info@business-institute.dk
Telefon: 98 18 80 00

# Informationsproces når persondata er blevet kompromitteret

**Følgende artikler i EU's persondataforordning behandles af dette dokument:**

**Artikel 33 - Anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden**

**Artikel 34 - Underretning om brud på persondatasikkerheden til den registrerede**

info@business-institute.dk
Telefon: 98 18 80 00

## Indhold

info@business-institute.dk
Telefon: 98 18 80 00

# 1 Introduktion

Denne procedure er beregnet til at blive brugt, når en hændelse af en eller anden art har fundet sted, der har resulteret i eller formodes at have resulteret i tab af persondata, som organisationen er ansvarlig for. Dette dokument skal bruges sammen med ”Håndtering af situationer hvor persondata bliver kompromitteret”, der beskriver den overordnede proces for at reagere på en hændelse, der berører informationssikkerheden for Business Institute A/S.

Det er et krav i EU's Persondataforordning fra 2016 (GDPR), at hændelser, der sandsynligvis vil medføre en risiko for de registreredes persondata, skal indberettes til tilsynsmyndigheden for databeskyttelse uden unødig forsinkelse, og hvor muligt inden for 72 timer efter at være opmærksom på det. I tilfælde af at 72-timers målet ikke er opfyldt, skal årsagerne til forsinkelsen gives.

Hvor en hændelse påvirker personoplysninger, skal der træffes afgørelse om omfanget, timingen og indholdet af kommunikationen med de registrerede. GDPR kræver, at kommunikationen skal ske "uden unødig forsinkelse", hvis overtrædelsen sandsynligvis vil resultere i høj risiko for kompromittering af fysiske personers data.

De handlinger, der er beskrevet i dette dokument, bør kun bruges som vejledning ved besvarelse af en hændelse. Den konkrete karakter af en hændelse og dens indvirkning kan ikke altid forudsiges, og det er derfor vigtigt, at der anvendes en god grad af sund fornuft, når man beslutter hvad man skal gøre. Det er dog meningen, at de trin, der er beskrevet her, vil vise sig nyttige for at sikre, at vores forpligtigelser under GDPR er opfyldt.

# 2 Informationsproces når persondata er blevet kompromitteret

Når det er blevet besluttet, at der er sket brud omhandlende persondata, er der to parter, som ifølge GDPR muligvis har krav på at blive informeret. Disse er:

1. Tilsynsmyndigheden
2. De berørte personer

Det er ikke en automatisk konklusion, at overtrædelsen skal meddeles; dette afhænger af en vurdering af risikoen for, at overtrædelsen indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder (GDPR artikel 33). De følgende afsnit beskriver, hvordan denne beslutning skal træffes, og hvad man skal gøre, hvis der kræves anmeldelse.

## 2.1 Tilsynsmyndigheden

Tilsynsmyndigheden vedrørende GDPR for Business Institute A/S er:

| | |
|---|---|
| **Navn:** | Datatilsynet |
| **Adresse:** | Borgergade 28, 5<br>1300 København |
| **Telefon:** | |
| **Email:** | |
| **Andet:** | |

*Tabel 1 – Kontakt informationen for tilsynsmyndigheden*

Hvis organisationen opererer internationalt, er ovenstående detaljer for den udpegede hovedtilsynsmyndighed.

### *2.1.1 Beslutning om hvorvidt Tilsynsmyndigheden skal underrettes*

GDPR fastslår, at et persondatabrud skal meddeles tilsynsmyndigheden "medmindre overtrædelsen af personoplysninger sandsynligvis ikke medfører risiko for fysiske personers rettigheder og friheder" (GDPR artikel 33). Dette kræver, at organisationen vurderer risikoniveauet, inden det afgøres, om myndighederne skal informeres.

Faktorer, der skal tages i betragtning som en del af denne risikovurdering, bør omfatte:

- Om personoplysningerne var krypteret
- Hvis krypteret, hvor stærk var krypteringen
- I hvilket omfang dataene blev pseudoanonymiseret (dvs. om levende individer med rimelighed kan identificeres ud fra data)
- Data involveret f.eks. navn, adresse, bankoplysninger, biometri
- Mængden af involverede data
- Antallet af registrerede berørte
- Typen af overtrædelsen f.eks. tyveri, utilsigtet ødelæggelse
- Andre faktorer, der anses for relevante

Parter, der er involveret i denne risikovurdering, kan omfatte repræsentanter fra følgende områder, afhængigt af arten og omstændighederne i forbindelse med kompromitteringen af personoplysninger:

- Ledelse
- Drift områderne
- IT

Risikovurderingsmetoden, dens begrundelse og dens konklusioner skal være fuldt dokumenteret og underskrevet af ledelsen. Resultatet af risikovurderingen skal indeholde en af følgende konklusioner:

1. Bruddet på personlige data kræver ikke anmeldelse
2. Persondatabruddet kræver kun underretning til tilsynsmyndigheden
3. Persondatabruddet kræver underretning både til tilsynsmyndigheden og de berørte registrerede

Disse konklusioner kan ændres på baggrund af feedback fra tilsynsmyndigheden og yderligere oplysninger, der opdages som led i den igangværende undersøgelse af hændelsen.

