Checklista för GDPR

Den 25 maj 2018 kommer den allmänna dataskyddsförordningen (GDPR) ersätta personuppgiftslagen och tillämpas i svensk lag. Förordningen omfattar alla organisationer som på något sätt behandlar personuppgifter, såsom företag och myndigheter. Syftet med förordningen är att säkerställa den personliga integriteten hos alla EU/EES-medborgare. Om din organisation har exempelvis ett CRM-system, register över anställda, eller behandlar personuppgifter som en del av organisationens verksamhet så kommer organisationen att behöva efterleva dataskyddsförordningen.

Personuppgifter kan vara allt som direkt kan kopplas till personer som namn, personnummer och email. Personuppgifter omfattar även information som indirekt kan knytas till personer som yrke, plats, fysiska egenskaper och sociala status. Exempelvis så är "säkerhetskonsult + Frösunda" en personuppgift eftersom med denna information kan man indirekt koppla till ett väldigt fåtal indentifierbara personer i Frösunda. Ett rättesnöre som brukar användas är att om informationen kan kopplas till mindre än sju personer så räknas det som en personuppgift.

Vi har sedan länge haft svensk lagstiftning som PuL (personuppgiftslagen) och PDL (patientdatalagen) för att skydda den personliga integriteten hos fysiska personer, men det har saknats eftertryckliga konsekvenser för de som inte har efterlevt regelverken. PuL uppstod 1998 från den Europeiska kommissionens dataskyddsdirektiv som trädde i kraft 1995. Införandet av Big data-analyser, utvecklingen av marknadsföring och informationssamhällets tjänster som Facebook har förstärkt debatten om personlig integritet. I january 2012 kom den Europeiska kommissionen med förslaget att genomförligt reformera dataskyddsdirektivet. Följden av detta blev att direktivet utökades och omvandlades till en förordning – en rättsakt som ska tillämpas i sin helhet bland alla EU/EES-länder under ett visst datum – med mycket större fokus på personers rättigheter och sanktionsavgifter.

Övergripande skillnader mellan PuL och GDPR:

- GDPR sätter den registrerades rättigheter mer i fokus än tidigare.
- Tillsynsmyndighetens möjligheter till sanktioner stärks – max sanktionsavgift på 4% av den globala omsättningen av föregående år eller 20.000.000 EUR, vilket som är större.
- Privacy by design – integritetsskydd ska finnas inbyggd i system redan från början och genomsyra hela livscykeln av systemet.
- Större krav på analyser, rutiner och dokumentation.
- Samtycket måste vara tydligare och krävs under fler omständigheter.
- Informationskravet till registrerade är hårdare.
- "Rätten att bli glömd" kommer att lagfästas i GDPR. Detta innebär att organisationer måste under vissa omständigheter radera alla personuppgifter tillhörande registrerade ifall dessa registrerade kräver det.
- Behandling av barns uppgifter kommer att kräva samtycke från vårdnadshavare för informationssamhällets tjänster (ex. Facebook, Instagram).
- Nya förutsättningar inom marknadsföringen (profilering/selektering).
- Din organisation måste under vissa omständigheter anlita ett dataskyddsombud.
- Leverantören (personuppgiftsbiträdet) blir tillsynsobjekt. Personuppgiftsbiträden, som inte kunde bli straffade genom PuL, kan nu få sanktionsavgifter om de bryter mot förordningen.
- Det ställs större krav på biträdesavtalen, de kommer att behöva skrivas om.
- Missbruksregeln i PuL förvinner. All behandling av ostrukturerad data (e-post, fritext i dokument, ljudfiler) omfattas av hela lagen utan att det finns särskilda undantag.
- Hårdare krav när det kommer till incidenthantering – incidentrapporter kommer att behöva skickas till datainspektionen inom 72 timmar för större incidenter.

Den nya förordningen kommer att kräva nya organisatoriska och tekniska åtgärder i din organisation. Ledningen bör initiera projektet för GDPR-efterlevand och fördela ansvar och nödvändiga resurserna. Det är viktigt att det finns ett samarbete mellan alla relevanta avdelningar i organisationen och att de efterstävar samma mål, detta är INTE bara ett IT-projekt som bara rör IT-avdelningen.

Det finns två sidor av ett dataskyddsprojekt

1. Den mjuka delen – Ledning, dokumentation, policy, utbildning, administration.
2. Den hårda delen – IT-säkerhet och rena systemkrav.

Mjuka krav:

1. Upprätta ett register som omfattar bland annat kategorier av personuppgifter som behandlas, ändamål med behandlingen, biträden/ansvariga där det finns överföring av personuppgifter, etc. (Artikel 30) Denna registerföring samt kartläggning av system är ett första steg till en åtgärdsplan.
2. Avgör den lagliga grunden för behandling av personuppgifter. Här bör samtycke alltid övervägas sist av alla möjliga grunder. (Artikel 6)
3. Avgör ifall organisationen följer principerna i förordningen. (Artikel 5)
4. Avgör ifall organisationen kan tillförse de registrerade de rättigheter som finns i förordningen (rätten till radering, rätten till dataportabilitet, rätten till tillgång...)
5. Ta reda på ifall organisationen behöver anlita ett dataskyddsombud. (Artikel 37)
6. Uppdatera biträdesavtalen – fastställ era förpliktelser inom GDPR gentemot era kunders/leverantörers förpliktelser. (Artikel 28)
7. Framställ integritetspolicy. Det är dags att öppna sig till intressenter med vad/hur/varför personuppgifter behandlas i organisationen. Öppenhetsprincipen kräver att denna information ska vara lättillgänglig och att enkelt språkbruk används.
8. Framställ dataskyddspolicy, intern information där det bland annat finns en dokumenterad process för incidenthantering.
9. Avgör ifall organisationen behöver genomföra en konsekvensbedömning. (Artikel 35)
10. Om din organisation är verksam internationellt så måste det fastställas var organisationen har sin centrala förvaltning så att organisationen svarar under korrekt tillsynsmyndighet. I Sverige är tillsynsmyndigheten datainspektionen.

Hårda krav:

1. Privacy by design – System kommer att behöva ett inbyggt dataskydd som genomsyrar hela livscykeln, från kravinsamling till förvaltning.
2. Pseudonymisering och kryptering – behandling av känsliga/extra skyddsvärda personuppgifter kommer att kräva starkare integritetsskydd.
3. Gallring – framställning av rutiner och tekniska lösningar för gallring av personuppgifter.
4. Behörighetskontroller – Bara personer med rätt behörighet ska ha åtkomst till personuppgifter. Fördela roller inom organisationen och gör så att anställda bara har tillgång till den information som är nödvändig för yrkesrollen.
5. Logghantering – Införande av loggar som ger adekvat spårbarhet. Vid en personuppgiftsincident är det väsentligt att det finns bevisunderlag och det kommer loggar att kunna bidra med.
6. Sårbarhetsanalyser – penetrationstester och sårbarhetsskanning kan kartlägga sårbarheter i systemen.
7. Övriga tekniska åtgärder – SNTP, härdning av system, övervakningssystem, brandvägg-/antivirus konfiguration.

Lycka till önskar vi från 24 Solutions och Legalworks!