**Vejledning til anvendelse   
af Wired Relations’ skabeloner**A black background with black lines

Description automatically generated

Wired Relations’ skabeloner\* kan anvendes direkte i jeres arbejde med databeskyttelse og informationssikkerhed – 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 virksomheder. 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 virksomhedens navn eller andet. Dette vil i så fald være markeret jf. følgende: [*indsæt virksomhedens navn*].

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

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

|  | Her er nogle ekstra tips til brug af Wired Relations' skabeloner: |  |
| --- | --- | --- |
|  | * I kan tilføje eller fjerne sektioner, ændre ordlyd og tilføje virksomhedens eget logo og branding. |  |
|  | * Hold skabelonerne opdaterede. Krav til databeskyttelse og informationssikkerhed ændrer sig konstant, så det er vigtigt at sikre, at skabelonerne altid er opdaterede. |  |

**Procedure for håndtering af anmodning om indsigt**

Denne procedure er udformet som en tjekliste over de forskellige trin, som skal huskes hver gang en indsigtsanmodning skal besvares.

**1. Modtagelse af en indsigtsanmodning**

Når du modtager en indsigtsanmodning, kontakter du [*indsæt relevant person i virksomheden*], som er ansvarlig for at vurdere og besvare indsigtsanmodninger i *[Indsæt virksomhedens navn]*

En indsigtsanmodning skal besvares snarest muligt, og senest en måned efter at anmodningen er fremsat.

**2. Afgrænsning**

Indledningsvist skal det vurderes, om anmodningen kan besvares i den nuværende form, eller om det er relevant at undersøge, om anmodningen kan afgrænses, fx hvis personen ønsker indsigt i et bestemt område eller en bestemt sag.

Vær opmærksom på, at man ikke kan afvise at besvare en indsigtsanmodning i det tilfælde, at den registrerede ikke ønsker at præcisere anmodningen.

**3. Sikring af den registreredes identitet**

Når en person henvender sig og anmoder om indsigt i, hvilke personoplysninger der behandles om vedkommende, skal det indledningsvist fastslås, at den, der fremsætter anmodningen, også er den, som vedkommende udgiver sig for at være. På den måde sikres det, at der ikke sker utilsigtet videregivelse af personoplysninger til uvedkommende.

Hvis den registrerede lader sig repræsentere af andre, kan det være relevant at anmode om fuldmagt.

Når identiteten på den registrerede er fastlagt, og der er foretaget en evt. afgrænsning af anmodningen, sendes der en kvittering til den registrerede for modtagelsen af anmodningen.

**4. Identificér og indsaml de personoplysninger, der behandles om vedkommende**

[*indsæt relevant person i virksomheden*] er ansvarlig for at identificere og indhente de personoplysninger, der behandles om vedkommende.

**5. Gennemgå materialet**

Når det relevante materiale er identificeret og sendt til [*indsæt relevant person i virksomheden]*, skal materialet gennemgås.

Hvis der i dokumenter e. lign. fremgår personoplysninger om andre end den pågældende, skal disse sløres eller på anden måde fjernes fra dokumenterne.

**6. Udarbejd besvarelse til den registrerede**

Når materialet er gennemgået, skal der udarbejdes en besvarelse til den registrerede.

Udover at den registrerede skal have udleveret en kopi af de personoplysninger, der behandles om vedkommende, skal besvarelsen også indeholde oplysninger om:

* formålet med behandlingen af personoplysningerne
* oplysninger om de berørte kategorier af personoplysninger
* oplysninger om de modtagere eller kategorier af modtagere, som personoplysningerne er eller vil blive videregivet til, navnlig hvis modtagerne findes i tredjelande eller er internationale organisationer

Desuden skal følgende også oplyses:

* Hvis du overfører personoplysninger til usikre tredjelande eller internationale organisationer, og der er fastsat fornødne garantier for databeskyttelsen, skal du informere den registrerede om disse garantier.
* Om muligt skal du også oplyse om det tidsrum, du opbevarer personoplysningerne i, eller, hvis det ikke er muligt, de kriterier du anvender til at fastlægge dette tidsrum.
* Herudover skal du oplyse den registrerede om, at vedkommende har ret til at anmode om berigtigelse, sletning eller begrænsning af behandlingen, at den registrerede har ret til at gøre indsigelse mod behandlingen i særlige situationer, og at den registrerede har ret til at indgive klage over behandlingen til en tilsynsmyndighed (Datatilsynet eller Domstolsstyrelsen).
* Du skal også oplyse om, hvorfra personoplysninger stammer. Dette gælder dog kun, hvis de pågældende personoplysninger er indsamlet hos andre end den registrerede selv.
* I tilfælde af, at du benytter automatiske afgørelser, herunder profilering, skal du oplyse om, at den registrerede undergives en sådan behandling, samt logikken i de automatiske afgørelser. Dette indebærer bl.a. en beskrivelse af, hvilke overvejelser, der ligger til grund for behandlingen, samt hvordan ”systemet” kommer frem til afgørelserne.

I praksis udarbejdes der en besvarelse med ovenstående punkter, og kopi af personoplysningerne (dokumenter, rapporter, overvågningsbilleder mv.) vedlægges hertil.

**7. Send besvarelsen til den registrerede**

Hvis besvarelsen af en indsigtsanmodning indeholder følsomme personoplysninger, skal besvarelsen sendes sikkert, f.eks. via e-boks. Indeholder besvarelsen ingen følsomme personoplysninger kan denne sendes via mail.

| **Særligt vedrørende vores rolle som databehandler**  Såfremt vores kunder (den dataansvarlige) har behov for bidrag i forhold til at de skal besvare en indsigtsanmodning sker dette typisk via vores almindelige support. |
| --- |

**Bilag 1 – ansvarlige for indsamling af materiale**

| Her kan I med fordel opliste de systemer, hvori I behandler personoplysninger. Hvis I som dataansvarlige bliver mødt af en indsigtsanmodning, vil det typisk være fra jeres medarbejdere eller kunder/potentielle kunder.  **NB. Hvis I anvender Wired Relations som GRC platform, vil systemerne være kortlagt der, og I kan derfor i de fleste tilfælde undvære bilag 1.** |
| --- |

| **Systemer** | **Systemansvarlig/kontaktperson** |
| --- | --- |
| *HR-system* |  |
| *Økonomisystem* |  |
| *Kursusadministration* |  |
| *E-mail* |  |
| *Drev, etc.* |  |
|  |  |

### 

### 

### 

**Dokumentinformation**

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