GDPR krav og regler. Der er mange komplekse regler i GDPR. I denne artikel kan du få en gennemgang af nogle af kravene, som du skal overholde.

Hvad skal man sørge for at have styr på som virksomhed eller organisation i forhold til GDPR?

Det kan du læse om i denne artikel, hvor du får en guide til reglerne og kravene i GDPR.

Hvis du har brug for hjælp til at sørge for at overholde reglerne og blive 'compliant', er du velkommen til at [kontakte os](https://persondatakonsulenterne.dk/om-os/kontakt/).

GDPR krav

Efter GDPR fik virkning 25. maj 2018 er der en række krav, som virksomheder og organisationer skal overholde.

Kravene kan virke komplekse og forvirrende. Derfor har vi her hos Persondatakonsulenterne lavet denne artikel. Artiklen nævner nogle af de vigtigste regler i GDPR.

GDPR kaldes på dansk for "persondataforordningen". Eller "den nye persondataforordning". Faktisk er det rigtige navn for loven "databeskyttelsesforordningen". Det er en 'lov' fra EU, som bestemmer, hvordan virksomheder, organisationer, myndigheder og lignende skal behandle personoplysninger.

Kravene i GDPR er bl.a., at du skal:

* Påvise at du overholder reglerne i GDPR
* Behandle personoplysninger lovligt og kun så længe, at det er lovligt
* Indgå databehandleraftaler, når det er påkrævet
* Overholde reglerne for samtykke
* Overholde reglerne for nyhedsbreve og nyhedsbrevstilmelding
* Oplyse den registrerede tilstrækkeligt, så oplysningspligten overholdes
* Tage stilling til, om du har behov for en DPO eller ej

Lad os se lidt nærmere på reglerne og kravene.

Du skal kunne påvise, at du overholder reglerne i GDPR

Et af de nye krav i persondataretten er, at du skal kunne påvise, at du overholder reglerne i GDPR.

Det betyder, at du skal kunne vise over for Datatilsynet, at du overholder reglerne og kravene. Du skal kunne vise, at du har indgået de nødvendige databehandleraftaler, har styr på samtykkerne, oplysningspligten osv.

Derudover er det et krav for mange, at de skal lave en såkaldt fortegnelse - den kaldes også for en 'artikel 30-fortegnelse'.

Artikel 30-fortegnelsen skal kunne fremvises til Datatilsynet, hvis de skulle banke på døren. Her hos Persondatakonsulenterne kan vi hjælpe med at lave din artikel 30-fortegnelse og påvise, at du overholder reglerne i GDPR.

Hvor længe må man opbevare persondata?

Du må ikke behandle persondata længere end nødvendigt.

Der skal være et legitimt formål med at behandle personoplysningerne. Hvis der ikke længere er et legitimt formål, skal oplysningerne slettes.

Dog skal du ikke skynde dig og slette alt, hvad du har af personoplysninger. Sletning af nødvendige personoplysninger før tid kan også have konsekvenser.

Lad os tage et eksempel.

*Jonas' læge har hørt om GDPR og persondataforordningen. Derfor har Jonas' læge besluttet sig for, at alle journaler fremover skal slettes efter 1 måned. Jonas' læge har nemlig fået at vide, at det er 'følsomme personoplysninger'.
Det vil dog være i strid med GDPR, fordi Jonas' læge stadig har et legitimt formål - lægen skal kunne se tilbage i journaler ift. hvad Jonas tidligere har fejlet og lignende. Dermed bliver personoplysningerne slettet før, at det er nødvendigt.*

Et andet eksempel er bogføringsmateriale som for eksempel fakturaer. Disse skal først slettes efter 5 år, da det er et krav, at materialet gemmes i 5 år. Fakturaer og lignende må derfor ikke slettes efter for eksempel 2 år, men må heller ikke først slettes efter 10 år.

