Fra GDPR-plan til handling.

Guide til at effektuere jeres GDPR-mål og få organisationen til at sikre I overholder compliance og får ryddet op i jeres data.

Formpipe.

Fra plan til handling

Det er efterhånden længe siden (den 25. maj 2018), at persondataforordningen trådte i kraft, og medførte en lang række overvejelser og tiltag omkring GDPR i virksomheder og organisationer for at sikre et højt informationssikkerhedsniveau.

Vi oplever fortsat usikkerhed og mangel på konkret viden hos mange organisationer om, hvordan data opbevares og anvendes i forskellige systemer, eks. Exchange, Fildrev, OneDrive, Teams osv.

Der kan f.eks. være tale om, at I fortsat har data, der:

- Ikke må opbevares på grund af netop GDPR
- Ikke er opdaterede eller er ukorrekte, men anvendes alligevel
- Kan tilgås af medarbejdere som ikke burde have adgang
- Ikke kan tilgås, da de ligger et forkert sted, eller tilhører en tidligere medarbejder
- Bruges i ”skyggeprocesser”, som reelt ikke er tilladt!

Hvis ikke GDPR-compliance overholdes, så er der en stor risiko forbundet med opbevaring og behandling af data. Det kan være alvorlige økonomiske tab, personlige konsekvenser, tab af kundernes eller borgernes tillid, offentlig kritik eller bøder m.v.

Selvom I er kommet i mål, så er det måske tid til en genovervejelse eller justering af jeres planer, eksekvering og opfølgning omkring hvordan principperne for behandling af persondata overholdes hos jer.

Vi håber, at denne guide og handlingsplan kan hjælpe jer med at sikre et højt informationssikkerhedsniveau, og at de daglige opgaver omkring behandling af jeres data udføres på en sådan måde, at I kan efterleve offentlige såvel som jeres egne interne politikker.

Opnå et højt sikkerhedsniveau

Sikkerdigital omtaler 6 principper for korrekt behandling af persondata, nemlig:

1. Behandling af data skal være lovlig, rimelig og gennemsigtig
2. Data må kun indsamles og anvendes til det angivne formål
3. Data skal være tilstrækkelige, relevante og begrænset til det nødvendige
4. Data skal være korrekte og ajourførte
5. Data må ikke opbevares længere end formålet kræver
6. Data skal behandles på en måde, der sikrer tilstrækkelig sikkerhed for beskyttelse af data

Der er dermed mange virkemidler, som kan tages i brug for at sikre et højt informationssikkerhedsniveau.

Kender dine medarbejdere principperne?

- Bruger du principperne til at lave en test af jeres behandling af persondata?
- Kan du som leder stå inde for, at I overholder principperne? Kan du dokumentere det?

Sikring af et højt informationssikkerhedsniveau

GDPR definerer ikke specifikke roller, men taler om den dataansvarliges ansvar. Reelt er det op til den enkelte virksomhed at definere hvem, der er tovholder i organisationen på de enkelte dele af det ansvar.
Med udgangspunkt i materiale fra Sikkerdigital omtaler vi opgaver/områder og de mulige personer der er involveret. Opgaverne kan være anderledes fordelt i din organisation.

1. RESSOURCER

Du skal sikre, at der er allokeret tilstrækkeligt med ressourcer til, at de, af ledelsen definerede informationssikkerhedsmæssige mål kan nås.

Der skal være nok ressourcer tilstede til, at informationssikkerhedsindsatsen i praksis er egnet til at understøtte organisationens opgaver og sikre implementering af nødvendige kontroller. Det betyder:

- Kontrollerne er dokumenteret
- De krævede aktiviteter rent faktisk udføres og at status rapporteres
- Ressourcer bør være eksplicit afsat i budgetter linje med alle andre omkostninger

2. KOMPETENCER

Du skal sikre, at de nødvendige informationssikkerhedsfaglige kompetencer er tilstede i relation til at styre informationssikkerhed.

