|  **Vejledning til anvendelse af Wired Relations’ rammeværktøj** |
| --- |

Wired Relations’ rammeværktøj\* kan anvendes direkte i jeres arbejde med databeskyttelse – men kan selvfølgelig også anvendes som inspiration til jeres eget materiale. I kan ændre efter behov, så det bliver præcis, som I ønsker det.

**OBS!** Der kan være afsnit, som ikke er relevante for alle organisationer. Hvis dette er tilfældet, vil det tydeligt fremgå af teksten.

Der vil være steder i teksten, hvor der er lagt op til, at I indsætter organisationens navn eller andet. Dette vil i så fald være markeret jf. følgende: [*indsæt organisationens navn*].

| Tekstboksene i dokumentet indeholder opmærksomhedspunkter og gode råd til dig som dataansvarlig eller databehandler. Vær opmærksom på, at tekstboksene bør fjernes fra den endelige udgave af den konkrete politik eller procedure.  |
| --- |

I bunden af hvert dokument vil der fremgå en tabel, som giver et overblik over dokumentets version, seneste opdatering, samt hvem der har ansvaret for dokumentet.

**Procedure for håndtering af brud på persondatasikkerheden**

Denne procedure er udarbejdet som en tjekliste over de forskellige steps, der skal håndteres i forbindelse med et brud på persondatasikkerheden.

Når et brud på persondatasikkerheden er konstateret, skal du:

**1. Danne dig et overblik**

Sørg for at få identificeret og beskrevet det, som er muligt på nuværende tidspunkt. På den måde er du bedre hjulpet til de næste trin i processen.

**2. Standse ulykken**

Hvis der er tale om et igangværende brud på persondatasikkerheden, er det meget vigtigt at få standset dette, således at eventuelle konsekvenser for den registrerede minimeres. Samtidig er det vigtigt, at de faktiske omstændigheder dokumenteres løbende, da vigtig information, som er afgørende i forhold til vurderingen af risikoen for den registrerede og en eventuel anmeldelse til Datatilsynet, ellers kan gå tabt.

**2. Vurdere om bruddet på persondatasikkerheden skal anmeldes til Datatilsynet**

Som udgangspunkt skal alle brud på persondatasikkerheden anmeldes til Datatilsynet indenfor 72 timer. Det er således kun, hvis det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder, at der ikke skal ske anmeldelse.

Vurderingen af om der er en risiko for den registreredes rettigheder eller frihedsrettigheder skal tage udgangspunkt i:

* typen af sikkerhedsbrud, herunder om der er sket tab af oplysninger, brud på fortroligheden eller en integritetskrænkelse
* oplysningernes art og omfang
* om risikoen for at den/de registrerede kan identificeres
* konsekvenser bruddet kan have for de registrerede
* hvorvidt bruddet omfatter særlige registrerede (fx hvis der er tale om børn eller særligt udsatte)
* Antallet af berørte fysiske personer

Det er altafgørende, at vurderingen er saglig og objektiv – og derudover skal alle afvejninger og beslutninger i forløbet dokumenteres, se pkt. 5 nedenfor.

| Såfremt I allerede har foretaget risikovurderinger (i forhold til den registrerede) i jeres organisation, vil det være nærliggende at se på disse i denne sammenhæng, da de jo typisk vil give udtryk for risikoen for den registrerede i forhold til et system, proces eller behandlingsaktivitet.  |
| --- |

**4. Vurdere om den registrerede skal underrettes**

Hvis et brud på persondatasikkerheden skal anmeldes til Datatilsynet, skal det også vurderes, om den registrerede skal underrettes om databruddet.

Underretning af den registrerede skal ske, hvis databruddet sansynligvis vil medføre en høj risiko for den registreredes rettigheder eller frihedsrettigheder. Herved har den registrerede mulighed for at tage en række forholdsregler for at imødegå eventuelle risici.

4.1. Høj risiko

Der findes ingen fast definition på, hvad der karakteriseres som en høj risiko for den registrerede, men jo mere alvorlige konsekvenser databruddet vurderes at have, og jo større sandsynligheden er for at konsekvensen indtræder, des højere må risikoen for de berørte vurderes at være.

Alle mulige konsekvenser og negative virkninger, for den registrerede, skal tages i betragtning, når det vurderes, om der er en høj risiko for den registrerede.

4.2. Hvem, hvornår og hvordan skal underretningen ske

Det er den dataansvarlige, der underretter den registrerede.

Den registrerede skal underrettes uden unødigt ophold efter at bruddet på persondatasikkerheden er konstateret.

Underretningen skal ske direkte til den registrerede, fx via brev, e-mail eller sms. En pressemeddelelse er fx ikke tilstrækkelig.

| Hvis I allerede har en skabelon for underretning af den registrerede, kan der linkes til den her. Alternativt kan der linkes til Datatilsynets skabelon. |
| --- |

4.3. Undtagelser til kravet om underretning

Der er ikke krav om underretning, hvis:

* den dataansvarlige har gennemført passende tekniske og organisatoriske sikkerhedsmæssige foranstaltninger, som er blevet anvendt på de pågældende personoplysninger, der er berørt af databruddet, fx hvis oplysninger er beskyttet af kryptering.
* den høje risiko for den registrerede ikke længere er reel, fx i det tilfælde, hvor der har været mulighed for utilsigtet adgang til personoplysninger, men hvor det med sikkerhed er dokumenteret, at ingen uvedkommende har tilgået oplysningerne.
* underretningen kræver en uforholdsmæssig indsats. Det kan være i det tilfælde, hvor man i forbindelse med et databrud har mistet oplysningerne om de registrerede, som ret beset skulle underrettes. I dette tilfælde må der skulle ske en offentlig orientering, eller en tilsvarende foranstaltning.

**5. Huske den interne dokumentation**

Uanset om det er vurderet, at et brud på persondatasikkerheden skal anmeldes til Datatilsynet eller ej, skal det dokumenteres, herunder de faktiske omstændigheder, væsentlige vurderinger i forhold til håndtering af databruddet, samt foretagne foranstaltninger.

| **Orientering til [Indsæt relevante parter]**I nogle organisationer kan det være relevant, at der foretages en orientering/rapportering, når der er konstateret eller anmeldt et brud på persondatasikkerheden. Det kan eksempelvis være til nærmeste leder, direktionen, koncernledelsen, ministerium.  |
| --- |

**6. Evaluere**

Ethvert brud på persondatasikkerheden bør følges op af en evaluering, hvor følgende spørgsmål kan være aktuelle:

* Er det første gang denne type af brud på persondatasikkerheden er sket eller er der tale om en gentagelse?
* Hvis det er første gang denne type af brud på persondatasikkerheden konstateres, kan der med fordel følges op med ekstra awareness i den enkelte proces/afdeling eller sammen med den enkelte medarbejder.
* Hvis der er tale om en gentagelse, bør der kigges nærmere på processen for at vurdere, om der skal være yderligere awareness-tiltag, eller om der skal foretages mitigerende tiltag i processen.

Evalueringen bør også dokumenteres.

###

###

###

###

###

###

###

###

### **Dokumentinformation**

| Dokumentversion |  |
| --- | --- |
| Dato for udgivelse af denne version |  |
| Ansvarlig |  |
| Status |  |