

FORBLIV COMPLIANT MED DEN NYE PERSONDATALOV

Med EU's nye databeskyttelsesforordning fulgte en stor mængde forberedende aktiviteter, hvor virksomhedens fokus var at blive compliant. Nu er forordningen og den nye danske databeskyttelseslov trådt i kraft, og fokus er flyttet fra at blive compliant til at forblive compliant.

IT i praksis[®] har i de senere år givet indblik i, hvilke aktiviteter der skal til for at blive compliant med databeskyttelsesforordningen. Siden den 25. maj 2018 har flere virksomheder arbejdet på at færdiggøre de sidste aktiviteter for at blive compliant.

Overgangen har fyldt meget i offentlige såvel som private virksomheder, og fokus er nu på, hvad der skal til for at forblive compliant. Men hvad betyder det for en virksomhed at forblive compliant?

Formålet med EU's databeskyttelsesforordning er at beskytte de registrerede

virksomheder og sørge for, at de har den fornødne kontrol over egne personlige oplysninger. Enhver behandling af personoplysninger skal overholde følgende databeskyttelsesprincipper:

- Lovlighed, rimelighed og gennemsigtighed
- Formålsbegrænsning
- Dataminimering
- Rigtighed
- Opbevaringsbegrænsning
- Integritet og fortrolighed
- Ansvarlighed

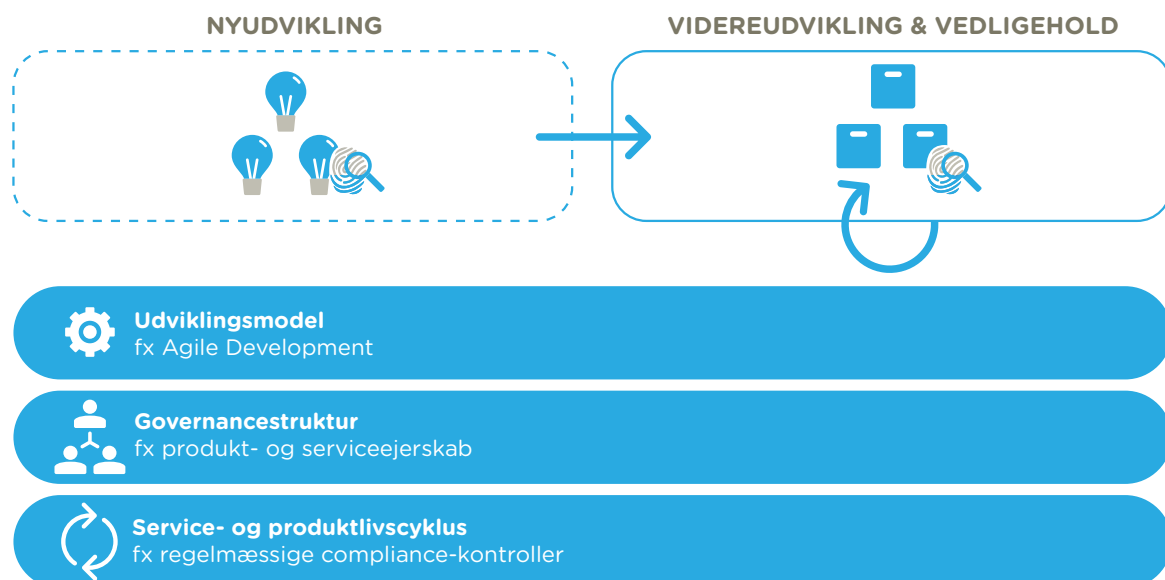
Derudover introducerer loven også principperne for databeskyttelse gennem design og standardindstillinger.

Disse principper skaber klare designkrav til de af fremtidens services og produkter, der behandler personoplysninger.

Virksomheder, der udvikler nye og videreudvikler eksisterende services og produkter, og som behandler personoplysninger, skal justere deres service- og produktudvikling efter databeskyttelsesprincipperne. En sådan justering omfatter alle udviklingsaktiviteter, governance-strukturer og styring af service- og produktlivscyklus for såvel interne som eksterne services og produkter. Interne services behandler i nogle tilfælde en række personoplysninger om medarbejdere, fx HR-funktioner.

DATABESKYTTESLOVENS INDVIRKNING PÅ UDVIKLINGSAKTIVITETER

Databeskyttelsesloven påvirker såvel udviklingen af nye som eksisterende services og produkter, uanset om disse er interne redskaber eller eksterne kundeløsninger.



Udviklingsmodel

Uanset om en virksomhed har anlagt en mere eller mindre agil udviklingsmodel, bør faser og beslutningspunkterne i modellen afspejle de nye databeskyttelsesprincipper. Man bør i designfasen være opmærksom på, hvorvidt den pågældende ide nødvendiggør behandling af personoplysninger, og i så fald hvilke typer af personoplysninger formålet berettiger behandling af.

Udviklingen af selve servicen eller produktet indebærer, at det skal sikres, at servicen eller produktet har det fornødne sikkerhedsniveau og funktionalitet til at efterkomme databeskyttelsesprincipperne og de registrerede virksomheders rettigheder.

Dette medfører ikke blot implementering af tekniske foranstaltninger (fx dataminimering gennem begrænset indsamling af personoplysninger),

men også implementering af organisatoriske foranstaltninger (fx procedurer, retningslinjer mv.).

Governancestruktur

Efter lancering af en ny service eller et nyt produkt er det vigtigt, at der etableres den rette governancestruktur. Dette indebærer at skabe det fornødne service- eller produkt-ejerskab, styring af databehandlere og underdatabehandlere samt organisering gennem procedurer, retningslinjer mv.

Governancestrukturen skal også sikre, at service- og produktejeren opdaterer virksomhedens fortegnelse over behandlingsaktiviteter med nye services eller produkter samt videreudvikling heraf.

På den måde sikrer virksomheden, at forudsætningerne for, at servicen eller produktets fremtidige compliance er på plads.




Service- og produktlivscyklus

Et af de mest anvendte retlige grundlag for behandling af personoplysninger er samtykke. For alle services og produkter, der behandler personoplysninger, er det derfor nødvendigt løbende at foretage styring af samtlige samtykker. Personoplysninger kan behandles, så længe det er nødvendigt ifølge formålet. Sletterutiner kan foregå løbende i service- og produktlivscyklussen.

Rambøll anbefaler, at virksomheder foretager et review af deres eksisterende udviklingsmodel og indlejrer de nødvendige compliance-elementer heri for at forblive compliant med databeskyttelsesloven.

Derudover anbefaler Rambøll, at virksomheder justerer den eksisterende governancestruktur eller etablerer en ny for service- og produktejerskab mv., og at samtykkestyring og sletterutiner mv. implementeres i virksomhedernes service- og produktlivscyklus.

ACTION ITEMS

- 
Foretag et review af udviklingsmodel og indlejrer aktiviteter, der tilsigter overholdelse af databeskyttelsesloven
- 
Juster eksisterende eller etabler ny governancestruktur for services og produkter for at forankre ansvar for compliance
- 
Implementer samtykkestyring og sletterutiner i service- og produktlivscyklus for at sikre kontinuerlig styring