GDPR – lagen som ersatte PUL 25/5 2018

The General Data Protection Regulation - Dataskyddsförordningen

GDPR ersatte PUL (personuppgiftslagen) och innebär att det krävs ett ökat lagligt stöd för behandling av personuppgifter. Lagen togs fram för att samordna och göra dataskyddslagstiftningen enhetlig inom hela EU och omfattar all information som kan knytas till en fysisk person som är i livet. Varsågod! Här följer en sammanfattning om GDPR.

Direkta personuppgifter är till exempel:

- Namn, adress, e-post
- Personnummer
- Foto (i de fall som personen känns igen)

Indirekta uppgifter kan vara:

- Ip-adress (datorns identitet)
- Registreringsnummer på bilen

Extra känsliga uppgifter är exempelvis:

- Ras och etniskt ursprung
- Inkomst, politisk åsikt
- Uppgifter som rör hälsa eller sexualliv

GDPR skiljer inte mellan olika data- och lagringsformat – all information som handlar om en identifierad eller identifierbar registrerad person måste förvaras säkert eller förstöras.

Begär inte in fler uppgifter än som verkligen behövs.

Gallra! När du inte längre har rätt att behandla vissa personuppgifter. Radera eller anonymisera dem.

”Rätten att bli glömd” - personuppgifter ska vid begäran tas bort utan dröjsmål.

Vissa uppgifter får registreras utan medgivande, som exempelvis kontaktuppgifter och leveransadress för att uppfylla ett avtal med en kund.

Respektera ett nej tack! Man får skicka nyhetsbrev och annan marknadsföring till sina kunder, men möjlighet för kunden att säga nej till fler i utskick ska finnas.

Rättslig grund för att samla personuppgifter

Vid insamling av personuppgifter måste man först informera om vilka uppgifter man vill samla in, syftet med dem och när de kommer att raders. Man ska också informera om vem man är och vilka rättigheter den registrerade har. Den rättsliga grunden måste också kommuniceras. Finns den inte är det förbjudet att behandla andras personuppgifter.

De rättsliga grunderna

- Samtycke - den registrerade har sagt ja till personuppgiftsbehandlingen
- Avtal - som ska kunna bevisas juridiskt, skriftligt är bäst

- Rättslig förpliktelse - lagar eller regler som gör att den personuppgiftsansvarige måste behandla vissa personuppgifter i sin verksamhet
- Grundläggande (vital) betydelse - personuppgifter får behandlas om det är nödvändigt för att rädda liv
- Allmänt intresse eller myndighetsutövning - men också av företag inom vård och skola
- Intresseavvägning - tredje man, förhindra bedrägerier, direktmarknadsföring (om intresset väger tyngre än den registrerades)

Webbplatsägare som använder kakor behöver besökarens samtycke

Som en följd av GDPR ställs också hårdare krav på webbplatsägare som behöver skydda besökares data och integritet. Säkerheten på webbplatsen måste vara hög så att datastöld kan undvikas. Cookies, som är små textfiler som lagras i besökarens webbläsare, används ofta för att kartlägga surfvanor och förbättra funktionalitet. Besökaren behöver informeras om dessa kakors syfte och ge sitt samtycke.

Ignorantia juris non excusat

Slarv, okunskap och naivitet är inga försvar. Ett företag som bryter mot reglerna i DSF kan få betala upptill 20 miljoner euro eller fyra procent av bolagets globala årsomsättning i sanktionsavgift.

Personuppgiftsansvarig kallas den som behandlar personuppgifter. Själva behandlingen kan överlåtas men aldrig ansvaret. Ett exempel på det är webbplatsägare som hyr webbhotell där kundregister lagras. Ett personuppgiftsbiträde kan behandla personuppgifter för en personuppgiftsansvarigs räkning. Personuppgiftsbiträdet finns alltid utanför den personuppgiftsansvariges organisation och de bör upprätta ett så kallat biträdesavtal.

De grundläggande sju principerna sammanfattar GDPR

1. Laglighet, korrekthet och öppenhet

Behandlingen av personuppgifter ska vara laglig med rättslig grund, med tillägg för annan eventuell lagstiftning.

2. Ändamålsbegränsning

Bara personuppgifter för särskilda, uttryckligt angivna och berättigade ändamål får samlas in. Ändamålen styr vad man får och inte får göra och hur länge de får sparas.

3. Uppgiftsminimering

Personuppgifter som behandlas ska vara adekvata, relevanta och inte för omfattande i förhållande till ändamålet.

4. Riktighet

Personuppgifter som behandlas ska vara riktiga och uppdaterade.

Felaktiga uppgifter ska rättas eller raderas och därför behövs bra rutiner hos den personuppgiftsansvarige.

5. Lagringsminimering

Man får bara spara personuppgifter så länge som de behövs för ändamålet.

6. Integritet och konfidentialitet

Behandling av personuppgifter måste ske så att uppgifterna skyddas med lämpliga säkerhetsåtgärder.

7. Ansvarsskyldighet

Man ansvarar för och måste kunna visa att att man följer de grundläggande principerna om personuppgiftsbehandling och på vilket sätt.