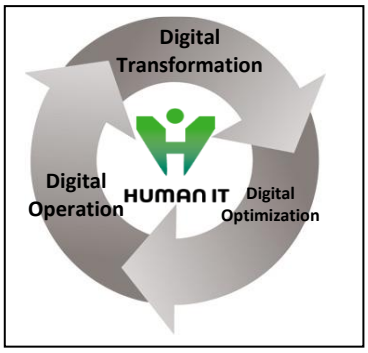
Om GDPR (EU´s Dataskyddförordning)

Ett Whitepaper från Human IT

av Lars Wendestam

Lars arbetar som senior Business Consultant på Human IT. Lars har lång erfarenhet av s.k. compliance gentemot standarder och regelverk inom IT-området. Lars har också utvecklat riskmodellen PRM som kan användas för att skräddarsy riskanalyser.



GDPR – Vad är det?

GDPR[1] (Genaral Data Protection Regulation) kallas på svenska för **Dataskyddsförordningen**. Denna utgör den lagstiftning avseende hantering av personuppgifter som ersätter PUL[2] (Personuppgiftslagen) den 25 maj 2018. PUL bygger på ett EU-direktiv från 1995 (kallad dataskyddsdirektivet 95/45/EG) och infördes som lag i Sverige den 1 oktober 2001. Med GDPR tas nästa steg mot en mer enhetligt lagstiftning inom hela EU. Dessutom har det hänt en hel del rörande informationsbehandling sedan mitten av 1990-talet, vilket har föranlett EU att skärpa dataskyddet för fysiska personer. GDPR gäller enbart för fysiska personer, ej för juridiska personer och ej heller för fysiska avlidna personer.

Skillnaden på en förordning och ett direktiv från EU

Det förra regelverket gällande dataskydd var ett direktiv, medan GDPR är en förordning. Vad är skillnaden? Vi är ganska vana vid att det kommer EU-direktiv som påverkar EU-ländernas befintliga lagstiftning. Därvid följer att ett direktiv ofta föranleder en omarbetning av en nationell lagstiftning. Exempelvis påverkade 1995-års dataskyddsdirektiv utformningen av PUL (lag 1998:204) som ersatte den tidigare Datalagen. Denna blev lag först 2001, vilket innebär att det uppstår en tidsförskjutning för att kunna skriva om en lag och sedan ersätta den baserat på ett EU-direktiv. När det gäller en förordning sker processen på ett helt annat sätt. En förordning blir lag samtidigt i alla EU-länder utan tidsförskjutning. Därför är det viktigt att inse att de nya regler som följer med GDPR kommer att bli lag direkt i Sverige den 25 maj 2018. Dessa innefattar också höga bötesbelopp om man inte följer

dem. Bötesbeloppen enligt GDPR kan uppgå till 4% av företagets globala omsättning alternativ 25 miljoner Euro. Risken att råka ut för dessa gigantiska bötesbelopp innebär givetvis att alla företag och organisationer behöver se över vilka konsekvenser GDPR-regelverket får i verksamheten. Det är också troligt att man behöver genomföra åtgärder för att kunna uppfylla förordningen.

Två år från beslut till lag

Dataskyddsförordningen antogs av Europarlamentet i april 2016 och man har därmed givet medlemsländerna 2 år på sig att säkerställa att förordningen efterlevs. Eftersom detta också påverkar beroenden till annan landspecifik lagstiftning samt förändringar i hur respektive lands kontrollmyndighet (motsvarigheter till svenska Datainspektionen) arbetar, är tiden knapp. Dessutom är företag och organisationer som ska följa regelverket beroende av att alla landspecifika beroenden är klarlagda. Med den respittid som regeringen givet för att ha detta arbete färdigställt, kommer den reella tiden för att få allt på plats bli mindre än ett år. Det är därmed viktigt att komma igång med GDPR-införandet i tid.

