av personuppgifter följer regelverket, att lämplig säkerhetsnivå skyddar uppgifterna som behandlas och att de registrerades rättigheter tillgodoses t.ex. information och rätt till registerutdrag, rättelse, radering, dataportabilitet etc.
- När en personuppgiftsansvarig t.ex. anlitar en molntjänstleverantör för att behandla personuppgifter måste den ansvarige se till att leverantören uppfyller ansvaret på samma sätt som den personuppgiftsansvarige skulle ha gjort.

Vilka uppgifter behandlas?

- Harmlösa
- Harmlösa men omfattande
- Integritetskänsliga t.ex. sekretessreglerade
- Känsliga t.ex. hälsa, politiska åsikter, medlemskap i fackförbund, religiös eller filosofisk övertygelse

- Ju känsligare uppgifter desto högre säkerhetskrav!

Hur får uppgifterna behandlas?

- Lagligt, korrekt, öppet
- Berättigade ändamål
- Uppgiftsminimering
- Lagringsminimering (OBS! undantag för arkiv, vetenskapliga eller historiska forskningsändamål eller statistik)
- Lämplig säkerhet

- Uppgifterna ska dessutom vara
  - adekvata och relevanta
  - korrekta och om nödvändigt uppdaterade

Lagligt stöd för behandling

- Vilket stöd finns för behandlingen?
  - Samtycke (särskilt begränsat i förhållande till myndigheter)
  - Avtal
  - Allmänt intresse (kräver författningsstöd, kollektivavtal eller beslut som har meddelats med stöd av författning)
  - Myndighetsutövning (kräver författningsstöd)
  - m.fl.

Några förändringar med GDPR

- Den personuppgiftsansvarige måste kunna VISA att GDPR efterlevs. Ställer krav på transparens och ordning och reda i den egna verksamheten. (Jfr hur vi arbetar med informationssäkerhet).
- Den registrerades rättigheter stärks t.ex. rätten till information, radering, dataportabilitet m.m. Dock ej absoluta rättigheter.
- Privacy by design och privacy by default.
- Rapportering av personuppgiftsincidenter till Datainspektionen (information till registrerade i vissa fall).
- Sanktionsavgifter.
- Myndigheter måste ha ett dataskyddsombud.

ANSVARSSKYLDIGHET OCH TRANSPARENS

Personuppgiftsbiträde

- Ett personuppgiftsbiträde är en aktör t.ex. en molntjänstleverantör, som behandlar personuppgifter på uppdrag av den personuppgiftsansvarige.
- Enligt GDPR kommer personuppgiftsbiträden få ett självständigt ansvar för t.ex. säkerhetsåtgärder.

Underleverantörer

- Om en leverantör (personuppgiftsbiträde) vill anlita underleverantörer måste detta föregås av ett skriftligt förhandstillstånd från den personuppgiftsansvarige.
- Har den personuppgiftsansvarige lämnat ett allmänt förhandstillstånd måste (huvud)leverantören informera om eventuella planer på att anlita ny underleverantör. Den personuppgiftsansvarige har rätt att göra invändningar.
- OBS! Underleverantörer är också personuppgiftsbiträden till den ansvarige. Samma krav gäller därför på avtal, villkor och regelefterlevnad.

Personuppgiftsbiträdesavtal

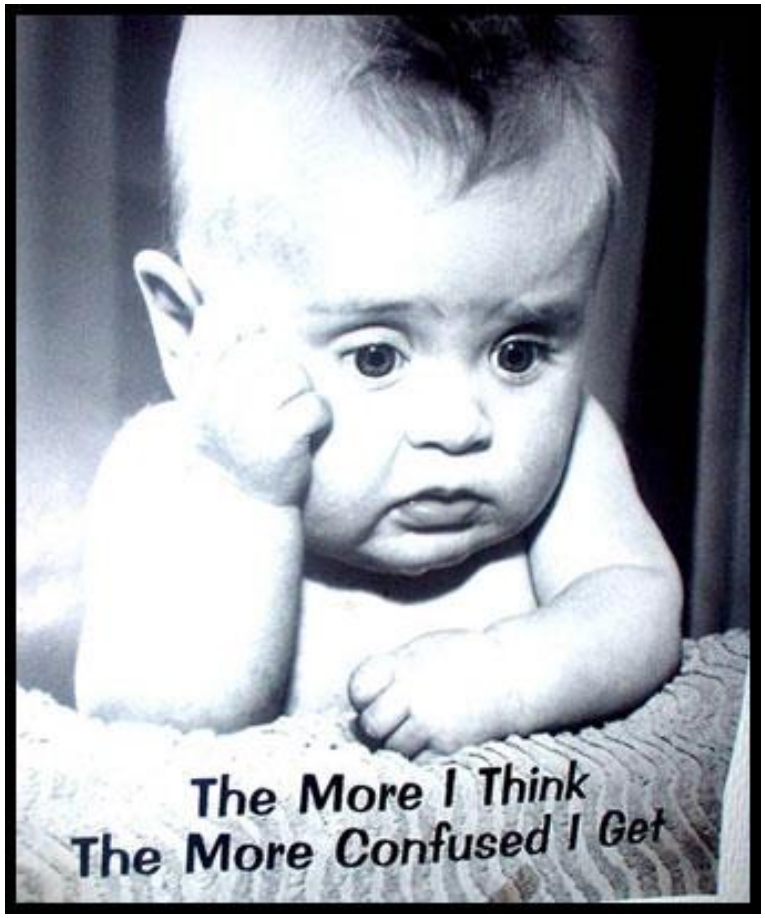
- Personuppgiftsbiträdesavtal måste ALLTID tecknas med en leverantör som behandlar personuppgifter. Utgå ifrån att molntjänstleverantörer kommer behandla personuppgifter.
- GDPR ställer högre krav på innehållet i biträdesavtal t.ex. ska det finnas instruktioner om
  - hur biträdet får behandla personuppgifter
  - överföring till tredje land är tillåtet
  - lämpliga tekniska och organisatoriska säkerhetsåtgärder
  - radering eller återlämning av uppgifter
  - rapportering av personuppgiftsincidenter
  - uppföljning/revision
  - m.m.

