



# Brug af cookies og lignende teknologier

## Vejledning

Maj 2025

# Indhold

---

<b>Forord</b>	<b>3</b>
<b>1. Hvad er cookies og lignende teknologier?</b>	<b>4</b>
1.1 Cookies	4
1.2 Pixels	4
1.3 Fingerprinting	4
1.4 Apps mv.	4
1.5 Andre lignende teknologier	5
<b>2. Hvilke regler gælder?</b>	<b>6</b>
2.1 Cookiebekendtgørelsen	7
2.2 Databeskyttelsesreglerne	7
2.2.1 Hvad er personoplysninger?	7
2.2.2 Behandlingsgrundlag	8
<b>3. Hvad følger af reglerne?</b>	<b>9</b>
3.1 Skal jeg indhente samtykke?	9
3.2 Hvad er kravene til et gyldigt samtykke?	10
3.2.1 Frivilligt	10
3.2.2 Specifikt	14
3.2.3 Informeret	15
3.2.4 Utvetydig viljestilkendegivelse	15
3.2.5 Adgang til at trække samtykke tilbage	16
3.3 Hvordan kan jeg indhente samtykke?	16
3.4 Hvor ofte skal jeg opdatere et samtykke?	18
3.5 Oplysningspligt	18
3.6 Hvem har ansvaret?	18
<b>4. Dokumentationskrav</b>	<b>22</b>

# Forord

---

I denne vejledning gennemgås og forklares de væsentligste regler i cookiebekendtgørelsen og databeskyttelsesforordningen, som du skal være opmærksom på, hvis du tilbyder f.eks. en hjemmeside eller en app og i den forbindelse bruger cookies eller lignende teknologier.

Cookies og lignende teknologier kan anvendes til at indsamle og analysere oplysninger om brugere af online tjenester. Teknologierne anvendes dels til teknisk nødvendige formål, f.eks. for at opnå tilstrækkelig sikkerhed på tjenesten, men de kan også anvendes til at registrere oplysninger om brugernes online færden. Disse oplysninger kan anvendes til at forbedre brugernes oplevelse af tjenesten, f.eks. ved at gemme indstillinger om sprog, loginoplysninger mv. Oplysningerne kan også anvendes til at følge brugernes færden på tværs af hjemmesiden eller appen og danne grundlag for statistik. Endelig kan teknologierne anvendes til at følge brugerne på tværs af platforme og tjenester med henblik på at foretage målrettet markedsføring over for brugerne.

Cookiebekendtgørelsen og databeskyttelsesreglerne gælder ofte sideløbende, men der er visse forskelle i reglerne. I de enkelte afsnit i vejledningen vil det blive specificeret, hvis der er væsentlige forskelle, som du skal være opmærksom på.

Vejledningen er udarbejdet af Digitaliseringsstyrelsen og Datatilsynet, som er de to myndigheder der fører tilsyn med, at reglerne bliver overholdt. Vejledningen er primært rettet mod ejere og udbydere af f.eks. hjemmesider og apps, som indsamler oplysninger, herunder personoplysninger, om brugere af tjenesten gennem cookies og lignende teknologier. Den fælles vejledning er udarbejdet med det formål at gøre det lettere at leve op til begge regelsæt.

# 1. Hvad er cookies og lignende teknologier?

---

Både cookiebekendtgørelsen og databeskyttelsesreglerne er teknologineutrale. Det udslagsgivende for, om du skal forholde dig til cookiebekendtgørelsen er, om du lagrer eller tilgår allerede lagrede oplysninger på brugernes udstyr. Med hensyn til databeskyttelsesreglerne er det afgørende, om du behandler personoplysninger i processen.

Cookiebekendtgørelsen har til formål at beskytte brugere mod uretmæssig lagring af oplysninger eller opnåelse af adgang til oplysninger, der allerede er lagret, i brugerens terminaludstyr (herefter "udstyr"). Med andre ord er formålet at beskytte den del af brugerens privatsfære, der udgøres af brugerens enheder. Derfor gælder reglerne også f.eks. ved adgang til oplysninger, der gemmes på brugerens bil, IoT-devices mv. Det betyder, at bekendtgørelsen ikke alene er rettet mod cookies, men også andre typer af teknologier.

Tilsvarende er formålet med databeskyttelsesreglerne at sikre beskyttelse af brugerne i forbindelse med behandling af deres personoplysninger. Reglerne gælder, uanset hvilken teknologi der bruges til at behandle personoplysninger.

