GDPR og operationel compliance

Jesper Husmer Vang og Sara Holst Sonne

Hvor er vi gået fra og til med GDPR?

- De opgaver der følger med forordningens artikel 5, stk. 2, og artikel 24 er kommet bag på mange
- Tidligere var det tilstrækkeligt, hvis man kunne fremlægge en fin persondatapolitik
- Nu skal man også efterleve politikken i praksis og kunne dokumentere dette

Datatilsynets slettetilsyn fra efteråret 2018

Læren af tilsynene:

- Man skal have styr på:
  1. Hvilke systemer man har
  2. Hvilke personoplysninger der behandles i systemerne
  3. Man skal fastsætte en passende slettefrist for de personoplysninger, man har i de enkelte systemer mv. og dokumentere de fastsatte frister (vi har set eksempler på, at fristerne ikke var nedskrevet nogen steder, men blot var inde i hovederne på udvalgte medarbejdere).
  4. Man skal vide og kunne dokumentere, hvordan sletningen understøttes teknisk samt manuelt og/eller automatisk (vi har f.eks. set eksempler på, at en "sletning" blot indebar, at der ikke længere kunne ske en kobling mellem sagsbehandlingssystem og database → dette er ikke en sletning)
  5. Man skal følge op på, om sletning rent faktisk finder sted og kunne dokumentere sine procedurer for denne opfølgning (stikprøvekontroller mv.)

- Datatilsynet vil på et tilsyn kontrollere ovennævnte samt lave stikprøvekontroller af, om der forefindes oplysninger i systemerne, der burde være slettet efter de fastsatte frister.

PLESNER

Compliance

Compliance
Det at efterleve en lov eller regel, eller at agere i overensstemmelse med en aftale

Cambridge dictionary

Compliancerisiko
virksomhedens manglende overholdelse af gældende lovgivning, markedsstandarder eller interne regelsæt (compliancerisici)

PLESNER

Accountabiliy - hvis det ikke er dokumenteret, er det ikke sket!

Hvordan er man accountable?

- Dokumenter at I har forholdt jer til hvordan I implementerer reglerne (politikker og procedurer)
- Dokumenter at *I rent faktisk gør det, I siger I gør!*

Eksempel

Det er ikke tilstrækkeligt at skrive i en procedure, at "*vi indhenter samtykke*".

Samtykket skal gemmes på kunden med datoangivelse, så det altid kan fremfindes.

Behovet for skriftlige politikker og dokumentation skal ses i forhold til virksomhedens størrelse, omfanget af behandlingsaktiviteterne og den iboende risiko

PLESNER

Nogle gode råd baseret på erfaringer

- Vurder jeres risiko, og prioriter flest ressourcer der hvor, risikoen er størst (sandsynlighed * konsekvens)
- Definer roller og ansvar og dokumenter i skriftlige procedurer (risiko ved udskiftning af medarbejdere, når alle har ansvaret har ingen ansvaret)
- Implementer passende foranstaltninger for at minimere risiko for fejl (fx fjerne muligheden for fritekstfelt)
- Husk, ingen skal vide alt, alle skal vide nok (Procedurer overkompliceres ofte, keep it simple)
- Definer kontroller, udfør, evaluer og rapporter
- Ressourcebehovet undervurderes ofte, opgaver nedprioriteres
- Manglende dokumentation
- Forordningen tænkes ikke ind i forbindelse med ændringer (nye produkter, systemer, organisationsændringer, osv.)

PLESNER

Case

I har konstateret, at medarbejderne i jeres call center ikke følger jeres interne GDPR procedurer.

De noterer følsomme oplysninger om kunderne i jeres CRM system, sender mails med personoplysninger til forkerte kunder og glemmer/undlader at indhente og registrere samtykke fra kunder.

Diskuter med sidemanden hvilke foranstaltninger I kan implementere for at minimere risikoen for non-compliance

- Forebyggende foranstaltninger
- Kontroller