Överföring till tredje land

- Om den personuppgiftsansvarige eller biträdet överför personuppgifter till tredje land, dvs. ett land utanför EU/EES-området, krävs ett lagligt stöd eller annat rättsligt instrument t.ex. standardavtalsklausuler och/eller Privacy Shield (gäller enbart anslutna företag som är etablerade i USA).
- Molntjänstleverantörer använder/erbjuder ofta en mix av standardavtalsklausuler och Privacy Shield.

Vad innebär en global hantering av personuppgifter?

- Personuppgifter som överförs till ett annat land kommer att exponeras för rättsordningen i detta land. Det innebär t.ex. att det andra landets myndigheter har en potentiell möjlighet att få åtkomst till informationen ifråga.
- MEN, det är alltid tillåtet att överföra personuppgifter fritt inom EU/EES-området. För alla övriga länder måste man kontrollera att det antingen finns stöd i GDPR, standardavtalsklausuler, Privacy Shield eller annat.



HUR GÅR DET TILL I PRAKTIKEN?

Varför så komplicerat?

- Samma regelverk gäller vid anlitande av molntjänstleverantör som vid all annan typ av outsourcing.

MEN

- När molntjänstleverantörer anlitas kan fler bestämmelser aktualiseras om
  - uppgifterna behandlas utanför Sveriges gränser, och
  - ett stort antal underleverantörer anlitas.
  - Dessutom kan avtalstecknandet ta lång tid i anspråk och kräva särskild kompetens.

Tågordning för att anlita PuB

- Är den behandling av personuppgifter vi utför förenlig med det regelverk vi måste följa? (GDPR, registerförfattning, offentlighets- och sekretesslagen, arkivlagen etc.)
- Är den hantering som molntjänstleverantören utför förenlig med samma regelverk?
- Uppfyller villkoren i biträdesavtalet kraven i GDPR?
- Anlitar molntjänstleverantören underleverantörer?
- Överförs personuppgifter till tredje land?
- Riskanalys och rättslig analys
- Avtala!

Avtal

- Globala molntjänstleverantörer använder sig oftast av sina egna standardavtal.
- Personuppgiftsbiträdesavtal, standardavtalsklausuler m.m. ingår inte alltid automatiskt.
- Avtalsspråket är ofta engelska.
- Avtalspaketet kan vara omfattande och ibland är det svårt att få en överblick.
- Det kan vara svårt att avgöra vilken rättslig status ett avtalsdokument har t.ex. policy, white paper m.m.
- Vad gäller för länkar i elektroniska avtalsdokument?
- Om leverantören kräver att slutanvändarna (dvs. era medarbetare, studenter) ska acceptera användarvillkor måste ni fundera över vad det innebär.

Avtalsinnehållet

- Innehållet i avtalet ska stämmas av både mot regelverk och mot verksamhetens behov. Följande punkter kan vara av särskilt intresse.
  - Hur behandlar leverantören uppgifterna (egna ändamål i regel ej tillåtet)
  - Radering och/eller återlämnande av informationen (format, kostnader m.m.)
  - Stäm av mot GDPR:s krav på biträdesavtal
  - Ansvarsbegränsningar
  - Force majeure
  - Underleverantörer
  - Rätt till uppföljning/revision

Standarder m.m.

- Det kan vara en kvalitetsstämpel att en leverantör är ansluten till olika standarder (t.ex. ISO), certifieringar eller uppförandekoder.
- Man bör dock ha en uppfattning om vad anslutningen innebär. Är det självcertifiering eller tredjepart som bedömer? Vad åtar sig leverantören att uppfylla och efterleva genom att ansluta sig till standarden, certifieringen eller uppförandekoden?

Vad är viktigast?

- Samarbeta tvärfunktionellt – inköp, it, juridik, informationssäkerhet m.fl. Alla kompetenser är nödvändiga.
- Kravställ rätt! För att en leverantör ska kunna tillmötesgå era krav måste de veta vilka krav ni har.
- Tar er tid att gå igenom och förstå avtalen.
- Vad är reglerat, vad är inte reglerat?
- Hur tydliga är avtalsvillkoren?
- Uppfyller avtalsvillkoren det regelverk ni måste följa?

- Förhandla alltid om avtalsvillkoren! (Ja det går, även med de allra största leverantörerna)

Tips på vägen

På Datainspektionens webbplats finns en sida om molntjänster och personuppgifter. Där hittar man vägledningar, information om Privacy Shield, länk till Pensionsmyndighetens rapport Molntjänster i staten och mycket mer.

http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/molntjanster/

Tack!