## 1.1 Cookies

Cookies er en af de mest udbredte former for teknologier, der anvendes til indsamling af oplysninger om brugerne af f.eks. hjemmesider. Det sker ved, at en cookie, som er en lille tekstfil med data, placeres på brugerens udstyr, når brugeren besøger en hjemmeside. Virksomheden eller myndigheden, der står bag hjemmesiden, kan herefter indsamle oplysninger om brugeren ved enten at lagre eller opnå adgang til oplysninger i disse cookies.

Cookies kan sættes af tjenesten selv (førstepartscookies) eller af en tredjepart (tredjepartscookies), og de kan have varierende levetid. Nogle cookies slettes, så snart brugeren lukker sit browservindue, mens andre kan være aktive flere år.

## 1.2 Pixels

En lignende og meget udbredt teknologi er pixels. En pixel, også kaldet en 'web beacon', er en lille grafik eller et billede, der er usynligt for brugeren. Pixels kan placeres på hjemmesider, hvor de bl.a. giver mulighed for at indsamle oplysninger om, hvilke undersider en bruger besøger på hjemmesiden. Pixels kan også placeres i e-mails, f.eks. nyhedsbreve, hvor de kan bruges til at spore, hvornår e-mailen åbnes, hvilke links i e-mailen brugeren tilgår, og hvornår dette sker.

## 1.3 Fingerprinting

Fingerprinting er en metode, der kan anvendes til at identificere og spore brugere ved at indsamle tekniske oplysninger om brugernes udstyr. Det kan f.eks. være oplysninger om en brugers browser, operativsystem, skærmopløsning, sprog, tidszone, installerede plugins, skrifttyper mv. Disse oplysninger bruges typisk til at sikre, at hjemmesiden eller appen vises i korrekt format og med korrekt indhold i forhold til brugernes type af udstyr. Oplysningerne kan dog også sættes sammen, og summen af disse oplysninger vil ofte være unik og gøre det muligt at udpege den enkelte bruger. Metoden kan derfor sammenlignes med et digitalt fingeraftryk, heraf navnet.

## 1.4 Apps mv.

For så vidt angår apps bruges enhedens identifikatorer som en almindelig metode til at indsamle data. Der er tale om unikke koder, der tildeles brugernes enhed eller app-installation såsom en iPhones UDID eller en Androids Reklame-ID. Tjenesteudbyderen kan benytte disse

identifikatorer til at spore brugerens aktiviteter inden for deres app samt på tværs af andre apps og hjemmesider, der benytter den samme identifikator.

## **1.5 Andre lignende teknologier**

Cookies, pixels eller fingerprints er ikke udtømmende for, hvad der kan være omfattet af reglerne. Anvender du andre lignende teknologier kan disse teknologier eller metoder også være omfattet af cookiebekendtgørelsen og databeskyttelsesreglerne. Du kan læse mere herom i vejledningens afsnit 2.

## 2. Hvilke regler gælder?

Når du bruger cookies eller lignende teknologier, skal du være opmærksom på reglerne i cookiebekendtgørelsen og databeskyttelsesreglerne.<sup>1</sup> Det skyldes, at du ofte vil indsamle og behandle personoplysninger, når du bruger disse teknologier. Det er bl.a. ofte tilfældet, hvis du bruger cookies og lignende teknologier til at indsamle statistik om unikke brugere eller til at målrette markedsføring.

Hvis du har en tjeneste såsom en hjemmeside eller en app, skal du sandsynligvis forholde dig til reglerne. I praksis skal du f.eks. være særligt opmærksom, hvis din tjeneste viser bannerreklamer, hvis du har indlejret plug-ins fra sociale medier, eller hvis du har et statistikmodul, der viser dig data om, hvem der besøger din tjeneste. Du skal også være opmærksom, hvis du generelt har indlejret plug-ins fra tredjeparter. Det kan være korttjenester, videoafspillere, logintjenester mv.

Hvis du er i tvivl om, hvorvidt du anvender cookies og lignende teknologier, bør du rådføre dig med en hjemmesideudvikler eller anden teknisk specialist. I sidste ende er det dog stadig dit ansvar at overholde reglerne.

