Johanna Ekerstrand 2018-01-18

GDPR ersätter PUL

Den 25 maj 2018 kommer den allmänna dataskyddsförordningen, på engelska General Data Protection Regulation (GDPR) att ersätta personuppgiftslagen (PUL) och tillämpas i svensk lag.

Den äldre dataskyddslagstiftningen var otidsenlig och tillämpades dessutom på olika sätt i EU:s medlemsländer. Målsättningen med den nya dataskyddsförordningen är att på ett effektivt sätt modernisera dataskyddsreglerna i EU:s medlemsländer som har släpat efter den digitala utvecklingen. Den nya lagen kommer att tydliggöra för företag vilka regler som gäller och vad som händer ifall man inte följer dem. Till skillnad mot den tidigare lagen som inte varit detaljreglerande får nu de nationella tillsynsmyndigheterna möjligheter att döma ut höga böter.

GDPR ställer högre krav på personuppgiftshantering och gäller för alla företag och organisationer som behandlar (samlar in, processar eller lagrar) personuppgifter som tillhör EU-medborgare, även om verksamheten befinner sig utanför EU-området. Förordningen omfattar såväl de som styr behandlingen av personuppgifter (personuppgiftsansvariga), men även eventuella tjänsteleverantörer (personuppgiftsbiträden).

Den nya lagen syftar även till att ytterligare stärka skyddet av den enskildes personuppgifter och samtidigt tillgodose till enskildes rätt att få åtkomst, få sina uppgifter korrigerade och ”rätten att bil glömd". Den enskilde har också rätt att bli informerad om vilket data som samlas in, i vilket syfte, lagringstid samt information om vilka som har åtkomst.

Utgångspunkten är att all behandling och användning av personuppgifter ska vara laglig, individen informerad om användningen på förhand, IT-miljön ska vara säker och individen ges rättigheter att motsätta sig, rätta och förhindra behandling.

Det innebär att många organisationer nu behöver göra en omfattande översyn och analys av vilka förändringar man behöver göra i processer, rutiner, system och dokumentation för att säkerställa korrekt behandling och lagring av personuppgifter- internt och/eller via sina underleverantörer.

Övergripande skillnader mot PUL:

- Kraven på hur personuppgifter hanteras kommer nu att vara desamma i hela EU.
- Högre krav ställs på företagen på hur personuppgifter hanteras.
- Ökat fokus på integritet och sekretess.
- Samtycket måste vara tydligare och krävs under flera omständigheter.
- Nya förutsättningar för marknadsföringen (profilering/selektering)
- Informationskravet till registrerade är hårdare.
- ”Rätten att bli glömd” förstärks så att personer som inte längre vill att personuppgifter om dem behandlas ska kunna begära att uppgifterna raderas, om det inte finns legitima skäl att behålla dem.

- Rätten till uppgiftsportabilitet. Företag ska vid förfrågan kunna utge de personuppgifter om en enskild till denna så att uppgifterna kan överföras till en annan tjänsteleverantör. Om det är tekniskt möjligt ska detta ske direkt till den nya leverantören.
- Behandling av barns uppgifter kommer att kräva samtycke från vårdnadshavare för informationssamhällets tjänster (ex. Facebook, Instagram).
- Större krav på översyn av system, analyser, processer, rutiner och dokumentation.
- ”Privacy by design”- integritetsskydd ska finnas inbyggd i system redan från början och genomsyra hela livcykeln i systemet.
- Missbruksregeln i PUL försvinner. All behandling av ostrukturerad data (e-post, fritext i dokument, ljudfiler) omfattas av hela lagen utan att det finns särskilda undantag.
- Företag får inte dela en europeisk individs personuppgifter till ett annat företag, eller lagra dessa uppgifter utan ett formellt avtal med den ansvarige för behandlingen (normalt den part som begärt in personuppgifterna från individen från början) som begränsar hur personuppgifterna kan behandlas. Detta kallas för ett personuppgiftsbiträdesavtal.
- En skyldighet för företag att till tillsynsmyndigheten, och i vissa fall den enskilde, anmäla dataintrång. Incidentrapporter kommer att behöva skickas till Datainspektionen inom 72 timmar för större incidenter.
- De nationella tillsynsmyndigheternas möjligheter till sanktioner stärks- max sanktionsavgift på 4 % av den globala omsättningen av föregående år eller 20 miljoner euro, vilket som är större.
- Enskilda ska kunna vända sig till ”sin egen” tillsynsmyndighet med klagomål som rör uppgifter som hanteras i ett annat land. En svensk ska alltså kunna vända sig till Datainspektionen med ett klagomål som rör ett företag i ex. vis Tyskland.
- Företagen kommer att vara skyldiga att både under beslut om på vilket sätt data ska behandlas, och under själva behandlingen, att införliva lämpliga dataskyddsprinciper, t.ex. dataminimering. (Förordningen tar ett flertal gånger upp ”psedonymisering” som exempel på en sådan säkerhetsåtgärd.)

Hur påverkas släktforskningen i stort?

Föreningen DIS har publicerat en bra sammanställning, skriven av Christian Juliusson, om just detta, som kan läsas i sin helhet här: https://www.dis.se/index.php/gdpr

- Förordningen omfattar inte privatpersoner och deras hobbys.
- Skyddsreglerna gäller inte för avlidna personer.
- Problem kan däremot uppstå när släktforskaren vill dela med sig av nu levande personers uppgifter i ex. vis en artikel, en släktbok eller på internet. Då krävs samtycke till publicering från varje enskild person.
- ”Eftersom förordningen inte gäller privatpersoners släktforskning (förutom vad som sagts ovan om spridning och publicering) vilar inget ansvar på aktörer som Ancestry, Geni och MyHeritage att radera uppgifter om de levande individer som inte gett sitt samtycke. Men den nya förordningen ger också rätten att få bli struken ur ett register om man så önskar.”

