IT-SÄKERHETSBOLAGET AB

Styrkan av ett **SYSTEMATISKT ARBETSSÄTT** och ett **ÅRSHJUL FÖR DATASKYDDSARBETET**

Styrkan av ett **SYSTEMATISKT ARBETSSÄTT** och ett **ÅRSHJUL FÖR DATASKYDDSARBETET**

Styrkan av ett systematiskt arbetssätt och ett årshjul för dataskyddsarbetet

IT-SÄKERHETSBOLAGET AB

Foto: 123RF

Produktion: IT-Säkerhetsbolaget, Sundsvall 2021

ISBN 978-91-519-2689-6

Version 2.0

Tredje tryckningen

Förord

I min roll som utbildningsledare på Sveriges mest ambitiösa utbildning för dataskyddsombud har jag och medlemmarna i kursledningen lagt ned avsevärd tid på att hitta olika metoder och arbetssätt hur man ska strukturera upp arbetet i dataskyddsorganisationens och dataskyddsombudets arbete.

Vår kurs ”Dataskyddombud – Certifierad” löper över en termin och deltagarna är dataskyddsombud som vill fördjupa sina kunskaper i sin yrkesroll. Efter att ha genomfört utbildningen under flera år ser vi att omvärlden har mognat och att rollen som dataskyddsombud tydligare går mot att vara den granskande roll som den är avsedd att vara. Vi har även använt årshjulet mot flertalet av våra kunder på IT-Säkerhetsbolaget där vi agerar Dataskyddsombud, Coacher till dataskyddsombudet eller arbetar i verksamheten.

Efter att ha samtalat med hundratals dataskyddsombud har en metod mognat fram kring hur ett effektivt arbete kring dataskydd bör läggas upp. Vi har kombinerat ett riskbaserat arbetssätt tillsammans med styrkan i ett årshjul för att strukturera upp de arbetsuppgifter som ett dataskyddsombud bör utföra.

Vi hoppas att denna metod kommer att vara till stor hjälp för dataskyddombud som exempelvis är nya i sin roll och inte vet vilka arbetsuppgifter som bör ligga på rollen men även till stor hjälp för erfarna dataskyddsombud och datskyddsorganisationer som vill ordna sina arbetsuppgifter enligt en tydlig struktur.

I denna text har vi även sammanfattat tankar och insikter kring dataskyddsombudet och dess roll i organisationen samt skapat en grund för hur dataskyddsombudet kan ta sig an rollen och hitta en balans mellan lagkraven och organisationens krav.

Jag vill rikta ett stort tack till alla som hjälp till att utveckla metoden kring årshjulet, deltagare på kursen, våra kunder inom dataskydd,

samtliga gästföreläsare på kursen Certifierat Dataskyddsombud. Ett speciellt tack vill jag rikta till Monica Wendleby som gästföreläser på kursen. Jag uppskattar hennes rättframma uppfattning om dataskyddsombudets integritet och hennes råd om ett riskbaserat arbetssätt vid årshjulets genomförande.

Sundsvall, februari 2021

Fredrik Jonasson

Utbildningsledare Certifierat Dataskyddsombud, redaktör GDPR.se samt grundare av IT-Säkerhetsbolaget

Innehåll

Inledning

Inledning

IT-Säkerhetsbolagets utgångspunkt vid arbete med dataskydds-frågor är hämtat från vår bakgrund och erfarenhet av informations-säkerhetsarbete.

Organisationer måste skydda all information som hanteras i olika grad. Personuppgifter är en specifik typ information som organisationer hanterar, en informationsmängd där ägandeskapet tillhör någon annan och ska därför hanteras särskilt varsamt. Hanteringen av personuppgifter har dessutom tydliga lagkrav för vad som organisationen måste uppnå för att tillvarata individens rättigheter.

Mycket av tankesätten sammanfaller dock mellan dataskydd och informationssäkerhet och vi vill inledningsvis förklara några koncept som är centrala inom informationssäkerhet och som vi använder som utgångspunkt när vi arbetar med dataskydd.

Med denna broschyr ska ni komma igång med att arbeta enligt årshjulet och utforma ert dataskyddsarbete. Är ni intresserade av extra hjälp att komma vidare har vi ramverksdokumentation och en app som kommer att lanseras under 2021 för att underlägga för er att bygga ett stabilt ramverk. Vi beskriver det i detalj under kapitlet nästa steg.

Ett systematiskt arbetssätt

Exempelvis inom hälso- och sjukvården ställs bland annat krav på att processer och rutiner är identifierade, beskrivna och fastställda i Socialstyrelsens föreskrifter och allmänna råd (2011:9) om ledningssystem för systematiskt kvalitetsarbete. Det innebär att rutinerna beskriver ett bestämt tillvägagångssätt för hur en aktivitet ska utföras och hur ansvaret är fördelat i verksamheten.

Att arbeta riskbaserat

Risk bör vara ett centralt begrepp för all hantering av information i verksamheten. En skillnad mellan framgångsrika och mindre framgångsrika organisationer är hur de hanterar risker. Att vara medveten om vilken nivå av risk som en organisation tar i sitt dataskyddsarbete blir allt mer väsentligt i en värld där personuppgiftsincidenter ökar i takt med nya tekniska möjligheter för att överföra information.

Från incidenter som sker ser vi hur stora konsekvenser det kan bli om man inte hanterar alla aspekter inom informationssäkerhet och dataskydd. Dataskyddet har tydliggjort detta genom att det finns tydliga sanktionsavgifter om man hanterar personuppgifter bristfälligt.

Inom de internationella ISO/IEC standarderna är begreppet risk centralt och när vi tagit fram vilka aktiviteter som dataskyddsombudet ska fokusera på har vi tagit avstamp i ISO/IEC 31000 standarden kring riskhantering.

