Nya EU-förordningen

Lösningar kring personligt dataskydd

Innehåll

1 Nya EU förordningen kring personligt dataskydd

1.1 NYA EU-FÖRORDNINGEN

Det har ju pratats länge om de nya reglerna för att skydda personlig integritet och underlätta IT utvecklingen med gemensamma lagar på området inom EU.

Plötsligt händer det upplever nu nog många! Med viss oro…..

Den nya dataskyddsförordningen ska ge enskilda större kontroll över sina personuppgifter men ändå tillgodose organisationers behov av att kunna behandla personuppgifter. Sverige har fått gehör för vår grundlagsreglering om offentlighetsprincipen och yttrandefriheten men behöver nu anpassa lagstiftningen på bästa sätt.

(Många har skrivit om vad förordningen innebär och för den som ännu inte är insatt kan mer information hämtas på exempelvis Datainspektionen och Regeringskansliets hemsidor.)

1.2 KONSEKVENSER OM MAN INTE UPPFYLLER KRAVEN

Men sett ur ett informationssäkerhetsperspektiv och om man arbetar med ett ledningssystem så är detta egentligen ”bara” ytterligare ett krav att ta hänsyn till. Låt vara att konsekvenserna nu är extra tydliga. Det är ju inte bara förtroende och varumärke som står på spel utan också viten på 20 M euro eller 4 % på global omsättning. Detta är en signal som är mycket tydligare och som säkert får många ledningar och styrelser att reagera och inte minst agera.

För den operativa ledningen så innebär det att man måste ha svar på hur man arbetar med frågan och försäkra styrelsen om att riskerna är under kontroll.

1.3 HUR ARBETAR MAN IDAG?

Det kan tyckas att 2018 när lagen träder i kraft ligger långt bort men ska man få ordning på det här så bör man oavsett börja det interna arbetet nu, speciellt om man är en större aktör med verksamhet i många länder.

Beroende på hur väl förberedd man är, ju lättare är det att svara för förstås. När vi ser på verksamheter i stort så är det två saker som kraftigt påverkar hur man ska agera:

1. Följer man PuL som lagen är tänkt idag?
2. Arbetar man strukturerat med informationssäkerhet enligt ett ledningssystem baserat på ISO/IEC 27001?

1.3.1 PuL

Att man följer PuL (1), inte bara pliktskyldigast utan verkligen har koll på hur man hanterar information som omfattas både internt och hos externa parter, så är det givetvis en bra start att se vidare på de nya kraven. Men vår bedömning är att man ändå ofta inte har arbetat på ett sådant sätt att man har kontroll på vilka informationsobjekt som kan vara aktuella och i vilka IT-system/tjänster dessa kan finnas. Både identifieringen och värderingen/”impact” saknas. Detta innebär att man inte följer nya förordningen. Detta innebär också att det inte går att göra korrekta riskbedömningar.

1.3.2 Ledningssystem för informationssäkerhet

Har man arbetat med ett ledningssystem på för informationssäkerhet (2) har man det betydligt enklare. Enklare, att både ha och få kontroll.

1.3.2.1 Ha kontroll

Enklare att ha kontroll genom att man redan har ett etablerat sätt att värdera information och se på risker utifrån olika krav/värden av informationen, samt sist men inte minst roller, ansvar och en tydlig ledningsprocess.

Ledningsprocessen, enligt ISO 27000 serien, innebär att en naturlig rapportering och beslutsprocess har skapats där ledningen kan ta sig an Informationssäkerhet från ett verksamhetsperspektiv.

Den processen kan även hantera den nya kravställningen i EU förordningen utan att behöva uppfinna eller skapa någon sidoprocess som både kräver extra resurser och fokus. Verksamheten kan hantera den nya uppgiften som vilken annan större förändring som helst, det finns 20 miljoner skäl att göra det ordentligt.

1.3.2.2 Få kontroll

I Ledningsprocessen ska den som har rollen som informationssäkerhetschef samordna rapportering om hur väl man presterar inom informationssäkerhet utifrån ett nuläge baserat på bl.a.:

- Revisioner
- Prestandamätningar
- Risker
- Incidenter
- Vidare ska också förslag på förbättringar föreslås/presenteras.

Allt detta sker vid vad man kallar ”ledningens genomgång”. I detta fall så är det naturligt att förutom de vanliga punkterna avsätta tid för en längre genomgång av hur läget ser ut i förhållande till den nya förordningen och som en del i förbättringsarbetet starta ett projekt där rapportering osv. sker till ledningen vid ”ledningens genomgång”. (Beroende på organisation, komplexitet, mognad hos ledningssystemet, projektmodell osv. kan detta givetvis se lite olika ut men processen, tidpunkten och de rätta personerna finns där redan.)

