Klientbriefing GDPR – del 3 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**”) 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 tredje av fyra delar och behandlar:

- den lagliga grunden *samtycke* för behandling av personuppgifter,
- övriga *lagliga grunder* för behandling av personuppgifter,
- skyldigheten att utse ett *dataskyddsombud*, samt
- *sanktioner* när personuppgifter behandlas i strid med GDPR.

Samtycke som laglig grund för behandling av personuppgifter

Samtycke enligt GDPR

För att behandling av personuppgifter ska vara tillåten krävs att det finns en *laglig grund* för behandlingen. Det finns olika lagliga grunder, en av dem utgörs av att den registrerade har lämnat sitt *samtycke* till att dennes personuppgifter behandlas. Samtycke enligt GDPR ska vara en viljeyttring som är

- frivillig,
- specifik, och
- tydlig.

Genom samtycket ska den registrerade – efter att ha fått information om behandlingen – godta att personuppgifterna i fråga behandlas. Samtycket ska lämnas genom en ”entydig bekräftande handling”.

Att samtycket måste vara *frivilligt* innebär att den registrerade ska ha en valmöjlighet att vägra lämna sitt samtycke till behandlingen av sina personuppgifter. Ett samtycke lämnas således inte frivilligt om den registrerade inte kan avstå från att lämna eller kan ta tillbaka sitt samtycke. Exempelvis ska den registrerade kunna återkalla sitt samtycke utan att det uppstår några kostnader för den registrerade. Vidare kan nämnas att ett samtycke inte anses vara frivilligt om det uppställs som villkor för genomförandet av ett avtal att ett samtycke till behandling av personuppgifter lämnas, trots att sådan behandling av personuppgifter inte är nödvändig för att genomföra avtalet.

Vid bedömningen av om ett samtycke är frivilligt ska hänsyn även tas till om det råder en obalans mellan den registrerade och den personuppgiftsansvarige (den som behandlar personuppgifterna). När det föreligger stor ojämlikhet mellan den registrerade och den personuppgiftsansvarige, exempelvis när den personuppgiftsansvarige är en myndighet eller en arbetsgivare, kan det vara svårt att säkerställa att samtycket är frivilligt. I en sådan situation kan behandlingen eventuellt stödjas på någon annan laglig grund.

För att det ska föreligga ett giltigt samtycke enligt GDPR måste det även vara *specifikt*. Det innebär att den registrerade måste lämna sitt samtycke till att personuppgifter behandlas för *ett eller flera specifika ändamål*. Om den personuppgiftsansvarige behandlar personuppgifter med stöd av samtycke och önskar behandla personuppgifterna för ett nytt ändamål måste den personuppgiftsansvarige inhämta ett nytt samtycke från den registrerade.

Kravet på att samtycket ska vara *specifikt* medför även att den registrerade måste känna till ändamålet med behandlingen av personuppgifterna. Att informera den registrerade innan samtycke lämnas är nödvändigt för att den registrerade ska kunna fatta beslut och förstå vad de samtycker till. Utöver ändamålen med behandlingen anses att den registrerade behöver få information om bland annat den personuppgiftsansvariges identitet, vilka personuppgifter som kommer att behandlas och möjligheten att återkalla ett lämnat samtycke.

Slutligen måste samtycket vara *tydligt*. I detta krav ligger att ett samtycke kräver en ”entydig bekräftande handling”. Samtycket kan lämnas genom en skriftlig, inklusive elektronisk, eller muntlig förklaring. Det kan exempelvis inbegripa att den registrerade kryssar i en ruta (checkbox) på en internetsida. Samtycke får inte lämnas genom ”tystnad” (dvs. att den registrerade är inaktiv) eller på förhand ikryssade rutor. Det måste vara tydligt att den registrerade samtycker till den specifika behandlingen. Samtycke kan endast i undantagsfall lämnas genom konkludent handlande.