Vi har haft ISO27001 och ISO27701 standarderna som inspiration till hur årshjulet är uppbyggt tillsammans med vår kunskap om hur man effektivt bedriver arbete med dataskydd i organisationen.

ISO27001 beskriver hur organisationer ska arbeta systematiskt med informationssäkerhet och ISO27701 utökar standarden med krav för dataskydd. Vi har gått igenom standarderna och mappat varje krav mot de komponenter som vi föreslår. Syftet med mappningen är att det ska vara tydligt vilka delar mot standarden som täcks när man arbetar med årshjulet. Ett ständigt pågående arbete som är intressant är att vi mappar de saktioner som fallit ut inom EU mot våra komponenter och påståenden. styrkan i detta arbetssätt är att ge organisationerna ett tydligt sätt att visa vart i organisationens dataskydd brister och vart man ligger riskmässigt i förhållande till de sanktioner som utfärdats runt om i EU.

Ett ledningssystem

I en optimalt fungerande organisation vet medarbetarna alltid var informationen finns och var man ska vända sig i varje givet läge. Har man ett befintligt kvalitetshanteringssystem kan synergieffekter skapas genom att integrera dataskyddets dokumentation i organisationens övriga lednings- och styrningsfunktioner. Exempelvis bör man verka för en enda gemensam incidentprocess, att dataskyddsfrågorna hanteras i samma beslutsprocesser som bolagets övriga frågor samt att om en riskmatris används att även dataskyddets risker finns med och ställs mot övriga risker i organisationen.

En viktig skillnad när det gäller dataskyddet måste dock förtydligas. Dataskyddsombudet ska verka för den enskilde individens fri och rättigheter. Konsekvensen av det kan bli att riskerna som dataskyddsombudet ser kanske inte alltid sammanfaller med organisationens övriga riskbedömning. Om/när så uppstår är det dataskyddsombudets skyldighet att särredovisa detta förhållande.

Dataskydds-ombudets roll och ställning

Dataskyddsombudets roll och ställning

I Dataskyddsförordningen har dataskyddsombudet en tydlig roll som beskrivs i artiklarna 37–39. Den beskrivna rollen är komplex med många uppgifter som vid en första anblick kan synas vara för vida för en person och i viss mån stå i konflikt med varandra. Nedan följer vår bild av hur ett dataskyddsombud kan arbeta för att leva upp till kraven. Vi beskriver även vår syn på vilket fokus dataskyddsombudet bör ha för att optimalt verka för ett bra dataskydd.

Dataskyddsombudets granskande roll

I samband med att dataskyddsförordningen började gälla var många dataskyddsombud mycket operativa gällande organisationernas dataskydd. Fler och fler organisationer börjar nu få till en typ av dataskyddsorganisation där flera kompetenser har ansvar att sköta de dagliga frågorna kring dataskyddet. Att dataskyddsombudet har en granskande roll innebär att exempelvis uppdatering av registerförteckning eller daglig hantering av individers rättigheter inte bör ingå i ansvar och arbetsuppgifter.

Ska dataskyddsombudets roll integreras i organisationens helhet, eller stå utanför?

Vår erfarenhet av att arbeta med standarder och ledningssystem har gjort oss övertygade om att ju fler av en organisations styrande och stödjande processer som kan integreras med varandra desto bättre. Organisationer bör därför sträva efter att integrera dataskyddet i sitt befintliga verksamhetsledningssystem. Exempelvis genom att inför ett enhetligt sätt att hantera incidenter och att processer för att tillgodose den registrerades rättigheter integreras i övriga kundprocesser. Det

finns dock ett läge där dataskyddombudets speciella roll måste beaktas.

Den yttersta uppgiften som dataskyddsombud är att skydda den registrerades rättigheter och friheter. Uppgiften att övervaka efterlevnaden är reglerad i dataskyddsförordningen och brister ska rapporteras till högsta förvaltningsorgan. Konsekvensen blir därför att vissa delar måste ett dataskyddsombud utföra oberoende och utan inblandning. Exempelvis att vid utförandet av sina arbetsuppgifter ta hänsyn till de risker som är förknippade med personuppgiftsbehandling, så att de registrerades fri- och rättigheter inte utsätts för kränkningar.

Dataskyddsombudet får inte ha arbetsuppgifter som leder till intressekonflikter, ska inte ta emot instruktioner som gäller utförandet av sina uppgifter och får inte avsättas eller bli föremål för sanktioner för att ha utfört sina uppgifter.

Vikten av en tydlig presentation för styrelsen

Ansvaret för dataskyddet och att dataskyddsförordningen följs ligger på den personuppgiftsansvarige, det vill säga organisationens ledning. De ska tillse att frågorna hanteras av någon i organisationen.

Ett dataskyddsombud ska rapportera till högsta förvaltningsnivå det vill säga myndighetschef eller VD. Tolkningar har även gjorts att det kan utgöra styrelsen. Det finns inga krav på att dataskyddsombudet personligen måste redovisa rapporten, men den får inte förvanskas eller redigeras på vägen fram till ledningen.

Vår uppfattning är att dataskyddsombudet, i fall det är möjligt, bör sträva efter att även ha en kontakt med styrelsen/ledningen för att ge förståelse för dataskyddsfrågorna. För att nå fram med budskapet till en styrelse bör man därför förbereda sitt budskap på ett sätt som är lättillgängligt för en styrelse dvs:

- Kopplat till påverkan på organisationens varumärke

- Kopplat till eventuell förlust av finansiella medel i form av sanktioner eller skadestånd
- Riskbaserat

En viktig del som en styrelse ofta fokuserar på men som inte är dataskyddsombudets roll är hur organisationen följer mot de uppsatta målen. De risker som dataskyddsombudet tar upp ska enbart ta hänsyn till påverkan mot individens rättigheter och friheter.

