|  **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 vil være afsnit, som ikke er relevante for alle organisationer. Hvis dette er tilfældet, vil det tydeligt fremgå af teksten. Fx vil afsnittet Databeskyttelsesrådgiver primært være relevant for de organisationer, der har udpeget en databeskyttelsesrådgiver.

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.

**Overordnet politik for databeskyttelse i *[indsæt organisationens navn]***

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

Enhver har ret til beskyttelse af sine personoplysninger, og enhver, der behandler personoplysninger om andre (undtagen i privat sammenhæng), er forpligtet til at iagttage disse rettigheder og til at beskytte personoplysningerne.

**Hvorfor er det vigtigt, at man ved noget om databeskyttelse?**

Det er altafgørende at alle medarbejdere, der behandler personoplysninger som led i deres arbejde, er klædt på til at behandle oplysningerne på den rigtige måde. Manglende viden på dette område medfører en øget risiko for brud på persondatasikkerheden, og dermed også en større risiko for den registrerede.

**Hvad er personoplysninger?**

En personoplysning er enhver form for information, der kan henføres til en bestemt person, også selv om personen kun kan identificeres, hvis oplysningen kombineres med andre oplysninger.

Databeskyttelsesforordningen opdeler personoplysninger i tre typer:

* Almindelige personoplysninger
* Følsomme personoplysninger
* Oplysninger om strafbare forhold (straffedomme og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger)

**Hvornår behandler man personoplysninger?**

Begrebet “behandling” af personoplysninger skal forstås meget bredt, og i praksis betyder det, at enhver håndtering af personoplysninger om andre er en *behandling.* Det kan fx være indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, samt genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse.

**Hvornår må man behandle personoplysninger?**

Når man behandler personoplysninger, er det et krav, at der er et retligt grundlag hertil, og dette afhænger af, hvilke typer af personoplysninger, der er tale om.

| Hvis man ønsker at få lidt mere tekst til dette afsnit, kan man vælge at sætte helt overordnede eksempler ind:* **Almindelige personoplysninger** – det retlige grundlag skal findes i databeskyttelsesforordningens artikel 6.
* **Følsomme personoplysninger** – det retlige grundlag skal findes i databeskyttelsesforordningens artikel 9.
* **Strafbare forhold** – det retlige grundlag skal findes i databeskyttelsesforordningens artikel 10.
* **CPR-nr.** – databeskyttelseslovens § 11.

Man kan også vælge at give konkrete eksempler fra jeres egen hverdag, fx i forhold til personaleadministration eller kundeservice.  |
| --- |

**Grundlæggende principper**

I databeskyttelsesforordningens artikel 5 er der en række principper, som er vigtige at kende til, når man behandler personoplysninger. Udover at der skal være et gyldigt behandlingsgrundlag, skal disse grundlæggende principper altid være opfyldt. Som ansat i [*Indsæt organisationens navn*],er det vigtigt, at man kender disse principper, og at man i hovedtræk ved, hvad de dækker over.

* Formålsbegrænsning
* Dataminimering
* Lovlighed, rimelighed og gennemsigtighed
* Rigtighed
* Integritet og fortrolighed
* Opbevaringsbegrænsning

Udover de grundlæggende principper er det altafgørende, at en organisation viser ansvarlighed og kan dokumentere, at organisationen efterlever databeskyttelsesforordningens regler, herunder de grundlæggende principper.

| Hvis det ønskes, at principperne beskrives mere udførligt, kan der tages udgangspunkt i nedenstående.Princippet om formålsbegrænsningNår en organisation indsamler personoplysninger om kunder eller ansatte, må de kun indsamle personoplysninger til klart definerede og specifikke formål. Formålet skal begrænses.Der må gerne indsamles og behandles personoplysninger til flere formål, hvis man har hjemmel til dette, fx ved at indhente et samtykke. Første gang en organisation indsamler personoplysninger til et specifikt formål, skal den registrerede (den man indsamler personoplysninger om) informeres om dette. Når personoplysninger indsamles til et specifikt formål, indebærer dette også, at man ikke må viderebehandle personoplysningerne til andre formål. Man må fx ikke videresælge personoplysninger, hvis man ikke har oplyst kunden om dette specifikke formål på indsamlingstidspunktet.Man må gerne viderebehandle de indsamlede personoplysninger til legitime eller saglige formål (så længe det er foreneligt med det oprindelige formål). Det følger eksempelvis af en handel med en kunde, at købet og transaktionen skal dokumenteres og bogføres. I dette tilfælde skal man naturligvis ikke bede en registreret om lov til at bogføre fakturaen eller opbevare en kopi af kontrakten.Princippet om dataminimeringMan skal kun indsamle de personoplysninger, der er nødvendige for at løse den pågældende opgave (formålet med behandlingen af personoplysningerne).Eksempelvis skal man naturligvis have kundens adresse, hvis man skal levere en pakke – men her vil det fx ikke være nødvendigt at indhente oplysning om civilstatus.Man skal altså kun indsamle relevante personoplysninger til det relevante formål.Princippet om lovlighed, rimelighed og gennemsigtighedEnhver behandling af personoplysninger skal være lovlig. En organisation skal have hjemmel i lovgivningen til at behandle personoplysninger, fx ved at indhente et samtykke hos kunden. Enhver behandling af personoplysninger skal være rimelig. Det er rimeligt at behandle personoplysninger sikkert og med udgangspunkt i best practice (fx tilgængelige teknologiske løsninger, management standarder, branchekodeks mv.). En organisation skal behandle personoplysninger på en gennemsigtig måde, og være i stand til at informere de registrerede herom. Der skal bruges et lettilgængeligt og letforståeligt sprog. Informationen skal være klar og tydelig for målgruppen. Undgå at bruge et juridisk sprog.Princippet om rigtighedEn organisation skal sikre, at de personoplysninger som behandles er rigtige. Dette indebærer, at personoplysningerne løbende skal ajourføres. Det kan også indebære, at man har nogle kontrolforanstaltninger i organisationen til at sikre, at personoplysningerne til enhver tid er korrekte. Princippet om integritet og fortrolighed*Integritet*En organisation skal sikre personoplysningernes integritet. Dette indebærer, at man skal sikre personoplysningernes troværdighed og korrekthed over tid.*Fortrolighed*En organisation skal sikre, at personoplysninger behandles med en passende fortrolighed. Uvedkommende skal ikke have adgang til personoplysninger. Uvedkommende kan være hackere og tyveknægte, men det kan også bare være almindelige medarbejdere i organisationen, som ikke har nogen arbejdsbetinget grund til at have adgang til specifikke personoplysninger.*Tilstrækkelig sikkerhed*For at sikre personoplysningers integritet og fortrolighed, kræver det, at organisationen har implementeret en tilstrækkelig og passende sikkerhed. “Tilstrækkelig sikkerhed” afhænger af organisationens situation og vurderes ud fra en risikobaseret tilgang.Et tilstrækkeligt sikkerhedsniveau kan variere internt i en organisation mellem de forskellige behandlinger af personoplysninger (formål). Man kan vurdere om man har en tilstrækkelig sikkerhed ved at foretage en risikovurdering af de enkelte behandlinger af personoplysninger. Og ud fra en risikovurdering kan man vurdere, om der er behov for yderligere tekniske eller organisatoriske foranstaltninger, som fx beskytter mod uautoriseret adgang til eller brug af personoplysninger, herunder hændeligt tab, tilintetgørelse eller beskadigelse af personoplysninger.Princippet om opbevaringsbegrænsningEn organisation bør kun opbevare personoplysninger, så længe det er nødvendigt for at løse en opgave (så længe der er et sagligt formål hermed). Når det ikke længere er nødvendigt at opbevare personoplysninger, bør oplysningerne slettes. Nogle systemer kan ikke håndtere, at man sletter personoplysninger. I disse tilfælde kan man i stedet anonymisere personoplysningerne, så man herefter ikke kan identificere en fysisk person ud fra oplysningerne. I dette tilfælde vil der ikke længere være tale om personoplysningerne – men blot oplysninger.Man bør aldrig opbevare eller behandle personoplysninger, fordi det er den nemmeste løsning eller fordi det er “nice-to-have” til evt. senere brug. I disse situationer bør personoplysningerne slettes.Se mere under “slettepolitik” og “sletteprocedure”.  |
| --- |

**Overordnede krav til sikkerhed i forbindelse med behandling af personoplysninger**

Databeskyttelsesforordningen stiller ingen specifikke krav til sikkerheden i forhold til at passe på personoplysninger. Det fremgår derimod at den dataansvarlige (eller databehandleren) skal gennemføre passende sikkerhedsforanstaltninger ud fra en konkret risikovurdering.

