Klientbriefing GDPR – del 2 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 andra av fyra delar och behandlar:

- när det är fråga personuppgifter,
- krav på att behandlingen ska vara helt eller delvis automatiserad eller avse ett register,
- vad som avses med anonymisering, pseudonymisering och kryptering av personuppgifter, samt
- krav på säkerhetsåtgärder.

Behandling av personuppgifter

Personuppgifter enligt GDPR

En grundläggande förutsättning för att GDPR ska vara tillämplig är att behandlingen ifråga avser *personuppgifter*. Med personuppgifter avses all slags information avseende en identifierad eller identifierbar fysisk person i livet. GDPR är alltså inte tillämplig på behandling av personuppgifter som rör avlidna personer, inte heller på uppgifter som rör en juridisk person. GDPR är inte heller tillämplig på anonymiserad information, dvs. information som avidentifierats (se s. 2).

En fysisk person kan identifieras *direkt* eller *indirekt* och genom en eller flera olika uppgifter, s.k. identifierare. En personuppgift kan exempelvis vara ett namn, en adress, ett personnummer eller ett fotografi, men det kan även vara en uppgift som endast *indirekt* med stöd av annan *kompletterande information* pekar ut viss person. Exempel på detta är bilregistreringsnummer, IP-adresser, användar-ID och bankkontonummer.

För att avgöra om en fysisk person är identifierbar måste man beakta alla hjälpmedel, som antingen av den personuppgiftsansvarige (den som behandlar personuppgifterna) eller av en annan person, *rimligen* kan komma att användas för att direkt eller indirekt identifiera den fysiska personen. Enligt GDPR bör man beakta samtliga objektiva faktorer, såsom kostnader och tidsåtgång för identifiering, med beaktande av såväl tillgänglig teknik vid tidpunkten för behandlingen som den tekniska utvecklingen. Att bedömningen kan vara vidsträckt framgår även av rättspraxis från EU-domstolen där det beaktats att den kompletterande informationen kunde erhållas från tredje man ytterst via domstolsförfarande.

Avgörandet från EU-domstolen rörde en dynamisk IP-adress (en IP-adress som ändras vid varje ny uppkoppling mot internet). EU-domstolen uttalade att adressen i sig själv inte utgör en sådan upplysning som avser en identifierbar fysisk person, eftersom en sådan uppgift *inte direkt* avslöjar identiteten på den fysiska person som använder den dator till vilken IP-adressen är kopplad.[2] En sådan IP-adress kan dock – med stöd av kompletterande information – identifiera en viss fysisk person, och därför utgöra en personuppgift. Kompletterande information om vem som står bakom IP-adressen kan exempelvis inhämtas från användarens internetleverantör. Enligt avgörandet fanns det *lagligt stöd* för att begära ut uppgifter från användarens internetleverantör om vem som stod bakom IP-adressen. Det fanns således hjälpmedel som med *rimlig* sannolikhet kunde användas för att identifiera personen i fråga. Om det inte hade funnits *lagligt stöd* för att begära ut sådana kompletterande uppgifter är det osäkert om EU-domstolen ansett att en dynamisk IP-adress utgör en personuppgift.

Om de uppgifter som behandlas inte anses utgöra personuppgifter, exempelvis för att uppgifterna endast indirekt pekar ut viss fysisk person och det inte finns hjälpmedel som rimligen kan komma att användas för att identifiera personen i fråga, eller för att det uppgifterna är *anonymiserade* (se nedan), regleras behandlingen inte av GDPR.

Krav på automatiserad behandling

En ytterligare förutsättning för att GDPR ska vara tillämplig är att det rör sig om *behandling* av personuppgifter. Med *behandling* avses enligt GDPR att en åtgärd med personuppgifter vidtas. Det kan exempelvis vara fråga om insamling, registrering, organisering, strukturering, lagring, kopiering, bearbetning, ändring, framtagning, läsning, eller utlämning genom överföring. I praktiken är det svårt att föreställa sig att en åtgärd som vidtas med personuppgifter inte anses utgöra *behandling* enligt vad som följer av GDPR. För att GDPR ska vara tillämplig krävs vidare som huvudregel att behandlingen sker helt eller delvis på *automatisk väg*. När behandling sker helt automatiserat rör det om behandling av personuppgifter i datorformat. Om behandling sker endast

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

2 Mål C-582/14, Patrick Breyer v Bundesrepublik Deutschland

delvis automatiserat kan det exempelvis vara att person-uppgifter samlas in manuellt för att sedan registreras i datorformat.

