QNISTER

VAD UNDRAR DU ÖVER?
- FAQ by Qnister

Vad är GDPR?

GDPR är EU:s nya Dataskyddsförordning (Europaparlamentets och rådets förordning (EU) nr 2016/679). GDPR står för ”General Data Protection Regulation”.

När börjar den gälla?

Förordningen är antagen sedan våren 2016 men börjar tillämpas först den 25 maj 2018.

Kommer PuL (Personuppgiftslagen) fortsätta att gälla?

En av grundidéerna med GDPR var att uppdatera nuvarande lagstiftning inom området för skydd av EU-medborgarnas personuppgifter. Det innebär bland annat att det föregående EU-direktivet, som genom PuL har implementerats i svensk lag, upphör att gälla och därmed även PuL. En EU-förordning blir direkt tillämplig i alla EU-länder och behöver således inte implementeras genom ny nationell lagtext.

Vi följer PuL idag, räcker det för att leva upp till GDPR?

Om ett företag till fullo lever upp till PuL idag är tröskeln inte lika hög för att uppnå den standard som GDPR sätter. Dock är det en hel del nyheter som måste ses över och på ett lämpligt sätt implementeras i företagets rutiner, dokument, system och arbetssätt.

Vad är en personuppgift?

En personuppgift är alla uppgifter som kan användas för att identifiera en fysisk person. Som exempel kan nämnas de klassiska uppgifterna personnummer, adress, namn, kontonummer osv. Men även flera uppgifter i kombination, som var för sig inte räcker för att identifiera en individ, anses vara personuppgifter. Om man t.ex. anger antal barn så är det i sig inte tillräckligt för att identifiera någon, men om man lägger till bostadsort och kön (sju barn, Gränna, man) så kan det räcka och dessa räknas då som personuppgifter.

QNISTER

När en person väl har identifierats utgör samtliga uppgifter som samlas in om den personen personuppgifter.

Vem är Personuppgiftsansvarig?

Personuppgiftsansvarig är den som beslutar om att uppgifter ska samlas in samt till vilket ändamål de ska användas. I ett aktiebolag är det den juridiska personen, själva bolaget, som är personuppgiftsansvarig. Om det däremot handlar om en enskild firma eller en privatperson som hanterar uppgifter på ett sätt som faller inom ramarna för förordningen så är det den fysiska personen som anses vara personuppgiftsansvarig.

Vad är ett Personuppgiftsbiträde?

Ett personuppgiftsbiträde är den som för och enligt personuppgiftsansvarigs räkning och instruktioner behandlar personuppgifter. Det kan t.ex. vara en leverantör av en molntjänst eller en extern IT-supportfunktion.

Vad är ett Dataskyddsombud?

Dataskyddsombud ersätter det som idag kallas personuppgiftsombud men det blir en lite annan rollbeskrivning. Personen som utses till dataskyddsombud ska bland annat ha kunskap om dataskyddsförordningen och agera kontaktperson både för Datainspektionen och för de registrerade vars uppgifter behandlas.

Vem behöver ett Dataskyddsombud?

Vissa organisationer, så som t.ex. myndigheter eller företag som sysslar med viss typ av övervakning, är skyldiga att utse ett dataskyddsombud. För övriga är det frivilligt. Om man inte anser sig tillhöra den typ av verksamhet som är skyldiga att utse ett dataskyddsombud, men kan tänkas hamna i ”gråzonen” vid en opartisk bedömning, ska beslutet att inte utse ett ombud dokumenteras för eventuell framtida kontroll.

Vad händer med missbruksregeln?

I PuL finns den så kallade ”Missbruksregeln” som innebär att behandling av personuppgifter som förekommer i ostrukturerat format, t.ex. i e-post, på internet eller i enklare listor, faller under enklare regler. Detta undantag för ostrukturerat material försvinner när GDPR ersätter PuL.

Vad innebär dataportabilitet?

Dataportabilitet innebär att den registrerade kan begära att dennes personuppgifter som behandlas lämnas ut till den registrerade i ett allmänt läsbart format. Detta för att enklare kunna byta leverantör av en viss tjänst vilket såklart underlättas om man kan få med sig den data man hittills har arbetat upp i exempelvis en streamingtjänst.

Behövs nya biträdesavtal?

Med den nya lagen kommer nya krav på vad dessa avtal ska innehålla – se till att gå igenom era befintliga avtal och uppdatera vid behov!

Vilken information ska lämnas till de registrerade?

De registrerade har generellt fått fler rättigheter och ett bättre och mer omfattande skydd. Bland annat har punkterna på listan över vilken information som ska lämnas till den registrerade i samband med påbörjad personuppgiftsbehandling blivit fler. Om den information ni har lämnat hittills inte uppfyller de nya kraven måste ny information gå ut när den nya lagen träder i kraft (eller redan nu för all del).

Vad gäller vid personuppgiftsincidenter?

En annan nyhet är att den personuppgiftsansvarige är skyldig att vid personuppgiftsincidenter inom 72 timmar anmäla incidenten till Datainspektionen. Undantaget från denna skyldighet är om det är osannolikt att incidenten medför en risk för fysiska personers rättigheter och friheter. Beslutet att inte anmäla måste då dokumenteras inför en eventuell kontroll.

Gäller GDPR endast inom EU?

EU anser att dess medborgares personuppgifter ska skyddas i största möjliga mån även utanför EU:s gränser. Därför omfattar lagen all behandling av EU-medborgares personuppgifter, oavsett om företaget eller organisationen som genomför behandlingen är lokaliserade inom EU eller inte. En shoppingsida i Kina som vänder sig till EU-medborgare (erbjuder hemsidan på engelska, euro som valbar valuta eller liknande) omfattas således av GDPR likväl som ett företag i Sverige.

Förändras kraven på ett giltigt samtycke?

Samtycke är en väldigt vanlig grund på vilken företag baserar sin behandling av personuppgifter. Med den nya lagen ökar dock kraven på vad som anses vara ett giltigt

samtycke. Frågan ska t.ex. vara särskild från övrig information (alltså inte gömd i något finstilt flersidigt dokument), den ska ställas på ett klart och tydligt språk anpassat efter den som ska ge sitt samtycke och det ska dessutom vara lika enkelt att återkalla samtycket vid ett senare tillfälle.

Vad händer om man inte uppfyller kraven i förordningen?

Då PuL har ansetts vara en ganska ”tandlös” lag kommer det bli en stor förändring när GDPR träder i kraft. Maxtaket för de sanktioner, böter, som kan dömas ut är 20 miljoner Euro alternativt upp till 4 % av den globala årsomsättningen, det beror på vilket som resulterar i högst summa. Detta för att även kunna få de stora globala koncernerna att rätta in sig i ledet och leva upp till lagens bestämmelser.

Självklart kommer det inte alltid dömas ut minst 20 MEUR, utan det bedöms från fall till fall och på vilken nivå Datainspektionen lägger sig återstår att se.

Var kan jag läsa mer?

Det pågår i nuläget ett antal nationella utredningar som har som uppgift att ta fram förslag på ny kompletterande lagstiftning alternativ hur nuvarande lagstiftning bör justeras för att samtliga krav ska kunna uppfyllas (t.ex. kräver GDPR att myndigheter för att ha rätt att behandla personuppgifter finner stöd för detta i nationell lagstiftning). Vi kommer kontinuerligt att lägga ut ny information allt eftersom EU, Datainspektionen eller utredningar lämnar besked i olika frågor.