ProcedureR for Håndtering af Brud på persondatasikkerheden i MKB

Dokumentet indeholder to procedurer:

1. Procedure for brud på persondatasikkerheden som skal indberettet til Datatilsynet
2. Procedure for brud på persondatasikkerheden, som kun kræver intern indberetning

# Versionshistorik

|  |  |  |  |
| --- | --- | --- | --- |
| **Version:** | **Dato:** | **Ændring:** | **Ansvarlig:** |
| 1.0 | 09.07.20 | Rettet til for at blive gældende for alle systemer i MKB. | Nanna Lange |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Indledning

Processerne for brud på datasikkerheden med og uden anmeldelse til Datatilsynet sikrer at der foreligger en klar præsentation af aktiviteter, roller og ansvar i det tilfælde af at der er sket et sikkerhedsbrud.

Et brud på persondatasikkerheden dækker over tilfælde, der fører til hændelig eller tilsigtet tab eller ændringer af personoplysninger såvel som uautoriseret videregivelse eller adgang til personoplysninger.

# Formål

Formålet med processen er at sikre en korrekt håndtering af eventuelle brud på persondatasikkerheden og at det sker i overensstemmelse med persondataforordningen.

# Ejerskab

Dokumentet ejes af ITK Digital som er ansvarlig for den videre udvikling og vedligeholdelse af processerne, samt at informere relevante medarbejdere om ændringer i den beskrevne procedurer.

# Anvendelse

Processerne anvendes når MKB:

* får en indberetning om at der sket et brud på persondatasikkerheden
* selv opdager at der er sket et brud på persondatasikkerheden

Eksempler for brud på persondatasikkerheden:

* Person får uautoriseret adgang til personoplysninger.
* Medarbejder ændrer eller sletter personoplysninger ved et uheld.
* Hackeangreb på server, hvor uvedkommende har fået indsigt i personoplysninger
* Medarbejdere videregiver ubevidst eller bevidst personoplysninger

# Procesbeskrivelse for brud på persondatasikkerheden som skal anmeldes til Datatilsynet

Udgangspunktet er at alle brud på persondatasikkerheden skal anmeldes til Datatilsynet. Det er kun, hvis det er usandsynligt, at bruddet indebærer en risiko for fysiske personers rettigheder, at der ikke skal ske en anmeldelse.

Hvor det er sandsynligt, at bruddet indebærer en risiko for fysiske personers rettigheder, skal der ske anmeldelse uden unødig forsinkelse og om muligt senest 72 timer efter, at den dataansvarlige er blevet bekendt med bruddet. Foretages anmeldelsen ikke inden for 72 timer, skal den ledsages af en begrundelse for forsinkelsen.

Hvis bruddets risikovurdering indebærer en høj risiko for den registreredes rettigheder, skal de registrerede underrettes. Den registrerede skal underrettes uden unødig forsinkelse efter, at bruddet er påvist

Hver magistrat har et antal personer, som kan foretage anmeldelse til Datatilsynet. For MKB er det sikkerhedsansvarlige personer, som skal lave anmeldelsen:

[Se hvem som er sikkerhedsansvarlige i MKB](http://it-sikkerhedshaandbog.adm.aarhuskommune.dk/main/policy/book/view?bookguid=SA14A0F89DF5AY54U0)

[Læs mere om hvordan selve anmeldelsen skal laves under kommunens procedure for brud på persondatasikkerheden](http://it-sikkerhedshaandbog.adm.aarhuskommune.dk/main/policy/book/view?bookguid=SA1631B06C5E8Y35AU0)

Nedenstående procesbeskrivelsen er vejledende og uddybende forklaring på de enkelte del-aktiviteter i arbejdsgangen.

