Dataskyddsförordningen (GDPR) för beslutsfattare och jurister

Staffan Wikell, Förbundsjurist SKL

November 2017

GDPR –
Vad händer den 25 maj 2018?

- EU:s dataskyddsförordning (EU) 2016/679 av den 27 april 2016 (GDPR) börjar gälla samtidigt i alla medlemsländer. PuL upphör.
- Skärpt ansvar för personuppgiftsansvariga organisationer
- Utökade rättigheter för registrerade individer
- Syftet med reglerna är detsamma som i PUL :
  - att skydda fysiska personers integritet vid behandling av deras personuppgifter

Några tydliga förändringar

Förstärkning av individers rättigheter

Ökat ansvar för PUA

Ökat ansvar för PUB

Accountability

Stärkt roll Dataskyddsombud

Fler sanktioner och ökad tillsyn

1. Är er organisation förberedd?

Förstärkning av individers rättigheter

Ökat ansvar för PUA

Accountability

Stärkt roll Dataskyddsombud

Det nya regelverket förutsätter att personuppgiftsansvariga:

- Tar sitt ansvar självständigt
- Kan redovisa hur man följer lagen och skyddar personuppgifterna (Accountability)
- Har dokumentation som kan bevisa det - Samla bevis!

2. Dokumentera vilka personuppgifter ni hanterar

- Registerförteckning
- Den personuppgiftsansvarige måste hålla ett uppdaterad förteckning över alla behandlingar av personuppgifter i verksamheten
- Både för strukturerad och ostrukturerad behandling

Nyheter: Den personuppgiftsansvarige ska ha en registerförteckning. Artikel 30

- Den personuppgiftsansvarige måste hålla ett register över alla behandlingsändamål i sin verksamhet, både för strukturerad och ostrukturerad behandling. Artikel 30.
- Den ska innehålla, namn och kontaktuppgifter för PuA och för dataskyddsombudet, ändamål med behandlingen, kategorier av registrerade, kategorier av personuppgifter, kategorier av mottagare av uppgifter, om uppgifter överförs till tredje land och vilket land det är, om möjligt bevarandetid för personuppgifter, och en allmän beskrivning av säkerhetsåtgärder.
- Idag gäller en likadan skyldighet för personuppgiftsombudet. Ostrukturerad behandling av personuppgifter omfattas inte.
- SKL ska ta fram en mall för hur förteckningen kan se ut.

Nyheter: utökad skyldighet att informera de registrerade. Artikel 13-14

- Information som PuA ska lämna självmant till den registrerade, utöver det som gäller idag ska information också lämnas om.
- 1.När uppgifter samlas in från den registrerade: Den rättsliga grunden för behandlingen, hur länge verksamheten avser att behandla personuppgifterna eller de kriterier som bestämmer lagringstiden. Rätten att inge klagomål till Datainspektionen. Dataskyddsombudets kontaktuppgifter. I förekommande fall överföring av uppgifter till tredje land, t ex lagring i molntjänster.
- 2. När uppgifter samlas in från någon annan, ska den pua lämna information senast när uppgifter lämnas ut första gången. Samma uppgifter som enligt ovan ska lämnas plus dessutom uppgift om varifrån personuppgifterna inhämtats och i förekommande fall om de har sitt ursprung i allmänt tillgängliga källor.

Undantag från informationsskyldigheten. Artikel 13-14

- Undantag från skyldigheten att lämna information gäller om den registrerade redan förfogar över informationen.
- Ifall personuppgifter inhämtas från annan än den registrerade, så behöver information inte heller lämnas om inhämtande eller utlämnande av personuppgifter föreskrivs i en medlemsstats nationella rätt. T ex behandling med stöd av patientdatalagen och socialtjänstens registerlag (SoL-PuL). Information behöver inte heller lämnas om det visar sig vara omöjligt eller skulle medföra oproportionell ansträngning att söka fram uppgifterna (särskilt arkiv, forskning och statistik)

Nyheter: De registrerades rättigheter stärks. Artikel 15 och 20

- De registrerade har rätt att på begäran få ett s k registerutdrag med ”sina uppgifter”. Nyhet att begäran ska kunna ges in elektroniskt. Utdraget med de uppgifter som behandlas ska kunna lämnas ut i ett elektroniskt, allmänt använt format.
- Den registrerade som begär registerutdrag måste kunna identifieras. Hur? E-underskrift eller på namnteckning på papper.
- Nyhet! Den registrerade har rätt till dataportabilitet, i de fall den rättsliga grunden för behandlingen är den registrerades samtycke eller ett avtal med den registrerade. Rätten innebär att den registrerade ska på begäran ha rätt att få de uppgifter som rör hen och som denne tillhandahållit. Den PuA ska kunna leverera uppgifterna i ett elektroniskt allmänt använt format. Dessutom, om den registrerade begär det, och det är tekniskt möjligt, ska PuA föra över uppgifterna till en annan PuA.

