Policy för tekniska och organisatoriska åtgärder för dataskydd

14 juni 2018

Peter Dickson

Innehåll

Inledning

PRI hanterar stora mängder skyddsvärd information som vi antingen själva ansvarar för eller som vi hanterar för andras räkning. Detta gäller bland annat personuppgifter samt egna och kunders affärshemligheter. Övergripande regler för hur detta ska göras finns i våra avtal och i olika lagar, som Dataskyddsförordningen. Internt regleras vårt arbete av riktlinjer och instruktioner, och beskrivs praktiskt i policies, processbeskrivningar och liknande.

Denna policy beskriver övergripande hur PRI konkret arbetar för att uppfylla sina åtaganden och minimera riskerna runt den hanterade informationen.

Ur teknisk synvinkel skiljer sig inte skyddet av personuppgifter nämnvärt från skyddet av annan känslig information, såsom affärshemligheter eller kurspåverkande ekonomisk information. Däremot innehåller Dataskyddsförordningen vissa specifika krav på hanteringen av personuppgifter, som givetvis ska uppfyllas.

Denna översikt anger den aktuella miniminivån på de säkerhetsåtgärder som ska tillämpas. Det ingår dock i PRI:s åtaganden att fortlöpande förbättra säkerheten och anpassa skyddet till de nya hot som uppträder i omgivningen och de nya tekniska hjälpmedel som finns för att skydda information. På grund av det tekniska landskapets föränderlighet måste därför denna sammanställning vara principiell och övergripande.

Avtal med kund kan i vissa fall medföra att striktare åtgärder tillämpas än de generella som beskrivs i denna policy.

I de fall PRI använder underleverantörer för att uppfylla sina åtaganden ska PRI säkerställa att underleverantörerna utför de säkerhetsåtgärder som krävs av dem för att denna policy ska uppfyllas.

Organisation

PRI ska basera sitt säkerhetsarbete på vid var tid gällande lagstiftning samt bolaget styrande dokument som fastställs av bolagets VD eller styrelse samt avtal med kunder. Bolagets Informationssäkerhetsansvarige ska ansvara för att leda och samordna arbetet med informationssäkerheten inom verksamheten, med bland annat följande uppgifter:

- Ansvarar för styrande dokument på informationssäkerhetsområdet och deras efterlevnad
- Genomför riskanalys och riskhantering runt informationssäkerhet
- Samordnar arbetet runt regelefterlevnad på informationssäkerhetsområdet
- Övergripande kravställning på olika säkerhetsåtgärder

Det direkta ansvaret för informationssäkerheten i respektive system ska ligga hos en utsedd systemägare. Ansvarig för det tekniska säkerhetsarbetet ska vara IT-säkerhetsansvarig, vars ansvar bland annat är:

- Ta fram och utveckla regelverk för IT-säkerhet
- Koordinera säkerhetsaktiviteter
- Analysera logiska (och fysiska) risker
- Leda hantering av säkerhetshot och säkerhetsincidenter

PRI ska vidmakthålla instruktioner för hur samtliga medarbetare inklusive underleverantörer ska agera för att minimera hot mot informationssäkerheten. Dessa instruktioner ska vara väl spridda till, förstådda av och tillämpade av samtliga berörda.

Allmänt om det tekniska säkerhetsarbetet

Grundprincipen för det tekniska säkerhetsarbetet hos PRI är att säkerhetsklassen avgör vilka krav som ställs på säkerhetsåtgärderna (typ av autentisering, kryptografiskt skydd etc.). De säkerhetsklasser som tillämpas är:

- Öppen - Information med full tillgänglighet för alla inom och utanför bolaget
- Intern - Information med tillgänglighet endast för medarbetare
- Konfidentiell - Information med tillgänglighet för ett fåtal medarbetare
- Hemlig - Mycket känslig information (till exempel känsliga personuppgifter) med tillgänglighet för ett fåtal medarbetare

Konfidentiell eller hemlig information ska alltid klassas. All information som tillhör kunder och alla personuppgifter är klassade som minst konfidentiella.

Konfidentiell eller hemlig information kallas i det följande ”skyddsklassad”.