Den personuppgiftsansvarige måste också kunna *visa* att den registrerade har samtyckt till behandlingen av personuppgifter. Bevisbördan för att ett giltigt samtycke föreligger åvilar således den personuppgiftsansvarige. Skyldigheten föreligger under hela den period som personuppgifterna behandlas med stöd av samtycke. GDPR föreskriver inte närmare hur detta ska gå till. Det kan dock vara lämpligt att den personuppgiftsansvarige

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

dokumenterar de samtycken som erhållits, genom exempelvis ett register. Det ska vara lika lätt att återkalla ett samtycke som det var att lämna det. Det innebär att den registrerade ska ha rätt att när som helst återkalla sitt samtycke.

Uttryckligt samtycke
GDPR skiljer mellan *samtycke* (med vilket avses ett uttalande eller en ”entydig bekräftande handling”) och *uttryckligt samtycke*. Ett uttryckligt samtycke krävs exempelvis när särskilda kategorier av personuppgifter (känsliga personuppgifter) ska behandlas, såsom uppgifter om hälsa eller politiska åsikter. För att säkerställa att ett samtycke är uttryckligt kan den personuppgiftsansvarige se till att den registrerade undertecknar en skriftlig bekräftelse. Ett uttryckligt samtycke kan dock inhämtas på andra sätt, genom exempelvis en elektronisk signatur eller ett mejl från den registrerade.

Det är inte helt tydligt var gränsen går mellan samtycke och uttryckligt samtycke, men ett uttryckligt samtycke måste komma till uttryck på ett särskilt tydligt sätt. Ett uttryckligt samtycke kan inte lämnas genom ett konkludent handlande.

Samtycke från barn
En nyhet i GDPR är att ett stärkt skydd för barns personuppgifter införs då barns personuppgifter anses vara särskilt skyddsvärda. Det förstärkta skyddet gäller när ”informationssamhällets tjänster” erbjuds till ett barn, med vilket avses sådana tjänster som normalt utförs mot ersättning på elektronisk väg. Typiskt sett är det fråga om onlinetjänster, såsom sociala nätverk. När sådana tjänster erbjuds måste vårdnadshavarens samtycke inhämtas för att barnets personuppgifter ska få behandlas. Enligt GDPR gäller det när barnet är under 16 år, men medlemsstaterna har möjlighet att bestämma en lägre åldersgräns. I Sverige har det föreslagits att ett barn som är minst 13 år ska kunna lämna sitt samtycke vid denna typ av behandling. I de fall samtycke krävs från vårdnadshavaren måste den personuppgiftsansvarige kunna visa att vårdnadshavarens samtycke har lämnats.

Kravet på att ett samtycke måste vara *informerat* gäller också när samtycke ska inhämtas från ett barn. När information riktas till ett barn föreskriver GDPR att det är särskilt viktigt att den information som lämnas utformas på ett tydligt och enkelt språk som barnet lätt kan förstå.

Andra lagliga grunder för behandling av personuppgifter

Fullgörande av avtal
Behandling av personuppgifter är även tillåten när det är nödvändigt *dels* för att fullgöra ett avtal med den registrerade, *dels* för att på den registrerades begäran vidta åtgärder innan ett avtal träffas.

I vissa fall kan fullgörandet av ett avtal med en registrerad göra det nödvändigt att behandla uppgifter om någon annan person, d.v.s. en tredje part. Exempelvis kan ett försäkringsbolag behöva registrera uppgifter om den försäkrades förmånstagare. Ett *avtal* kan dock inte berättiga en personuppgiftsansvarig att behandla uppgifter om andra än avtalsparten. Behandlingen av personuppgifter om en tredje part (såsom den försäkrades förmånstagare) kan dock vara tillåten med stöd av någon annan rättslig grund, såsom intresseavvägning (berättigat intresse).

Intresseavvägning (berättigat intresse)
Personuppgifter får behandlas med stöd av en intresseavvägning. För att en sådan behandling ska vara tillåten krävs att den är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen och att dessa intressen väger tyngre än den registrerades intresse av skydd för sina personuppgifter.