Att tolka nya Dataskyddsförordningen

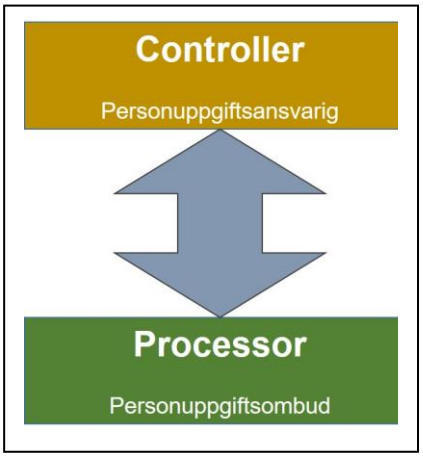
Den nya dataskyddsförordningen bygger givetvis på det äldre dataskyddsdirektivet, men man har också genomfört en hel del skärpningar gällande ansvaret för att skydda information rörande fysiska personer. Det är därför inte med automatik att man uppfyller GDPR, bara för att man uppfyller PUL. Under årens lopp har det också utformats rutiner för hur man kan hantera det gamla EU-direktivet om man t.ex. utgör en koncern med verksamhet i många länder. Bland annat genom s.k. CBR (Corporate Binding Rules) eller Bindande Företagsbestämmelser, som det kallas på svenska. Om man har sådana eller andra undantagsregler (t.ex. s.k. Private Shields) behöver dessa tolkas om gentemot GDPR. Det finns också många andra formuleringar i förordningen som behöver tolkas och förstås på ett riktigt sätt. Kan man t.ex. flytta ett tidigare medgivande enligt PUL till att automatiskt omfatta GDPR, eller måste alla tidigare medgivanden att lagra personlig information göras om?

Ett utökat skydd för individen

En viktig förändring i GDPR är ett utökat skydd för information som rör fysiska personer. Bland annat ska en fysisk person om vilken den lagras information ha rätt till följande:

- Behandling ska ske med samtycke (consent) från individen, med vissa undantag
- Samtycke av föräldrar rörande minderåriga, med vissa undantag
- Kunna ta tillbaka samtycket lika enkelt som det gavs, med vissa undantag
- Rätt att få veta vem som är ansvarig för de personuppgifter som lagras
- Rätt att få tillgång till information om vad som finns lagrat
- Rätt att få gjort rättelser om informationen är felaktig
- Rätt till radering (att få bli bortglömd) med vissa undantag
- Rätt till dataportabilitet, d.v.s. kunna föra över information via ett gränssnitt typ API eller liknande
- Rätt att göra invändning mot de uppgifter som finns registrerade
- Rätt att inte bli föremål för beslut enbart baserat på automatiserad behandling
- Rätt att bli informerad när en personuppgiftsincident uppstår

Controllers och Processors



En viktig del i förordningen är uppdelningen s.k. ”***Controllers***” och ”***Processors***”. Dessa finns redan i PUL, men ansvarsfördelningen har förändrats i GDPR. I den svenska översättningen, samt i PUL kallas motsvarande roller för ”***Personuppgiftsansvarig***” respektive ”***Personuppgiftsombud***”. De engelska begreppen är mer tydliga vad rollerna avser. En Controller (Personuppgiftsansvarig) ansvarar för skäl och syfte till varför uppgifterna lagras och bearbetas. En Processor (Personuppgiftsombud) är en enhet (intern eller extern) som processar informationen för en Controllers räkning. Således är en servicebyrå eller datadriftsenhet att betrakta som en Processor. En Controller är normalt en juridisk person, men kan i vissa fall även vara en fysisk person. En processor kan vara en fysisk eller juridisk person. Eller som definitionen säger, ”*En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgift-sansvariges räkning*” I PUL låg ansvaret för informationsbehandlingen på Controllern. I GDPR får Processorn utökat eget ansvar, vilket innebär att man behöver se över konsekvenserna om man t.ex. är involverad i outsourcing. Antingen som beställare eller utförare. Det får också konsekvenser när man använder moln-tjänster av olika slag. Se vidare om detta nedan.

