



GDPR

DATAINSPEKTIONEN INFORMERAR

De nya dataskyddsreglerna (GDPR)
börjar gälla i maj 2018.
Vad betyder det för dig?

di.ax
datainspektionen

Nu är det dags – de nya reglerna om dataskydd börjar tillämpas

Skydd av grundläggande rättigheter och friheter

Den 25 maj 2018 börjar EU:s dataskyddsförordning (GDPR) tillämpas. Syftet med dataskyddsförordningen är att skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Ett annat syfte är att skapa enhetlig och likvärdig nivå för skyddet av personuppgifter inom EU så att det fria flödet av uppgifter inom unionen inte hindras. Det uppnås genom att förordningen är direkt tillämplig i de olika medlemsstaterna. Dessutom har nya bestämmelser tagits fram för att modernisera dataskyddsdirektivets regler som är från 1995.

Vad betyder det för dig?

Har du ett kundregister, ett löne- eller personalregister eller hanterar du i andra sammanhang personuppgifter, det vill säga uppgifter om namn, personbeteckning, e-postadresser, bilder eller andra uppgifter som går att hänföra till en särskild fysisk person? EU:s dataskyddsförordning innehåller bestämmelser om hur personuppgifter får behandlas av bland annat myndigheter.

Mycket är oförändrat

Mycket i dataskyddsförordningen liknar de bestämmelser som finns i nuvarande lagstiftning. På samma sätt som idag kan personuppgifter behandlas med stöd av samtycke från de registrerade eller för att uppfylla ett avtal. De registrerade kommer även i fortsättningen att ha rätt att få information om den behandling av personuppgifter som sker och den som behandlar personuppgifter ska vidta tillräckliga säkerhetsåtgärder för att uppgifterna skyddas på rätt sätt. Särskilda krav ställs på behandling av uppgifter om hälsa, etniskt ursprung, politisk uppfattning eller religiös tro.

Följ Datainspektionen och arbetet med de nya bestämmelserna på www.di.ax

Vad blir nytt?

För privatpersoner innebär EU-förordningen

förstärkta rättigheter för den registrerade då:

- mera information ska lämnas,
- rätt till elektroniska registerutdrag,
- rätt att bli glömd/rätten till radering,
- dataportabilitet (i vissa fall finns en rätt att ta med sig sina personuppgifter till en annan serviceleverantör), och
- rätt att motsätta sig profilering

För myndigheter och andra personuppgiftsansvariga

innebär förordningen att vissa förebyggande åtgärder ska vidtas såsom

- uppgörande av konsekvensbedömning avseende dataskydd,
- upprättande av register över behandlingen av personuppgifter,
- anställande av dataskyddsombud
- anmälningsplikt av personuppgiftsincidenter
- krav på inbyggt dataskydd och data som standard
- personuppgiftsbiträden kommer att ha direkta skyldigheter och ansvar för behandling av personuppgifter.

Tillsynsmyndigheterna inom EU kommer att ha en samordnad tillsyn då den europeiska dataskyddsstyrelsen (EDPB) ger utlåtanden, rekommendationer och riktlinjer.

VAD KAN DU GÖRA I DIN DAGLIGA VERKSAMHET?



Följ Datainspektionen och arbetet med de nya bestämmelserna på www.di.ax

- Skaffa och sprid kunskap om reglerna till exempel genom att läsa vägledningar från Datainspektionen och genom utbildning. Tänk genom vilka yrkesgrupper som berörs av lagstiftningen.
- Ta upp frågan på arbetsplatsen. Följande frågor behöver besvaras: Ansvar, resurser, hur den nya lagstiftningen ska genomföras samt vilka blir konsekvenserna för avtal som ska ingås, system som ska utformas med mera.
- Inventera befintlig behandling av personuppgifter genom att ta ställning till nuvarande behandling, sker det behandling av känsliga personuppgifter, vilken information lämnas till de registrerade, vilka är säkerhetsrutinerna, hur ser avtal ut och överförs personuppgifter till tredje land.
- Analysera det rättsliga stödet för behandlingen av personuppgifter. Till stora delar är grunderna samma som idag. Behöver (nytt) samtycke inhämtas och nya avtal ingås?

DATA PROTECTION

- Genomför konsekvensbedömning avseende dataskydd om det finns en hög risk såsom behandling av känsliga personuppgifter i stor omfattning eller systematisk övervakning av allmän plats i stor omfattning
- Anpassa IT-system så att till exempel kravet på inbyggt dataskydd/dataskydd som standard och säkerhet uppfylls.
- Kontrollera om personuppgiftsbiträden kan uppfylla de krav som ställs, behöver personuppgiftsbiträdesavtal och instruktioner ses över samt sker överföring av personuppgifter till tredje land och på vilka grunder.
- Utse dataskyddsombud och uppfyll de krav som lagstiftningen ställer.
- Förbered rutiner för notifiering om personuppgiftsincidenter. Det föreligger alltid en skyldighet att dokumentera en incident såsom till exempel obehörig åtkomst eller oavsiktlig radering.
- Upprätta register över behandling av personuppgifter.

Vad är egentligen en personuppgift?

Personuppgifter är all slags information som kan knytas till en fysisk person som är i livet. Typiska personuppgifter är personbeteckningar, namn och adress. Även foton på personer klassas som personuppgifter. Till och med ljudinspelningar som lagras elektroniskt kan vara personuppgifter även om det inte nämns några namn i inspelningen. Registernumret på en bil kan vara en personuppgift om det går att knyta till en fysisk person medan registernumret till en bil som ägs av en myndighet och används av flera kanske inte är en personuppgift.

Exempel på personuppgifter:

- namn
- postadress
- e-postadress
- platsinformation
- bankuppgifter
- foton
- uppdateringst i sociala medier
- medicinsk information
- IP-adressen på en dator

Behandling:

En åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

Personuppgiftsansvarig:

En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvariga eller de särskilda kriterierna för hur denna ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt.

Personuppgiftsbiträde:

En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvarigas räkning.

Exempel på register du kan vara med i:

- Registret över födselar
- Befolkningsdatasystemet
- Hembygdsrättsregistret
- Körkortsregistret
- Fordonsregistret
- Kameraövervakningssystem som registrerar information (t.ex. bild eller ljud)
- Register över beviljade jakttillstånd
- Elev- eller studeranderegister
- Register över beviljade studiestöd
- Personal- och lönerogister
- Olika kund- och konsumentregister
- Pensionsdataregister
- Faktureringsregister
över olika kommunala avgifter
- Förtroendemannaregister
- Patientregistret
- Cancerregistret och massundersökningsregistret
- och det finns fler.....