

Klientbriefing GDPR – del 4 av 4

Den allmänna dataskyddsförordningen¹, 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") 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 sista av fyra delar och behandlar:

- rätten till *dataportabilitet*,
- rätten till *radering* och att bli "bortglömd",
- rätten att *begränsa behandling*,
- rätten att göra *invändningar* samt frågor om *profilering* och *automatiserat beslutsfattande*, samt
- när ett *personuppgiftsbiträdesavtal* måste ingås och vad det ska innehålla.

Dataportabilitet

En registrerad ska ha rätt att få ut de personuppgifter som rör honom eller henne i ett strukturerat, allmänt använt och maskinläsbart format. Rättigheten gäller dock endast sådana personuppgifter som denne tillhandahållit den personuppgiftsansvarige. För att rättigheten ska kunna göras gällande krävs även att behandlingen grundar sig på den registrerades *samtycke* eller på ett *avtal* med den registrerade (dvs. sker behandlingen exempelvis med stöd av en *intresseavvägning* finns ingen skyldighet att lämna ut uppgifterna, observera dock att ett *registerutdrag* normalt sett alltid behöver tillhandahållas). Därtill krävs att behandlingen är automatiserad för att rättigheten ska kunna påkallas.

XML, JSON och CSV är exempel på format som kan användas för att uppfylla kravet på tillhandahållande i ett strukturerat, allmänt använt och maskinläsbart format. Den registrerade ska även ha rätt att överföra uppgifterna direkt till en annan personuppgiftsansvarig, när detta är tekniskt möjligt.

Vid utövandet av denna rättighet är det viktigt att inte andras rättigheter och friheter påverkas på ett ogynnsamt sätt. Det är således viktigt att den personuppgiftsansvarige inte lämnar ut

uppgifter som även rör någon annan än den registrerade, i samband med att rätten till dataportabilitet utövas.

Artikel 29-gruppen har tagit fram riktlinjer om rätten till dataportabilitet som närmare behandlar bl.a. när dataportabilitet ska tillämpas och hur uppgifterna ska tillhandahållas.²

Rätten till radering och att bli "bortglömd"

Radering

En registrerad ska ha rätt att utan onödigt dröjsmål få sina personuppgifter *raderade*. Detta gäller dock endast i vissa situationer, nämligen om

- personuppgifterna inte längre är nödvändiga för det ändamål för vilket de samlats in,
- den registrerade återkallar sitt samtycke och det inte finns någon annan rättslig grund för behandlingen,
- den registrerade har invänt mot behandlingen och det visar sig att det saknas berättigade skäl för behandlingen,
- personuppgifterna har behandlats på ett olagligt sätt (exempelvis utan stöd av en rättslig grund),
- personuppgifterna måste raderas enligt EU- eller nationell rätt som den personuppgiftsansvarige omfattas av, eller
- personuppgifterna avser barn och har samlats in i samband med att barnet skapar en profil i ett socialt nätverk eller liknande (i samband med erbjudande av informationssamhällets tjänster).

Att bli "bortglömd"

Om den personuppgiftsansvarige har *offentliggjort* personuppgifterna (exempelvis på ett socialt nätverk) och är skyldig att radera dem enligt någon av punkterna ovan, ska den personuppgiftsansvarige *dels* själv radera uppgifterna, *dels* vidta alla rimliga åtgärder för att se till att eventuella länkar till uppgifterna eller kopior av personuppgifterna som andra personuppgiftsansvariga har också raderas.

Undantag

Det finns vissa undantag från rätten till radering och rätten att bli bortglömd. Den personuppgiftsansvarige är bl.a. inte skyldig att genomföra sådana åtgärder om behandlingen är nödvändig för att tillgodose andra viktiga rättigheter som till exempel rätten till yttrande- och informationsfrihet, för att uppfylla en rättslig förpliktelse, utföra en uppgift av allmänt intresse eller för att kunna fastställa, göra gällande eller försvara rättsliga anspråk.

¹ Förordning (EU) nr 2016/679, <http://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679&rid=1>.

² <https://www.datainspektionen.se/globalassets/dokument/riktlinjer-om-ratten-till-dataportabilitet.pdf>

Rätten att begränsa behandling

Den registrerade har rätt att kräva att en personuppgiftsbehandling *begränsas*, exempelvis om den registrerade har invänt att personuppgifterna är felaktiga och den personuppgiftsansvarige behöver viss tid för att kontrollera om uppgifterna är korrekta eller inte.

Begränsningen av personuppgiftsbehandlingen kan exempelvis ske genom att man tillfälligt flyttar de aktuella uppgifterna till ett annat databehandlingssystem, gör uppgifterna otillgängliga för användare eller tillfälligt avlägsnar offentliggjorda uppgifter från en webbplats. I automatiserade register bör begränsningen av behandlingen i princip ske med tekniska medel på ett sådant sätt att personuppgifterna inte blir föremål för ytterligare behandling och inte kan ändras.

En registrerad som har fått behandling begränsad ska underrättas av den personuppgiftsansvarige innan begränsningen av behandlingen upphör.

Rätten att göra invändningar m.m.

Invändningar

En registrerad har rätt att när som helst göra invändningar mot en behandling av dennes personuppgifter. Rätten att invända gäller dock endast när personuppgifter behandlas för att utföra en uppgift av *allmänt intresse*, som ett led i *myndighetsutövning* eller med stöd av en *intresseavvägning*.