DPO – Data Protection Officer

En tydliggjord roll i GDPR är en **DPO (Data Protection Officer)**. I den svenska översättningen kallas denna roll för ”Dataskyddsombud”. Kan nog tycka att denna översättning är lite olycklig. När vi tänker på rollen ”skyddsombud” allmänt så är det sällan en person som kan verka direkt mot en ledning eller styrelse. Rekommenderar därför starkt att använda det engelska begreppet i stället. Detta för att ge den kraft till rollens ansvar som efterfrågas. En DPO, eller i större organisationer en DPO-funktion bemannad av flera personer, ska agera som en kontrollfunktion för att GDPR-regelverket efterlevs. Rent ansvarsmässigt är det Controllern och/eller Processorn som ansvarar för compliance (uppfyllande av dataskydd). Därav behöver man i en verksamhet, baserat på hur denna utför behandling av information om fysiska personer, förhålla sig till hur en DPO, Controller och Processor samverkar och vem som gör vad. Det är även tillåtet att dela en DPO med andra. Även att låta en extern organisation utföra DPOns uppgifter. Rent praktiskt behöver en DPO kunna agera ungefär som en internrevisor. Bland annat att denne inte har andra parallella arbetsuppgifter som riskerar att komma i konflikt med vad som krävs som DPO.

Vad behöver göras innan den 25 maj 2018

Vad som behöver göras innan den 25 maj beror givetvis på vilken typ av verksamhet man är och i vilken grad man hanterar information rörande fysiska levande personer. Företag eller andra organisationer som har stor den av sin verksamhet inom B2C (Business to Consumer) får större påverkan än om man till största del arbetar inom B2B (Business to Business). Men även här finns HR-register m.m. så merparten av företag, myndigheter och organisationer berörs.

Rekommenderat är att under 2017-års första halva, genomföra en förstudie eller motsvarande där man belyser hur verksamheten berörs av GDPR-regelverket. Därefter behöver man tid att genomföra åtgärder. En aktivitet som alla måste göra är att gå igenom alla system och rutiner där man bearbetar personuppgifter. Sådana system och rutiner måste dokumenteras. Det finns även stor sannolikhet att man kan behöva göra förändringar eller tillägg i de system som används. Förutom detta behöver man införa nya rutiner och processer för att säkerställa att man inte bryter mot lagen. Bland annat finns en rapporteringsskyldighet till Datainspektionen (eller motsvarande organ i andra länder) gällande personuppgiftsincidenter. Detta ska ske inom 72 timmar. Vid allvarliga sådana ska också information ske till de som är berörda. Med tanke på hur ofta vi hör talas om hackerattacker där man kommit över känslig information blir det viktigt att sådana rutiner finns etablerade i förväg. Det behövs även tid för att tolka och förstå regelverket. En utgångspunkt kan vara det förhållningssätt man haft till PUL. GDPR bygger vidare på PUL, så har man t.ex. redan utsett dataskyddsombud enligt PUL, har man kommit en bit på väg för att etablera en DPO.

Hur göra om man har verksamhet i flera länder?

Om man är en verksamhet som finns i flera länder behöver man också förhålla sig till de regler som gäller avseende att överföra information om fysiska personer mellan länderna. Inom EU gäller förordningen i alla medlemsländer, men det finns delar som överlåtits till varje land att utforma mer specifikt. En grundläggande princip är att identifiera vad som är ”huvudsakligt verksamhetsställe”, bland annat i syfte att identifiera vilken kontrollmyndighet som har huvudansvaret. Landsfrågan har olika nivå av komplikation om man verkar enbart inom EU, eller om även andra länder utanför EU är involverade. Man behöver också se över hur man t.ex. använder outsourcing i lågprisländer som Indien eller Filippinerna. Enligt regelverket måste sådana länder ha en ”adekvat skyddsnivå”. Vad detta innebär behöver närmare tolkas. Viktigt är även att beakta all typ av information. I det gamla direktivet, som PUL baserats på, fanns en undantagsregel för information som fanns i ostrukturerad data. Detta undantag är numera borttaget vilket t.ex. innebär att även information som berör bildövervakning m.m. behöver beaktas.

I det befintliga regelverket har det utvecklats praxis for hur man kan hantera ansvar för en global koncern som finns i många länder. Bland annat genom BCR (Binding Corporate Rules). Dessa har sedan förfinats genom BCR-C för Controllers och BCR-P för Processors). Detta alternativ finns även i GDPR, men man behöver se över befintliga BCR så att de även täcker in nya krav enligt GDPR.

