Wolters Kluwer Danmark A/S
Fåborgvej 65A
5700 Svendborg

Telefon: 62 21 53 53
itrevisor@wolterskluwer.dk
www.wolterskluwer.dk

Emne: Risikovurdering og konsekvensanalyse

Risikovurdering

Virksomhederne har ansvaret for at etablere et sikkerhedsniveau, der matcher den risiko for de registreredes rettigheder, som er forbundet med behandling af personoplysninger. Derfor skal virksomhederne foretage en risikovurdering for at fastsætte og implementere det rette sikkerhedsniveau.

Kravet gælder både for dataansvarlige og for databehandlere.

Udgangspunktet er en vurdering af risikoen for at personoplysninger, der opbevares, videregives eller på anden måde behandles, herunder om der fx er risiko for

- Hændelig eller ulovlig tilintetgørelse,
- Tab,
- Ændring,
- Uautoriseret videregivelse eller
- Uautoriseret adgang.

Risikovurdering kan baseres på tre parametre: Fortrolighed, integritet og tilgængelighed. Spørgsmålet er om den pågældende risiko kan medføre

- at data ikke længere vil være fortrolige
- at data ikke længere er tilgængelige eller
- at datas integritet sættes på spil

På baggrund af risikovurderingen skal virksomheden implementere det nødvendige sikkerhedsniveau, hvilket sker ved at gennemføre tekniske og organisatoriske sikkerhedsforanstaltninger.

En teknisk sikkerhedsforanstaltning kan fx være brug af password for at få adgang til et system, kryptering, etablering af bruger-ID, kontrol med hacking osv.

En organisatorisk sikkerhedsforanstaltning kan fx være uddannelse af medarbejdere i databeskyttelse, etablering af forskellige autorisationsniveauer for adgang til et system, diverse procedurer osv.

Det er som udgangspunkt op til virksomheden selv at vurdere, hvilke foranstaltninger, der skal gennemføres. Ved vurderingen skal man dog lægge vægt på:

- Det aktuelle tekniske niveau.
- Implementeringsomkostningerne.
- Behandlingens karakter, omfang, sammenhæng og formål.
- De sandsynlige risici for den registreredes rettigheder og frihedsrettigheder.

Behandler virksomheden følsomme personoplysninger, bør virksomhedens systemer vurderes på bl.a. disse parametre:

- Kan en hændelse medføre at den registrerede lider økonomiske tab?
- Kan en hændelse medføre at den registreredes omdømme tager skade
- Kan en hændelse medføre tyveri af den registreredes identitet?

Wolters Kluwer Danmark A/S
Fåborgvej 65A
5700 Svendborg

Telefon: 62 21 53 53
itrevisor@wolterskluwer.dk
www.wolterskluwer.dk

Konsekvensanalyse

Hvis behandlingerne af personoplysninger er forbundet med høj risiko for den registreredes rettigheder, skal en dataansvarlig virksomhed udarbejde en konsekvensanalyse.

Hvad er en konsekvensanalyse?

En konsekvensanalyse er en analyse af de risici eller den negative påvirkning den registrerede udsættes for, når virksomheden behandler vedkommendes personoplysninger. Risikoen kan bestå i en faktisk eller potentiel risiko i forhold til at blive udsat for diskrimination, for ID-tyveri, økonomisk tab, tab af omdømme eller datafortrolighed osv.

Med denne analyse får en dataansvarlig virksomhed mulighed for at identificere potentielle risici – inden de opstår – og får hermed mulighed for at imødegå de pågældende risici.

Vurderingen af risiko og konsekvenser bør løbende være ajourført.

CVR-nr. 13 38 62 93

Wolters Kluwer Danmark A/S
Fåborgvej 65A
5700 Svendborg

Telefon: 62 21 53 53
itrevisor@wolterskluwer.dk
www.wolterskluwer.dk

Emne: Eksempler på spørgsmål til checkliste til risikovurdering (ikke udtømmende)

1) Er virksomheden dataansvarlig og/eller databehandler?
2) Involverer processen behandling af følsomme personoplysninger, fx race, etnisk oprindelse, politisk eller filosofisk overbevisning, seksuelle forhold?
3) Er det hensigten at anvende data til andre formål end formålet oplyst af den dataansvarlige?
4) Bygger databehandlingen på én af følgende grunde?
   a) Behandlingen sker med samtykke for den registrerede.
   b) Behandlingen er nødvendig for at opfylde eller indgå en kontrakt, som den registrerede er part i.
   c) Behandlingen er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige.
   d) Behandlingen er nødvendig for at beskytte den registreredes vitale interesser.
   e) Behandlingen er nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som hører under offentlig myndighed.
   f) Behandlingen er nødvendig for at den dataansvarlige kan forfølge en legitim interesse som er vigtigere end den registreredes interesser eller grundlæggende rettigheder.
5) Er behandlingsformålet tilstrækkeligt og detaljeret beskrevet?
6) Benyttes data til andre formål end det, hvortil de pågældende data er indsamlet?
7) Er data pseudonymiseret eller anonymiseret før brug til andre formål end det oprindelige?
8) Er data indsamlet pseudonymiseret eller anonymiseret?
9) Er databehandlingen kompatibel med det oprindelige formål, hvortil dataene er indsamlet?
10) Er adgang til data og servere tilstrækkeligt beskyttet?
11) Er teknisk sikkerhed i øvrigt tilstrækkelig (sikkerhedskopiering, virus, spam)?
12) Er password politik tilstrækkelig (krav til kompleksitet, ændring)?
13) Er medarbejdere tilstrækkeligt uddannet i brugen af virksomhedens programmer og i GDPR?
14) Er der implementeret tilstrækkelige politikker for behandling af personoplysninger?