Ved brug af cookies eller lignende teknologier gælder cookiebekendtgørelsen, uanset hvilke oplysninger du indsamler. Indsamler du personoplysninger gennem cookies eller lignende teknologier, gælder databeskyttelsesreglerne også. Behandler du personoplysninger, som du har indsamlet ved brug af cookies og lignende teknologier, vil denne efterfølgende behandling også være omfattet af databeskyttelsesreglerne.



Cookiebekendtgørelsen stiller krav om at indhente brugernes samtykke og give dem en række oplysninger, når du bruger cookies og lignende teknologier.

Databeskyttelsesreglerne stiller krav, når du behandler personoplysninger som f.eks. indsamles eller genereres ved hjælp af cookies og lignende teknologier. Efter disse regler er der f.eks. krav om, at du har et behandlingsgrundlag, og at du opfylder oplysningspligten.

Digitaliseringsstyrelsen fører tilsyn med overholdelse af cookiebekendtgørelsen, og Datatilsynet fører tilsyn med overholdelse af databeskyttelsesreglerne.

<sup>1</sup> Databeskyttelsesforordningen (GDPR) og databeskyttelsesloven.

## 2.1 Cookiebekendtgørelsen

Hvis du indsamler oplysninger om brugerne af din tjeneste gennem cookies og lignende teknologier, skal du som udgangspunkt indhente brugerens samtykke til dette. Det gælder også, hvor tredjeparter gennem cookies og lignende teknologier indsamler oplysninger om brugerne på din tjeneste – også selvom du ikke selv får adgang til de indsamlede oplysninger. Hvis du anvender værktøjer og indhold, som f.eks. skrifttyper, billedmateriale, korttjenester, statistikprogrammer mv., der udbydes af tredjeparter, kan disse tredjeparter ofte indsamle eller få adgang til oplysninger om brugerne af din tjeneste.

Reglerne omfatter indsamling af eller adgang til oplysninger på brugerens udstyr. Udstyr kan være computere, smartphones, tablets, smartwatches og andre IoT-enheder såsom smart fridges. Der er tale om et område under konstant udvikling, og det skal derfor ikke forstås som en udtømmende liste. I praksis omfatter "udstyr" også brugerens browser, idet browseren vurderes at være uløseligt forbundet med brugernes udstyr.

Du skal dog ikke indhente et samtykke fra brugeren, når du anvender cookies eller lignende teknologier, som er teknisk nødvendige for at få en funktionalitet på din tjeneste til at virke. Du kan læse mere om dette i afsnit 3.1 nedenfor.

## 2.2 Databeskyttelsesreglerne

Når du behandler personoplysninger, skal du overholde databeskyttelsesreglerne. Du behandler personoplysninger, når du f.eks. indsamler, registrerer eller videregiver oplysninger, som kan forbindes til en bestemt person.

Du skal altid have et retligt grundlag for at behandle personoplysninger – et såkaldt behandlingsgrundlag.

### 2.2.1 Hvad er personoplysninger?

En personoplysning er enhver form for information, der kan forbindes til en bestemt person. Det gælder også, hvis personen kun kan identificeres, når informationen kombineres med andre oplysninger. Personen, som oplysningerne vedrører, kaldes i databeskyttelsesreglerne for "den registrerede".

Når du bruger cookies og lignende teknologier, vil de registrerede typisk være brugerne af din tjeneste, f.eks. hjemmesidebesøgende eller appbrugere. Personoplysningerne, som du behandler om brugerne, kan f.eks. være MAC-adresser, reklame ID'er, pixel tags, identifikationsnumre, IP-adresser, lokaliseringsdata eller andre oplysninger, som alene – eller i kombination med andre – er unikke for den pågældende bruger.

Der er i sådanne tilfælde tale om personoplysninger, uanset om brugeren kan identificeres via sit borgerlige navn eller tilsvarende. Det skyldes, at en person efter databeskyttelsesreglerne kan være unikt identificeret via andet end sit navn.

I tilfælde, hvor en oplysning ikke i sig selv er en personoplysning, kan en kombination af flere oplysninger i nogle tilfælde gøre det muligt at identificere brugeren. Dette ses f.eks. ved teknologien *fingerprinting*, hvor de enkelte oplysninger hver for sig ikke er unikke for den pågældende bruger, f.eks. at brugerens sprogindstilling er dansk, men hvor kombinationen af oplysninger om enhedens tekniske specifikationer og indstillinger tilsammen gør den enkelte bruger unik og identificerbar.