Konsekvenser om man använder ”Cloudlösningar”

Om man använder molntjänster (Cloudlösningar) behöver dessa beaktas speciellt. I det nuvarande EU-direktivet låg ansvaret primärt på Controllern och inte på Processorn. En cloudleverantör är att betrakta som en Processor, varför nu även denne får utökat eget ansvar. Därav behöver man definiera det ansvar som åligger cloudleverantören i egenskap av att vara en Processor. Finns

dessutom Cloudleverantören i ett annat land, kanske även utanför EU, behöver man även förhålla sig till rätten att behandla informationen i detta land. Man behöver därmed veta var cloudlösningen fysiskt finns placerad.

Det är rimligt att anta att stora cloudaktörer som AWS (Amazon), Azure (Microsoft) med flera kommer att beskriva sin roll som Processor och hur de uppfyller GDPR-regelverket. Dock är informationen som behandlas kundunik varför man behöver analysera sin egen specifika situation.

Beroenden gentemot andra standarder och lagstiftning

GDPR är en lag som i sig måste följas, men den har också beroende till andra lagar. Ett exempel är den svenska patientdatalagen[3] (lag 2008:355). Justitiedepartementet utreder f.n. sådana beroenden och ska komma med en slutrapport den 12 maj 2017. Förutom beroenden till andra lagstiftningar bör man även förhålla sig till andra standarder som berör hur man hanterar känslig information om fysiska personer. Exempel är:

- PCI DSS[4] gällande säkerhet för betalkort (PCI Data Security Standards)
- ISO 27001 gällande Informationssäkerhet
- ISO 27018 och 27018 som berör kompletterande Informationssäkerhet rörande cloudlösningar

Lämpligt är att man tar hjälp av de standarder som finns för att skapa rutiner och verktyg för att upprätthålla en tillräckligt bra säkerhet. I detta ingår att etablera rutiner och processer för att kontinuerligt utvärdera och förbättra säkerheten.

GDPR om man har egen systemutvecklingsenhet

GDPR berör även området när det gäller att utveckla egna lösningar där man bearbetar information om fysiska personer. Att redan i designen av nya lösningar ta hänsyn till att man inte lagrar mer information än vad som behövs. Även att säkerställa att man gör gallring av sådant som inte längre behöver sparas, eller anonymiserar så att kopplingen till en fysisk identifierbar individ inte längre finns. Detta går under begreppet ”***Privacy by design***” och behöver arbetas in i rutiner och regler hos den egna utvecklingsavdelningen.

I detta sammanhang kan det också finnas skäl att förhålla sig till ramverk som stödjer hur man utvecklar ”säker kod”. Det är ofta här det brister, när hackers lyckas komma över sådan information som utgör personuppgiftsincidenter. Det finns ett antal ramverk som stödjer att utveckla system och kod på ett säkert sätt. Dessa går under beteckningen ”Software Security Frameworks” eller SSFs. Några av dem är SAFECode[5], BSIMM[6] och Microsoft SDL[7]. Kombinationen att inte hantera mer personlig information än vad som behövs och att använda stöd för att utveckla säkrare kod är områden som båda kan minska risken för att personuppgiftsincidenter uppstår.

Riskanalyser

För att kontinuerligt kunna bedöma och utveckla säkerheten behöver man löpande genomföra riskanalyser. Till ISO 27001 finns standarden ISO 27005 som beskriver riskanalyser relaterat Informationssäkerhet. Alternativt kan man förhålla sig till den generella ISO standarden för riskanalyser (ISO 31000). Även GDPR beskriver ett behov av att göra löpande ”konsekvensbedömningar” gällande hur man hanterar personuppgifter. Dessa kallas för ***DPIA (Data***

Protection Impact Assements) i den engelska utgåvan. Ett lämpligt förhållningssätt kan vara att genomföra en riskanalys som tar ett helhetsgrepp. En riskanalys som inte bara berör bedömningen av hur man hanterar behandling av personuppgiftsdata, utan som del i en helhet i vad man brukar kalla för ERM (Enterprise Risk Management). Lämpligt är att hur man hanterar information som behandlas i GDPR, finns upplyft som en ”Corporate Risk Factor” som kommenteras löpande i årsredovisningen, Om man etablerar rutinerna på ett sådant sätt kommer en DPO-roll eller DPO-funktion lättare att för rätt mandat i organisationen.

