Klientbriefing GDPR – del 1 av 4

Den allmänna dataskyddsförordningen[1], i dagligt tal benämnd **GDPR**, reglerar hur personuppgifter får behandlas. GDPR ska tillämpas i alla EU:s medlemsstater från och med den 25 maj 2018. GDPR kommer att gälla som lag i Sverige och medför att den nuvarande svenska personuppgiftslagen (**PUL**) från 1998 samtidigt upphör att gälla.

Det övergripande syftet med GDPR är att modernisera och harmonisera personuppgiftslagstiftningen inom EU samt, särskilt mot bakgrund av den tekniska utvecklingen som skett de senaste 20 åren, förstärka skyddet för de enskildas personuppgifter.

Denna klientbriefing om GDPR är den första av fyra delar och innehåller

- en beskrivning av de huvudsakliga nyheterna i GDPR, samt
- en checklista till hjälp för att inleda arbetet med att säkerställa efterlevnaden av GDPR.

De huvudsakliga nyheterna i GDPR

Stärkta rättigheter för de registrerade
GDPR stärker de *registrerades* (de fysiska personer som är föremål för personuppgiftsbehandlingen) rättigheter i förhållande till de *personuppgiftsansvariga* (de som behandlar personuppgifter).

De registrerade har med vissa begränsningar bl.a.

- rätt till *tillgång* (att få veta om personuppgifter som rör denne behandlas),
- rätt till *rättelse* (att få felaktiga personuppgifter rättade),
- rätt till *radering* (att få personuppgifter raderade och därigenom kunna bli ”bortglömd”),
- rätt till *begränsning* (att kräva att personuppgifts-behandlingen avbryts under viss tid),
- rätt att göra *invändningar* (att kräva att personuppgifter inte behandlas), samt
- rätt till *dataportabilitet* (att få ut och överföra personuppgifterna till annan, se vidare nedan).

Administrativa sanktioner
Om en personuppgiftsansvarig eller ett personuppgiftsbiträde inte följer GDPR kan tillsynsmyndigheten (i Sverige är Data-inspektionen tillsynsmyndighet) ytterst utdöma administrativa sanktionsavgifter på upp till 20 miljoner euro eller på upp till 4 procent av årsomsättningen.

Både personuppgiftsansvariga och personuppgiftsbiträden kan bli föremål för sådana sanktioner. Storleken på sanktionerna ska bestämmas bl.a. utifrån hur allvarlig överträdelsen är, om den skett avsiktligt eller inte och vilka åtgärder som vidtagits för att begränsa skadan.

Anmälan av personuppgiftsincidenter
Enligt GDPR ska *personuppgiftsincidenter* anmälas till tillsynsmyndigheten. En personuppgiftsincident är en säkerhetsincident som leder till att en obehörig får åtkomst till de personuppgifter som behandlas eller att personuppgifter oavsiktligt förstörs, förändras, etc. Så kan exempelvis vara fallet vid dataintrång eller IT-haverier.

Om en personuppgiftsincident inträffar ska den personuppgiftsansvarige utan onödigt dröjsmål (typiskt sett inom 72 timmar) anmäla incidenten till tillsynsmyndigheten och beskriva bl.a. vad som hänt, hur många som berörs och vilka åtgärder som har vidtagits eller ska vidtas för att hantera situationen. Om incidenten är allvarlig kan det uppstå en skyldighet att även underrätta de registrerade.

Konsekvensbedömning
Om en behandling av personuppgifter kan leda till särskilda risker för de registrerade måste konsekvenserna av en sådan behandling utredas i förväg genom en *konsekvensbedömning*. Kravet aktualiseras bl.a. om känsliga personuppgifter (exempelvis uppgifter om hälsa eller medlemskap i fack-förening) ska behandlas i stor omfattning.

Om konsekvensbedömningen visar att behandlingen leder till hög risk för de registrerade om åtgärder inte vidtas för att minska risken ska samråd med tillsynsmyndigheten ske innan personuppgiftsbehandlingen påbörjas.

Krav på dataportabilitet
Om personuppgifter behandlas med stöd av samtycke eller för att kunna uppfylla ett avtal med den registrerade har den registrerade i vissa fall en rätt till *dataportabilitet*. Det innebär att han eller hon har rätt att få ut de personuppgifter som lämnats och som rör denne, för att kunna föra över uppgifterna till en annan personuppgiftsansvarig. Uppgifterna ska utlämnas i ett strukturerat, allmänt använt och maskinläsbart format.

Inbyggt dataskydd och dataskydd som standard
Mot bakgrund av de senaste årens tekniska utveckling ställer GDPR upp krav på *inbyggt dataskydd* (privacy by design) och *dataskydd som standard* (privacy by default). I korthet innebär detta att verksamhetsutövare måste ta hänsyn till skyldigheten

[1] Förordning (EU) nr 2016/679, www.eur-lex.europa.eu/legal-content/SV/TXT/?uri=celex%3A32016R0679

att skydda personuppgifter när IT-system konstrueras samt att säkerställa att personuppgifter inte behandlas i onödan.