Det krävs en noggrann bedömning för att fastställa om ett berättigat intresse föreligger. Bedömningen ska särskilt ta hänsyn till om den registrerade, när personuppgifterna inhämtas, rimligen kan förvänta sig att behandling för visst ändamål kan komma att ske. Om personuppgifter behandlas under sådana omständigheter där den registrerade inte rimligen kan förvänta sig den avsedda behandlingen, anses den registrerades skydd för sina personuppgifter typiskt sett väga tyngre.

Personuppgiftsansvariga som ingår i en koncern kan ha ett berättigat intresse att överföra personuppgifter inom koncernen för interna administrativa ändamål, bland annat för behandling av kunders eller anställdas uppgifter. Det är inte heller ovanligt att det i koncerner finns ett bolag som lagrar data centralt, s.k. data warehouse, och att övriga koncernbolag via sina system hämtar in uppgifter därifrån för sin verksamhet. Även behandling av personuppgifter för direktmarknadsföring kan betraktas som ett berättigat intresse. Det är inte tillåtet för myndigheter att stödja behandling av personuppgifter på en intresseavvägning när de fullgör sina uppgifter.

Rättslig förpliktelse
Personuppgifter får behandlas om det är nödvändigt för att uppfylla en *rättslig förpliktelse*. Den rättsliga förpliktelsen ska åvila den personuppgiftsansvarige och följa av EU-rätt eller nationell rätt. Som exempel på rättslig förpliktelse kan nämnas skyldigheten för en arbetsgivare att lämna kontrolluppgifter för anställdas inkomster och förmåner samt skyldigheten som gäller för vissa bolag att inhämta kundkännedomsuppgifter.

Skydd för grundläggande intressen
Det är tillåtet att behandla personuppgifter om det är nödvändigt för att skydda intressen som är av *grundläggande betydelse* för den registrerade eller för en annan fysisk person. Typiskt sett ska det vara frågan om sådana intressen som är av avgörande betydelse för den registrerades eller någon annan persons liv. I sådana fall kan behandling exempelvis vara nödvändig av humanitära skäl, såsom att övervaka epidemier och deras spridning i humanitära nödsituationer.

GDPR stadgar dock att behandling av personuppgifter på grundval av en annan fysisk persons grundläggande intressen i princip endast bör äga rum om behandlingen inte uppenbart kan ske med stöd en annan rättslig grund.

Allmänt intresse och myndighetsutövning
Behandling av personuppgifter är tillåten om den är nödvändig för att utföra en *uppgift av allmänt intresse*. Uppgiften bör ha en grund i EU-rätt eller nationell rätt där behandlingens syfte fastställs. Som exempel på sådan behandling kan nämnas kreditupplysningsverksamhet och förande av offentliga fastighetsregister.

Behandling av personuppgifter är också tillåten om den är nödvändig som ett led i den personuppgiftsansvariges *myndighetsutövning*. Myndighetsutövningen ska grundas på EU-rätt eller nationell rätt. Myndighetsutövning är vanligtvis en uppgift för myndigheter, såsom domstolar och förvaltningsmyndigheter, men kan under vissa omständigheter utövas av bolag eller föreningar med stöd av lag.

Skyldigheten att utse ett dataskyddsombud

I PUL förekommer begreppet ”personuppgiftsombud”, vilket är en fysisk person vars uppgift är att självständigt se till att personuppgifter behandlas på ett korrekt och lagligt sätt. Det föreligger ingen absolut skyldighet enligt PUL att utse ett ”personuppgiftsombud”, utan det är ett frivilligt åtagande. En nyhet i GDPR är att det vid vissa givna omständigheter är *obligatoriskt* för en personuppgiftsansvarig och ett personuppgiftsbiträde (den som behandlar personuppgifter för den personuppgiftsansvariges räkning) att utse ett så kallat *dataskyddsombud*.

Skyldigheten att utse ett dataskyddsombud föreligger i vissa specifika situationer, exempelvis om *kärnverksamheten* består av behandling som kräver regelbunden och systematisk övervakning av de registrerade *i stor omfattning*. Den som vill får utse ett dataskyddsombud även när en uttrycklig skyldighet enligt GDPR inte föreligger.

