Från GDPR-plan till handling.

En guide för att hjälpa er organisation att genomföra uppsatta GDPR-mål. Som säkerställer att ni följer efterlevnaden och får ordning på er data.

Formpipe.

Från plan till handling

Det har gått ganska lång tid (den 25 maj 2018) sen dataskyddsförordningen trädde i kraft. Det medförde en lång rad överväganden och åtgärder kring GDPR, i företag och organisationer, för att säkerställa en hög informationssäkerhetsnivå.

Vi upplever fortfarande osäkerhet och kunskapsbrist hos många organisationer om hur data lagras och används i olika system, t.ex. Exchange, OneDrive, Microsoft Teams osv.

Det kan till exempel handla om att data ligger kvar som:

- Inte får lagras på grund av GDPR
- Inte är uppdaterade eller är felaktiga, men ändå används
- Kan nås av medarbetare som inte borde ha åtkomst
- Inte kan nås eftersom de ligger på fel plats eller tillhör en tidigare medarbetare
- Används i ”skuggprocesser” som egentligen inte är tillåtna!

Om GDPR-efterlevnad inte följs, finns det stora risker förknippade med lagring och behandling av data. Det kan innebära allvarliga ekonomiska förluster, personliga konsekvenser, förlust av kunders eller medborgares förtroende, offentlig kritik eller böter m.m.

Även om ni har uppnått era mål, kan det vara dags för en översyn eller justering av era planer, genomförande och uppföljning kring hur principerna för behandling av personuppgifter efterlevs hos er.

Vi hoppas att denna guide och handlingsplan kan hjälpa er att säkerställa en hög informationssäkerhetsnivå och att de dagliga uppgifterna kring behandling av er data utförs på ett sätt så att ni kan efterleva både offentliga- och egna interna policys.

Uppnå en hög säkerhetsnivå

Sikkerdigital nämner 6 principer för korrekt behandling av personuppgifter, nämligen:

1 Behandling av data ska vara laglig, rimlig och transparent

2 Data får endast samlas in och användas för det angivna ändamålet

3 Data ska vara tillräckliga, relevanta och begränsade till det nödvändiga

4 Data ska vara korrekt och uppdaterad

5 Data får inte lagras längre än vad ändamålet kräver

6 Data ska behandlas på ett sätt som säkerställer tillräcklig säkerhet för skydd av data

Det finns därmed många åtgärder som kan användas för att säkerställa en hög informationssäkerhetsnivå.

Vet dina medarbetare om principerna?

- Använder du principerna för att göra en test av er behandling av personuppgifter?
- Kan du som ledare garantera att ni följer principerna? Kan du dokumentera det?

Läs mer på de följande sidorna och hämta ytterligare inspiration på www.sikkerdigital.dk.

Säkring av en hög informationssäkerhetsnivå

GDPR definierar inte specifika roller, men talar om den dataansvariges ansvar. I praktiken är det upp till varje företag att definiera vem som är ansvarig för de olika delarna av ansvaret i organisationen.

Med utgångspunkt i material från Sikkerdigital diskuterar vi uppgifter/områden och de möjliga personer som är involverade. Uppgifterna kan vara fördelade på olika sätt i din organisation.

1. RESURSER

Du ska säkerställa att tillräckliga resurser är avsatta för att de informationssäkerhetsmål som ledningen har definierat kan uppnås.

Det måste finnas tillräckligt med resurser för att informationssäkerhetsarbetet i praktiken ska stödja organisationens uppgifter och säkerställa implementeringen av nödvändiga kontroller. Det innebär:

- Kontrollerna är dokumenterade
- De nödvändiga aktiviteterna utförs faktiskt och att status rapporteras
- Resurser bör vara avsatta i budgetarna och i linje med alla andra kostnader

2. KOMPETENSER

Du ska säkerställa att de nödvändiga informationssäkerhetskompetenserna finns tillgängliga för att hantera informationssäkerheten.

Det innebär att ett tillräckligt antal medarbetare ska ha rätt utbildningsbakgrund och erfarenhet för att ni ska kunna uppnå era mål för informationssäkerheten.

Det är inte alla organisationer som har en IT-säkerhetskoordinator på heltid, och några av uppgifterna kan vara fördelade på flera personer.

Det slutliga ansvaret för en organisations informationsresurser är dock alltid förankrat hos ledningen.

Organisationen ska upprätthålla och utveckla kompetenser i takt med att risklandskapet och hoten utvecklas.