Som exempel kan nämnas att IT-systemen ska vara konstruerade så att kunduppgifter inte sprids inom ett företag till fler personer än vad som är nödvändigt och att användare av sociala medier behöver göra ett medvetet val för att andra personer ska kunna ta del av deras personuppgifter.

Dataskyddsombud
Enligt GDPR ska ett *dataskyddsombud* utses i vissa situationer, bl.a. om personuppgifter behandlas i stor omfattning och verksamheten kräver regelbunden och systematisk övervakning av de registrerade (det kan bl.a. vara fallet när kunder genomgår kreditprövningar eller är föremål för kundkännedomsåtgärder).

Ett dataskyddsombud ska utses på grundval av yrkesmässiga kvalifikationer och, då särskilt sakkunskap om lagstiftning och praxis avseende dataskydd samt förmågan att fullgöra de uppgifter som åligger denne enligt GDPR.

I dataskyddsombudets uppgifter ingår att informera och ge råd inom den egna organisationen avseende vilka skyldigheter som gäller enligt GDPR och fungera som kontaktpunkt för tillsynsmyndigheten.

Ett dataskyddsombud har inget personligt ansvar för det fall den personuppgiftsansvarige eller personuppgiftsbiträdet inte uppfyller kraven i GDPR. Dataskyddsombudets kontaktuppgifter ska anmälas till tillsynsmyndigheten.

Checklista GDPR

Nedanstående tio frågor kan vara till hjälp för att påbörja arbetet med att kartlägga den personuppgiftsbehandling som genomförs i verksamheten samt utreda om kraven i GDPR efterlevs redan i dag eller om ytterligare åtgärder måste vidtas. Checklistan tar upp många av de viktigaste frågorna men ska inte betraktas som uttömmande.

1. Behandlas personuppgifter?
Med *personuppgifter* avses något förenklat all information som direkt eller indirekt kan hänföras till en fysisk person i livet. Det kan exempelvis vara namn och adress eller personnummer men även så kallade onlineidentifikatorer såsom IP-adresser och cookies etc. Uppgifter som inte går att hänföra till någon fysisk person, exempelvis helt anonymiserade uppgifter, utgör inte personuppgifter.

Med *behandling* avses i princip alla slags åtgärder som vidtas med personuppgifter, såsom insamling, lagring, kopiering, överföring etc.

- Den första frågan är om, och i så fall vilka, personuppgifter som behandlas i verksamheten. Endast om personuppgifter behandlas är GDPR tillämplig.

2. Vem bestämmer varför och hur personuppgifterna ska behandlas?
Den som behandlar personuppgifter kan vara antingen *personuppgiftsansvarig* eller *personuppgiftsbiträde*. Personuppgiftsansvarig är den som bestämmer ändamålen (varför) och medlen (hur) för personuppgiftsbehandlingen, och personuppgiftsbiträde är den som behandlar personuppgifter för annans räkning enligt dennes instruktioner.

En personuppgiftsansvarig och ett personuppgiftsbiträde kan vara såväl fysiska som juridiska personer men typiskt sett är den juridiska personen ansvarig respektive biträde om behandlingen sker inom ett bolag eller annan juridisk person.

- Den andra frågan är om personuppgifter behandlas i egenskap av personuppgiftsansvarig eller personuppgiftsbiträde. De flesta skyldigheter i GDPR gäller endast för den personuppgiftsansvarige. Ett personuppgiftsbiträdes huvudsakliga skyldighet är att behandla personuppgifter endast i enlighet med de instruktioner som den personuppgiftsansvarige lämnar.

3. Finns det personuppgiftsbiträdesavtal?
Om en personuppgiftsansvarig använder ett personuppgiftsbiträde för behandling av personuppgifter ska det finnas ett avtal mellan parterna som reglerar behandlingen. GDPR ställer upp omfattande krav på vad ett sådant personuppgiftsbiträdesavtal ska innehålla.

Avtalet ska bl.a. reglera *vad* som ska behandlas, hur *länge* och för vilket *ändamål*. Avtalet ska även ålägga personuppgiftsbiträdet att vidta ett antal åtgärder, såsom lämpliga säkerhetsåtgärder för att skydda personuppgifterna och säkerställa att alla personer som behandlar uppgifterna omfattas av tystnadsplikt.

- Den tredje frågan är om personuppgiftsbiträdesavtal finns och om dessa uppfyller samtliga de krav som GDPR uppställer.

4. På vilken grund behandlas personuppgifter?
En personuppgiftsansvarig får endast behandla personuppgifter med stöd av en *uttrycklig grund*. De grunder för behandling av personuppgifter som anges i GDPR är i princip överensstämmande med de grunder som återfinns i PUL.