Dataskyddombudets placering i organisationen

Var i organisationen rollen ska placeras är inte reglerat i dataskyddsförordningen. Datainspektionen anser att det inte är lämpligt att dataskyddsombudet sitter i organisationens ledning eller är med och fattar strategiska beslut.

Utifrån vår erfarenhet tenderar dataskyddsombud på lägre positioner att i större omfattning arbeta operativt med dataskyddsfrågor och mindre med den granskande delen av sina arbetsuppgifter. De som har positioner nära ledningen i staber eller liknande alternativt är externa dataskyddsombud har oftare rena granskande roller och arbetar mer strategiskt med dataskyddsfrågorna.

Därför är det viktigt att se över var i organisationsschemat dataskyddombudet lämpligen bör placeras för att nå den långsiktigt bästa effekten för dataskyddsarbetet. Särskilt i offentlig sektor bör delegationsordningar och beslutsmandat ses över för att möjliggöra förutsättningar för dataskyddsombudet att utföra sitt arbete effektivt och med genomslagskraft.

Vad fungerar bäst, det interna eller det externa dataskyddsombudet?

Skillnaden mellan det interna och externa dataskyddsombudet är främst att ett internt dataskyddsombud har insikt i det dagliga arbetet och känner verksamheten på ett sätt som det är svårt för ett externt dataskyddsombud att uppnå.

När en dataskyddsorganisation ska införas är det viktigt att det görs internt och utifrån organisationens förutsättningar. Ett fungerande och trovärdigt dataskyddsarbete är beroende av att hela organisationen känner till och förstår grunderna i dataskydd och hur man hanterar personuppgifter. En central framgångsfaktor är att utse dataskyddsrepresentanter, ambassadörer, ute i organisationen som får extra ansvar och utbildning och som kan bygga upp ett fungerande dataskyddsarbete.

I en uppbyggnadsfas kan det vara en fördel om dataskyddsombudet är internt och det är även vanligt att ombudet är aningen mer operativ där en stor del av arbetsuppgifterna är av utbildande karaktär.

I en förlängning där en fungerande dataskyddsorganisation är på plats kan ett externt professionellt dataskyddsombud vara en lyckad lösning. Det externa ombudets fördelar är bland annat att personen ofta har erfarenhet av flera andra organisationer och att omvärldsbevakning av rättsområdet och praxis ingår som en del av arbetsuppgifterna. Ett externt ombud är inte heller bunden av någon särskild plats i organisationshierarkin och riskerar inte att bli begränsad i sin opartiskhet på grund av det. Vid upphandling av ett externt dataskyddsombud är det viktigt att en viss lägstanivå garanteras.

Det är den personuppgiftsansvarige som ansvarar gentemot de registrerade och i förhållande till Datainspektionen för att principerna för behandling av personuppgifter följs. Dataskyddombudets roll är att övervaka efterlevnaden genom granskningar och påpekanden. En organisation som utser ett internt dataskyddsombud som saknar mandat och resurser att utföra sina arbetsuppgifter löper högre risk för betydande intressekonflikter.

Ett dataskyddsombud i beslutande positioner

Europeiska dataskyddsstyrelsen anser att ett uppdrag som företrädare för den personuppgiftsansvarige inte är förenligt med uppdraget som dataskyddsombud. Datainspektionens undersökning från februari 2019 visar att det finns ett stort antal dataskyddsombud som sitter i ledande ställning och även innehar rollen som dataskyddsombud. Det är inte en önskvärd situation då det kan leda till problem i oberoendet mellan rollerna. Trenden är dock att flertalet av dessa ersätts med interna resurser eller att externa dataskyddsombud upphandlas.

Det riskbaserade årshjulet för data-skyddsombudets arbete

Det riskbaserade årshjulet för dataskyddsombudets arbete

När vi i kursledningen satte oss ned för att utforma ett årshjul var det med utgångspunkten att vissa aktiviteter kan prioriteras och fördelas någorlunda fast över året medan andra måste utföras löpande när behov uppstår.

Löpande aktiviteter är därmed av den typen som beror på omvärlden och som inte kan planeras eller prioriteras.

Faktorer som påverkar årshjulet utformning kan vara följande:

- Identifierade risker i dataskyddsaktiviteter
- Organisationens storlek
- Organisationens verksamhet
- Ledningens engagemang
- Omfattning av DSO-rollen
- Organisationens dataskyddsmognad
- Etcetera

Frågor du tidigt bör ställa dig är hur ofta rapportering till ledning respektive styrelse ska ske och hur den ska gå till. Dessa faktorer är av avgörande betydelse för hur årshjulet ska läggas upp och planeras över året.

Löpande aktiviteter

Som dataskyddsombud har du aktiviteter som alltid behöver utföras (ytterligare kan tillkomma beroende på organisation).

Exempelvis:

- Hantera personuppgiftsincidenter
- Omvärldsbevakning
- Rådgivning och utbildning
- Rådgivning vid konsekvensbedömning
- Rapportering till ledning och Datainspektionen
- Löpande utvärdera risknivåer

Aktiviteter som kan delas upp över tid, årshjulets komponenter

De aktiviteter som vi föreslår ska ingå i årshjulet är följande:

1. Genomföra riskanalys och strukturera årshjul
2. Granska registret över behandlingar
3. Granska intern kommunikation och utbildning
4. Granska personuppgiftsincidentsprocessen
5. Granska avtalsrelation och personuppgiftsbiträdesavtalen (PUBA)
6. Granska underleverantörers arbete med dataskyddsregelverket
7. Granska processen för de registrerades rättigheter
8. Planera och genomföra revision
9. Granska processen för konsekvensanalyser
10. Granska inbyggt dataskydd, dataskydd som standard och säkerhet vid behandlingar
11. Granska extern kommunikation
12. Granska dataskyddsorganisationen
13. Granska att interna dokument och intern information följer GDPR
14. Granska lagringsminimering och gallring