|  |  |  |
| --- | --- | --- |
| **Trin** | **Rolle** | **Ansvar** |
| 1 | Anmelder (fx borger, leverandør, medarbejder) | Konstaterer et muligt brud på persondatasikkerheden |
| 2 | Modtager af anmeldelsen (fx medarbejder, leder) | Ved modtagelse om brud på persondatasikkerheden skal afdelingsleder/systemejer kontaktes. |
| 3 | Afdelingsleder/systemejer/sikkerhedsansvarlig | Kontakter MKB-sikkerhedsansvarlig |
| 4 | Magistratens sikkerhedsansvarlige | Foretager en vurdering af, hvad bruddet har af betydning og risiko for den eller de registrerede.  Ved vurdering kan følgende personer inddrages:   * Den datatansvarlige * Systemejeren * Relevante medarbejdere * DPO   (Hvis anmeldelsen ikke kræver indberetning til Datatilsynet, skal procedure for intern anmeldelse følges – se nedenfor)  (Hvis anmeldelsen ikke er et reelt brud, stopper proceduren her) |
| 5 | Systemejer/afdelingsleder | Afhængig af hvilken type af brud, der er sket, skal den ansvarlige sørge for at der rettes op på skaden.  (Fx skal eventuelle offentliggjorte personoplysninger fjernes fra internettet.) |
| 6 | Systemejer/afdelingsleder | Foretager kontinuerlig dokumentation af bruddet og orienterer relevante personer, når der er nyt |
| 7 | Systemejer/afdelingsleder | Laver en analyse af bruddets omfang.   * Hvilke type data er der tale om? * Hvor stort er omfanget? (laver fx liste over berørte registrerede) * Er skaden udbedret?   Systemejer udfylder blanketten på til Datatilsynet på forhånd. Se blanketten som skal udfyldes |
| 8 | Magistratens sikkerhedsansvarlige | Laver indberetning til Datatilsynet hurtigst muligt -senest 72 timer efter at man er blevet bekendt med bruddet (inkl. weekender). Anmeldelsen til Datatilsynet skal som minimum indeholde:   1. Beskrivelse af karakteren af bruddet samt hvor det er muligt:    1. Kategorier af registrerede    2. Antal af berørte registrerede    3. Kategorier af personoplysninger    4. Antal af berørte registreringer af personoplysninger 2. Navn og kontaktoplysninger på databeskyttelsesrådgiver 3. Beskrivelse af mulige konsekvenser af sikkerhedsbruddet 4. Beskrivelse af de tekniske og organisatoriske foranstaltninger, som er truffet eller foreslår truffet for at håndtere bruddet.   Indberetningen laves på [virk.dk](https://indberet.virk.dk/myndigheder/stat/ERST/Indberetning_af_brud_paa_sikkerhed) eller på [datatilsynet.dk](http://www.datatilsynet.dk)  (Indberetningen vil automatisk blive sendt til Datatilsynet. Datatilsynet vil kontakte kommunen, hvis de finder det relevant)  Husk at downloade en kopi af blanketten, når den er sendt. Det er denne kopi, som vil være dokumentation på at indberetningen er blevet foretaget.  Blanketten skal journaliseres i e-Doc.  En kopi af indberetningen skal sendes til kommunens databeskyttelsesrådgiver via e-mail: [databeskyttelsesraadgiver@aarhus.dk](mailto:databeskyttelsesraadgiver@aarhus.dk)  (Bemærk at DPO eller andre sikkerhedsansvarlige kan være behjælpelig med indberetningen i tilfælde af ferie eller sygdom.) |
| 8 | Magistratens sikkerhedsansvarlige | Sikrer at den interne dokumentation på bruddet laves i regnearket på eDoc-sag 18/063865.  Anmeldelsen skal indeholde:   * Dato og tidspunkt for bruddet * Hvad der skete i forbindelse med bruddet * Hvad årsagen til bruddet var * Hvilke typer personoplysninger, som var omfattet * Hvilke konsekvenser bruddet har for de berørte personer * Hvilke afhjælpende og forebyggende foranstaltninger der er truffet * Hvorvidt der er sket anmeldelse til Datatilsynet |
| 9 | Afdelingsleder/systemejer | Underretter de registrerede hvis bruddets risikovurdering indebærer en høj risiko for den registreredes rettigheder.  [Se skabelon og vejledning til brug for underretning af den registrerede](http://it-sikkerhedshaandbog.adm.aarhuskommune.dk/main/policy/book/view?bookguid=SA172EB7D9AF9Y347U0) |

## 

# Procesbeskrivelse for brud på persondatasikkerheden som kun kræver intern anmeldelse

Hvis oplysningerne om de registrerede, som er blevet lækket, offentliggjort eller ændret, er forholdsvis harmløse og fx kun omhandler en enkelt person vil en underretning til Datatilsynet ikke være nødvendig, men kræves alligevel dokumenteret ved en intern anmeldelse.

Nedenstående procesbeskrivelsen er vejledende og uddybende forklaring på de enkelte del-aktiviteter i arbejdsgangen.

|  |  |  |
| --- | --- | --- |
| **Trin** | **Rolle** | **Ansvar** |
| 1 | Anmelder (fx borger, leverandør, medarbejder) | Gør opmærksom på at der er sket et brud på persondatasikkerheden |
| 2 | Modtager af anmeldelsen (fx medarbejder, leder) | Ved modtagelse om brud på persondatasikkerheden skal afdelingsleder/systemejer kontaktes. |
| 3 | Afdelingsleder/systemejer/sikkerhedsansvarlig | Kontakter MKB-sikkerhedsansvarlig |
| 4 | Magistratens sikkerhedsansvarlige | Foretager en vurdering af, hvad bruddet har af betydning og risiko for den eller de registrerede.  Ved vurdering kan følgende personer inddrages:   * Den datatansvarlige * Systemejeren * Relevante medarbejdere |
| 5 | Systemejer/afdelingsleder | Afhængig af hvilken type af brud, der er sket, skal den ansvarlige sørge for at der rettes op på skaden. Fx skal eventuelle offentliggjorte personoplysninger fjernes fra internettet. |
| 6 | Magistratens sikkerhedsansvarlige | Sikrer at den interne dokumentation på bruddet laves i regnearket på eDoc-sag 18/063865 samt sender dokumentationen til kommunens databeskyttelsesrådgiver via e-mail: [databeskyttelsesraadgiver@aarhus.dk](mailto:databeskyttelsesraadgiver@aarhus.dk)  Anmeldelsen skal indeholde:   * Navn og kontaktoplysninger på databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes * Beskrivelse af de sandsynlige konsekvenser af bruddet * Beskrivelse af de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet |
| 7 | Afdelingsleder | Den ansvarlige ledelse skal gennemgå interne procedurer for håndtering af fortrolige data og personoplysninger. Der er fx ekstra sikkerhedsforanstaltninger og -procedurer som skal indføres  Lederen skal sikre, at medarbejderne har fået eller får den nødvendige instruktion i at håndtere følsomme og fortrolige data og evt. indskærpe reglerne. |