Kvalitetsledelse

GDPR og IT-sikkerhed som en del af audit

Agenda

En kort indflyvning:

- Introduktion
- Kort om IT-sikkerhed og GDPR
- IT-sikkerhed og GDPR som en del af audit – hvor passer det ind?

En praktisk tilgang:

- Hvad kan du gøre som auditor?
- Eksempler på punkter til din audit checkliste

Afrunding og spørgsmål

Thomas Riisager

Dcide ApS og AddBusiness ApS

Baggrund

- Uddannet produktionsingeniør
- Lead Auditor uddannet
- Plesner Certifikat i Persondataret (GDPR).
- Mini MBA i Sustainability Management

Kompetencer

- Mere end 20 års erfaring som proceskonsulent, facilitator og træner inden for procesoptimering, GDPR og digital transformation.
- Har desuden arbejdet med etablering af ledelsessystemer inden for kvalitet, miljø og arbejdsmiljø.
- Hjælper virksomheder med at gøre bæredygtighed til en god forretning

Hvorfor skal du interessere dig for IT-sikkerhed og GDPR?

- Fordi du beskytter kritiske forretningsdata mod cybertrusler og derved opretholder tillid og omdømme blandt dine interessenter

- Fordi det er med til at gøre din virksomhed mere robust

Kort om IT-sikkerhed og GDPR

Hvad er IT-sikkerhed?

- Et værn, der beskytter din organisations data mod digitale trusler og risici.
- Mere end teknologi – Det handler om at etablere en kultur hvor bevidsthed og compliance er bærende elementer.
- Konstant udvikling, ikke et fast mål – Det handler om at tilpasse sig nye trusler og muligheder.

Grundelementerne i IT-sikkerhed

- Risikovurdering og -styring
- Sikkerhedspolitikker og -procedurer
- Styring af informationsaktiver – data, hardware og software
- Bevidsthed og kompetencer
- Løbende overvågning og forbedring

Hvad er GDPR?

- EU lovgivning, der beskytter dig mod ulovlig og urimelig behandling af dine personoplysninger.
- Krav om dokumentation – Dette omfatter dokumentation af formålet med behandlingen, datakategorier, opbevaringsperioden, m.m..
- Overvågning og gennemgang – Løbende overvågning af databehandlingsaktiviteter og håndtering af afvigelser og databrud. Dette omfatter logning og underretning af myndigheder og berørte personer

Grundelementerne i GDPR

- Lovligt, retfærdigt og gennemsigtigt
- Formålsbegrænsning
- Dataminimering
- Nøjagtighed
- Opbevaringsbegrænsning
- Integritet og fortrolighed
- Ansvarlighed

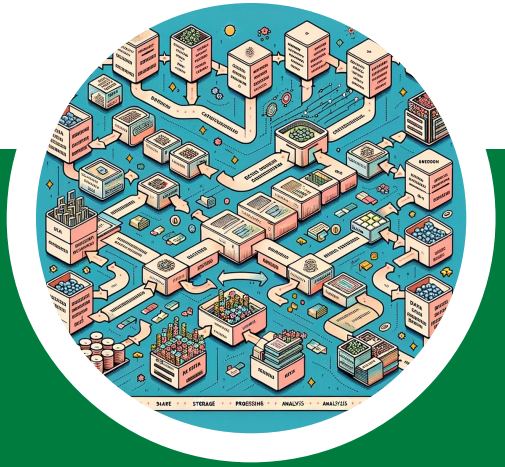
Hvordan får vi det naturligt med i audit?

Alignment

Ved at relatere elementerne til specifikke områder i ISO 9001, skaber du en naturlig sammenhæng

Fokus på risiko

Det handler om risikominimering, så sæt fokus på de risikoelementer der er i processerne



Data i virksomheden

Få styr på hvor i jeres processerne der håndteres data og hvilke data I sender og modtager

Hvor passer elementerne ind?

Rammer og vilkår – afsnit 4

- IT-sikkerhed og GDPR bør tænkes ind som elementer i forståelsen af de eksterne og interne forhold, der er relevante for organisationens formål og strategiske retning (afsnit 4.1)
- Er der taget højde for det i interessentanalysen? (afsnit 4.2)

Lederskab – afsnit 5

- Ledelsen skal demonstrere engagement i forhold til IT-sikkerhed og GDPR, og sikre, at disse er integrerede dele af forretningsstrategien (afsnit 5.1.1 og 5.1.2)
- Der bør være en IT-sikkerhedspolitik og denne skal være kommunikeret ud i organisationen og evt. til interessenter (afsnit 5.2.1 og 5.2.2)

