GDPR

General Data Protection Regulation

Här får du som medlem i Sveriges Annonsörer en lätt överskådlig information om General Data Protection Regulation (GDPR) som träder i kraft i maj 2018.

Sveriges Annonsörer

Intro:

Personuppgiftslagen (PUL) som har styrt hur och vem som får hantera personuppgifter kommer att bli ersatt av General Data Protection Regulation (GDPR) från och med maj 2018. GDPR kommer att slå fast reglerna för all form av behandling av information som direkt eller indirekt kan knytas till en fysisk person. Detta innebär mer eller mindre förändringar för alla företag, myndigheter och organisationer som på något sätt hanterar personuppgifter.

Syfte:

Syftet med den nya lagstiftningen är dels att få till en harmonisering mellan EU:s medlemsstater vilket i sin tur ska underlätta för konsumenten. Samtidigt har det legat mycket fokus på ett ökat integritetsskydd för medborgarna.

Kraven ökar på att företag och andra organisationer ska informera hur de hanterar uppgifter, vilka uppgifter och varför. Nu blir personuppgifter en mänsklig rättighet. Det ska också under vissa omständigheter gå att säga nej till att personuppgifterna används. Till exempel blir det lättare att slippa direktreklam.

I det ökade medborgarskyddet ingår också rätten att bli glömd. Alltså den chans en person har att begära att få uppgifter på sökmotorer bortplockad. För det krävs att sökresultatet är oriktigt, irrelevant, eller överflödigt.

Vad är en personuppgift:

- All data som kan användas för att identifiera en person till exempel genom namn, e-postadresser, IP adress men även indirekta hänvisningar såsom personnummer och målnummer i en dom.
- En personuppgift kan även vara data som identifierar faktorer som är specifika för hans/hennes fysiska, fysiologiska, psykiska, ekonomiska, kulturella eller sociala identitet.
- All slags information som direkt eller indirekt kan knytas till en fysisk person som är i livet.
- Även bild- och ljuduppgifter om en person räknas som personuppgifter, även om inga namn nämns.
- Krypterade eller kodade uppgifter är också personuppgifter om någon har en nyckel som kan koppla dem till en person.

Sanktionsavgifter:

Till skillnad från PUL där det egentligen inte hände så mycket när något gick fel har den nya dataskyddslagen, GDPR fått mer muskler. Om ett företag brister i sin behandling av personuppgifter kan de tvingas betala en så kallad administrativ sanktionsavgift på upp till 20 miljoner euro eller fyra procent av deras globala omsättning. En bedömning av eventuell överträdelse kommer att verkställas av respektive tillsynsmyndighet, i Sveriges fall Datainspektionen. Det kommer även finnas en central dataskyddstyrelse i EU som tar fram riktlinjer och fattar beslut om tolkningar.

Missbruksregeln ryker:

I Sverige har vi tidigare haft en förenkling av personuppgiftslagen. Har man behandlat personuppgifter i löpande text och enklare listor har den hanteringen kunnat göras med stöd i missbruksregeln. Det har gjort det möjligt att hantera personuppgifter så länge det inte är kränkande för någon. Den regeln försvinner helt och hållet i och med den nya lagen.

Portabilitet:

Varje individ har rätt att begära ut all den information som företaget har registrerat och att flytta över den till en annan aktör. Om personen har bett om informationen digitalt är det ett krav informationen tillhandahålls digitalt. Det är företagets ansvar att se till att de har ett system som säkerställer att uppgifterna inte kommer i fel händer. Grundförutsättningen för säker personuppgifts-hantering är – precis som för all annan säkerhet – pålitliga identiteter. Om du inte vet vem eller vad du har att göra med spelar det ingen roll hur pålitliga dina skyddsmekanismer är.

Håll koll på vilken information ni har och varför:

Framför allt gäller det att ha koll på informationen. I förordningen finns något som kallas privacy by default vilket i korthet betyder att ni måste känna er data, och de system som hanterar informationen. Det är inte heller något som företaget kan lägga över på en IT-leverantör. Har ni full koll på varför ni har uppgifterna, hur samlas de in och vem har tillgång till dem? På ett mer konkret plan innebär GDPR att företag ska visa vad de vill göra med personuppgifter. PUL har mer varit inriktat på hur data hanteras när ett företag väl har skaffat dem. Det blir med andra ord mycket svårare att ha dolda syften med sin insamling. Personuppgifter som samlas in och lagras/sparas för ”good to have” blir betydligt svårare.