Nyheter: Skyldighet att ha dataskyddsombud. Artikel 37-39

- Gäller bl a för alla myndigheter och offentliga organ.
- Varje nämnd ska förordna en person att vara dataskyddsombud. Flera nämnder kan förordna samma ombud. Kan vara anställd i organisation eller en extern uppdragstagare.
- Den PuA ska på olika sätt stödja dataskyddsombudet i dennes roll, bl a genom att tillhandahålla resurser, se till att ombudet bjuds in att delta i alla frågor som rör planering och uppbyggnad av nya typer av behandling av personuppgifter i verksamheten, informationssäkerhet m.m. Den Pua ska säkerställa att det inte finns några intressekonflikter för ombudet i utövandet av uppdraget, samt att denne inte tar emot några instruktioner som gäller utövandet av sina uppgifter.
- Dataskyddsombudet ska informera den PuA och de anställda om relevanta lagar och regler inom persondataskyddsområdet. Övriga uppgifter räknas upp i förordningen.

Nyheter:Rapporteringsskyldighet vid personuppgiftsincidenter. Artikel 33-34

- En PuA som drabbas av en personuppgiftsincident måste anmäla den till Datainspektionen, om möjligt, senast inom 72 timmar från det att man fick vetskap om att den inträffat. Incidenten kan t ex ha skett genom dataintrång (brottsligt angrepp) eller utlämnande eller förstöring av uppgifter genom slarv el olyckshändelse.
- Förordningen innehåller krav på vad incidentrapporten ska innehålla och att rapporten ska sparas, vilket tillsammans med den korta tidsfristen, gör att man måste ha rutiner på plats för att utreda, dokumentera, rapportera en sådan incident. T ex bör ansvaret för att göra en anmälan om inträffad incident pekas ut i organisationen.
- Om det är osannolikt att en inträffad incident medför risk för de registrerades integritet så behöver anmälan inte göras.
- Om incidenten kan leda till allvarliga risker för de registrerades integritet så ska också de registrerade som drabbats informeras om händelsen.

Nyheter: Konsekvensbedömning avseende dataskydd. Artikel 35

- Om behandling av personuppgifter planeras och den sannolikt leder till hög risk för enskildas friheter och rättigheter ska den PuA göra en konsekvensbedömning avseende dataskyddet.
- Det kan handla om behandling i stor omfattning av känsliga personuppgifter, en systematisk bedömning av fysiska personers personliga egenskaper inbegripet profilering eller systematisk kameraövervakning av allmän plats.
- Samråd med Datainspektionen ska göras.
- Datainspektionen ska komma med vägledning om vilka typer av behandling som ska omfattas av kravet på konsekvensbedömning.

Nyheter: utvidgade krav på avtalen med personuppgiftsbiträden. Artikel 28

- Personuppgiftsbiträde är en som behandlar personuppgifter för den PuA:s räkning. Särskilt biträdesavtal ska finnas.
- Ett biträde måste i avtalet kunna ge tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder, på sådant sätt att behandlingen uppfyller förordningens krav och att man säkerställer att de registrerades rättigheter skyddas.
- För att biträdet ska få anlita ”underbiträden” krävs ett särskilt eller allmänt skriftligt förhandstillstånd från den PuA. Om ett allmänt förhandstillstånd erhållits ska biträdet informera PuA om eventuella planer på att anlita nya underbiträden så att PuA kan göra invändningar mot förändringen.
- Biträdet ska i avtalet säkerställa att alla personer hos biträdet med behörighet att behandla personuppgifter har åtagit sig att iaktta konfidentialitet eller omfattas av lämplig lagstadgad tystnadsplikt.

Nyheter: utvidgade krav på avtalen med personuppgiftsbiträden. Artikel 28

- Avtalet ska innehålla att biträdet ska hjälpa den PuA med att se till att skyldigheterna i artiklarna 32-36 fullgörs.
- Avtalet ska innehålla att biträdet, vid avtalets upphörande, ska beroende vad den PuA väljer, radera eller återlämna alla personuppgifter till den PuA, och radera alla befintliga kopior såvida inte lagring fortsatt krävs enligt unionsrätten eller nationell rätt i medlemsstaten.
- Om personuppgiftsbiträdet anlitar underbiträden för utförande av specifik behandling på PuA:s vägnar så ska det biträdet genom avtal åläggas samma skyldigheter ifråga om dataskydd som det som gäller i avtalet mellan PuA och PuB. Om underbiträdet inte fullgör sina skyldigheter ifråga om dataskyddet så ska PuB vara fullt ansvarig gentemot PuA för utförandet av underbiträdets skyldigheter

Nyheter: Sanktionsavgifter

- Skyldighet för den PuA eller personuppgiftsbiträdet att betala sanktionsavgift vid överträdelse av de flesta av förordningens bestämmelser. Reglerna gäller direkt för privat sektor. Om medlemsstaten beslutar, så gäller den även för offentliga myndigheter och organ. Förslag finns i SOU 2017:39 ”Dataskyddslag”.
- Sanktionsavgifter påförs av tillsynsmyndigheten=Datainspektionen
- Maximibeloppen för privat sektor är 10 milj. euro respektive 20 milj. euro, beroende på typ av överträdelse. För offentlig sektor är förslaget max 10 milj kr resp 20 milj kr.
- Sanktionsavgiftens storlek i det särskilda fallet beror på en sammanvägd bedömning av överträdelsens karaktär, svårighetsgrad, varaktighet, antalet berörda registrerade, vilken skada de lidit, om överträdelsen skett av oaktsamhet eller uppsåt.