3. UTBILDNING OCH MEDVETENHET

Utbildningsaktiviteter ska säkerställa att organisationens medarbetare är medvetna om och förstår hur de ska agera för att minimera risken för säkerhetshändelser. Det innebär att det ska finnas en medvetenhet om dataskydd i organisationen och att arbetet med informationssäkerhet prioriteras på alla nivåer.

Som utgångspunkt ska innehållet i informations-

säkerhetspolicyn och grundläggande beteendenormer i förhållande till medarbetarnas hantering av informationsresurser, inklusive IT-utrustning, förmedlas till medarbetarna. Detta gäller även rapportering av händelser och sanktioner vid överträdelser av informationssäkerhetspolicyn.

Utbildningsaktiviteterna kan med fördel kombineras med interna kurser och liknande. Till exempel kan informationssäkerhet ingå som en fast del av introduktionsprogrammet för nya medarbetare.

4. KOMMUNIKATION

Kommunikation, både internt och externt, är en mycket viktig del av informationssäkerheten och måste styras noggrant och med tydliga riktlinjer på området.

Kommunikation inom organisationen om informationssäkerhet ingår i utbildningsaktiviteterna. Dessutom ska rapporteringsprocedurer upprättas så att tillräcklig information finns tillgänglig för att ledningen ska kunna utöva sina befogenheter på ett rättidigt och informerat sätt.

4. A. ANVÄND BEFINTLIGA KANALER

Rapporteringen bör ske via de befintliga kanalerna för kommunikation av ledningsinformation.

4. B. MEDARBETARKOMMUNIKATION

Det kan också finnas behov av kommunikation till medarbetarna, vilket vanligtvis är aktuellt vid säkerhetshändelser eller om det finns behov av att ändra ett visst beteende eller öka vaksamheten i förhållande till exempelvis ett nytt hot.

Ledningens generella kommunikation till medarbetarna om informationssäkerhet är också en viktig del i förankringen.

4. C. PUNKTER FÖR BESLUT KRING KOMMUNIKATION

När det gäller kommunikation gäller att följande ska vara beslutat och dokumenterat:

- Vad ska kommuniceras?
- När?
- Till vem?
- Av vem?
- Via vilka kommunikationskanaler?

5. DOKUMENTATION

Dokumentation är ett centralt element i etableringen och driften av informationssäkerheten, men inte allt behöver dokumenteras.

Till exempel anger ISO 27001 vilka specifika dokument som ska upprättas om styrningen av informationssäkerheten, men dokumentationsbehovet beror på den konkreta organisationens storlek, typer av aktiviteter, komplexitet och mognadsgrad.

Personer och uppgifter

Hela organisationen är med och säkerställer i praktiken att de enskilda uppgifterna utförs på ett sätt så att din organisation följer både lagstiftningen och sina egna interna policyer. Detta för att undvika allvarliga ekonomiska förluster, personliga konsekvenser, förlust av medborgares eller kunders förtroende, offentlig kritik och böter m.m.

I det följande har vi beskrivit de personer i organisationen som typiskt är involverade.