Komponenterna i detalj

1. Genomföra riskanalys och strukturera årshjul

I planeringsstadiet inför varje årshjul bör varje aktivitet granskas utifrån den risk som den utgör för de registrerade i organisationens dataskydd. Riskanalysen ligger till grund för hur arbetet prioriteras och läggs ut över det kommande året. Slutresultatet av denna övning är en uppdaterad riskanalys och ett årshjul för årets arbete samt en uppdaterad plan över hur årets granskning ska gå till som kan utkommuniceras till relevanta parter

2. Granska registret över behandlingar

Registret över behandlingar är kanske den mest centrala delen i organisationens dataskyddsarbete. Att upprätthålla registret innebär stora utmaningar och kräver tid av organisationen. Ett korrekt uppdaterat register kan ha stora nyttor för många delar i organisationen. Granskningen går ut på att bland annat verifiera om registret är komplett, har uppdaterats löpande, inkluderar ostrukturerad information och om det är en naturlig del i organisationens arbete.

Förslag på KPI:

- Totalt antal behandlingar som finns i register över behandlingar
- Antal behandlingar som någon gång under perioden uppdaterats
- Antal behandlingar som innehåller samtlig lagstadgad information alternativt all infomration som krävs av organisationen.

3. Granska intern kommunikation och utbildning

Intern kommunikation och utbildning är en central del i ett fungerande dataskyddsarbete. Granskningen går ut på att kontrollera:

- Nivån av kunskap hos medarbetare och ledning kring dataskydds-frågor
- Om utbildningar är uppdaterade med dataskydd och har relevant innehåll

- Om skriftlig kommunikation/dokumentation är GDPR-anpassad
- Om medarbetare är medvetna om sina rättigheter

Förslag på KPI:

- Andel anställda/konsulter i organisationen som har fått relevant utbildning inom dataskydd inom en viss tidsperiod

4. Granska personuppgiftsincidentsprocessen

Incidentprocessen är pulsen i organisationen och visar på hur pass väl dataskyddet fungerar. I en väl fungerande organisation ska det registreras dataskyddsincidenter eftersom vi fortfarande lever i en manuell värld där incidenter sker.

Granskningen går ut på att kontrollera:

- Att processer för att anmäla incidenter och återrapportera till registrerade finns och stämmer överens med kraven i GDPR
- Vilka lärdomar organisationen har tagit från inrapporterade incidenter
- Status på incidentregistret
- Är nivån rätt för vad som ska skickas vidare till Datainspektionen och sådant som enbart dokumenteras och rapporteras till ledningen
- Hur stort är mörkertalet kring vad som inte rapporteras
- Registrerades uppfattning kring hur incidenter har hanterats av organisationen.

Förslag på KPI:

- Antal inc rapporterade till DI
- Totalt antal rapporterade incidenter
- Uppskattning mörkertal

5. Granska ansvarsrelation och personuppgiftsbiträdesavtalen (PUBA)

Tidigare skiftade personuppgiftsbiträdesavtalen både i kvalitet och innehåll. Numera går de mot en högre grad av standardisering.

Granskningen går ut på att kontrollera:

- Finns ett underskrivet, skäligt avtal med biträden och ansvariga?
- Är den egna mallen uppdaterad?
- Är den egna checklistan uppdaterad?
- Finns ett underskrivet, skäligt avtal med underbiträden?
- Finns biträden i tredje land och är överföringen laglig?

Förslag på KPI:

- Andel korrekta avtal

6. Granska underleverantörers arbete med dataskyddsregelverket

Något som inte uttryckligen regleras i dataskyddsförordningen, men är centralt i ett systematiskt informationssäkerhetsarbete är att säkerställa hela kedjan där informationen hanteras. Aktiviteten består i att granska utvalda underleverantörer med vilka befintliga biträdesrelationer finns. Det kan göras genom att kräva in tredjepartsrevisioner eller utföra granskning på plats hos biträdet.

Granskningen går ut på att kontrollera:

- Om det som avtalats stämmer, exempelvis backup, restore, tillgänglighet, tillgång till personuppgifter etcetera
- Hur personuppgiftincidentprocessen ser ut hos biträdet
- Hur registret över behandlingar ser ut hos biträdet
- Nivån och innehåll på underbiträdesavtal
- Om biträdet arbetar strukturerat med inbyggt dataskydd, dataskydd som standard och säkerhet vid behandling

Förslag på KPI:Antal genomförda granskningar

- Antal grova avvikelser

7. Granska processen för de registrerades rättigheter

Alla organisationer inom EU som hanterar personuppgifter måste ha processer på plats för att leva upp till de rättigheter som varje registrerad har. Granskningen går ut på att ta reda på upp till vilken nivå som respektive rättighet efterlevs.

Granskningen går ut på att kontrollera:

- Finns processer för samtliga rättigheter?
- Svarar organisationen i tid?
- Hur säkerställer organisationen att identifieringen är tillräcklig?
- Går någon process att optimera?

Förslag på KPI:

- Antal lämnade registerutdrag
- Antal lämnade registerutdrag i tid

8. Planera och genomför revision

Beroende på hur fördelningen av aktiviteter i årshjulet ser ut behövs olika grad av planering inför årsrevision och styrelserapportering. Att framföra sitt budskap till ledningen kräver att man är förberedd, vet vilka frågor ledningen tycker är viktiga samt att budskapet förs fram på ett pedagogiskt sätt. Sammanfatta gärna fakta och resultat på ett grafiskt tilltalande sätt som tydligt visar på dataskyddets behov.

9. Granska processen för konsekvensbedömningar

Denna komponent innebär att granska hur processen för konsekvensbedömningar fungerar. Görs det tillräckligt många konsekvensbedömningar utifrån den verksamhet som man bedriver? Finns det en dataskyddsorganisation som hanterar uppgifterna eller faller operativa uppgifter på dataskyddombudets roll med risk för intressekonflikter?