Det indebærer, at et passende antal medarbejdere skal have den rette uddannelsesmæssige baggrund og erfaring med opgaven til, at I kan realisere jeres mål for informationssikkerheden.

Det er ikke alle organisationer, som har en IT-sikkerhedskoordinator på fuldtid, og nogle af opgaverne kan være fordelt på flere. Det endelige ansvar for en organisations informationsaktiver er dog altid forankret hos ledelsen af organisationen.

Organisationen skal vedligeholde og opbygge kompetencer i takt med at risikolandskabet og truslerne udvikler sig.

3. UDDANNELSE OG BEVIDSTHED

Uddannelsesaktiviteter skal sikre, at organisationens medarbejdere har kendskab til og forstår, hvordan de skal agere for at minimere risikoen for sikkerhedshændelser. Det vil sige, at der skal være en bevidsthed omkring beskyttelse af data i organisationen, og at arbejdet med informationssikkerhed prioriteres på alle niveauer.

Som udgangspunkt skal indholdet af informationssikkerhedspolitikken og basale adfærdsnormer

i forhold til medarbejdernes omgang med informationsaktiver, herunder IT-udstyr, formidles til medarbejderen. Det gælder også rapportering af hændelser og sanktionsmuligheder ved overtrædelse af informationssikkerhedspolitikken.

Uddannelsesaktiviteterne kan med fordel kombineres med interne kurser og lignende. F.eks. kan informationssikkerhed indgå som en fast del af et introduktionsforløb for nye medarbejdere.

4. KOMMUNIKATION

Kommunikation, både internt og eksternt, er en meget vigtig del af informationssikkerheden, og skal styres med hård hånd og med præcise retningslinjer på området.

Kommunikation, internt i organisationen om informationssikkerhed, er uddannelsesaktiviteter. Derudover skal der etableres rapporteringprocedurer, så der er tilstrækkelig information tilstede, for at ledelsen kan udøve sine beføjelser på et rettidigt og oplyst grundlag.

4. A. BRUG EKSISTERENDE KANALER

Rapporteringen bør ske via de eksisterende kanaler for kommunikation af ledelsesinformation.

4. B. MEDARBEJDERKOMMUNIKATION

Der kan også være behov for kommunikation til medarbejderne. Det er som regel aktuelt ved sikkerhedshændelser, eller hvis der er behov for ændring af en bestemt adfærd eller agtpågivenhed i forhold til fx en ny trussel.

Endelig er ledelsens generelle kommunikation til medarbejderne om informationssikkerhed et vigtigt led i forankringen.

4. C. DOKUMENTERET

Fælles for kommunikation gælder, at følgende skal være besluttet og dokumenteret:

- Hvad skal kommunikeres?
- Hvornår?
- Til hvem?
- Af hvem?
- Og via hvilke kommunikationskanaler?

5. DOKUMENTATION

Dokumentationen er et centralt element i etablering og drift omkring informationssikkerhed, men det er ikke alt, der behøver at skulle dokumenteres.

F.eks. angiver ISO 27001 hvilke konkrete dokumenter, der skal være udarbejdet om styringen af informationssikkerhed, men dokumentations-behovet afhænger af den konkrete organisations størrelse, typer af aktiviteter, kompleksitet og modenhed.

Personer og opgaver

Hele organisationen er med til, i praksis, at sikre, at de enkelte opgaver udføres på en måde, så din organisation efterlever både lovgivningen og egne interne politikker – for at undgå alvorlige økonomiske tab, personlige konsekvenser, tab af borgere eller kunders tillid, offentlig kritik og bøder m.v.

I det følgende har vi beskrevet de personer i organisationen, der typisk er involveret.

De anbefalede opgaver skal i princippet udføres, men vær opmærksom på at ikke alle roller findes i netop din organisation.

Personer...

Topledelse

Har det overordnede ansvar og fordeler roller og ansvar i organisationen.