Vem är ansvarig för personuppgifterna?

Dataskyddsförordningen gör gällande att den personuppgiftsansvarige måste visa att förordningen följs. Troligtvis kommer det att öka kraven på dokumentation. En personuppgiftsansvarig är för det mesta en juridisk person som alltså är ansvarig för vad som görs med personuppgifter. Ett personuppgiftsbiträde/ombud är den som behandlar personuppgifter för den personuppgiftansvariges räkning. Vad som är nytt är däremot kravet på att det ska finnas ett dataskyddsombud i organisationer som hanterar särskilt känsliga uppgifter eller om det innebär en kartläggning av enskilda människors beteende.

Krav på rapportering vid dataintrång:

Om det inträffar något som riskerar att personuppgifter hamnar i orätta händer måste detta nu rapporteras till Datainspektionen. Det kan gälla både dataintrång eller att man själva begått ett misstag. Ett nytt krav i den nya dataskyddförordningen är att de vars uppgifter läckt ut måste informeras inom 72 timmar.

Grunder för laglig behandling:

I GDPR är samtycke en av grunderna för laglig behandling av personuppgifter. Ett samtycke måste vara frivilligt, specifikt, informerat och otvetydigt. Bland andra skäl till att samla in personuppgifter märks att fullgöra avtal och rättsliga förpliktelser, skydda individers intressen och utföra uppgifter av allmänt intresse eller för myndighetsutövning. Det finns även en bestämmelse som innebär att man gör en intresseavvägning mellan den personuppgiftsansvariges intressen å ena sidan samt samt den registrerades intressen av grundläggande rättigheter och friheter å den andra. Vad som är viktigt är att dokumentera varje avvägning.

GDPR i korthet:

Tillgänglighet:

Alla individer har rätt att ta del av de uppgifter ett företag har registerat om dem. Det är företagets ansvara att se till att information inte kommer till fel person!

Spårbarhet:

Ditt företag måste kunna visa upp hur ni har använt informatonen, vilka som har sett den och vilka som har haft tillgång till den.

Medgivande:

Ditt företag måste alltid få ett aktivt medgivande för att kunna registrera personuppgifter. Det får inte ske som ett krav för att få gå vidare förutom i undantagsfall.

Transparens:

Det måste framgå i klartext hur din organisation använder personlig data.

Portabilitet:

Individen har alltid rätt att begära att informationen du registrerat överlämnas till en annan part.

Korrigering:

Individen har rätt att få felaktig information om sig rättad.

Borttagning:

Individen har rätt att bli borttagen ur era register. Det här gäller även om personen tidigare godkänt lagring av persondata.

Checklista:

Få en budget för att leva upp till de nya kraven GDPR medför.

Skapa insikt i att det kan bli skadestånd om de nya kraven inte efterlevs?

Kartlägg alla ställen där ni registrerar personuppgifter. (T.ex: HR, hemsida)

Kartlägg alla dataflöden där personuppgifter behandlas. (T.ex Hogia, Wordpress)

Kontrollera att varje del av vårt företag har rättslig grund för insamling och användning av personuppgifter?

Skapa rutiner för att klara av att meddela berörda parter inom 72 timmar i händelse av dataintrång.

Skapa rutiner för att inte samla in mer personuppgifter än nödvändigt och inte spara dem för länge.

Skapa rutiner för att säkerställa att insamlad data för ett användningsområde inte används för något annat vid ett senare tillfälle?

Skapa en process för att ge individer till sina uppgifter om de frågar efter dem.

Implementera en process för att ge individer tillgång till sina uppgifter när de frågar efter dem på ett säkert sätt?

Kontrollera hur ditt företag hanterar de nya kraven på gränsöverskridande dataöverföringar?

Hanterar ni personlig data på uppdrag av andra organisationer se till att ni upprätt-håller de skyldigheter det medför?

Skapa en process för att radera uppgifter när en person begär det?

Utse ett dataskyddsombud och planera för utbildning av denna person.

För information och rådgivning kontakta:

Tobias Eltell
Förbundsjurist
Mail:
tobias.eltell@annons.se
Telefon:
08-545 252 42
Mobil:
0766-29 12 90