GDPR är dock även tillämplig på *manuell behandling* av personuppgifter om personuppgifterna ingår eller är avsedda att ingå i ett *register*.[3] För att det ska anses vara fråga om ett register enligt GDPR måste det vara sökbart enligt särskilda *kriterier*. En hög med papper på ett skrivbord som endast är sorterade i datumordning är inte ett sådant sökbart register som medför att GDPR blir tillämplig. Om däremot samma papper sorteras i bokstavsordning efter de registrerades namn och läggs i märkta hängmappar i ett dokumentskåp är det sannolikt fråga om personuppgifter som ingår i ett register.

Sammanfattningsvis krävs att följande förutsättningar föreligger för att GDPR ska vara tillämplig:

- behandlingen avser *personuppgifter,* och
- behandlingen genomförs på *helt eller delvis automatisk väg*, *eller*
- behandlingen avser personuppgifter som ingår eller är avsedda att ingå i ett register som är sökbart enligt särskilda kriterier.

Anonymisering, pseudonymisering och kryptering

Anonymisering
Behandling av *anonym information* anses inte utgöra behandling av personuppgifter, eftersom uppgifterna inte går att knyta till viss fysisk person i livet.

Som ovan konstaterats krävs att alla hjälpmedel som *rimligen* kan komma att användas för att identifiera vissa person beaktas. För att information ska anses vara anonym krävs således att det inte är möjligt att identifiera en viss person med de uppgifter som är tillgängliga. Det är alltså inte tillräckligt att exempelvis *kryptera* personuppgifter, eftersom krypterad information normalt sett kan dekrypteras med hjälp av ett lösenord eller liknande. GDPR föreskriver inte någon särskild metod för att anonymisera personuppgifter, det avgörande är att uppgifterna inte kan hänföras till någon person.

I sammanhanget ska även uppmärksammas GDPR:s princip om *lagringsminimering*. Principen innebär att personuppgifter inte får sparas i en form som möjliggör identifiering av en person under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas.

Av principen om *lagringsminimering* följer att en personuppgiftsansvarig bör införa tidsfrister för *radering* av personuppgifter. Om uppgifterna inte längre behövs för de ändamål som de samlades in ska uppgifterna som regel raderas eller anonymiseras. Vid *radering* av personuppgifter ska alla kopplingar till och kopior eller reproduktioner av personuppgifterna raderas.

Eftersom anonymiserade uppgifter inte längre utgör personuppgifter kan uppgifterna behandlas utan att en verksamhetsutövare behöver uppfylla kraven enligt GDPR. Det innebär exempelvis att de anonymiserade uppgifterna kan användas för andra ändamål än för vilka de samlades in och att de kan lagras under en obestämd tid. Anonymisering är således en åtgärd som kan användas för att uppfylla GDPR:s princip om *lagringsminimering* samtidigt som de anonymiserade uppgifterna kan vara värdefulla i verksamheten och bevaras exempelvis för genomförande av undersökningar och statistiska analyser.

Pseudonymisering
Ett nytt begrepp som förekommer i GDPR är *pseudonymisering*. När personuppgifter pseudonymiserats innebär det är de inte kan tillskrivas en specifik registrerad utan att *kompletterande information* används. Ett exempel på pseudonymisering är att en personuppgift, såsom ett namn eller ett personnummer (direkt identifierare), ersätts med ett unikt attribut, såsom en sifferkombination eller ett kundnummer (indirekt identifierare). I samband med det upprättas en separat lista i vilken det framgår vilket unikt attribut (pseudonymiserad uppgift) som hör ihop med vilket namn eller personnummer. För att pseudonymiseringen ska uppnå sitt syfte måste den kompletterande informationen förvaras separat från de pseudonymiserade uppgifterna och omfattas av tekniska (exempelvis kryptering) och organisatoriska åtgärder som skyddar den från olovlig tillgång.

Pseudonymiserade uppgifter utgör fortfarande personuppgifter, eftersom det är möjligt att *indirekt* identifiera och särskilja en enskild person med de uppgifter som hålls avskilda. *Pseudonymisering* av personuppgifter skiljer sig således från *anonymisering* av personuppgifter, eftersom personuppgifter som har anonymiserats inte längre går att hänföra till en viss fysisk person.

Kryptering
Kryptering är ett annat begrepp som förekommer i GDPR. Med *kryptering* avses att personuppgifterna genom tekniska åtgärder görs oläsbara för alla personer som inte är behöriga att få tillgång till uppgifterna.

Kryptering av exempelvis lagrade personuppgifter eller personuppgifter som överförs genom mejlkorrespondens kan vara lämpligt att använda när den som behandlar personuppgifter vill försäkra sig om att endast behöriga personer får åtkomst till personuppgifterna.