Granskningen går ut på att kontrollera:

- Genomförs konsekvensbedömning innan riskfyllda behandlingar påbörjas?
- Genomförs åtgärder som beslutats och följs de upp?

Förslag på KPI:

- Antal konsekvensbedömningar som genomförts under perioden

10. Granska inbyggt dataskydd, dataskydd som standard och säkerhet vid behandlingar

Dataskyddsförordningen ställer krav på att både organisatoriska och tekniska skyddsmekanismer ska vara på plats för de personuppgifter som organisationen hanterar. Denna aktivitet granskar hur detta fungerar.

Granskningen går ut på att kontrollera:

- Finns ett fullgott tekniskt stöd som säkrar skyddet för personuppgifterna?
- Är all information i organisationen klassificerad?
- Finns definierade skyddsnivåer för hur man hanterar olika typer av information?
- Är IT-arkitekturen anpassad till inbyggt dataskydd, dataskydd som standard och säkerhet vid behandlingar?
- Finns det någon process som hanterar brister där personuppgifter har undermåligt skydd?

11. Granska extern kommunikation

En av de lägst hängande frukterna när det gäller dataskyddsarbetet är att granska och säkerställa kvaliteten på den externa informationen. Hemsida, nyhetsbrev, reklamblad, integritetsmeddelanden och hantering av personuppgifter vid externa tillställningar vilket ofta är det första externa intressenter ser av organisationen.

Granskningen går ut på att kontrollera hur väl hemsidan är anpassad till dataskyddsregelverket:

- Är informationskraven i GDPR tillgodosedd
- Dataskyddsinformation
- Om hemsidan är krypterad (https)
- Hur referrers hanteras
- Vilka externa tjänster som används och om dessa uppgifter säljs vidare
- Cookiepolicys

Motsvarande gäller för nyhetsbrev och sociala kanaler som organisationen använder samt events. Informationsblanketter till de registrerade ska finnas upprättade.

12. Granska dataskyddsorganisationen

Hur fungerar den organisation som finns kring dataskyddet, Finns tillräckliga resurser utifrån de behov som finns. Finns det en skillnad mellan dataskyddsorganisation och dataskyddsombud. Finns ekonomiska förutsättningar att bedriva arbetet?

Granskningen går ut på att kontrollera:

- Har organisationen en fungerande dataskyddsorganisation?
- Är mandat och rapporteringsvägar tydliga?
- Finns tillräcklig budget för dataskyddsorganisationen och för dataskyddsombudet?

Förslag på KPI:

- Antal FTE i dataskyddsorganisationen
- Antal rapporter gjorda till högsta beslutande organ

13. Granska att interna dokument och intern information följer GDPR

Behandlar organisationen personuppgifterna lagligt utifrån GDPR.

Den ostrukturerade informationen finns i alla organisationer. Enligt dataskyddsförordningen finns inga undantag för denna personuppgiftshantering.

Granskningen går ut på att kontrollera:

- Finns policydokument och är de uppdaterade med relevant information om GDPR
- Följer organisationen den antagna policyn
- Har samtliga behandlingar en laglig grund, särskilt viktigt när känsliga personuppgifter behandlas
- Vilka typer av ostrukturerade data finns i organisationen
- Finns planer på att hantera situationen

14. Granska lagringsminimering och gallring

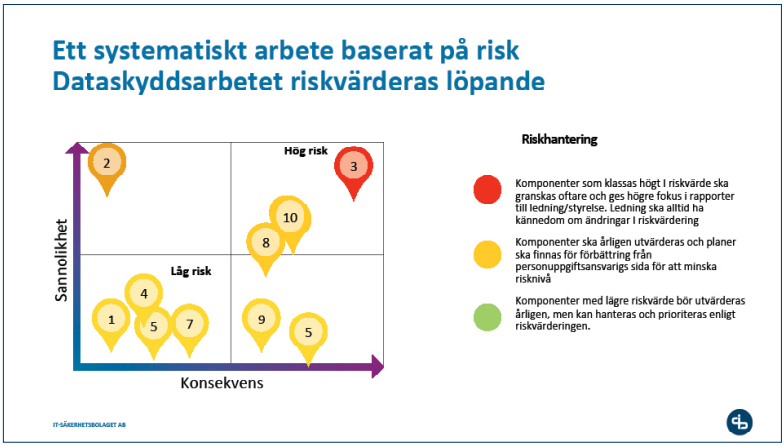
Hur gallras informationen i organisationen, finns det en plan för detta och följer man upp den planen? Sker detta på prioriterade system eller på samtliga. Hur kommunicerar vi detta till de registrerade? Hur säkerställer vi att vi inte behandlar mer data än vi har laglig grund till?

Ett riskbaserat angreppssätt

Genomför årsvis en riskanalys för att identifiera och kvantifiera organisationens risker inom olika områden.

Med fördel används en enkel riskmodell som kan kommuniceras vidare i form av sannolikhet och konsekvens.

En tydligt grafisk presentation i en klassisk riskmatris gör det tydligt för ledning, styrelse och andra intressenter att motivera prioritering av det fortsatta arbetet.