Det er derfor vigtigt, at have styr på, hvornår personoplysninger skal slettes, og hvornår de ikke skal.


*Du skal have styr på, hvor længe du må/skal opbevare persondata. Du skal både passe på ikke at slette personoplysninger for hurtigt samt passe på ikke at få slettet personoplysninger i tide. Du skal slette persondata, når der ikke længere er et legitimt formål med at behandle dem.*

GDPR krav om databehandleraftale

Du skal indgå de nødvendige databehandleraftaler, hvis du benytter dig af databehandlere.

Dette har været et vanskeligt område for mange. for hvornår er nogle en databehandler? Og hvornår behandler databehandleren personoplysninger på vegne af dig som dataansvarlig?

Kort fortalt skal du lave en databehandleraftale, hvis du er dataansvarlig og instruerer en databehandler i at behandle personoplysninger på vegne af dig.

Typiske databehandlere er bl.a.:

* Bogholdere og bogføringssystemer som for eksempel Dinero, e-conomics og lignende
* Lønsystemer som for eksempel Dataløn, Danløn, Bluegarden osv.
* Nyhedsbrevsudsendere som for eksempel Mailchimp, Active Campaign osv.

Du kan læse mere om databehandleraftaler og kravene i vores artikel om [databehandleraftale](https://persondatakonsulenterne.dk/blog-om-gdpr/databehandleraftale/).

Hvornår skal man have samtykke?

Det er et krav i GDPR, at du behandler personoplysninger lovligt. Du skal have en gyldig grund til at behandle personoplysningerne.

En gyldig grund kan være, at du har fået samtykke.

Samtykke betyder, at du har fået lov til at behandle personoplysningerne.

Der er dog en række krav til samtykket i GDPR. Kravene er bl.a.:

* Du skal kunne dokumentere, at du har fået samtykket korrekt for eksempel ved at få det på skrift, ved at have optaget det eller på anden måde
* Samtykket må ikke være passivt, men skal være en aktiv viljestilkendegivelse
* Samtykket skal være ***frivilligt***
* Samtykket skal være ***informeret***
* Samtykket skal være ***specifikt***
* Samtykket skal være ***utvetydigt***

Du kan læse mere om kravene til samtykkerne i vores artikel om [samtykke](https://persondatakonsulenterne.dk/blog-om-gdpr/samtykke/).

*I en række tilfælde skal du have samtykke. Samtykket skal overholde kravene i GDPR - for eksempel skal du kunne påvise, at du har fået samtykket.*

Nyhedsbreve, nyhedsbrevstilmelding og GDPR

Siden GDPR fik virkning d. 25. maj 2018 har der været særlig fokus på nyhedsbreve, nyhedsbrevstilmelding og reglerne for dette ifølge GDPR.

Disse regler skal dog ses i forlængelse af reglerne for markedsføring i markedsføringsloven. Markedsføringsloven har altid været gældende - også før GDPR fik virkning.

Derfor skal du først og fremmest overholde markedsføringsloven. Det betyder bl.a., at du ikke uanmodet må rette henvendelse via elektronisk post (e-mail og lignende) - du skal først have fået lov til det.

Du kan få lov til det ved at indhente et korrekt samtykke. Du kan læse vores artikel om [samtykke](https://persondatakonsulenterne.dk/blog-om-gdpr/samtykke/) for at læse mere om reglerne for samtykke.

Du skal for eksempel kunne påvise, at du har indhentet samtykket korrekt.

Der er desuden forskel på, hvornår du indhenter samtykket til for eksempel sign-up til et nyhedsbrev. Er det, når kunden skal til at betale for en vare, eller er det på din hjemmesides forside?

Du kan læse mere om dette i vores artikel om [GDPR og nyhedsbreve](https://persondatakonsulenterne.dk/blog-om-gdpr/gdpr-og-nyhedsbreve-saadan-er-reglerne-for-tilmeldingsformular/).