Med ”kärnverksamhet” avses den *primära verksamheten* för den personuppgiftsansvarige eller personuppgiftsbiträdet. Det är således den verksamhet som är nödvändig för att uppnå målen. Som exempel kan nämnas ett privat säkerhetsföretag som bedriver övervakning på allmänna platser. Detta företags ”kärnverksamhet” utgörs av sådan personuppgiftsbehandling vilket typiskt sett kräver att företaget utnämner ett dataskyddsombud. I GDPR anges inte uttryckligen vad som avses med ”behandling i stor omfattning” men det är en faktor som, tillsammans med typen av uppgifter som behandlas samt behandlingens varaktighet och geografiska räckvidd, ska beaktas vid bedömningen av om ett dataskyddsombud behöver utses.

Ett dataskyddsombud ska utses på grundval av yrkesmässiga kvalifikationer och, i synnerhet, sakkunskap om lagstiftning och praxis avseende dataskydd samt förmågan att fullgöra de uppgifter som åligger denne enligt GDPR. Dataskyddsombudet får vara anställd hos den personuppgiftsansvarige eller personuppgiftsbiträdet, men kan även utföra sina uppgifter på grundval av ett tjänsteavtal. En koncern kan utse ett dataskyddsombud för flera bolag inom koncernen under förutsättning att ombudet finns lätt tillgängligt för varje bolag.

I likhet med ett personuppgiftsombuds uppgifter enligt PUL består ett dataskyddsombuds uppgifter bland annat av att övervaka den interna efterlevnaden av GDPR, informera och ge råd till personuppgiftsansvariga och personuppgiftsbiträden om deras skyldigheter och fungera som kontaktpunkt för tillsynsmyndigheten och samarbeta med denna. Därutöver ska dataskyddsombudet ge råd avseende den konsekvensbedömning som ska göras enligt GDPR när behandling av personuppgifter kan leda till en hög risk för de registrerade. Dataskyddsombudet kontaktuppgifter ska anmälas till tillsynsmyndigheten (Datainspektionen) i syfte att underlätta den behöriga tillsynsmyndighetens kontakt med dataskyddsombudet.

Sanktioner enligt GDPR

Datainspektionen kan komma att utdöma administrativa sanktionsavgifter för en personuppgiftsansvarig eller ett personuppgiftsbiträde som bryter mot GDPR. Tillsynsmyndighetens befogenhet att utdöma administrativa sanktionsavgifter är helt ny i förhållande till PUL. Vid beslut om administrativa sanktionsavgifter ska påföras och vid bedömningen av avgiftens storlek ska tillsynsmyndigheten ta hänsyn till en rad olika kriterier, bl.a. hur allvarlig överträdelsen är, om överträdelsen skett avsiktligt eller inte, vilka åtgärder som har vidtagits för att minska skadan, om ekonomisk vinst på grund av överträdelsen har uppkommit samt om det föreligger andra försvårande eller förmildrande omständigheter.

Tillsynsmyndigheten kan besluta om administrativa sanktionsavgifter på upp till 10 miljoner EUR eller 20 miljoner EUR eller, om det gäller ett företag, på upp till 2 procent eller 4 procent av den totala globala årsomsättningen under föregående budgetår. Den maximala storleken på den administrativa sanktionsavgiften är beroende av vilken bestämmelse överträdelsen avser. Som exempel kan nämnas följande situationer. Om en personuppgiftsansvarig behandlar personuppgifter utan att någon laglig grund för behandlingen föreligger, kan den högre administrativa sanktionsavgiften komma att dömas ut. Vid underlåtelse att utnämna ett dataskyddsombud när en sådan skyldighet föreligger är det den lägre administrativa sanktionsavgiften som kan aktualiseras.

Tillsynsmyndigheten har också så kallade *korrigerande befogenheter*, såsom att utfärda varningar och reprimander, vilka som regel bör aktualiseras innan administrativa sanktionsavgifter. De administrativa sanktionsavgifterna kan dock påföras utöver eller istället för sådana korrigerande åtgärder. Det är tillsynsmyndigheten som ansvarar för att välja den mest lämpliga åtgärden vid överträdelser av förordningens bestämmelser.

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