En riskmetod som tillåter att man skräddarsyr olika typer av riskanalyser från olika standarder och ramverk är PRM[8]. Med PRM kan man sätta samman riskanalyser som kombinerar t.ex. GDPR krav, med ISO 27001 krav samt andra mer verksamhetsspecifika krav.

Behöver du mer hjälp och vägledning?

Detta Whitepaper har berört GDPR översiktligt med syfte att ge en insikt i hur det kan påverka verksamheten och vilka typ av frågeställningar som behöver beaktas när man skall förhålla sig till att kunna följa den nya lagstiftningen. Detta täcker dock ej allt, utan alla områden kan fördjupas ytterligare.

Vi har tagit fram en processmodell som stödjer ett arbetssätt att initiera, analysera och genomföra det arbete som krävs enligt GDPR.

Kontakta gärna något av våra kontor för att diskutera ditt behov rörande att uppnå en GDPR-efterlevnad.

Om GDPR Processmodell

Vår processmodell för att uppnå en GDPR-efterlevnad i organisationen beskriver ett fasindelat arbetssätt för att på kort tid kunna genomföra det analysarbete som är nödvändigt. Modellen innehåller också ett steg för att genomföra en GDPR-Asssement.

Om Human IT

Human IT´s framgång bygger på riktigt nöjda kunder och engagerande medarbetare. Vi levererar det stora företagets IT-kompetens med den enskilde konsultens engagemang.

Vi hjälper våra kunder och stärker deras konkurrenskraft genom att tillföra generell samt strategisk IT-kompetens, åtaganden och lösningar med engagerade konsulter.

Våra kunder är i första hand organisationer och företag som har behov av konsulter och lösningar inom olika erbjudandeområden och söker en snabb, kvalitativ och engagerad leverantör. Genom att kombinera teknisk spetskompetens inom områdena Infrastruktur, Applikation samt Business Consulting och kunskap om våra kunders verksamhet tillför vi en helhetssyn inom IT-området. Human IT startade 2007 och finns idag med egna kontor i Stockholm, Göteborg, Malmö.

Human IT arbetar inom området som berör den förändring som krävs både organisatoriskt och verksamhetsmässigt för att möta den ökande digitaliseringen i samhället. Detta är en kontinuerlig process som vi valt att dela upp i:

- **Digital Transformering**
- **Digital Optimering**
- **Digital Operation**

Inom området **Digital Transformering** ingår analyser och genomförande av utredningar för att göra förändringar i verksamheter för att möta det ökande behovet av digitalisering. Det handlar om att organisera och etablera verksamhetsfunktioner för att understödja tjänster i så väl offentliga verksamheter som privata företag. Med **Digital Optimering** avses förbättringar i nuvarande tjänster som krävs för att kunna uppnå de effekter som efterfrågas i en digital transformering. Det berör utveckling och stöd inom internetbaserade tjänster som Web-services, API-Management, IoT (Internet of Things), Internet of Value med flera. I **Digital Operation** ingår att kunna etablera tjänster som i allt högre grad sker i ”molnet” genom att utnyttja ”**cloudtextjänster**” från leverantörers som AWS (Amazon Web Sevices), Microsoft Azure med flera. För att möta alla utmaningar som finns i den pågående digitaliseringen krävs ett kontinuerligt arbete med att transformera, optimera och etablera nya tjänster med ny eller gammal infrastruktur.

För mer information, se http://humanit.se

Noter

1. GDPR I svensk översättning - http://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=OJ:L:2016:119:FULL&from=SV
2. PUL (Personuppgiftslagen) - http://www.notisum.se/rnp/SLS/lag/19980204.HTM
3. Patientdatalagen - http://www.notisum.se/rnp/sls/lag/20080355.htm
4. PCI DSS - https://www.pcisecuritystandards.org/
5. SAFECode - https://safecode.org/
6. BSIMM - https://www.bsimm.com/
7. Microsoft SDL - http://www.microsoft.com/en-us/sdl/default.aspx
8. PRM - http://www.ekerlids.com/Ta-kontroll-over-riskprojekten%21-p2046