Privatlivspolitik, persondatapolitik osv. og oplysningspligten

Mange tror, at det er lovpligtigt med en privatlivspolitik eller en såkalt 'persondatapolitik'.

**Det er dog forkert!**

Men i en række tilfælde har du en oplysningspligt over for den registrerede (kunden, samarbejdspartneren eller hvem det nu er). Mange vælger at overholde oplysningspligten i sådan en privatlivspolitik eller persondatapolitik.

Problemet er dog, at disse politikker ofte bliver alt for generelle og dermed overholder de ikke kravene om oplysningspligten i GDPR.

I persondataforordningens artikel 13 og 14 står der, at du bl.a. skal oplyse den registrerede om:

* Formålet med behandlingen
* Den legitime interesse, hvis der er en (skal ikke oplyses, hvis du fx har fået samtykke eller har indgået en aftale)
* Modtagere eller kategorier af modtagere af personoplysningerne
* Det tidsrum, hvor personoplysningerne vil blive opbevaret
* Den registreredes rettigheder

Det er vigtigt at overholde oplysningspligten. Hvis du er i tvivl om, hvorvidt du overholder oplysningspligten, er du velkommen til at kontakte os for at høre nærmere om, hvordan vi kan hjælpe dig.

DPO eller ej?

Mange er i tvivl om, hvorvidt de skal have en DPO eller ej.

Men hvad er en DPO overhoved?

DPO er en forkortelse på titlen "*data protection officer*". På dansk kaldes denne titel også for *databeskyttelsesrådgiver.*En DPO kan være en jurist, en IT-kyndig eller lignende, der har et indgående kendskab til GDPR og persondataret.

For nogle er en DPO lovpligtig. Det gælder for eksempel for alle offentlige myndigheder. Visse virksomheder skal også have det, men kun hvis de skal overholde kravene. Men for de fleste private virksomheder og organisationer er det ikke et krav.

Private (altså, ikke-offentlige) skal have en DPO, hvis:

1. Der er tale om en offentlig myndighed eller et offentligt organ - eller:
2. Det er privat såsom et selskab, en forening eller lignende, hvor de 3 betingelser er tilstede (1: kerneaktivitet, 2: stort omfang og 3: regelmæssig/systematisk overvågning eller følsomme/strafbare oplysninger/forhold)

Men hvad er opgaverne så for en DPO?

Opgaverne står nævnt direkte i persondataforordningen (GDPR). Der står nævnt, at opgaverne bl.a. er:

* Underrette og rådgive organisationen og de ansatte om databeskyttelse
* Overvåge overholdelsen af de databeskyttelsesretlige regler i organisationen
* Rådgivning i forbindelse med konsekvensanalyse, hvis en sådan skal udarbejdes
* Samarbejde med Datatilsynet på vegne af organisationen
* Være Datatilsynets kontaktpunkt i spørgsmål vedrørende behandling bl.a. ved forudgående høring, hvis en konsekvensanalyse er foretaget, som viser at behandlingen vil føre til høj risiko i mangel af foranstaltninger

Hvis du vil høre nærmere om, hvorvidt du har brug for en DPO i jeres organisation og måske hjælp til DPO-rollen til en god pris, er du velkommen til at [kontakte os](https://persondatakonsulenterne.dk/om-os/kontakt/) her hos Persondatakonsulenterne.

Brug for mere hjælp til GDPR krav og regler eller lignende?

Har du stadig brug for hjælp til GDPR krav og regler? Eller bare sikre dig, at jeres virksomhed/organisation overholder GDPR?

Så kan vi her hos Persondatakonsulenterne hjælpe.

Vi er specialiseret inden for persondata, GDPR og persondataforordningen. Vi kan hjælpe med at sørge for, at I overholder reglerne og bliver 'compliant'.

Kontakt os via linket herunder for at høre nærmere om, hvordan vi kan hjælpe dig: