**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. |  |

**Politik for behandling af personoplysninger**

**1. Formål**

| Formålet med denne politik er at give virksomhedens medarbejdere et overordnet indblik i databeskyttelse, herunder de rettigheder og pligter, der følger af databeskyttelsesforordningen. De mere operationelle forhold, såsom konkret håndtering af sikkerhedsbrud og indsigtsanmodninger, kan med fordel beskrives i særskilte procedurer. Wired Relations har også skabeloner hertil. |
| --- |

Denne politik beskriver de grundlæggende begreber, principper og retningslinjer som er vigtige for dig som medarbejder at kende og arbejde ud fra, når du behandler

personoplysninger.

**2. Indledning**

Den databeskyttelsesretlige lovgivning, herunder databeskyttelsesforordningen (GDPR), opstiller en række regler for, hvordan en virksomhed må behandle personoplysninger.

Virksomheden skal i den forbindelse fastsætte retningslinjer for, og instruere dig i, hvordan du som medarbejder er med til at sikre, at virksomheden overholder lovgivningen.

Som medarbejder i *[indsæt virksomhedens navn]* er du forpligtet til at handle i overensstemmelse med denne politik.

**3. Vigtige begreber**

Den databeskyttelsesretlige lovgivning gælder for en virksomheds *behandling* af *personoplysninger.* Det er derfor vigtigt, at du ved, hvad det vil sige at behandle personoplysninger.

En *personoplysning* er en oplysning, der kan bruges til at identificere en bestemt person, eller en oplysning om en person, der allerede er identificeret.

En *behandling* betegner *alt,* hvad du kan gøre med en personoplysning. Det er fx en behandling, når du indsamler, registrerer, opbevarer eller videregiver en personoplysning.

Både begrebet *personoplysning* og begrebet *behandling* skal forstås meget bredt.

**4. Kategorier af personoplysninger**

Der skelnes mellem almindelige og følsomme personoplysninger. Det er vigtigt, at du ved, om du behandler almindelige eller følsomme personoplysninger, fordi der gælder forskellige regler for de to kategorier af personoplysninger.

Derudover skal du vide, at CPR-nummer og oplysninger om strafbare forhold er særskilt regulerede, og at der derfor gælder særlige regler, når/hvis du behandler disse.

*Almindelige personoplysninger*

Almindelige personoplysninger er alle personoplysninger, der ikke kan kategoriseres som følsomme. Eksempler på almindelige personoplysninger er navn, adresse, lønoplysninger, skostørrelse og hårfarve.

*Følsomme oplysninger*

Følsomme oplysninger er udtømmende oplistet i databeskyttelsesforordningen, og er oplysninger om:

* Race eller etnisk oprindelse
* Politisk, religiøs eller filosofisk overbevisning
* Fagforeningsmæssigt tilhørsforhold
* Genetiske data
* Biometriske data mhp. entydig identifikation
* Helbredsoplysninger
* Seksuelle forhold eller seksuel orientering.

| Det afgørende for, om en oplysning skal anses for fortrolig, vil være en vurdering af, om oplysningen efter den almindelige opfattelse i samfundet bør kunne forlanges unddraget offentlighedens kendskab, jf. straffelovens § 152 sammenholdt med forvaltningslovens § 27.  Følsomme personoplysninger vil utvivlsomt være fortrolige oplysninger. Omvendt er en fortrolig oplysning ikke altid følsom.  Ikke-følsomme personoplysninger kan i visse situationer være fortrolige. Datatilsynet nævner eksempler såsom indtægts- og formueforhold, arbejds-, uddannelses- og ansættelsesmæssige forhold og interne familieforhold. Derudover vil et personnummer (CPR nummer) også anses for at være en fortrolig personoplysning. |
| --- |

Er du i tvivl om, hvorvidt du må behandle konkrete personoplysninger, skal du kontakte *[indsæt relevant kontaktpunkt, f.eks. DPO].*

**5. Vigtige principper**

Den databeskyttelsesretlige lovgivning opstiller en række principper, som du skal følge hver gang, du behandler en personoplysning.

Dette afsnit fremhæver de principper, som det er særligt vigtigt, at du kender og bruger aktivt, når du behandler personoplysninger.

Principperne skal sikre, at en behandling af personoplysninger altid er begrænset til, hvad der er nødvendigt for at sikre, at en behandling sker på en sikker måde til et sagligt og legitimt formål.

5.1. Lovlighed

Personoplysninger skal behandles lovligt. Det betyder, at du skal have en hjemmel til at foretage en behandling. Hvis du er i tvivl om, om du har hjemmel til at foretage en behandling af en personoplysning, er du forpligtet til at få dette afklaret med *[indsæt relevant kontaktpunkt, f.eks. DPO]*.

5.2 Gennemsigtighed

Personoplysninger skal behandles gennemsigtigt. Det betyder, at den registrerede skal vide, *hvilke* personoplysninger, der behandles om den pågældende. Dette vil den registrerede som udgangspunkt være informeret om i virksomhedens privatlivspolitik.