Afdelingsleder

Har ansvar for at informationssikker-heden bliver indarbejdet i arbejdsgange og processer.

Data- og systemejer

Har ansvar for data og de systemer, data ligger i.

Informationssikker-hedskoordinator

Organisationens tværgående daglige sikkerhedsleder.

Databeskyttelses-rådgiver (DPO)

Rådgiver og hjælper organisationen med at overholde de lovgivningen og skal inddrages i alle spørgsmål om beskyttelse af persondata.

Medarbejdere

Har ansvar for at overholde gældende politikker og rapportere risici og hændelser.

Hent inspiration i Rejsefortællingen fra www.sikkerdigital.dk. Materialet er udarbejdet og formidlet af digitaliseringsstrategien, KL og Danske Regioner.

Topledelse

Har det overordnede ansvar og fordeler roller og ansvar i organisationen.

Rolle i sikkerhedsarbejdet

Har det overordnede ansvar for informationssikkerheden i organisationen herunder at fastlægge sikkerhedsniveauet.

Har ansvar for, at medarbejderne er kvalificerede til at arbejde sikkert med organisationens informationer.

Træffer de overordnede beslutninger vedrørende informationssikkerhed og forholder sig til økonomiske, forretningsstrategiske, ressourcemæssige og organisatoriske konsekvenser.

Opgaver der typisk skal udføres

- Sikre at arbejdet med informationssikkerhed har ledernes opbakning.
- Holde sig ajour med det aktuelle risikobillede ved at samarbejde med sikkerhedskoordinatoren og de personer, der har ansvar for informationsaktiverne
- Etablere et rammeværktøj for politikker, procedurer, processer, organisatoriske beslutningsprocesser og aktiviteter, som er dele af organisationens styring af informationssikkerhed.
- Vurdere om der er behov for ekstern rådgivning og hjælp til sikkerhedsarbejdet.

Som medarbejder

- Overholde gældende politikker
- Udpege mangler i gældende politikker og efterlevelsen af disse
- Rapportere risici og hændelser på en proaktiv måde

Hent inspiration i Rejsefortællingen fra www.sikkerdigital.dk HER:
https://sikkerdigital.dk/myndighed/iso-27001-implementering/forstaa-arbejdet-med-informationssikkerhed/roller-og-ansvar
Materialet er udarbejdet og formidlet af digitaliseringsstrategien, KL og Danske Regioner.

Afdelingsleder

Har ansvar for at informations-sikkerheden bliver indarbejdet i arbejdsgange og processer.

Rolle i sikkerhedsarbejdet

Er ansvarlig for operativ implementering og løbende kontrol med overholdelsen af politikker, retningslinjer, procedurer, budget mv.

Bidrager til at højne opmærksomheden omkring informationssikkerhed, og fungerer som sparringspartner for medarbejdere ift. at efterleve sikkerhedsforanstaltninger.

Opgaver der typisk skal udføres

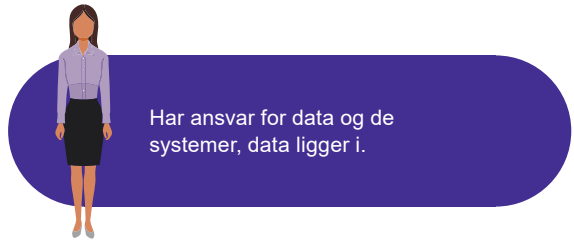
- Ansvar for at sikre udarbejdelse af de detaljerede procedurer, instrukser og tjeklister ift. rammerne for sikkerhedsniveauer topledelsen har fastlagt
- Sikre at organisationens arbejde planlægges på en måde, så informationssikkerheden understøttes
- Følger op på sikkerhedsinitiativer i forhold til medarbejdernes daglige arbejde, herunder sikre høj awareness om informationssikkerhed
- Sikrer at medarbejdere gennemgår organisationens uddannelseslektioner om informationssikkerhed
- Drøfter løbende medarbejdernes håndtering af informationssikkerhed på faglige møder i afdelingen
- Gør informationssikkerhed til et tema for at sikre medarbejdere får en generel forståelse for informationssikkerhed og arbejder med, hvordan de understøtter den i hverdagen.
- Afholder formidlingsmøder og følger op