Indsamling af oplysninger om brugere af onlinetjenester vil ofte udgøre behandling af personoplysninger.

Oplysninger om brugerne vil i nogle tilfælde være så detaljerede, at det er muligt at udlede særlige kategorier af oplysninger om brugerne. Det kan være i tilfælde, hvor oplysningerne danner baggrund for en meget detaljeret profil af brugerne, eller hvor det ud af sammenhængen er muligt at udlede oplysninger om f.eks. brugernes seksualitet, religion, race, fagforeningsmæssige forhold eller helbreds- og sundhedsmæssige forhold. Dette er særligt relevant for tjenester som f.eks. datingsider eller -apps, onlineapoteker mv., da der er særlige krav til behandling af denne type oplysninger.

Ved vurderingen af om du behandler personoplysninger, skal du derfor nøje overveje, hvilke oplysninger du indsamler om brugerne af din tjeneste, og om det er muligt at identificere disse.

### **2.2.2 Behandlingsgrundlag**

Når du behandler personoplysninger, skal du sikre, at databeskyttelsesreglernes betingelser for behandling af personoplysninger er opfyldt. Betingelserne – der også kaldes behandlingsgrundlag – findes i databeskyttelsesforordningens artikel 6.

Behandling af personoplysninger kan bl.a. ske, hvis det er nødvendigt af hensyn til udførelse af en opgave, som henhører under offentlig myndighedsudøvelse.

For private virksomheders vedkommende kan det også ske, hvis det er nødvendigt for, at virksomheden kan forfølge en legitim interesse, og den registreredes interesser og grundlæggende rettigheder ikke går forud herfor.

Ligeledes kan det ske, hvis den registrerede har givet samtykke til behandling af sine personoplysninger til et eller flere specifikke formål. Når du skal identificere det passende behandlingsgrundlag, skal vurderingen foretages på baggrund af alle relevante omstændigheder omkring behandlingen.

Hvis du behandler særlige kategorier af personoplysninger, skal du være opmærksom på, at det som udgangspunkt er forbudt at behandle disse oplysninger, medmindre du kan identificere en undtagelse, som gælder for din behandling. Undtagelserne findes i databeskyttelsesforordningens artikel 9. En af disse undtagelser er f.eks. at indhente udtrykkeligt samtykke til behandlingen.

## 3. Hvad følger af reglerne?

---

### 3.1 Skal jeg indhente samtykke?

Cookiebekendtgørelsen stiller krav om, at brug af cookies og lignende teknologier som udgangspunkt kun må ske efter samtykke fra brugerne. Du skal derfor indhente samtykke, hvis du bruger cookies og lignende teknologier til f.eks. generere besøgsstatistik, eller vise personaliserede annoncer.

Hvis du bruger cookies og lignende teknologier til at indhente og behandle personoplysninger, kan du med fordel indhente ét samlet samtykke for at overholde såvel cookiebekendtgørelsen som databeskyttelsesreglerne.

Cookies og lignende teknologier kan dog anvendes uden samtykke i det omfang, teknologien er teknisk nødvendig for, at tjenesten virker efter hensigten, og de indsamlede oplysninger ikke anvendes til andre formål end til at sikre tjenestens funktionalitet.

#### **Eksempler på teknisk nødvendige teknologier**

##### **Log-in og brugervalidering**

Teknologier som husker, at brugeren er logget ind på en tjeneste og sikrer, at brugeren fortsætter med at være logget ind. Ligeledes teknologier som anvendes til at sikre mod (gentagne) fejl ved login.

##### **Elektroniske indkøbskurve**

Teknologier som husker de varer, som brugeren har tilføjet til indkøbskurven, imens brugeren navigerer rundt på tjenesten.

##### **Brugerdefinerede indstillinger**

Indstillinger, som brugeren selv aktivt har valgt, f.eks. valg af sprog, skriftstørrelse eller land. Det kan også være levering af f.eks. skrifttyper fra tredjeparter. Det forudsætter dog, at de oplysninger, som tredjeparten herigennem indhenter fra brugeren kun bruges til at levere skrifttyperne og ikke f.eks. anvendes til at spore brugeren på tværs af hjemmesider og platforme.

##### **Autentificeringsteknologier**

Teknologier, som anvendes til at bekræfte brugerens identitet på tjenester med begrænset adgang.