### *2.1.2 Hvordan informeres tilsynsmyndigheden*

I tilfælde af, at det er besluttet at underrette tilsynsmyndigheden, kræver GDPR, at dette gøres "uden unødig forsinkelse og, hvor det er muligt, højst 72 timer efter at have fået kendskab til bruddet" (GDPR artikel 33). Hvis der er rimelig grund til ikke at have anmeldt bruddet inden for den angivende tid, skal disse grunde gives som en del af anmeldelsen.

Meddelelsen skal sendes via passende sikre midler til den myndighed, der er angivet i tabel 1.

Følgende informationer skal oplyses som led i anmeldelsen:

a) Typen af persondata kompromitteret, herunder, hvis det er muligt:

   i. Omtrentlig antal berørte personer

   ii. Omtrentlige antal berørte personoplysninger

b) Navn og kontaktoplysninger til den databeskyttelsesansvarlige eller til andet kontaktperson, hvor der kan indhentes flere oplysninger

c) En beskrivelse af de sandsynlige konsekvenser af kompromitteringen af persondata

d) En beskrivelse af de trufne eller foreslåede foranstaltninger, der skal træffes for at imødegå brud på persondata, herunder om nødvendigt, foranstaltninger til afhjælpning af eventuelle negative virkninger

e) Hvis meddelelsen falder uden for 72-timers vinduet, forklares årsagen til, at den ikke blev indsendt tidligere.

f) Skriftlig bekræftelse skal indhentes fra tilsynsmyndigheden om, at meddelelsen om krænkelse af personoplysninger er blevet modtaget, herunder dato og klokkeslæt, hvor den blev modtaget. Om nødvendigt tillader GDPR, at oplysningerne gives i faser uden unødig yderligere forsinkelse.

Dokumentation af overtrædelsen af personoplysninger, herunder dens virkninger og afhjælpende foranstaltninger, vil blive udarbejdet som en del af ”Håndtering af situationer hvor persondata bliver kompromitteret”.

## 2.2 Data Subjektet

### *2.2.1 Beslutning om hvorvidt de berørte personer skal underrettes.*

GDPR fastslår, at berørte personer skal informeres hvis der har været et databrud "når overtrædelsen af personoplysninger sandsynligvis vil medføre stor risiko for fysiske personers rettigheder og friheder" (GDPR-artikel 34). Bemærk tilføjelsen af ordet "stor" ud over definitionen i artikel 33.

Den risikovurdering, der blev foretaget tidligere i denne procedure (afsnit 2.1.1), vil have fastslået, om risikoen for de berørte registreres rettigheder og frihedsrettigheder vurderes at være tilstrækkelig høj til at begrunde en underretning til dem.

Hvis der senere er truffet foranstaltninger med henblik på at begrænse risikoen for de registrerede, så risikoen ikke længere er sandsynligt, vil kommunikationen til de registrerede ikke kræves af GDPR.

Meddelelse til berørte registrerede er heller ikke påbudt af GDPR, hvor den "ville indebære uforholdsmæssig indsats" (GDPR-artikel 34). I dette tilfælde skal der i stedet bruges en form for offentlig kommunikation.

Igen kan dette ændre sig på baggrund af retningslinjer fra tilsynsmyndigheden og yderligere oplysninger, der opdages som led i den igangværende undersøgelse af overtrædelsen.

### *2.2.2 Hvordan informeres de berørte personer*

Når det er besluttet, at bruddet berettiger til information til de registrerede, kræver GDPR, at dette sker uden unødig forsinkelse.

Meddelelsen til de berørte registrerede "skal klart og tydeligt beskrive karakteren af overtrædelsen af personoplysninger" (GDPR-artikel 34) og skal også omfatte:

a) Navn og kontaktinformationer til den databeskyttelsesansvarlige eller anden kontaktpunkt, hvor der kan fås flere oplysninger

b) En beskrivelse af de sandsynlige konsekvenser af tabet af persondata

c) En beskrivelse af de trufne eller foreslåede foranstaltninger, der skal træffes for at imødegå brud på persondata, herunder om nødvendige foranstaltninger til afhjælpning af eventuelle negative konsekvenser

Ud over de punkter, der kræves af GDPR, kan det være hensigtsmæssigt at give råd til den registrerede om de handlinger, de kan tage for at reducere de risici, der er forbundet med kompromitteringen af deres persondata.

I de fleste tilfælde vil det være hensigtsmæssigt at underrette de berørte registrerede via brev eller e-mail eller begge dele for at sikre, at meddelelsen er modtaget, og at de har mulighed for at træffe de nødvendige foranstaltninger.

## Dokumentinformation

**Dokumentinformation**:
Kritikalitet: Offentlig
Dokumentforfatter: direktør Lars Ib
Dokumentansvarlig: direktør Lars Ib
Godkendt af: bestyrelsesformand Jan Holmsgaard

| Version | Ikrafttrædelses-dato | Tekst / ændringer | Hvem | Dokumentnavn |
|---|---|---|---|---|
| 1.0 | 23.04.2018 | Nyt dokument. | Lars Ib | Procedure ved persondatabrud web |