Som medarbejder

- Overholde gældende politikker
- Udpege mangler i gældende politikker og efterlevelsen af disse
- Rapportere risici og hændelser på en proaktiv måde

Hent inspiration i Rejsefortællingen fra www.sikkerdigital.dk HER:
https://sikkerdigital.dk/media/6819/sikkerdigital-rejsefortaelling-mellemleder-2020.pptx
Materialet er udarbejdet og formidlet af digitaliseringsstrategien, KL og Danske Regioner.

Data- og Systemejer



Rolle i sikkerhedsarbejdet

Dispositionsret til data og ansvar for behandling af data.

Ansvar for informationssikkerheden for det/de systemer man ”ejer” herunder ansvar for udarbejdelse af operationelle procedurer, instrukser og tjeklister inden for rammerne af de sikkerhedsniveauer organisationens topledelse har fastlagt.

Ansvar for at føre løbende kontrol med overholdelse af retningslinjer og procedurer, samt vedligeholdelse af systemer, processer, interessenter, aktiver, kontrakter etc.

Opgaver der typisk skal udføres

- Skabe overblik over, hvilke forretningsprocesser systemer og data understøtter. Overblikket bruges til at sikre, at der stilles relevante og tilstrækkelige sikkerhedsmæssige krav med udgangspunkt i organisationens sikkerhedsniveauer
- Klassificere aktiver og specificere sikkerhedsmæssige krav samt godkende anskaffelser og installation af hvert aktiv
- Give adgang til systemer og data
- Godkende placering af kritiske aktiver samt udviklings- og hjælpemiljøer
- Godkende beredskabsplaner og følge op på sikkerhedshændelser
- Delegere rutinemæssige opgaver til en person (entitet), der dagligt holder øje med aktiverne, men har stadig det endelige ansvar for systemets informationssikkerhed i hele systemets levetid

Som medarbejder

- Overholde gældende politikker
- Udpege mangler i gældende politikker og efterlevelsen af disse
- Rapportere risici og hændelser på en proaktiv måde

Hent inspiration i Rejsefortællingen fra www.sikkerdigital.dk HER:
https://sikkerdigital.dk/media/6820/sikkerdigital-rejsefortaelling-systemejer-2020.pptx
Materialet er udarbejdet og formidlet af digitaliseringsstrategien, KL og Danske Regioner.

Informations-sikkerhedskoordinator

Rolle i sikkerhedsarbejdet

Bør referere direkte til topledelsen, men uanset den organisatoriske placering er det vigtigt, at ansvar og beføjelser præciseres af topledelsen.

Opgaver der typisk skal udføres

- Lede risikovurderinger og komme med forslag til opdatering af informationssikkerhedspolitikken
- Registrere og rapportere kritiske hændelser
- Evaluere og benchmarke organisationens sikkerhed
- Skabe opmærksomhed om informationssikkerhed blandt organisationens medarbejdere
- Indkalde til møder og være sekretær for Informationssikkerhedsudvalget
- Afklare snitflade i forhold til øvrige politikker i organisationen og vurdere behovet for drøftelse af informationssikkerhedspolitikken internt

Som medarbejder

- Overholde gældende politikker
- Udpege mangler i gældende politikker og efterlevelsen af disse
- Rapportere risici og hændelser på en proaktiv måde

Databeskyttelses-rådgiver (DPO)

Rådgiver og hjælper organisationen med at overholde de lovgivningen og skal inddrages i alle spørgsmål om beskyttelse af persondata.