##### **Load balancing teknologier**

Teknologier, som anvendes til at allokere brugere til en specifik server for at balancere adgangen til en tjeneste.

## Når cookiereglerne ikke stiller krav om samtykke

Der kan være særlige tilfælde, hvor du ikke er forpligtet efter cookiebekendtgørelsen til at indhente samtykke, men hvor de oplysninger, som du indsamler og behandler, udgør personoplysninger. Dette gør sig gældende i tilfælde, hvor der er tale om teknisk nødvendige cookies og lignende teknologier. I de tilfælde vil behandlingen kun være omfattet af databeskyttelsesreglerne, og du kan efter omstændighederne og til visse formål behandle oplysningerne, hvis du har en legitim interesse heri.

Det kræver dog en teknisk og juridisk analyse af, om din specifikke opsætning falder inden for dette.

Brugen af denne såkaldte *interesseafvejningsregel* forudsætter en konkret vurdering. Du skal konkret afveje din legitime interesse i at behandle oplysningerne mod brugernes interesse i, at oplysningerne ikke behandles.

Det bemærkes også, at interesseafvejningsreglen ikke almindeligvis vil kunne udgøre et behandlingsgrundlag til brug for målrettet markedsføring på baggrund af oplysninger om brugernes adfærd på tværs af tjenester og lokation ved hjælp af cookies og lignende teknologier. I de tilfælde vil det korrekte behandlingsgrundlag derimod være samtykke fra brugerne.<sup>2</sup>

Offentlige myndigheder kan på tilsvarende vis behandle oplysningerne, hvis indsamlingen og behandlingen af oplysningerne er nødvendig for at udføre deres myndighedsudøvelse.

Der gælder ingen specifik tidsfrist for, hvor længe et samtykke er gyldigt. Det afhænger af sammenhængen, omfanget af det oprindelige samtykke og brugernes forventninger. Et samtykke kan bortfalde efter en vis tidsperiode og skal derfor med jævne mellemrum indhentes på ny.

Hvis du ændrer, hvilke cookies mv., som du bruger og til hvilke formål, gælder det oprindelige samtykke heller ikke længere, og du skal også her indhente et nyt. Det kan være tilfældet, hvor du f.eks. ønsker at bruge de indsamlede personoplysninger til andre formål end det oprindelige, eller hvor du ønsker at videregive personoplysninger til nye tredjeparter.

## 3.2 Hvad er kravene til et gyldigt samtykke?

For at være gyldigt skal et samtykke opfylde en række betingelser. Betingelserne skal sikre, at brugerne har kontrol over deres personoplysninger, og at kontrollen ikke bliver illusorisk.

Et gyldigt samtykke er en frivillig, specifik, informeret og utvetydig viljestilkendegivelse fra brugeren, hvor brugeren accepterer, at du og eventuelle tredjeparter indsamler og behandler personoplysninger om vedkommende. Et gyldigt samtykke skal desuden kunne dokumenteres i forhold til, hvad samtykket omfatter, hvornår det er afgivet, og hvilken samtykkeløsning der blev anvendt. Det skal også kunne trækkes tilbage lige så let, som det er givet.

Samtykke skal indhentes fra brugeren, *inden* du indsamler og behandler oplysninger ved brug af cookies og lignende teknologier, dvs. inden du f.eks. placerer cookies i brugerens browser.

### 3.2.1 Frivilligt

Et samtykke skal være frivilligt. Årsagen hertil er, at brugeren skal kunne foretage et valg og have kontrol over sine oplysninger.

Giver du ikke brugeren et reelt eller frit valg, vil samtykket ikke være frivilligt. Du skal derfor give brugeren en mulighed for at afslå brugen af cookies og lignende teknologier. Det skal altid

<sup>2</sup> Der kan for nærmere herom bl.a. henvises til eksempel 10 i Datatilsynets vejledning om direkte markedsføring.

være tilsvarende let at afstå fra at give samtykke til behandling af sine oplysninger, som det er at give det.

### Eksempel 1: Kun mulighed for at acceptere

Her er det ikke muligt for brugeren at afslå at give samtykke til brug af cookies og lignende teknologier. Brugeren tilbydes heller ikke et andet alternativ, og der er således ikke tale om et frivilligt valg. Et sådant samtykke opfylder derfor ikke kravet om frivillighed.

