



Snabba fakta om GDPR

Vad?

Om du hanterar personuppgifter i företaget behöver du veta att EU har beslutat om en ny dataskyddsförordning (GDPR) som innehåller regler om hur man får behandla personuppgifter. Det har tagit EU:s tyngsta instanser fyra år att komma överens om en ny lagtext och denna förordning kommer att ersätta nuvarande svensk personuppgiftslag PUL.

När?

Förordningen börjar tillämpas den 25 maj 2018.

Varför?

Den nya dataskyddsförordningen införs för att ge ett ökat skydd för alla personer som är registrerade, som är anpassat efter dagens teknologi. Ytterligare en anledning till ny lagstiftning är att harmonisera personuppgiftsbehandlingen i alla EU-länder samt i de länder som väljer att följa den, exempelvis Norge.

Vad är en personuppgift?

Personuppgifter är all information som kan knytas till en fysisk person som är i livet. Typiska personuppgifter är personnummer, namn och e-post. Även foton på personer klassas som personuppgifter. Ett organisationsnummer är oftast inte en personuppgift, men handlar det om en enskild firma är även detta en personuppgift. Registreringsnumret på en bil kan vara en personuppgift om bilen är registrerad på en fysisk person medan registreringsnumret på en firmabil som används av flera, kanske inte är en personuppgift.

Hur?

Mycket i GDPR liknar de regler som finns i Sverige idag i personuppgiftslagen. En viktig nyhet är att det uttryckligen anges att den som behandlar personuppgifter ska ansvara för och kunna visa att man följer reglerna i den nya dataskyddsförordningen (ansvarsskyldighet). De företag som behandlar personuppgifter måste alltså aktivt ta ansvar för att se till att förordningens regler följs och kunna visa det. Allt som har att göra med personuppgiftsbehandling ska finnas dokumenterat.

När och för vem gäller dataskyddsförordningen?

Dataskyddsförordningen gäller för alla verksamheter som behandlar personuppgifter, både när företaget själv bestämmer över behandlingen (personuppgiftsansvarig) och när företaget utför den på uppdrag av någon annan (personuppgiftsbiträde). Det är alltid den personuppgiftsansvarige som har ansvaret gentemot de registrerade.

Får man samla in och behandla personuppgifter?

Det är även i fortsättningen tillåtet att samla in, behandla och spara personuppgifter. Ändamålet med insamlingen och den rättsliga grunden för att hantera personuppgifter är avgörande. All behandling av personuppgifter måste uppfylla kraven i GDPR och ni ska kunna visa att det finns stöd i lagen för er



personuppgiftsbehandling. En sådan rättslig grund kan exempelvis vara samtycke eller om personuppgiftsbehandlingen är nödvändig för att fullgöra ett avtal med den registrerade. Här följer fyra "rättsliga grunder" som företag kan använda som skäl (se vidare i artikel 6 i GDPR):

- ✓ **Rättslig förpliktelse** - I vissa fall är företag skyldiga att registrera personuppgifter, som exempelvis för att uppfylla bokföringsskyldigheten i bokföringslagen.
- ✓ **Avtal** - Anställningsavtal, kundavtal och leverantörsavtal är exempel på avtal som innebär att företag måste registrera och hantera personuppgifter (endast uppgifter som är nödvändiga).
- ✓ **Intresseavvägning** - Om företaget kan visa att dess intresse av att hantera personuppgifterna väger tyngre än den enskildes rätt till privatliv.
- ✓ **Samtycke** - Ett alternativ är att fråga personen att få registrera uppgifter om honom/henne.

Utöver ovan finns två ytterligare skäl som kan tillämpas, men som inte är lika vanligt förekommande:

- ✓ **Skydd för grundläggande intressen**
- ✓ **Allmänt intresse och myndighetsutövning**

Vad gäller för insamling av personuppgifter?

Personuppgifter får endast samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Det innebär att om du som kund ska spara personuppgifter måste du ha ändamålen klara för dig redan innan insamlingen av personuppgifter börjar. Detta ska också dokumenteras skriftligt.

Mängden uppgifter ska även begränsas till vad som är nödvändigt för ändamålen. Uppgifterna får inte senare behandlas på ett sätt som är oförenligt med dessa ändamål och inte heller sparas längre än nödvändigt. Företaget som behandlar personuppgifter måste kunna visa att reglerna följs.

Vem kontrollerar att den nya lagen efterlevs?

Datainspektionen kontrollerar att GDPR efterlevs i Sverige och kan besluta om sanktionsavgift på upp till 20 miljoner euro för den som bryter mot förordningens regler. Hur stort beloppet blir beror på regelbrottets art, till exempel om det var avsiktligt eller inte, hur och om företaget åtgärdat regelbrottet och om företaget gjort vinst på detsamma.

Idag kan en person göra en anmälan till Datainspektionen om han/hon anser att den personliga integriteten har blivit kränkt och då kan ett tillsynsärende påbörjas. Men det är oklart om den nya EU-lagen kommer att innebära exempelvis stickprovskontroller. En nyhet är att personer ska kunna vända sig till "sin egen" dataskyddsmyndighet med klagomål som rör uppgifter som hanteras i ett annat land.

Vad är ett Dataskyddsombud och vilka företag behöver en DPO?

Alla företag där kärnverksamheten består av hantering av känslig information eller information som kräver regelbunden och systematisk övervakning i stor omfattning kommer behöva tillsätta ett dataskyddsombud, Data Protection Officer (DPO). Den här personen har till uppgift att övervaka så att företaget följer GDPR och annan dataskyddslagstiftning. Företag i koncern och även fristående företag kan ha ett gemensamt dataskyddsombud. Myndigheter och offentligt organ ska alltid ha en DPO.