Checklista/tips till föreningarna

Vad räknas som personuppgifter?

Med personuppgift avses all information som går att koppla till en individ. Det kan vara uppenbara saker som exempelvis ett namn, med det kan också vara information som i kombination med andra uppgifter för det möjligt att identifiera en person.

Exempel på personuppgifter:

- Ett namn
- En postadress
- En e-postadress
- Platsinformation
- Bankuppgifter
- Ett foto
- En uppdatering i sociala medier
- Medicinsk information
- En dators IP-adress
- Anställningsnummer
- Registreringsnummer

Hur säkerställer vi att det finns en laglig grund och krävs det alltid samtycke?

Innan organisationen kan behandla personuppgifter måste det finnas en laglig grund för behandlingen. Det behöver inte nödvändigtvis innebära att det kommer att krävas samtycke till all behandling av personuppgifter. Behandling är endast laglig om åtminstone ett av följande villkor är uppfyllt:

- Den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller fler ändamål.
- Behandlingen är nödvändig för att fullgöra ett avtal i vilken den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.
- Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.
- Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.
- Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.
- Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskild när den registrerade är ett barn.

Vad innebär ”berättigat intresse” och kommer det fortfarande vara lagligt med direktmarknadsföring?

Berättigat intresse innebär att det görs en intresseavvägning mellan nyttan av behandlingen och risken för enskildas personliga integritet. Om risken för att registrerades personliga integritet blir kränkt är större än den nytta personen och organisationen kommer att ha med behandlingen kan denna grund inte hävdas. Det står uttryckligen i skäl (47) i förordningen att direktmarknadsföring är ett berättigat intresse. Detta betyder att det fortfarande kommer att finnas möjlighet att använda direktmarknadsföring utan samtycke, men bara ifall nyttan väger högre än risken.

Vad ska vi börja tänka på när det gäller GDPR?

Gå igenom och dokumentera vilka personuppgifter ni har, hur ni behandlar dem, samt vem som hanterar dem. Det är en god idé att skapa policydokument för verksamhetens behandling av personuppgifter.

Behandlar vi personuppgifter lagligt och transparent?

- Personuppgifter ska hanteras enligt dataskyddsförordningen.
- Personuppgifter får behandlas om den registrerade samtyckt till behandlingen eller om någon annat villkor för laglig grund kan anses vara uppfyllt.
- Krav på transparens. Den registrerade har rätt att få känna till alla personuppgifter som finns registrerade samt för vilket ändamål dessa används och lagringstid för personuppgifterna.

Behandlar vi uppgifter för bara begränsade ändamål?

- Personuppgifter får bara användas för det specifikt angivna ändamål som den registrerade har informerats om. Exempel på ändamål: marknadsföring, fakturering.

Behandlar vi fler personuppgifter än nödvändigt?

- Föreningen får bara behandla de personuppgifter som krävs för att uppfylla ändamålet. Uppgifterna måste därför vara relevanta och får inte vara fler än nödvändigt.

Är alla personuppgifter korrekta?

- Föreningen måste ha korrekta uppgifter.

Gallrar vi bland personuppgifterna?

- Föreningen får inte lagra personuppgifter under längre tid än vad som är nödvändigt för att uppfylla de ändamål för vilka de samlades in.

Hur ska vi tillmötesgå de registrerades rättigheter?

De registrerade ska ha rätt att:

- Få tillgång till sina personuppgifter
- Få felaktiga personuppgifter rättade
- Få sina uppgifter utlämnade så att uppgifterna kan överföras till en annan tjänsteleverantör
- Få sina personuppgifter raderade (om det inte finns legitima skäl att behålla dem)

Vad ska vi göra vid personuppgiftsincidenter?

Vid t.ex. dataintrång måste händelsen dokumenteras. Om incidenten medför risker för enskildas fri- och rättigheter måste incidenten anmälas till tillsynsmyndigheten inom 72 timmar.

GDPR för hemsida

Samtyckesavtal vid registrering av konton, formulär och kommentarsfält. Det räcker inte med en på förhand ikryssad ruta på webbplatsen.

Giltigt samtycke betyder i praktiken att registrering av personuppgifter måste vara en informerad, frivillig och specifik viljeyttring från användarens sida.

Samtyckesavtal ska innehålla en fullständig beskrivning av vilka uppgifter som samlas, till vilket ändamål samt hur länge uppgifterna lagras. Det ska också framgå hur man kan avsluta sitt konto och radera sina uppgifter.

Källor och mer information

Sammanfattningen ovan är i huvudsak ett hopplock av den information som finns publicerat på följande hemsidor:

- **GDPR.se**
- **Datainspektionen.se**

Datainspektionen har publicerat en mer utförlig vägledning till personuppgiftsansvariga, som går att läsa och skriva ut som PDF här: https://www.datainspektionen.se/Documents/vagledning-forberedelser-pua.pdf

- **Unionen.se medlemsskapet/bransch/organisationer-föreningar/Så påverkar det nya dataskyddet civilsamhället**
- **Juridiskvagledning.se/ny-dataskyddsforordning/**
- **Olingo.se/pul-ersatts-av-ny-lag/**
- **24solutions.com/sv/compliance/folj-kraven-i-nya-dataskyddslagen-gdpr/gdpr-jamfort-med-pul**

En kostnadsfri GDPR-guide finns att ladda ner här: https://www.24solutions.com/sv/wp-content/uploads/sites/2/2017/06/24-Solutions-GDPR-Guide-inledning.pdf