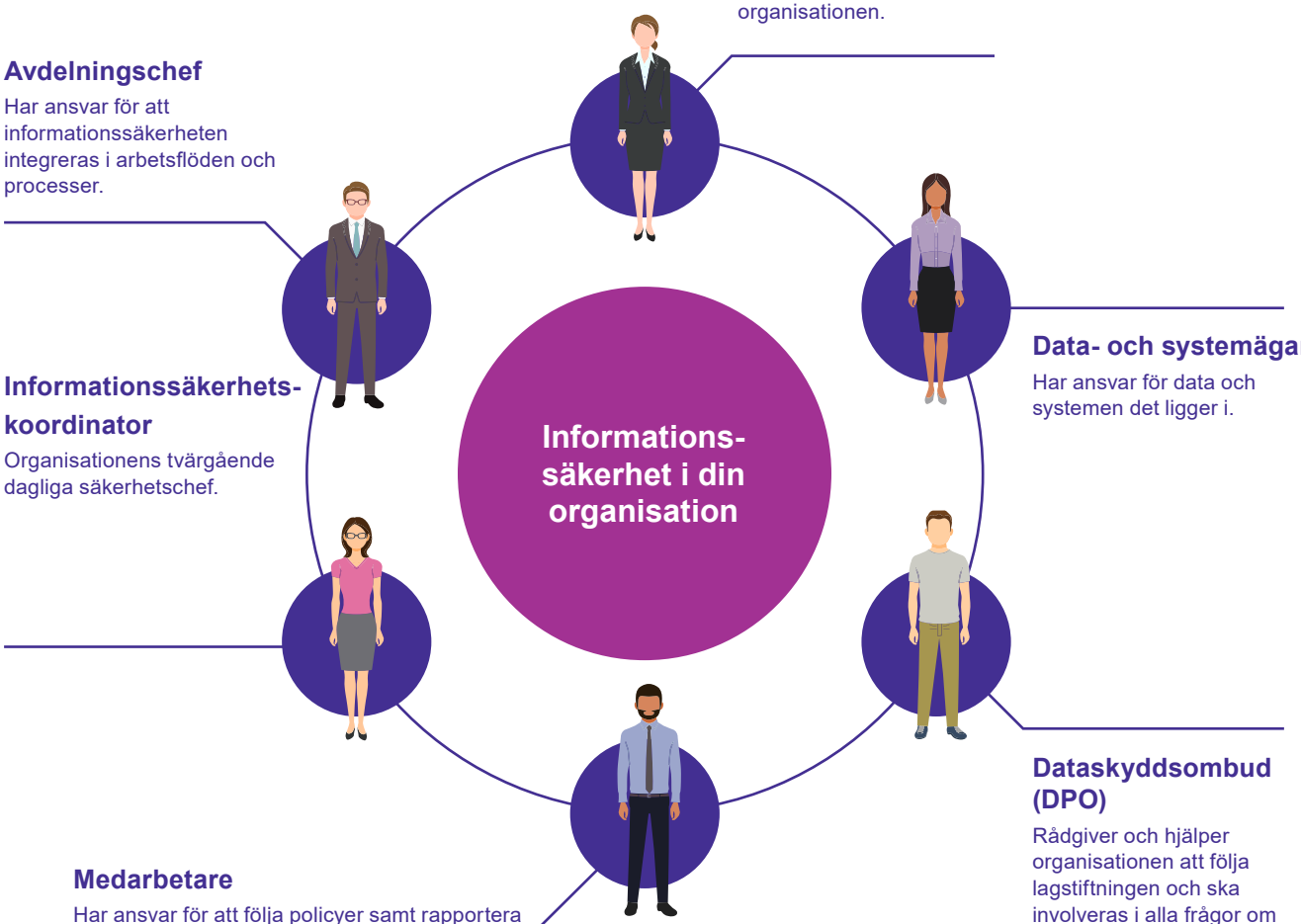
De rekommenderade uppgifterna ska i princip utföras, men observera att alla roller kanske inte finns i just din organisation.

Personer...

Ledning
Har det övergripande ansvaret och fördelar roller och ansvar i organisationen.

Avdelningschef
Har ansvar för att informationssäkerheten integreras i arbetsflöden och processer.

Informationssäkerhets-koordinator
Organisationens tvärgående dagliga säkerhetschef.



Data- och systemägare
Har ansvar för data och systemen det ligger i.

Dataskyddsombud (DPO)
Rådgiver och hjälper organisationen att följa lagstiftningen och ska involveras i alla frågor om skydd av personuppgifter.

Medarbetare
Har ansvar för att följa policyer samt rapportera risker och händelser.

Ledning

Har det övergripande ansvaret och fördelar roller och ansvar i organisationen.

Roll i säkerhetsarbetet

Har det övergripande ansvaret för informationssäkerheten i organisationen, inklusive att fastställa säkerhetsnivån.

Har ansvar för att medarbetarna är kvalificerade att arbeta säkert med organisationens information.

Förstår de övergripande besluten gällande informationssäkerhet och tar hänsyn till ekonomiska, affärsstrategiska, resursmässiga och organisatoriska konsekvenser.

Uppgifter som ska utföras

- Säkerställa att arbetet med informationssäkerhet har ledningens stöd.
- Hålla sig uppdaterad om det aktuella riskläget genom att samarbeta med säkerhetskoordinatorn och de personer som ansvarar för informationsresurserna.
- Etablera ett ramverk för policyer, procedurer, processer, organisatoriska beslutsprocesser och aktiviteter som ingår i organisationens styrning av informationssäkerhet.
- Bedöma om det finns behov av extern rådgivning och hjälp i säkerhetsarbetet.

Som medarbetare

- Följa policyer.
- Identifiera brister i policyer och efterlevnaden av dessa.
- Rapportera risker och incidenter på ett proaktivt sätt.

Hämta inspiration från Reseskildringen på www.sikkerdigital.dk HÄR:
https://sikkerdigital.dk/myndighed/iso-27001-implementering/forstaa-arbejdet-med-informationssikkerhed/roller-og-ansvar
Materialet är utarbetat och framtaget av digitaliseringsstrategin, KL och Danske Regioner.

Avdelningschef

Har ansvar för att informationssäkerheten integreras i arbetsflöden och processer.