Grunden för behandling av personuppgifter utgörs många gånger av *samtycke* från den registrerade. En annan grund kan vara att behandlingen av personuppgifter är nödvändig för att fullgöra ett *avtal* med den registrerade eller att uppfylla en *rättslig skyldighet*.

- Den fjärde frågan är på vilken grund personuppgifterna behandlas.

5. Behandlas känsliga personuppgifter?

Vissa personuppgifter anses vara mer känsliga än andra. Som utgångspunkt är det enligt GDPR förbjudet att behandla personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening. Det är även förbjudet att behandla genetiska uppgifter, biometriska uppgifter, uppgifter om hälsa samt uppgifter om sexualliv eller sexuell läggning. Behandling som är nödvändig för vissa särskilda ändamål kan utgöra undantag från förbudet.

- Den femte frågan är om känsliga personuppgifter behandlas och i sådant fall vilket undantag som är tillämpligt för att sådan behandling ska anses tillåten.

6. Vilken information lämnas till de registrerade?

Enligt GDPR krävs att information lämnas till de registrerade i vissa situationer. Om personuppgifter samlas in från den registrerade eller erhålls från en annan källa ska den registrerade typiskt sett underrättas om vad syftet med behandlingen är och vilken grund som föreligger för behandlingen.

- Den sjätte frågan är vilken information de registrerade erhåller om personuppgiftsbehandlingen och om informationen omfattar alla uppgifter som GDPR kräver.

7. Uppfyller IT-systemen kraven på dataskydd?

GDPR ställer upp krav på *inbyggt dataskydd* (privacy by design) och *dataskydd som standard* (privacy by default). Det innebär bl.a. att lämpliga tekniska och organisatoriska åtgärder ska vidtas för att skydda personuppgifterna som behandlas. Det kan exempelvis vara fråga om att IT-systemen är konstruerade så att kunduppgifter inte sprids inom ett företag till fler personer än vad som är nödvändigt.

- Den sjunde frågan är om kraven på inbyggt dataskydd och dataskydd som standard uppfylls.

8. Har IT-systemen stöd för att tillgodose rätten till dataportabilitet?

Om personuppgifter behandlas med stöd av samtycke eller för att kunna uppfylla ett avtal med den registrerade har den registrerade en rätt till *dataportabilitet*, dvs. rätt att få ut sina personuppgifter och överföra dem till en annan personuppgifts-ansvarig. Uppgifterna ska utlämnas i ett strukturerat, allmänt använt och maskinläsbart format.

- Den åttonde frågan är om IT-systemen har stöd för att tillgodose den registrerades rätt till dataportabilitet.

9. Finns det integritetsrisker med behandlingen av personuppgifter?

En konsekvensbedömning måste genomföras om behandling av personuppgifter kan leda till särskilda risker för de registrerade. Det kan vara fallet bl.a. om känsliga person-uppgifter ska behandlas i stor omfattning. I sådant fall måste bedömas vilka risker som är förenade med behandlingen och vilka åtgärder som kan vidtas för att hantera riskerna. Vidare kan samråd med tillsynsmyndigheten krävas innan person-uppgiftsbehandlingen inleds.

- Den nionde frågan är om det finns särskilda risker med personuppgiftsbehandlingen och, i sådant fall, om en konsekvensbedömning har genomförts.

10. Ska ett dataskyddsombud utses?

Enligt GDPR ska att ett dataskyddsombud utses i vissa situationer, bl.a. om personuppgifter behandlas i stor omfattning och verksamheten kräver regelbunden och systematisk övervakning av de registrerade (det kan bl.a. vara fallet när ett större antal kunder genomgår kreditprövningar eller är föremål för kundkännedomsåtgärder).

- Den tionde frågan är om ett dataskyddsombud måste utses och i sådant fall om det har skett. Dataskydds-ombudets kontaktuppgifter ska anmälas till tillsynsmyndigheten.

Kontakt

Vid eventuella frågor eller för mer information, vänligen kontakta:

Mats Hugoson
Partner/Advokat
Gernandt & Danielsson Advokatbyrå KB
Dir +46 8 670 66 43
Mob +46 734 15 26 43
mats.hugoson@gda.se

Niclas Rockborn
Partner/Advokat
Gernandt & Danielsson Advokatbyrå KB
Dir +46 8 670 66 46
Mob +46 734 15 26 46
niclas.rockborn@gda.se

Olle Asplund
Senior Associate/Advokat
Gernandt & Danielsson Advokatbyrå KB
Dir +46 8 670 64 61
Mob +46 734 15 24 61
olle.asplund@gda.se

Erik Sandgren
Senior Associate/Advokat
Gernandt & Danielsson Advokatbyrå KB
Dir +46 8 670 64 46
Mob +46 734 15 24 46
erik.sandgren@gda.se