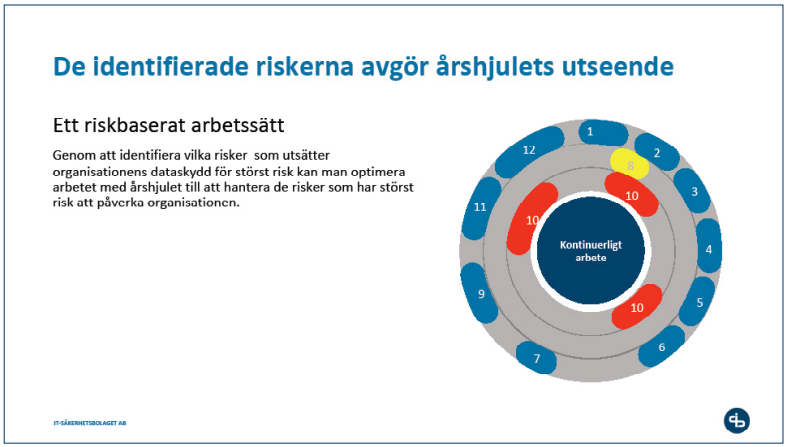
Figur 1. Riskmatris för en organisations olika dataskyddaktiviteter

Ett årshjul för dataskyddsarbetet

Metodiken bygger på att arbetet med dataskyddet delas upp i ett årshjul, där varje månad är indelad i ett fokusområde som dataskyddsombudet kan fokusera på. I årshjulet delas arbetsuppgifterna upp i löpande aktiviteter som utvärderas, granskas och förbättras. Där progressen kan följas år från år.

Riskanalysen ovan avgör vilka av aktiviteterna som bör prioriteras över varandra. Om man identifierar större risker i exempelvis incidentflödet

bör dessa återkomma i rapporteringen flera gånger under varje år för att sätta press på ledning och beslutsfattare att åtgärda problemen.



Figur 2. Aktiviteter fördelade över året baserat på hur dess bedömda risknivå ser ut.

Årshjulet har visat sig vara ett effektivt sätt att strukturera dataskyddsarbetet. Det är även ett bra sätt att fördela uppgifter mellan dataskyddsombud och dataskyddsorganisationen samt stärka den granskande rollen för dataskyddsombudet.

Givetvis ska aktiviteterna anpassas efter organisationens förutsättningar, men vi rekommenderar att samtliga delar av årshjulet analyseras varje år samt att det görs en uppskattning av organisationens mognad och nivåer av risker.

Ytterligare en fördel med att arbeta utifrån ett årshjul är att den löpande granskningen sker över hela året och sammanfattas och rapporteras till ledningen vid givna tillfällen. I modellen ingår mallar för respektive månad samt en mall för revisionsrapport där organisationens mognadsgrad uppskattas och följs upp under åren.

Exempel på årshjul för en organisation

I exemplet nedan har vi satt samman ett förslag på ett balanserat årshjul utifrån att samtliga aktiviteter hanteras under ett år. I exemplet har rapportperioden förlagts till augusti – september i syfte att överensstämma med organisationens budgetperiod. På detta sätt underlättas äskandet av medel för dataskyddsombudet och dataskyddsorganisationen inför kommande år.

Januari

1. Genomföra riskanalys och strukturera årshjul
13. Granska ostrukturerad information

Februari

2. Granska registret över behandlingar

Mars

3. Granska intern kommunikation och utbildnin
14. Granska lagringsminimering och gallring

April

4. Granska personuppgiftsincidentsprocessen

Maj

5. Granska personuppgiftsbiträdesavtalen

Juni

6. Granska underleverantörers arbete med dataskyddsarbetet

Juli

Semester

Augusti

7. Granska processen för de registrerades rättigheter

September

8. Planera och genomföra revision

Oktober

9. Granska processen för konsekvensanalyser
10. Granska inbyggt dataskydd, dataskydd som standard och säkerhet vid behandlingar

November

11. Granska extern kommunikation

December

12. Granska dataskyddsorganisationen
13. Granska att interna dokument följer GDPR

Vilken nivå av dataskydd är optimal för organisationen

Olika organisationer har olika krav som de måste nå upp till när det gäller arbetet med dataskydd, exempelvis har vissa organisationer speciallagstiftning att ta hänsyn till. En del grundkrav i dataskyddsregleringen måste dock alla nå upp till. Vissa organisationer eftersträvar en högre kvalitet för att visa kunder och medarbetare att dataskyddet är en viktig del i deras varumärkesarbete. Vilken typ av personuppgifter som hanteras i organisationen avgör också vilken nivå av dataskydd som måste eftersträvas i organisationen.

Genom att beskriva den önskade mognadsnivåer för respektive aktivitet och låta ledningen styra vilken nivå är det möjligt att få en målstyrning på den önskade nivån av dataskyddet.

Figur 3. Föreslagna mognadsnivåer. Använd dessa för att utvärdera vilken mognadsnivå som är ledningens vilja och styr dataskyddsarbetet

Svar	Nivå	Mognad	Förklaring
-	Ej applicerbar		
1	Instämmer inte alls	Initial	Dataskyddet som helhet kännetecknas av att den skapas varje gång för ett specifikt projekt, och ibland till och med som kaotiskt. Endast ett fåtal processer identifieras, och framgången beror på individers insatser.
2		Repeterbar	De viktigaste delarna i dataskyddsprocesserna har upprättats som gör att du kan spåra hur du ska arbeta. Processen är etablerad, vilket är nödvändigt för att upprepa de framgångar som uppnåtts tidigare.
3		Definierad	Dataskyddsprocessen dokumenteras och standardiseras för både lednings- och designarbete. Denna process är integrerad i organisationens övriga processer som informationssäkerhet och kvalitetsprocesser. Alla i organisationen följer anvisade processer.
4		Strukturerad	Detaljerade kvantitativa indikatorer för dataskyddsprocessen och kvaliteten på den hur dataskyddet i organisationen mäts. Kvaliteten på dataskyddet utvärderas och kontrolleras ur kvantitativ synvinkel.
5	Instämmer helt	Optimerad	Kontinuerlig processförbättring uppnås genom kvantitativ feedback från processen och implementering av avancerade idéer och tekniker.

mot denna.

Rapportering av dataskyddsarbetet

Utöver aktiviteterna i årshjulet rekommenderar vi att dataskydds-ombudet tar fram en periodisk rapport som dels presenterar genomförda aktiviteter och visar på organisationens riskuppskattning och mognadsgrad i sitt dataskyddsarbete.