[3] I den engelskspråkiga versionen av GDPR används uttrycket ”filing system”.

Det kan vara särskilt lämpligt att använda kryptering när känsliga personuppgifter behandlas, såsom uppgifter om hälsa eller politiska åsikter. Vidare kan kryptering vara till fördel även vid annan personuppgiftsbehandling. Om en *personuppgifts-incident* inträffar, exempelvis att någon får obehörig åtkomst till personuppgifter som lagrats av en personuppgiftsansvarig (datorintrång), krävs som huvudregel att den personuppgifts-ansvarige anmäler incidenten till Datainspektionen. Vid en personuppgiftsincident finns i vissa fall även skyldighet att informera de personer som berörs av incidenten. Skyldigheten att informera, vilket kan vara betungande för många verksamheter, gäller dock inte om personuppgifterna som påverkades av personuppgiftsincidenten var föremål för kryptering som skyddsåtgärd (Datainspektionen ska dock fortfarande underrättas). Detta är en fördel med krypterade personuppgifter.

Säkerhet för personuppgifter

Allmänt om säkerhetsåtgärder

När personuppgifter behandlas kan det uppstå risker för fysiska personers rättigheter och friheter. Riskerna kan leda till fysiska, materiella och/eller immateriella skador. Om en obehörig person får del av personuppgifter kan det exempelvis orsaka skada hos en registrerad i form av identitetsstöld.

För att upprätthålla säkerheten när personuppgifter behandlas och för att förhindra att behandling sker i strid med GDPR bör de som behandlar personuppgifter utvärdera riskerna med behandlingen samt vidta *tekniska och organisatoriska åtgärder*. Vilka *åtgärder* som ska vidtas beror på bland annat kostnaderna för att genomföra åtgärderna, vilken typ av behandling som sker, riskerna med behandlingen och de tekniska möjligheter som idag finns tillgängliga. Åtgärderna som vidtas bör säkerställa en lämplig säkerhetsnivå i förhållande till risken med behandlingen.

För att bedöma en lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandlingen medför, i synnerhet risken för oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som behandlas.

Om en verksamhetsutövare skulle åsidosätta sin skyldighet att vidta tekniska och organisatoriska åtgärder kan det ytterst medföra att Datainspektionen utdömer administrativa sanktionsavgifter på upp till 10 miljoner euro eller, om det gäller ett företag, på upp till 2 procent av den globala årsomsättningen under föregående budgetår (beroende på vilket värde som är högst).

Säkerhetsåtgärder enligt GDPR

Pseudonymisering och *kryptering* av personuppgifter anges i GDPR som exempel på tekniska åtgärder som kan vidtas för att säkerställa en lämplig säkerhetsnivå och därmed minska risken med behandling av personuppgifter. En annan sådan åtgärd kan vara att ha ett system för att regelbundet testa och utvärdera effektiviteten hos de åtgärder som ska säkerställa behandlingens säkerhet.

Varken *pseudonymisering* eller *kryptering* av personuppgifter är obligatoriskt enligt GDPR men metoderna är värdefulla som verktyg för dataskydd och kan lämpligen användas för att uppfylla det generella kravet att genomföra tekniska och organisatoriska åtgärder i syfte att minska riskerna med behandling av personuppgifter.

Inbyggt dataskydd och pseudonymisering

Pseudonymisering och kryptering är ett exempel på tekniska åtgärder som kan integreras i verksamhetsutövares IT-system för behandling av personuppgifter för att uppfylla dataskyddsprincipen om *privacy by design* (inbyggt dataskydd). Principen är ny i förhållande till PUL och innebär i korthet att verksamhetsutövare måste beakta skyldigheten att skydda personuppgifter redan när IT-system utformas.

Principen om *privacy by design* är en av flera principer i GDPR om *dataskydd*. Principen om *privacy by design* kompletteras bland annat av principerna om *uppgiftsminimering* och *lagringsminimering*, vilka innebär att den personuppgifts-ansvarige inte ska behandla och lagra fler uppgifter än vad som är nödvändigt för att nå ändamålet med behandlingen. Det är med andra ord inte tillåtet att samla in personuppgifter för obestämda framtida behov. *Pseudonymisering* vid behandling av personuppgifter kan vara en relevant åtgärd (av flera) att genomföra för att uppfylla kraven på *uppgiftsminimering* och inbyggt dataskydd och anonymisering kan vara en relevant åtgärd för att uppfylla kraven på lagringsminimering.

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