**Samtykke til brug af cookies**

Vi vil gerne registrere og opbevare personoplysninger om dine seneste besøg på vores hjemmeside, og om hvordan du færdes på de forskellige dele af vores hjemmeside til analyseformål for at forstå, hvordan forskellige mennesker bruger vores hjemmeside, så vi kan gøre det mere intuitivt.

**Tillad**

[Læs mere om vores behandling af personoplysninger](#)

### Cookie walls

For at samtykke kan anses for at være givet frivilligt, må adgangen til din tjeneste eller til funktionerne på din hjemmeside eller app som udgangspunkt ikke være betinget af brugerens samtykke.

### Eksempel 2: Cookie wall

En hjemmesideejer forhindrer fra start brugerne i at se indhold på sin hjemmeside. Når brugerne tilgår hjemmesiden, dukker der en pop-up meddelelse frem, som anmoder brugerne om at acceptere brugen af cookies. Brugere kan ikke få adgang til hjemmesidens indhold, medmindre brugeren accepterer cookies.



Eftersom det ikke er muligt for brugerne at tilgå hjemmesidens indhold og funktioner uden at acceptere anvendelsen af cookies, og da der ikke tilbydes et alternativ, vil samtykket ikke opfylde kravet om frivillighed. Brugeren får derved ikke et reelt valg.

Du kan i visse tilfælde anvende såkaldte *cookie walls*, hvis du giver brugerne et alternativ til at give samtykke. Det afgørende er, om brugeren tilbydes et tilfredsstillende alternativ. Ved brug

af betaling som alternativ skal du i din vurdering af alternativet være opmærksom på følgende fire kriterier. Du skal sikre, at:

- Alternativet er rimeligt
- Alternativet har en rimelig pris
- Du kun indsamler personoplysninger til de formål, der er nødvendige for at modsvare betaling fra brugeren
- Der ikke behandles yderligere personoplysninger, end hvad der er nødvendigt, for at tjenesten kan leveres i de tilfælde, hvor brugeren betaler for adgang til tjenesten.

Det *første kriterie* om, at alternativet skal være rimeligt, indebærer, at tjenesten i vidt omfang skal være tilsvarende, uanset om brugerne giver samtykke eller betaler for at få adgang til tjenesten.

Det *andet kriterie* om, at prisen skal være rimelig, indebærer, at du ikke må fastsætte en urimelig høj pris for betalingsalternativet. Du er dermed ikke afskåret fra at tilbyde adgang mod betaling som alternativ til samtykke, men prissætningen må ikke være så høj, at brugernes valgfrihed i praksis bliver illusorisk. Du har et vidt skøn ved fastsættelsen af det specifikke beløb, så længe brugerne i praksis har et reelt valg.

Det *trejde kriterie*, om at behandlingen skal være begrænset til det nødvendige for at modsvare betaling indebærer, at du skal kunne påvise, at alle de formål, som du indhenter samtykke til, udgør en nødvendig del af betalingsalternativet. Hvis du vurderer, at behandling til flere formål ikke er nødvendig, skal du gøre det muligt for brugerne at give særskilt samtykke til disse formål.

Ofte er det brugernes samtykke til behandling af personoplysninger i markedsføringsøjemed, der udgør den ønskede fordel for virksomheden. I så fald er det kun samtykke til dette formål, der er en nødvendig del af alternativet til adgang mod betaling.

Efter det *fjerde kriterie* må du som udgangspunkt kun behandle de oplysninger, der er nødvendige for, at du kan levere din tjeneste. Det kan f.eks. være, at leveringen af tjenesten forudsætter oprettelse af en konto eller brugerprofil. Hvis brugerne har betalt for adgang til din tjeneste, må du som udgangspunkt ikke behandle oplysninger til flere formål end det, der er nødvendigt for, at tjenesten kan leveres. Det kan f.eks. være personalisering eller markedsføring. Det udelukker dog ikke, at brugerne – også i disse tilfælde – kan beslutte efterfølgende at give samtykke til behandling af sine oplysninger til disse formål.<sup>3</sup>