Om rättigheten utövas får den personuppgiftsansvarige endast fortsätta att behandla uppgifterna om det går att visa att det finns *tvingande berättigade skäl* till att uppgifterna måste behandlas och dessa väger tyngre än den enskildes intressen, rättigheter och friheter, eller om behandlingen sker för fastställande, utövande eller försvar av rättsliga anspråk.

Om personuppgifterna behandlas för *direkt marknadsföring* ska dock den registrerade ha rätt att när som helst invända mot behandling för sådant syfte. I sådant fall får personuppgifterna inte längre behandlas för sådana ändamål.

Automatiserat beslutsfattande

En registrerad har rätt att inte bli föremål för ett beslut som enbart grundas på någon form av *automatiserat beslutsfattande* om beslutet kan ha rättsliga följder för honom eller henne eller påverka denne på liknande sätt i betydande grad. Exempel på sådant beslutsfattande är kreditansökningar, ansökningar om försäkring eller rekrytering via internet som behandlas på ett helt automatiserat sätt (utan mänsklig inverkan).

Automatiserat beslutsfattande är dock tillåtet om den registrerade har lämnat sitt samtycke till det, eller om det är nödvändigt för ingående eller fullgörande av ett avtal mellan den registrerade och den personuppgiftsansvarige. Det kan även vara tillåtet enligt särskild lagstiftning. Den personuppgiftsansvarige måste informera de registrerade om automatiserat beslutsfattande används.

Profilerings

Med *profilerings* avses varje form av automatisk behandling av personuppgifter som består i att personuppgifterna används för att bedöma vissa personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga denna fysiska persons arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar.

Automatiserade beslut kan fattas med eller utan profilering. Omvänt kan profilering användas utan att det leder till ett automatiserat beslut. Profilering i sig är inte otillåtet men kan innebära risker för enskildas rättigheter och friheter som kräver lämpliga skyddsåtgärder. Den personuppgiftsansvarige måste informera de registrerade om förekomsten av profilering.

Krav på personuppgiftsbiträdesavtal

Personuppgiftsbiträde

Med *personuppgiftsbiträde* avses en fysisk eller juridisk person, en offentlig myndighet, en institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning. Det kan vara svårt att bedöma om en behandling av personuppgifter sker för egen eller annans räkning. För att fastställa vem som är ansvarig för behandlingen måste det klargöras vem som bestämmer *ändamålet* (varför) med behandlingen och genom vilka *medel* (hur) behandlingen ska utföras. Det kan även uppstå situationer där man bedömer att exempelvis två företag är *gemensamt* personuppgiftsansvariga eller är varandras biträden men för olika behandlingar.

Personuppgiftsbiträdesavtal

Personuppgiftsbiträdets skyldigheter gentemot den personuppgiftsansvarige måste regleras i ett avtal eller annan rättsakt där föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade, samt den personuppgiftsansvariges skyldigheter och rättigheter anges.

I ett sådant *personuppgiftsbiträdesavtal* ska föreskrivas att personuppgiftsbiträdet

- endast får behandla personuppgifter på dokumenterade instruktioner från den personuppgiftsansvarige,
- säkerställer att de som behandlar uppgifterna iakttar konfidentialitet eller omfattas av tystnadsplikt,
- vidtar nödvändiga åtgärder för att skydda personuppgifterna,
- i den mån som är möjligt, ska hjälpa den ansvarige med lämpliga tekniska och organisatoriska åtgärder för att den ansvarige ska kunna fullgöra sina skyldigheter gentemot de registrerade,
- ska bistå den ansvarige vid personuppgiftsincidenter, utlämnande av information till de registrerade och genomförande av konsekvensbedömningar m.m.,
- ska radera eller lämna tillbaka personuppgifterna när behandlingen avslutas, samt

- ska ge den ansvarige tillgång till all information som krävs för att visa att biträdet uppfyller sina skyldigheter samt möjliggöra och bidra till granskningar och inspektioner.

I avtalet ska även fastställas att ett personuppgiftsbiträde inte får anlita ett annat biträde (*underbiträde*) utan att på förhand få ett skriftligt tillstånd av den personuppgiftsansvarige. Tillståndet kan vara *särskilt* eller *allmänt*. Ett särskilt tillstånd omfattar ett visst specifikt underbiträde, medan ett allmänt tillstånd möjliggör för personuppgiftsbiträdet att endast informera den ansvarige om planerna på att anlita ett underbiträde, så den ansvarige på så vis ges möjlighet att komma med eventuella invändningar.

Skadestånd mm

En person som har lidit skada på grund av att hans eller hennes personuppgifter har behandlats i strid med GDPR kan ha rätt till skadestånd. I en sådan situation kan den registrerade kräva ersättning av den personuppgiftsansvarige som medverkat vid behandlingen. Även ett personuppgiftsbiträde kan dock bli skadeståndsskyldigt om behandlingen som denne

utfört skett i strid med de instruktioner som den ansvarige lämnat. Det är därför viktigt att personuppgiftsbiträdet säkerställer att det alltid finns tydliga instruktioner från den ansvarige som omfattar den personuppgiftsbehandling som utförs.

Den som lidit skada har i princip rätt att få ersättning för hela skadan av antingen den personuppgiftsansvarige eller personuppgiftsbiträdet. Dessa får sedan i sin tur reglera ansvaret sinsemellan.

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