En sikkerhedsforanstaltning er fx, at der udarbejdes skriftlige politikker og retningslinjer for, hvordan man behandler personoplysninger.

Udover denne overordnede politik for databeskyttelse har vi i *[indsæt organisationens navn]* udarbejdet forskellige retningslinjer, som alle har det formål at sikre bedre databeskyttelse og mindske risikoen for brud på persondatasikkerheden. Disse findes [*Indsæt link til det sted, hvor I opbevarer de udarbejdede retningslinjer]*

| Man skelner mellem tekniske og organisatoriske sikkerhedsforanstaltninger. Tekniske sikkerhedsforanstaltninger kan fx være antivirusprogrammer, kryptering, logning, pseudonymisering mv., og organisatoriske sikkerhedsforanstaltninger vedrører træning og awareness af organisationens medarbejdere samt fastlæggelse af retningslinjer og politikker for behandling af personoplysninger.  |
| --- |

**Sådan behandles personoplysninger pr. e-mail**

Det meste af vores kommunikation sker pr. e-mail, og mange af de personoplysninger, vi behandler, kommer ind via e-mail. Mailsystemet er ikke et journaliseringssystem, og for at sikre, at der ikke behandles og opbevares personoplysninger, som for længst skulle have været slettet eller journaliseret, er det vigtigt, at mailsystemet (indbakke, undermapper, sendt post og slettet post) gennemgås.

| Det er meget forskelligt hvilken tilgang, der passer til den enkelte organisation. Nedenfor har vi givet et eksempel på, hvordan retningslinjer for behandling og forsendelse af af e-mails kan se ud. **EKSEMPEL***Almindelige personoplysninger*Almindelige personoplysninger kan sendes og modtages pr. e-mail. E-mails, der indeholder almindelige personoplysninger, kan opbevares i mailsystemet så længe, der er et sagligt formål hermed og så længe, det er nødvendigt for opgaveløsningen. Herefter skal oplysningerne slettes eller journaliseres, hvis der er en forpligtelse til at opbevare oplysningerne i længere tid, fx regnskabsbilag. *Følsomme og fortrolige personoplysninger*E-mails med følsomme og/eller fortrolige personoplysninger skal altid sendes via en sikker kommunikationsform, *[indsæt de sikre kommunikationsformer jeres organisation anvender].* I de tilfælde hvor du skal modtage en mail med følsomme og/eller fortrolige personoplysninger, bør du henvise afsenderen til at sende oplysningerne på en sikker måde. Følsomme og fortrolige personoplysninger skal slettes fra mailsystemet senest 30 dage efter modtagelse/afsendelse. Hvis der er en forpligtelse til at opbevare oplysningerne i længere tid, skal oplysningerne journaliseres (dette kan være tilfældet i forbindelse med dokumentation af sygdomsforløb, som kræver refusion - i dette tilfælde skal oplysningerne journaliseres i den pågældende medarbejders personalemappe). Husk at gennemgå både indbakke, sendt post og slettet post. E-mails med følsomme og/eller fortrolige personoplysninger bør håndteres med det samme.  |
| --- |

**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 organisation 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)
 |
| --- |

**Databeskyttelsesrådgiver**

| Såfremt jeres organisation 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: organisationens navn*] er [*indsæt: navn på databeskyttelsesrådgiver*]. Databeskyttelsesrådgiverens primære opgave er at rådgive organisationen i alle databeskyttelsesretlige spørgsmål, og det er derfor vigtigt, at databeskyttelsesrådgiveren bliver inddraget rettidigt. Man bør fx altid rådføre sig med databeskyttelsesrådgiveren, hvis der skal indkøbes et nyt IT-system, indgås aftale med ny leverandør, hvis man påtænker at iværksætte ny proces, som vedrører behandling af personoplysninger, eller hvis der er sket et brud på persondatasikkerheden. |
| --- |

###

###

###

###

###

###

###

###

###

###

###

###

###

###

###

### **Dokumentinformation**

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