### *Nudging*

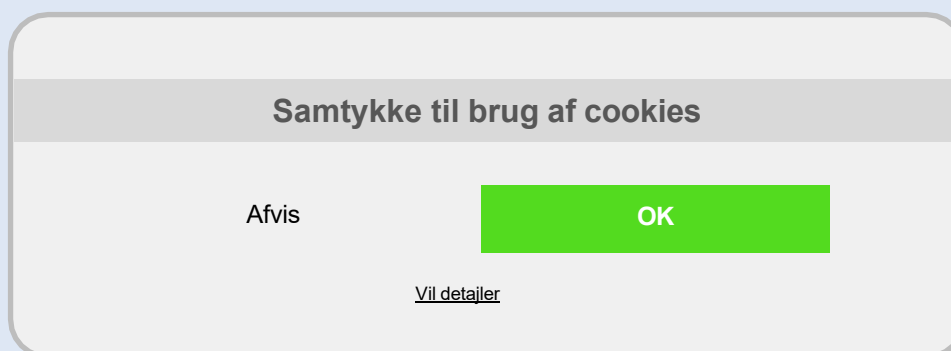
Enhver form for disproportionelt pres på eller påvirkning af brugernes frie vilje kan medføre, at samtykket er ugyldigt. Du skal derfor være omhyggelig i dine overvejelser om, hvordan du beder om samtykke. Du bør f.eks. ikke presse dine brugere til at afgive samtykke ved gentagne gange at præsentere dem for muligheden for at acceptere brugen af cookies og lignende teknologier under deres besøg på din hjemmeside eller app. Du skal også være påpasselig med at bruge et sprog eller forklaringer, der presser brugerne i retning af at give samtykke.

Brug af forskellige farver ved valg af responsknapper kan også efter omstændighederne påvirke brugerne til at foretage bestemte valg. Særligt vil bestemte farvevalg kunne udgøre en form for nudging, ligesom knapper, der går i et med baggrunden, kan påvirke brugernes valg. Sådanne designs vil efter omstændighederne være i strid med cookiebekendtgørelsen og databeskyttelsesreglerne.

---

<sup>3</sup> Du kan læse mere om cookie walls på Datatilsynets hjemmeside: <https://www.datatilsynet.dk/regler-og-vejledning/cookies-og-lignende-teknologier>

### Eksempel 3: Nudging ved brug af farver



Her er "accepter"-knappen markeret tydeligt med en grøn farve, mens "afvis"-knappen kun svagt skiller sig ud fra baggrunden. Muligheden for at afslå brugen af cookies og lignende teknologier skal fremstå ligeså tydelig som muligheden for at acceptere dem.

Du har en betydelig designmæssig frihed med hensyn til layout og indhold, så længe det ikke fører til uigennemsigtighed eller urimelige situationer for brugerne.<sup>4</sup>

#### *Granularitet*

Granularitet er et væsentligt element i vurderingen af, om et samtykke er frivilligt. Granularitet indebærer, at brugerne skal have mulighed for at give særskilt samtykke til forskellige formål.

Ønsker du at behandle oplysninger til flere formål, må brugerne dermed ikke tvinges til at give samtykke til samtlige formål.

---

<sup>4</sup> Læs mere herom i [Datatilsynets afgørelse i sagen vedrørende JP/Politikens samtykkeløsning](#)

#### Eksempel 4: Behandling til flere formål på baggrund af ét samlet samtykke

##### Samtykke

Vi vil gerne registrere og opbevare personoplysninger om dine seneste besøg på vores hjemmeside, og om hvordan du færdes på de forskellige dele af vores hjemmeside til analyseformål for at forstå, hvordan forskellige mennesker bruger vores hjemmeside, så vi kan gøre det mere intuitivt.

Tilsvarende registrerer vi oplysninger om, hvilke varer du har købt, og hvilke varer du har kigget på, og benytter oplysningerne til at målrette reklamer på dette websted til dig, der er relevante i forhold til dine interesser, som vi har afdækket på baggrund af dine køb og varer, du har kigget på.

OK

NEJ

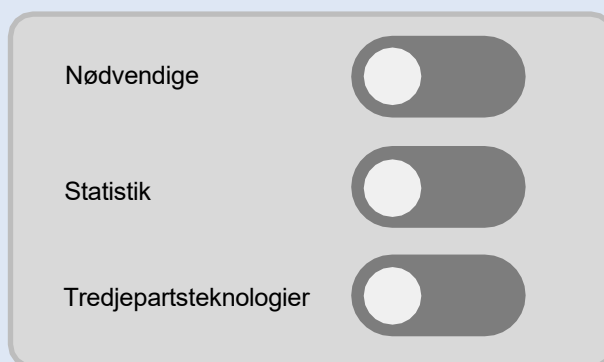
I dette tilfælde er det muligt at foretage et frit valg med hensyn til at til- eller fravælge den samlede behandling af personoplysninger. Der sker dog indsamling og behandling til flere forskellige formål på baggrund af ét samlet samtykke. Det opfylder derfor **ikke** betingelserne om frivillighed, da de registrerede ikke har et tiltrækkeligt frit valg i forhold til at kunne til- eller fravælge blandt de to forskellige formål.