Den registrerede har også ret til at få at vide, *hvordan* du behandler den pågældendes personoplysninger. Det er derfor vigtigt, at du altid behandler personoplysninger på en måde, som kan tåle at komme til den registreredes kendskab.

Hvis du foretager en behandling, hvor du er i tvivl om, hvorvidt den registrerede er blevet oplyst om behandlingen, er du forpligtet til at afklare dette med *[indsæt relevant kontaktpunkt, f.eks. DPO]*.

Det er også vigtigt, at du involverer *[indsæt relevant kontaktpunkt, f.eks. DPO]*, hvis du påtænker at begynde en ny type behandling af personoplysninger. Det skyldes, at virksomheden er forpligtet til at oplyse den registrerede om behandlingen og til at føre en fortegnelse over de behandlinger, der foretages i virksomheden.

5.3. Formål

Personoplysningerne må kun indsamles til udtrykkeligt angivne og legitime formål. Det betyder, at du altid skal kunne redegøre for, til hvilket formål du har indsamlet en oplysning. Du skal også kunne redegøre for, til hvilket formål du foretager en viderebehandling af en oplysning, som du allerede har.

Hvis du er i tvivl om den behandling, du ønsker at foretage, sker til et legitimt formål, er du forpligtet til at afklare dette med *[indsæt relevant kontaktpunkt, f.eks. DPO]*.

5.4. Dataminimering

Behandlingen af personoplysninger skal være tilstrækkelig, relevant og begrænset til, hvad der er nødvendigt. Det betyder, at du ikke må behandle personoplysninger, som går ud over, hvad der er nødvendigt for at opfylde behandlingens formål.

Du kan skelne mellem personoplysninger, der er ‘nice to have’ og personoplysninger, der er ‘need to have’. Du må kun behandle oplysninger, der er ‘need to have’.

Du må også kun opbevare personoplysningerne, så længe det er nødvendigt. Det betyder, at du skal slette personoplysninger, når du ikke længere har et formål med at opbevare dem.

Du skal altid kunne redegøre for, hvorfor du er i besiddelse af en personoplysning.

5.5. Integritet og fortrolighed

Du skal behandle personoplysninger på en sikker måde. Det betyder, at du skal passe på de personoplysninger, som du behandler. Det gør du først og fremmest ved at overholde denne politik samt ved at følge virksomhedens øvrige retningslinjer, politikker og procedurer.

Såfremt du mener, at der bør træffes yderligere foranstaltninger, for at en behandling er sikker, er du forpligtet til at træffe disse.

Hvis du opdager, at nogle af de personoplysninger, du behandler, er ukorrekte, er du

også forpligtet til at berigtige eller slette dem.

**6. Opbevaring af fysisk materiale med personoplysninger**

Der gælder principielt de samme regler for sikker opbevaring af personoplysninger, hvad enten det er fysisk eller digitalt materiale, der indeholder personoplysninger. Derfor er det også kun betroede personer med et sagligt behov, der skal have adgang til fysiske dokumenter med personoplysningerne.

| Hvis I i jeres virksomhed har fastsat retningslinjer for opbevaring af fysisk materiale, der indeholder personoplysninger, kan det med fordel beskrives nedenfor.  Eksempler:   * Det fysiske materiale med personoplysninger skal opbevares aflåst, når det ikke bruges * Det fysiske materiale med personoplysninger må kun være tilgængeligt for betroede medarbejdere, der har et sagligt behov for at kunne tilgå materialet * Det fysiske materiale skal destrueres på en forsvarlig måde, når formålet med opbevaringen ophører (beskriv evt. hvordan) |
| --- |

**7. Databeskyttelsesrådgiver**

| Såfremt jeres virksomhed er forpligtet til at udpege en databeskyttelsesrådgiver, eller hvis I frivilligt har udpeget en databeskyttelsesrådgiver, kan I under dette afsnit beskrive funktionen nærmere.  Eksempel:  Databeskyttelsesrådgiveren i [*Indsæt: virksomhedens navn*] er [*indsæt: navn på databeskyttelsesrådgiver*]. Databeskyttelsesrådgiverens primære opgave er at rådgive virksomheden i alle databeskyttelsesretlige spørgsmål, og det er derfor vigtigt, at databeskyttelsesrådgiveren bliver inddraget rettidigt.  Du bør fx altid rådføre sig med databeskyttelsesrådgiveren, hvis der skal indkøbes et nyt IT-system, indgås aftale med ny leverandør, hvis du påtænker at iværksætte en ny proces, som vedrører behandling af personoplysninger, eller hvis der er sket et brud på persondatasikkerheden. |
| --- |

**8. Opfølgning**

Denne politik evalueres én gang om året af virksomhedens interne compliance-team.

### 

### 

### **Dokumentinformation**

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