Nästa steg är att informationssäkerhetschefen utnyttjar de verktyg som finns på plats genom att arbeta enligt ISO 27000 serien. Detta betyder främst:

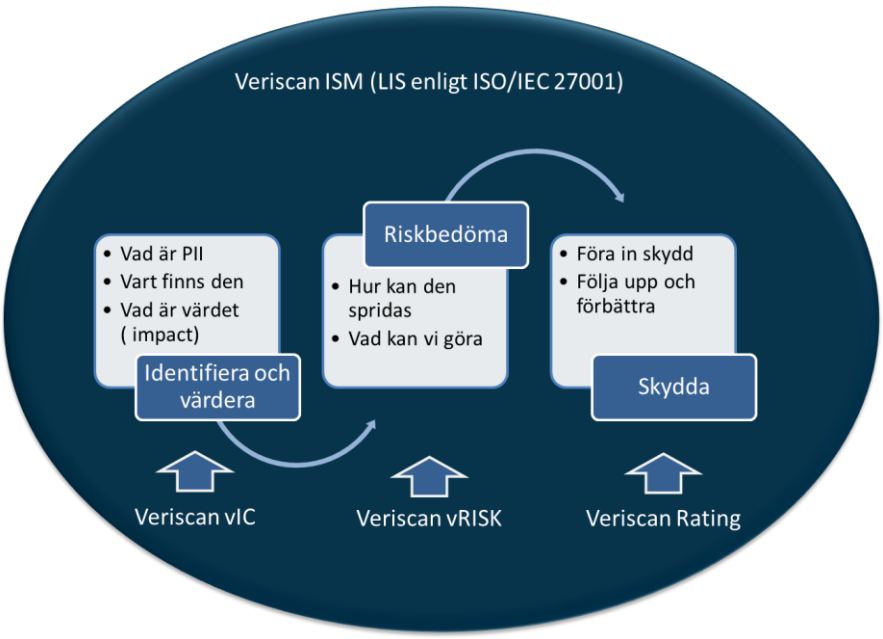
- Riskhanteringsprocess inkl. metod, roller och kriterier för riskacceptans.

- Klassificeringsmodell för identifiering och värdering av tillgångar inkl. register och ägare.

1.4 ANVÄND VERKTYGEN I VERKSAMHETEN

Vår långa erfarenhet av att arbeta med de här uppgifterna är att även om verktygen finns på plats så ställer den nya förordningen tydligare krav på att man måste använda dessa på ett mera heltäckande sätt. Verktygen måste användas ute i verksamheten mera konsekvent samtidigt som man måste man ha en överblick för att ge ledningen en så rätt bild som möjligt.

2 Vad kan Veriscan stödja med?



Bilden beskriver hur Veriscans verktyg och metoder används i de olika stegen som stöd att följa EU förordningen.

2.1 ERFARENHETER OCH VERKTYG

Vi på Veriscan har använt vår erfarenhet och kunskap från olika internationella standarder och utvecklat mjukvarustöd för att arbeta strukturerat med informationssäkerhet. Dessa verktyg gör det enklare att lösa kraven som den nya förordningen ställer. Verktyg som Veriscan vRISK™ och Veriscan vIC™ är applikationer som stödjer arbetet, men ger också möjligheter till samordning och analyser av aggregerad information.

2.2 KRAV PÅ DOKUMENTATION

Att arbeta med båda verktygen genererar enkel och tydlig dokumentation vilket EU förordningen kräver avseende dokumentation för identifiering och bedömning av personlig information samt risk. Givetvis ger verktygen även stöd för rapportering till ledning och styrelse.

2.3 UTVÄRDERING AV PRESTANDA

Nyttan och omfattningen av arbetet med informationssäkerhet kan vara svår att överblicka och det är ännu svårare att kunna styra prioriteringarna rätt. För att ytterligare öka på transparensen och bedömningen så bör prestandan mätas vilket kan ske med hjälp av Veriscan Rating.

2.4 LEDNINGSSYSTEM EN FRÅGA FÖR LEDNINGEN

Men för de organisationer som inte har ett ledningssystem för informationssäkerhet baserat på ISO 27000 så bör man även fundera lite till. Om informationssäkerhet är, eller att man bedömer att den blir, en ledningsfråga så bör man bedöma om man ska införa ett ledningssystem. Inte bara för att få stöd i att följa EU förordningen utan för att ha ett systematiskt sätt kunna hantera ett område som inte kommer att minska i betydelse i framtiden.

Naturligtvis med vår erfarenhet, både praktiskt och med internationella standarder som bas, har vi goda möjligheter att med olika stöd i metoder och verktyg inom Veriscan ISM att effektivt stödja ett införande av ett ledningssystem enligt ISO/IEC27001. Om en organisation ska certifiera sig eller inte, är en fråga vi kan hjälpa till att bedöma.

3 Framtiden för personlig information

Det är inte förvånande att EU agerar på detta område. Även om det kan ses som en utmaning så lägger arbetet med att följa förordningen grunden för en säkrare digital utveckling så att vi både kan nyttja de fantastiska möjligheter som begrepp som ”Big Data” och ”Internet of Things” (IoT) ger.

Helt enkelt, genom att veta vems informationen är och hur viktig den är, kan man därmed avgöra vilka IT lösningar och skydd som är lämpliga. I förlängningen, att också veta vem vi kan lita på kan hantera din och min personliga information. Vi har två år på oss men utmaningen är stor så låt oss inte vänta.

Veriscan
Verifying security since 1999