Kontinuitetsplanering

PRI ska vidmakthålla kris- och beredskapsplaner för sin informationsbehandling med syfte att minimera störningar i verksamheten inklusive åtaganden i förhållande till kunder vid extrema händelser såsom till exempel brand i datahall.

Åtkomst/behörighet

Skyddsklassad information ska skyddas från alla former av otillåten behandling, såsom oavsiktlig och avsiktlig förstöring, obehörig tillgång och otillåten spridning.

Åtkomsten till skyddsklassad information ska begränsas till personer som arbetar på PRI eller på uppdrag av PRI och som dessutom behöver informationen för att utföra sina arbetsuppgifter. Varje individs åtkomst ska begränsas till den information och de rättigheter som behövs för uppgiftens fullgörande.

PRI ska ha behörighetskontrollsystem som förhindrar obehörig åtkomst till skyddsklassad information. Åtkomst till informationen ska ske med personliga användaridentiteter. Åtkomst till hemlig information, exempelvis känsliga personuppgifter, ska kräva speciell behörighet och/eller förstärkt skydd.

Det ska finnas utpekade funktioner som får godkänna, ändra eller återkalla behörigheter. Behörigheter som inte används ska inaktiveras.

Behörigheter avseende åtkomst till skyddsklassad information ska revideras minst en gång per år eller oftare utifrån säkerhetsklass.

Ansvarsfördelning

Fördelning av ansvar mellan individer ska göras så att risken för missbruk minimeras, till exempel så att samma individ inte kan genomföra en systemändring och sedan produktionssätta ändringen.

Tester

Skyddsklassad information får inte finnas i test- eller utvecklingsmiljöer och får inte användas i system- eller enhetstester.

Dualitet

Dualitet ska tillämpas för riskutsatta åtgärder, såsom utbetalningar. Detta innebär att åtgärden inte kan genomföras om inte två individer med tillräcklig behörighet har godkänt den.

Spårbarhet

Riskfulla systemåtgärder som utförs av användare ska automatiskt loggas i en separat tabell, som inte kan förändras av användarna. Åtgärd, användare och - i förekommande fall - före- och eftervärde ska sparas.

Övervakning

Övervakning av teknisk infrastruktur ska utföras kontinuerligt och utvärderas dagligen.

Fysisk säkerhet och miljöskydd

PRI ska begränsa åtkomsten till lokaler och anläggningar, där informationssystem som behandlar skyddsklassad information finns, till att endast omfatta identifierade behöriga personer. Lokalerna ska skyddas med larm för brand och inbrott.

Teknisk säkerhet

PRI ska ha säkerhetsåtgärder på plats för att minska risken för att skadlig programvara exekveras i IT-miljön. Dessa inkluderar brandväggar, skiktade nätverk samt att aktuella antivirusprogram med uppdaterade definitioner ska finnas på alla arbetsstationer. För servrar tillämpas en kombination av antivirusprogram och andra åtgärder, till exempel övervakning av trafik.

Lagring och överföring

Skyddsklassad information får endast då det är nödvändigt flyttas utanför PRI:s och dess underleverantörers anläggningar. Om det gäller kunds information måste flytten även vara i överensstämmelse med uppdraget och gällande avtal.

Skyddsklassad information får inte lagras på arbetsstationer, bärbara datorer eller mobila enheter utan kryptering. Den får inte heller överföras på publika nätverk utan kryptering.

Media som har använts för skyddsklassad information som tas ur drift måste rensas från all information på ett säkert sätt. Utskrivet material med skyddsklassad information ska förvaras på säkert sätt och destrueras när det inte längre behövs.

Säkerhetskopiering och återställning

PRI ska regelbundet minst dagligen göra säkerhetskopior av all information som inte är av temporär natur, samt minst årligen genomföra återställningstester.

Säkerhetskopiorna och dataåterställningsrutinerna ska lagras på en annan säker plats än där den primära datorutrustningen som behandlar informationen finns.

Efterlevnad av övriga GDPR-krav

PRI ska vid förfrågan bistå personuppgiftsansvarig med att ta fram/ändra individers person-uppgifter för vilka personuppgiftsansvarig ansvarar.

PRI ska vid avtalets upphörande, om inget annat avtalats, ta bort all information som omfattas av avtalet så länge detta inte hindras på legal grund.