Figur 4. Revisionsrapport som ingår i mallbibliotek tillsammans med frågebatteri för varje aktivitet

Rapporten bör vara utformad på en tillräcklig detaljnivå att ledningen kan fatta lämpliga beslut utifrån dess innehåll, men ändå ge en översikt.

Mappning ISO27001 och ISO27701

Kopplingen mellan Informationssäkerhet och dataskydd är stark. Detta är tydligt i ISO standarden ISO27000 som beskriver kraven för ett ledningssystem för Informationssäkerhet. ISO standarden har även utökats med ISO27701 där ISO27001 har kompletterats med krav inom dataskydd. I dagsläget kan man enbart certifiera en organisation om man har ett ISO27001 certifikat sedan tidigare.

Tabell 1, Mappning mellan komponentfrågor i årshjulet samt kontrollpunkter i ISO27001 samt ISO27701.

	Komponent namn	ISO27001	ISO27701
2	Granska registret över behandlingar		
	1	8.1.1	-
	2	8.1.1	A.7.2.1
	3	8.1.1, 8.1.3, 8.2.2	A.7.2.1
	4	8.1.2, 8.2.1, 8.1.3,8.2.2, 8.2.3	-
	6	8.1.2	-
3	Granska intern kommunikation och utbildning		
	1	-	-
	2	-	-
	3	11.1.1, 7.2.2, 7.2.3	-
	4	11.1.1, 7.2.2, 7.2.3	-
	5	7.2.2, 16.1.3	-
	6	7.2.2	-
4	Granska personuppgiftsincidentprocessen		
	1	12.6.1, 16.1.2, 16.1.4, 16.1.5	A.7.5.4
	2	12.6.1, 16.1.1	-
	4	12.6.1, 16.1.1	-
	5	12.6.1, 16.1.1, 16.1.5	A.7.5.4
	7	12.6.1, 16.1.1, 1, 16.1.3, 16.1.2	-
5	Avtal och biträdesprocess		
	1	15.1.1, 16.1.1	-
	2	16.1.1	A.7.2.6
	4	-	-
	5	13.2.2, 13.2.4	-
	6	-	-
	9	-	-
	10	13.2.1, 13.2.2, 13.2.4, 15.1.2, 15.1.3,	A.7.3.1
	11	-	A.7.2.7
	12	-	A.7.5.1, A.7.5.2, A.7.5.3
6	Underleverantörers arbete med dataskydd		
	1	14.2.7, 15.2.1, 15.2.2	-
	3	14.2.7, 15.2.1	-
	4	14.2.7, 15.2.1, 13.2.1	-
	5	14.2.7, 15.2.2	-
	6	-	A.7.3.7
7	Process för de registrerades rättigheter		
	1	-	A.7.3.1
	2	-	A.7.3.1, A.7.3.8
	3	-	A.7.3.1, A.7.3.6
	4	-	A.7.3.1, A.7.3.6

	5	-	A.7.3.1, A.7.3.5
	6	-	A.7.3.1
	7	-	-
	8	-	-
8	Genomförande av revison		
	1	5.1.2	-
	3	-	-
	4	-	-
	5	18.1.5	-
	6	18.2.2, 18.2.3	-
9	Granska processen för konsekvensbedömningar		
	1	14.2.2	-
	3	13.2.3, 14.1.1	A.7.2.5
	4	-	-
10	Dataskydd som standard och säkerhet vid behandlingar		
	3	6.1.5	-
	4	12.1.4, 14.2.1, 14.2.8, 14.2.9	-
	5	12.1.4. 14.3.1, 14.1.1	-
	6	-	-
	7	-	A.7.4.9
	8	9.1.1, 9.1.2, 9.2.1, 9.2.2, 9.2.3, 9.2.4, 9.2.5, 9.2.6	-
	9	-	-
	10	8.3.1	-
	11	8.3.2, 11.2.7	A.7.4.8
	12	8.3.3, 9.2.4, 9.3.1, 9.4.2, 9.4.3	-
	13	9.4.1, 13.1.13	-
	14	9.4.5	-
	15	11.1.1, 11.1.2, 11.1.3, 11.2.1, 11.2.8, 11.2.9, 12.1.2	-
	16	11.1.4, 17.1.1, 17.1.2, 17.1.3	-
	17	11.2.4, 12.2.1, 12.6.2	-
	18	11.2.5	-
	19	14.2.3	-
	20	12.3.1	-
	21	-	A.7.4.2
	22	(tom)	(tom)
	23	(tom)	A.7.4.6
11	Extern kommunikation		
	1	-	A.7.3.1, 7.3.2
	2	-	-
	3	-	A.7.3.1
	4	-	-

	5	-	-
	6	-	A.7.3.1
	7	-	A.7.3.1, 7.3.2
	8	-	-
	9	-	-
	10	-	A.7.2.3
	11	-	A.7.3.4, A 7.2.4
	12	-	A.7.3.10
	(tom)	(tom)	A.7.3.9
12	Granska dataskyddsorganisationen		
	1	6.1.1a, 6.1.1b, 5.1.1	-
	2	-	-
	3	-	-
	4	-	-
	6	6.1.2	-
	7	-	-
	8	6.1.3	-
	9	6.1.4	-
	10	6.1.2	-
		(tom)	(tom)
13	Granska att interna dokument och intern information följer GDPR		
	1	-	-
	2	-	A.7.3.1
	3	-	-
	4	-	-
	5	-	A.7.2.2
	6	11.1.1, 11.1.2, 11.1.3, 11.1.4, 11.2.5, 11.2.8, 11.2.9, 12.1.2, 12.2.1, 12.6.2, 13.2.1, 14.2.1, 14.2.2, 14.2.8, 14.2.9, 6.2.1b, 8.1.3, 8.1.4, 8.3.1, 8.3.2, 8.3.3, 9.1.1, 9.1.2, 9.2.1, 9.2.2, 9.2.3, 9.2.4, 9.2.5, 9.2.6, 9.3.1 9.4.2, 9.4.3, 9.4.4,	A.7.2.8, A.7.3.9, A.7.4.4
	7	6.2.2	-
	8	7.1.2	-
	9	7.3.1, 8.1.4	A.7.4.5
14	Granska lagringsminimering och gallring		
	1	-	A.7.4.1
	2	-	-
	3	-	A.7.4.6
	4	-	A.7.3.1
	5	-	A.7.4.7, A.7.4.8
Totalsumma			

