GDPR PROJEKTPLAN – I KORTE TRÆK

STEP 1:
PROJEKTPLANLÆGNING

- Nedsæt en projektgruppe og udpeg en eller flere projektansvarlige.
- Det er en tværfaglig øvelse. IT, HR, Jura skal alle være med om bordet.
- Fastlæg ønsket compliance-niveau (fuldt eller risikobaseret, gerne opdelt på områder)
- Få buy-in fra toppen af organisationen.
- Projektet skal tildeles ressourcer (økonomi og tid).
- Projektgruppen skal have overordnet kendskab til og træning i reglerne i GDPR.
- Læs f.eks. DI's notat: Persondataforordningen – i kort form og gå på kurser om GDPR.

STEP 2:
DATASTRØMSANALYSE

- Afdæk først de processer, hvori I behandler personoplysninger, og udvælg de processer, der skal udfyldes spørgeskemaer for (om ikke alle).
- Anvend DI's vejledning til procesafdækning.
- Book interviews og på baggrund af disse interviews med repræsentanter fra afdelingerne udfylder I spørgeskemaet for hver proces.
- Anvend f.eks. DI´s standardspørgeskema for at afdække f.eks.:
  - Hvilke personoplysninger behandler I, og til hvilke formål?
  - Giver den registrerede samtykke til behandlingen?
  - Giver I den registrerede oplysning om behandlingen?
  - Sletter I oplysninger (og hvornår)?

Dansk Industri

STEP 3:
GAP-ANALYSE

- Analyser de udfyldte spørgeskemaer.
- Identificer de gennemgående områder, hvor reglerne ikke overholdes.
- Fastsæt kriterier for at udvælge og prioritere tiltag på baggrund af det ønskede compliance-niveau, tiden og de tildelte ressourcer.

STEP 4:
COMPLIANCE OG DOKUMENTATION

- Vælg hvilke tiltag, der skal prioriteres og implementeres.
- Udarbejd en to-do liste og en implementeringsplan.
- Udarbejd og tilpas de nødvendige dokumenter, f.eks. procedurer og retningslinjer for behandlingen af personoplysninger, samtykketekster, privatlivspolitikker, indsigelsestekster, databehandler-aftaler, brevskabeloner til registrerede og myndighederne mv.
- Udarbejd beredskabsplaner til håndtering af sikkerhedsbrud.
- Indgå (nye) databehandleraftaler med databehandlere, f.eks. leverandører af IT-systemer, og eventuelle dataansvarlige, som I behandler personoplysninger for.
- Tilpas IT-systemerne f.eks. til sletning og håndtering af registreredes rettigheder.
- Udarbejd art. 30-dokumentation.
- Anvend f.eks. DI´s format til dokumentation af Personoplysninger.
- Undervis medarbejdere, der behandler personoplysninger.
- Indarbejd fortrolighedsklausuler i ansættelseskontrakter.
- Tilrettelæg et compliance-årshjul med løbende kontrol og interne inspektioner af den interne data behandling og databehandleres databehandling.
- Følg op på problematiske forhold identificeret som led i kontrollerne.