Rolle i sikkerhedsarbejdet

Skal overvåge og rådgive, så organisationen overholder både lovgivningen og interne politikker ift. beskyttelse af personoplysninger.

Involveret i spørgsmål vedrørende beskyttelse af personoplysninger og fungerer desuden som kontaktperson for de registrerede og databeskyttelsesmyndigheder.

Må ikke modtage instrukser om opgaver, og skal rapportere direkte til øverste ledelse.

Opgaver der typisk skal udføres

- Overvåge, underrette og rådgive organisationen om behandlingsaktiviteter for beskyttelse af personoplysninger, implementering og overholdelse af både lovgivningen og interne politikker ift. beskyttelse af persondata
- Rådgive i forhold til interne politikker for beskyttelse af personoplysninger, så behandling af persondata sikres ved kontrakt- og leverandørstyring mv
- Rådgive om udvikling og vedligeholdelse af intern dokumentation om beskyttelse af personoplysninger
- Fungere som kontaktperson for de registrerede og databeskyttelsesmyndigheder om evt. brud på datasikkerheden og mere generel information omkring rettigheder
- Overvåge og rådgive om konsekvensanalyse vedrørende behandlingsaktiviteter for beskyttelse af personoplysninger, når der er en høj risiko for at behandling af oplysninger krænker den registrerede

Som medarbejder

- Overholde gældende politikker
- Udpege mangler i gældende politikker og efterlevelsen af disse
- Rapportere risici og hændelser på en proaktiv måde

Hent inspiration i Rejsefortællingen fra www.sikkerdigital.dk HER:
https://sikkerdigital.dk/myndighed/iso-27001-implementering/forstaa-arbejdet-med-informationssikkerhed/aarshjul-og-planlaegning
Materialet er udarbejdet og formidlet af digitaliseringsstrategien, KL og Danske Regioner.

Medarbejdere

Har ansvar for at overholde gældende politikker og rapportere risici og hændelser.

Rolle i sikkerhedsarbejdet

Har den vigtigste rolle i forhold til informationssikkerheden. Skal sikre, at de uddelegerede opgaver udføres på en måde, så organisationen efterlever lovgivningen, interne politikker og retningslinjer.

Kan naturligvis have meget forskellig berøring med data, information og fysisk sikkerhed. Og kan dermed have forskellige roller i sikkerhedsarbejdet.

Opgaver der typisk skal udføres

- Overholde gældende politikker
- Udpege mangler i gældende politikker og efterlevelsen af disse
- Rapportere risici og hændelser på en proaktiv måde

Automatiser jeres oprydning med Adoxa

Adoxa kan hjælpe din organisation med at overholde de 6 principper for korrekt behandling af persondata.

Vores løsning kan nemlig agere teknisk bagstopper og hjælper, så:

- Dine medarbejdere kender principperne
- Du kan følge op på hvordan I behandler persondata
- Du kan som leder dokumentere, at I efterlever principperne.

Adoxa er et datakvalitetsværktøj, der søger og behandler data på tværs af datakilder, som dermed hjælper dig og dine medarbejdere med oprydning i jeres data, som understøtter GDPR samt interne og eksterne compliancekrav.

- ☑ Indeholder +100 prædefinerede søgeregler
- ☑ Nemt selv at implementere nye regler efter behov
- ☑ Giver besked, hvis der er noget der kræver handling
- ☑ Oprydning kan foretages direkte fra besked eller brugerportal - uanset datakilde
- ☑ Politikker og eskalering sikrer fremdrift i oprydningen
- ☑ Ledelsesmæssigt og individuelt overblik for aktuel status på indsats og opgaver

Adoxa benyttes af +200.000 brugere inden for både den private og offentlige sektor.

Kontakt os i dag og se, hvilken forskel Adoxa kan gøre for jer.

Per Søndergaard
Business Development Manager
+45 7220 8151
per.soendergaard@formpipe.com

Formpipe.