Årshjulets koppling till ISO27000 och ISO27701 standarder

I det fördjupande materialet som ingår i årshjulspaketet finns en mappning av varje påstående till vilket krav i ISO 27000 serien som det utvärderar. Genom att arbeta med granskningsprotokollet får man en god grund att verifiera vilka delar i ISO27000 man uppfyller. Tabell 1 visar komponenternas koppling till kraven i ISO27000 serien.

För att få en detaljerad genomgång av varje påstående hanvisar vi till den detaljerade genomgången av årshjulspaketet som finns på IT-Säkerhetsbolagets hemsida.

Sanktioner och årshjulet

Inom EU har ett stort antal sanktioner utdelats. I februari 2021 var det över 540 sanktioner utdelade till ett belopp på knappt 275M Euro. (2,78 Mdr SEK). Årshjulets komponenter byggs upp av standardiserade påståenden. Varje påstående har till syfte att utvärdera någon aspekt inom organisationens dataskydd. Vårt mål är att samtliga sanktioner ska vara mappade mot våra komponenter och påstående som finns i årshjulet. Resultatet är en överblick där varje påstående i årshjulet kan värderas utifrån hur stort utfall i sanktioner det har varit.

Vi ser att detta är ett utmärkt sätt att värdera vilka delar inom dataskyddet som är viktiga att fokusera på.

Organisationens beredskap utifrån risk att få sanktioner

Vid en revision av organisationen rekommenderar vi att alla delar där organisationen får ett lägre betyg utvärderas mot vilka sanktioner som har fallit ut. Detta kan vara argument som kan motivera hela organisationen att arbeta mer aktivt i de delar av dataskyddet som inte är fullt fungerande.

Nästa steg

Vill du komma vidare?

Det kompletta paketet för att komma vidare med årshjulet

IT-Säkerhetsbolaget har tagit fram ett bibliotek med mallar och rutinbeskrivningar som möjliggör ett systematiskt dataskyddsarbete. Mallbiblioteket innehåller rapportmall för revisionsrapporten samt ett komplett frågebatteri dataskyddsombudet kan använda vid granskning av respektive komponent.

De komponenter vi delat upp dataskyddet i har vi standardiserat i över 120 påståenden som organisationen granskas utifrån. Samtliga påståenden har följande attribut kopplade till sig:

- Bakgrund, en förklarande text varför påståendet är viktigt och kopplat till artiklar i GDPR
- Metod att granska, tyliga råd hur du ska genomföra en granskning i din organisation
- Värdering, varje påstående har en standardiserad värdering mellan 1-5. Det finns en förklaring till hur varje värde skall tolkas för att underlätta standardisering
- Koppling till ISO standard, Koppling till ISO27001 och ISO27701 standardernas olika kontrollpunkter
- Koppling till sanktioner, En summering vilka saktioner som har utfallit i EU för respektive påstående, därigenom ges man möjligheten att summera samtliga sanktioner som utfallit per påstående.

Biblioteket innehåller även djupare beskrivningar hur granskning genomförs och uppdateras ständigt.

Mallbiblioteket används i de fall IT-Säkerhetsbolaget agerar externa

dataskyddsombud men kan även köpas separat via vår hemsida

Mallarna har hela vårt riskbaserade koncept inbyggt för att möjliggöra en tydlig rapportering. På hemsidan finns även förklarande videos och dokumentaton kring årshjulspaketet

https://itsakerhetsbolaget.se/vad-vi-gor/dso-som-tjanst/#mallbibliotek

Kurser, utbildningar & föreläsningar

Intensivkurs om årshjulet och dess användning

1 dags utbildning med fördjupning och kunskaper i metoden som presenterats i denna broschyr. Kursen utbildar er i hur ni får ett riskbaserat systematiskt dataskyddsarbete i er organisation. Kursen vänder sig till alla i er organisation som arbetar med dataskydd.

Dataskyddsombud Certifierad

Terminskurs med över 60 timmars lärarledd utbildning under 8 dagars kurs (under 4 månader) för att fördjupa kunskaperna i att vara dataskyddsombud med två hemuppgifter och ett avslutande certifieringsprov. Kursen hålls i samarbete med Dataföreningen Kompetens i deras lokaler i Stockholm.

https://www.dfkompetens.se/utbildning/dataskyddsombud-certifiering/

Dataskyddsombud som tjänst

https://itsakerhetsbolaget.se/vad-vi-gor/dso-som-tjanst/

Vi kan vara ert externa dataskyddsombud. Samtliga våra dataskyddsombud är certifierade dataskyddombud och vi arbetar i team för att komplettera med alla kompetenser som krävs.

Vi arbetar enligt den metodik som vi beskriver i detta dokument och

kan även utbilda er organisation att arbeta enligt ett systematiskt och riskbaserat sätt för dataskyddsarbetet.

www.itsakerhetsbolaget.se

Är du intresserad av att veta mer om hur vi kan hjälpa er med ert dataskydd? Gå gärna in på vår hemsida där vi har en tydlig beskrivning kring vårt erbjudande inom dataskydd eller läs mer om våra tjänster och kurser.

IT-SÄKERHETSBOLAGET AB
Storgatan 73, 852 30 Sundsvall
+46 (0)60-55 62 60 • info@itsakerhetsbolaget.se