C-cure
Dronninggårdss Allé 138
DK-2840 Holte
Tel. +45 4541 1446
Web: www.c-cure.dk

10. december 2018

Hvornår skal man udføre en konsekvensanalyse (DPIA)?

Dette er C-cure´s fri danske oversættelse af Datatilsynets engelske liste over situationer, hvor dataansvarlige altid skal udarbejde konsekvensanalyser. Datatilsynets udkast blev publiceret 2/11-2018 og godkendt d. 4/12-2018.

Det er et krav i databeskyttelsesforordningen, at de nationale datatilsyn i alle EU-lande hver især skal udarbejde lister over situationer, hvor det er obligatorisk at foretage konsekvensanalyser. Listen er godkendt af Det Europæiske Databeskyttelsesråd (EDPB).

Behandlingsaktiviteter er underlagt kravet om en konsekvensanalyse/vurdering (artikel 35, stk. 4, GDPR).

Datatilsynets liste over situationer, hvor der skal udarbejdes konsekvensanalyse

Udførelsen af en DPIA, er kun obligatorisk for den registeransvarlige i henhold til artikel 35, stk. 1, GDPR hvor dataprocesser "sandsynligvis vil medføre høj risiko for fysiske personers rettigheder og friheder".

Artikel 35, stk. 3 GDPR illustrerer, hvad der sandsynligvis vil medføre høj risiko. Dette er en ikke-udtømmende liste. WP 29's (Artikel 29 – Gruppen's) retningslinjer for konsekvensanalyse om databeskyttelse, som godkendt af EDPB, har præciseret kriterier, der kan hjælpe med at identificere, hvornår behandlingerne er underlagt kravet om en DPIA.

WP 29-retningslinjerne WP248 angiver, at en dataansvarlig, i de fleste tilfælde bør overveje, at udføre en DPIA, ved databehandling hvor to kriterier opfyldes; men der er også tilfælde hvor den dataansvarlige kan overveje, at udføre en DPIA, selvom kun et kriterie opfyldes.

Denne liste understøtter det samme mål, dvs. at identificere behandlingsaktiviteter, der sandsynligvis vil resultere i en høj risiko og behandlingsaktivitet, der derfor kræver en DPIA.

Datatilsynet gør opmærksom på at, WP 29-retningslinjerne WP248 er et kerneelement for sikring af konsistens i hele Unionen. I den henseende er denne liste baseret på WP248 retningslinjerne. Listen som er udarbejdet af Datatilsynet supplerer og præciserer retningslinjerne yderligere, og det skal understreges, at dette er en ikke-udtømmende liste over tilfælde hvor en DPIA skal udføres.

Disse behandlingsaktiviteter vil altid med stor sandsynlighed medføre høj risiko, og en DPIA skal udføres:

1. Behandling af biometriske data med det formål at unikt identificere en fysisk person, i forbindelse med mindst et andet kriterium fra WP29, retningslinjer (WP 248 rev. 01).
2. Behandling af genetiske data sammen med mindst et andet kriterium fra WP29, Retningslinjer (WP 248 rev. 01).
3. Behandling af lokaliseringsdata i forbindelse med mindst et andet kriterium fra WP29, Retningslinjer (WP 248 rev. 01).
4. Behandling med brug af nyskabende teknologi i forbindelse med mindst et andet kriterium fra WP29, Retningslinjer (WP 248 rev. 01).
5. Behandling, der fører til beslutninger om individets adgang eller ret til et produkt, service, mulighed eller fordel, hvilket er baseret på enhver form for automatiseret beslutningstagning (herunder profilering).
6. Behandling, der omfatter profilering af enkeltpersoner i stor skala som defineret i WP29, Retningslinjer (WP 248 rev. 01).

C-cure
Dronninggårdss Allé 138
DK-2840 Holte
Tel. +45 4541 1446
Web: www.c-cure.dk

7. Behandling af personoplysninger for udsatte personer eller på personoplysninger om særlige kategorier, som brug profilering eller anden automatiseret beslutningstagning.
8. Behandling hvor et brud på sikkerheden vedr. personoplysninger kan have direkte indvirkning på fysisk sundhed eller sikkerhed for enkeltpersoner.

Om konsekvensanalyse

En konsekvensanalyse vedrørende databeskyttelse er en proces, der har til formål at beskrive behandlingen af personoplysninger, vurdere behandlingens nødvendighed og proportionalitet, samt bidrage til at håndtere de risici for fysiske personers rettigheder og frihedsrettigheder, som behandlingen af personoplysninger medfører.

Vurdering af risici er også en del af kravene til behandlingssikkerhed generelt, men konsekvensanalysen går et skridt videre, ved at inkludere en proces, der blandt andet kan omfatte høring hos Datatilsynet og indhentning af de registreredes synspunkter vedrørende den planlagte behandling. Det er endvidere en proces, hvor der stilles specifikke krav til dokumentation.

Det er kun i visse situationer, at den dataansvarlige skal lave en konsekvensanalyse. Der er databehandlinger, hvor det er specielt påkrævet at udføre en konsekvensanalyse. Ved andre behandlinger beror det på en konkret vurdering, hvorvidt en konsekvensanalyse er påkrævet. Det er i første omgang den dataansvarlige selv, der skal foretage denne vurdering.

Rettigheder og pligter

Som dataansvarlig har du pligt til at foretage en konsekvensanalyse, når der sandsynligvis vil være en høj risiko for fysiske personers rettigheder og frihedsrettigheder. Herunder skal du, hvis det er relevant, høre de registreredes eller deres repræsentanters synspunkter vedrørende din planlagte behandling af deres personoplysninger.

Pligten til gennemføre en konsekvensanalyse, når en sådan er påkrævet, er en del af det ansvar, du har som dataansvarlig. Det angår gennemførsel af passende tekniske og organisatoriske foranstaltninger for at du kan sikre og for at du kan være i stand til at påvise, at din behandling er i overensstemmelse med databeskyttelsesforordningen.

Man skal som dataansvarlig endvidere foretage en forudgående høring af Datatilsynet, hvis en konsekvensanalyse viser, at en behandling, selv efter eventuelt indførte foranstaltninger, sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder.

Som databehandler har man pligt til at hjælpe den dataansvarlige med at udføre konsekvensanalysen.

Hvis man ønsker at følge en standard

Der findes internationale standarder, som dækker samme emne. Dog kan man ikke antage, at en efterlevelse af disse standarder sikrer efterlevelse af databeskyttelsesforordningen. Sandarder kan dog være en hjælp til at komme rundt om alle de vigtige elementer i en konsekvensanalyse, og de kan dermed mindske risikoen for at man laver en mangelfuld konsekvensanalyse.

DS/ISO/IEC 29134 er et eksempel på en standard.

Sidst revideret af C-cure d. 10. december 2018