Roll i säkerhetsarbetet

Är ansvarig för operativ implementering och löpande kontroll av efterlevnaden av policyer, riktlinjer, procedurer, budget m.m.

Bidrar till att öka medvetenheten om informationssäkerhet och fungerar som samtalspartner för medarbetare när det gäller att följa säkerhetsåtgärder.

Uppgifter som ska utföras

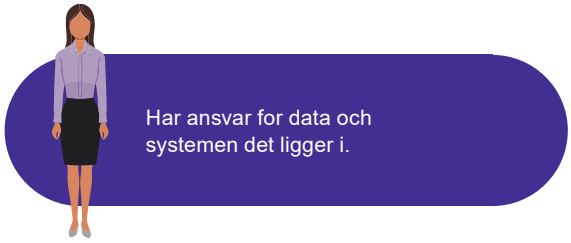
- Ansvarar för att säkerställa utarbetandet av detaljerade procedurer, instruktioner och checklistor i enlighet med de säkerhetsnivåer som ledningen har fastställt.
- Säkerställer att organisationens arbete planeras på ett sätt som stöder informationssäkerheten.
- Följer upp säkerhetsinitiativ i förhållande till medarbetarnas dagliga arbete, inklusive att säkerställa hög medvetenhet om informationssäkerhet.
- Säkerställer att medarbetare genomgår organisationens utbildningssessioner om informationssäkerhet.
- Diskuterar regelbundet medarbetarnas hantering av informationssäkerhet på professionella möten i avdelningen.
- Gör informationssäkerhet till ett tema för att säkerställa att medarbetare får en generell förståelse för informationssäkerhet och arbetar med hur de stödjer den i vardagen.
- Håller informationsmöten och följer upp.

Som medarbetare

- Följa policyer.
- Identifiera brister i gällande policyer och efterlevnaden av dessa.
- Rapportera risker och incidenter på ett proaktivt sätt.

Hämta inspiration från Reseskildringen på www.sikkerdigital.dk HÄR:
https://sikkerdigital.dk/media/6819/sikkerdigital-rejsefortaelling-mellemleder-2020.pptx
Materialet är utarbetat och framtaget av digitaliseringsstrategin, KL och Danske Regioner.

Data- och Systemägare



Roll i säkerhetsarbetet

Dispositionsrätt till data och ansvar för behandling av data.

Ansvar för informationssäkerheten för det/de system man ”äger”, inklusive ansvar för utarbetande av operativa procedurer, instruktioner och checklistor inom ramarna för de säkerhetsnivåer som organisationens ledning har fastställt.

Ansvar för att löpande kontrollera efterlevnaden av riktlinjer och procedurer, samt underhåll av system, processer, intressenter, tillgångar, kontrakt m.m.

Uppgifter som ska utföras

- Skapa överblick över vilka affärsprocesser system och data stödjer. Överblicken används för att säkerställa att relevanta och tillräckliga säkerhetskrav ställs utifrån organisationens säkerhetsnivåer.
- Klassificera tillgångar och specificera säkerhetskrav samt godkänna anskaffning och installation av varje tillgång.
- Ge åtkomst till system och data.
- Godkänna placering av kritiska tillgångar samt utvecklings- och hjälpmiljöer.
- Godkänna beredskapsplaner och följa upp på säkerhetshändelser.
- Delegera rutinmässiga uppgifter till en person (entitet) som dagligen övervakar tillgångarna, men har fortfarande det slutliga ansvaret för systemets informationssäkerhet under hela systemets livslängd.

Som medarbetare

- Följa policyer.
- Identifiera brister i gällande policyer och efterlevnaden av dessa.
- Rapportera risker och incidenter på ett proaktivt sätt.

Hämta inspiration från Reseskildringen på www.sikkerdigital.dk HÄR:
https://sikkerdigital.dk/media/6820/sikkerdigital-rejsefortaelling-systemejer-2020.pptx
Materialet är utarbetat och framtaget av digitaliseringsstrategin, KL och Danske Regioner.

Informations-säkerhetskoordinator

Organisationens tvärgående dagliga säkerhetschef.

Roll i säkerhetsarbetet

Bör rapportera direkt till ledningen, men oavsett organisatorisk placering är det viktigt att ansvar och befogenheter preciseras av ledningen.