Planlægning – afsnit 6

- Risikostyringsprocesser i IT-sikkerhed er direkte sammenlignelige med ISO 9001's krav til håndtering af risici og muligheder (afsnit 6.1)

- Overholdelse af GDPR-krav bør overvejes, når man planlægger ændringer (afsnit 6.3)

Støtteaktiviteter og –funktioner – afsnit 7

- Der skal tages hensyn til nødvendigheden af ressourcer til IT-sikkerhed og GDPR, herunder hardware og software (afsnit 7.1.3) og tilgængelighed af viden om IT-sikkerhed og GDPR (afsnit 7.1.6)

- Dokumenteret information, der kræves af GDPR, skal sidestilles med dokumentations-kravene i ISO 9001 (afsnit 7.5)

Drift – afsnit 8

- IT-sikkerhed og databeskyttelse tænkes ind i procesdesign, produktdesign og i levering af virksomhedens produkter og ydelser (afsnit 8.1, 8.2 og 8.3)

- I forhold til styring af processer, produkter og ydelser leveret udefra, bør krav til IT-sikkerhed og databeskyttelse også være afdækket (afsnit 8.4)

Præstationsevaluering – afsnit 9

- Sideløbende med overvågning, måling og analyse af ledelsessystemets præstation, bør informationssikkerheds- og databeskyttelsesprocesser også overvåges, måles og analyseres (afsnit 9.1)

- GDPR-kravene vedr. tilsyn med databehandlere, bør integreres i den løbende evaluering af eksterne leverandører (afsnit 9.1.3)

Forbedring – afsnit 10

- Brud på datasikkerheden eller forsøg på uautoriseret adgang til data, bør håndteres på samme måde som afvigelser i ledelsessystemet (afsnit 10.2)

- Brud på persondatasikkerheden skal håndteres efter fastlagte procedurer med krav om rapportering til myndigheder og berørte personer i visse situationer (afsnit 10.2)

Hvad kan du gøre som intern auditor?

Hvordan får du mest muligt ud af audit?

- Sæt dig ind i kravene i GDPR og ISO 27001
- Sæt dig ind i hvilke IT-systemer I anvender og de sikkerhedsrisici der er ved disse
- Blend dine spørgsmål ind i din checkliste, så de kommer naturligt bland de øvrige

Eksempler til audit checkliste - #1

Rammer og vilkår

- Anerkendes vigtigheden af informationssikkerhed og databeskyttelse i den organisatoriske kontekst og strategi?
- Er eksterne og interne faktorer relateret til datasikkerhed og beskyttelse af persondata identificeret og dokumenteret?

Lederskab

- Viser ledere engagement i at opretholde og forbedre IT-sikkerheden og efterlevelse af GDPR?
- Er ansvar for databeskyttelse og informationssikkerhed fastsat på ledelsesniveau?

Eksempler til audit checkliste - #2

Planlægning

- Identificeres, analyseres og styres risici relateret til informationssikkerhed og databeskyttelse?
- Er der en proces for adressering af IT-sikkerhed og GDPR-krav i styring af forandringer?

Støtteaktiviteter og -funktioner

- Er der afsat tilstrækkelige ressourcer til IT-sikkerhed og GDPR (f.eks. uddannelse, software)?
- Er der løbende uddannelse og sikring af bevidsthed blandt medarbejderne om databeskyttelse og informationssikkerhed?

Eksempler til audit checkliste - #3

Drift

- Er der taget hensyn til krav til IT-sikkerhed og GDPR i operationelle processer og procedurer?
- Er der en proces til evaluering af databeskyttelse og sikkerhedsforanstaltninger i forbindelse med levering af produkter/ydelser?

Præstationsevaluering

- Er der regelmæssige kontroller for at vurdere overholdelse af IT-sikkerhedskrav og GDPR?
- Findes der en proces til overvågning og måling af effektiviteten af databeskyttelses- og informationssikkerhedstiltag?

Eksempler til audit checkliste - #4

Håndtering af hændelser og afvigelser

- Er der en procedure til håndtering af informationssikkerhedshændelser og databrud?
- Er der foretaget dokumenterede handlinger som reaktion på identificerede hændelser relateret til IT-sikkerhed og GDPR?

Forbedringer

- Er der en proces for løbende opdatering og forbedring af IT-sikkerheden og databeskyttelsestiltag?
- Føres erfaringer fra audits og afvigelser tilbage til systemet med henblik på løbende forbedringer?

Spørgsmål?

Kontaktinfo

tri@addbusiness.dk / thomas@dcide.dk

+45 6067 0910

Betonvej 10,
4000 Roskilde

www.addbusiness.dk / www.dcide.dk