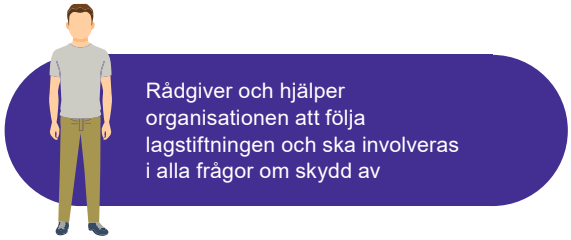
Uppgifter som ska utföras

- Leda riskbedömningar och föreslå uppdateringar av informationssäkerhetspolicyn.
- Registrera och rapportera kritiska händelser.
- Utvärdera och jämföra organisationens säkerhet.
- Öka medvetenheten om informationssäkerhet bland organisationens medarbetare.
- Kalla till möten och vara sekreterare för informationssäkerhetskommittén.
- Klargöra gränssnitt i förhållande till övriga policyer i organisationen och bedöma behovet av att diskutera informationssäkerhetspolicyn internt.

Som medarbetare

- Följa policyer.
- Identifiera brister i gällande policyer och efterlevnaden av dessa.
- Rapportera risker och incidenter på ett proaktivt sätt.

Dataskyddsombud(DPO)



Roll i säkerhetsarbetet

Ska övervaka och ge råd så att organisationen följer både lagstiftningen och interna policyer när det gäller skydd av personuppgifter.

Involverad i frågor gällande skydd av personuppgifter och fungerar även som kontaktperson för registrerade och dataskyddsmyndigheter.

Får inte ta emot instruktioner om uppgifter och ska rapportera direkt till högsta ledningen.

Uppgifter som ska utföras

- Övervaka, informera och ge råd till organisationen om behandlingsaktiviteter för skydd av personuppgifter, implementering och efterlevnad av både lagstiftningen och interna policyer för skydd av personuppgifter.
- Ge råd om interna policyer för skydd av personuppgifter för att säkerställa behandling av personuppgifter vid kontrakts- och leverantörshantering m.m.
- Rådgiva om utveckling och underhåll av intern dokumentation om skydd av personuppgifter.
- Fungerar som kontaktperson för registrerade och dataskyddsmyndigheter angående eventuella dataintrång och generell information om rättigheter.
- Övervaka och ge råd om konsekvensanalys av behandlingsaktiviteter för skydd av personuppgifter när det finns en hög risk att behandlingen av uppgifter kränker den registrerade.

Som medarbetare

- Följa policyer.
- Identifiera brister i gällande policyer och efterlevnaden av dessa.
- Rapportera risker och incidenter på ett proaktivt sätt.

Hämta inspiration från Reseskildringen på www.sikkerdigital.dk HÄR:
https://sikkerdigital.dk/myndighed/iso-27001-implementering/forstaa-arbejdet-med-informationssikkerhed/aarshjul-og-planlaegning
Materialet är utarbetat och framtaget av digitaliseringsstrategin, KL och Danske Regioner.

Har ansvar för att följa policyer samt rapportera risker och händelser.

Medarbetare

Roll i säkerhetsarbetet

Har den viktigaste rollen när det gäller informationssäkerhet. Ska säkerställa att de delegerade uppgifterna utförs på ett sätt som gör att organisationen följer lagstiftning, interna policyer och riktlinjer.

Kan naturligtvis ha mycket olika kontakt med data, information och fysisk säkerhet och kan därmed ha olika roller i säkerhetsarbetet.

Uppgifter som ska utföras

- Följa policyer.
- Identifiera brister i gällande policyer och efterlevnaden av dessa.
- Rapportera risker och incidenter på ett proaktivt sätt.

Automatisera er datauppstädning med Adoxa

Adoxa kan hjälpa din organisation att följa de 6 principerna för korrekt behandling av personuppgifter.

Vår lösning kan nämligen agera teknisk stöd och hjälp, så att:

- Dina medarbetare känner till principerna
- Du kan följa upp hur ni behandlar personuppgifter
- DDu som ledare kan dokumentera att ni efterlever principerna

Adoxa är ett datakvalitetsverktyg som söker och behandlar data över olika datakällor, vilket hjälper dig och dina medarbetare att rensa upp i era data och stödjer GDPR samt interna och externa efterlevnadskrav.

☑ Innehåller över 100 fördefinierade sökregler

☑ Enkelt att själv implementera nya regler efter behov

☑ Meddelar om något kräver åtgärd

☑ Uppstädning kan göras direkt från meddelandet eller användarportalen, oavsett datakälla

☑ Policys och eskalering säkerställer framsteg i uppstädningen

☑ Ledningsmässig och individuell översikt för aktuell status på insatser och uppgifter

Adoxa används av över 70 000 användare inom både privat och offentlig sektor.

Kontakta oss idag för att se, vilken skillnad Adoxa kan göra för er.

Tomas Maurd
Key Account Manager
Tomas.maurd@formpipe.com

Formpipe.