#### 3.2.2 Specifikt

At samtykket skal være specifikt indebærer bl.a., at samtykket skal være præcist og velafgrænset. Din samtykkeløsning må derfor ikke være generelt udformet eller uden en præcis angivelse af formålene med behandlingen af oplysninger, og hvilke oplysninger der vil blive behandlet.

#### Eksempel 5: Uspecifikke formål

Angiver man formålene med behandlingen på nedenstående måde er det ikke klart for brugeren, hvilke formål oplysningerne indsamles til, idet "tredjepartsteknologier" ikke siger noget specifikt om formålet med behandlingen. Du skal indhente samtykke til de specifikke formål, som du skal bruge oplysningerne til, og brugeren skal oplyses om, hvilke oplysninger der vil blive behandlet til hvert formål.



Nødvendige	<input checked="" type="checkbox"/>
Statistik	<input type="checkbox"/>
Tredjepartsteknologier	<input type="checkbox"/>

Ønsker du at behandle oplysninger til andre formål end det, brugerne oprindeligt har givet samtykke til, skal du indhente et nyt samtykke, der omfatter de nye formål.

### 3.2.3 Informeret

Samtykket skal være informeret, hvilket betyder, at brugerne skal vide, hvad de giver samtykke til. Du skal derfor, inden du indhenter samtykke, informere brugerne om bestemte elementer, der er afgørende for, at de kan træffe et valg. Hvis ikke du giver tilstrækkelige oplysninger, bliver brugernes kontrol illusorisk, og samtykket vil derfor være ugyldigt.

Du skal i forbindelse med indhentelsen af samtykke som minimum informere om din (og eventuelle samarbejdspartneres) identitet, formålene med behandlingen og typen af oplysninger, der vil blive indsamlet og behandlet. Du skal også informere om retten til at trække et samtykke tilbage.

#### *Identitet*

Du skal under alle omstændigheder identificere dig selv. Hvis der er tale om virksomhedens eller myndighedens egen hjemmeside eller tjeneste, vil identiteten ofte være indlysende.

Integrerer du indhold fra tredjeparter på din tjeneste, skal du også identificere og informere om disse (navngivne) tredjeparter.

#### *Formål og typen af oplysninger*

Du skal også informere brugerne om formålene med indsamling og behandling af oplysninger. Det er ikke tilstrækkeligt kun at oplyse, at der sker indsamling, registrering eller anden behandling af oplysninger.

Du skal i den forbindelse sikre, at brugerne har let ved at forstå, hvilke(t) formål der anmodes om samtykke til, ligesom det skal være tydeligt, hvilke type(r) af personoplysninger der behandles til de(t) specifikke formål.

### **Eksempel 6: Formål og typer af oplysninger**

En webshop har implementeret bannerannoncer fra en annoncør på sin hjemmeside, og i den forbindelse sker der behandling af personoplysninger om brugerne.

Webshoppen giver i sin samtykkeløsning følgende information:

*"Webshoppen indsamler oplysninger om, hvilke varer du har købt, og hvilke varer du har kigget på med henblik på at målrette reklamer på denne webshop til dig, der er relevante i forhold til dine interesser, som vi har afdækket på grundlag af de varer, du har kigget på og købt."*

I dette tilfælde vil samtykket være informeret og specifikt, da det er klart for brugerne, hvilken type oplysninger der indsamles, og til hvilket formål oplysningerne behandles.

#### *Retten til at trække samtykke tilbage*

Samtidig med at du indhenter samtykke, skal du også informere om, at samtykket kan trækkes tilbage. Er brugerne ikke informeret om retten til at trække samtykke tilbage, vil samtykket ikke være gyldigt.

#### *Indhentning af samtykke fra børn*

Brugerens alder og modenhed spiller en væsentlig rolle i forhold til evnen til at give et gyldigt samtykke. Børn nyder en særlig beskyttelse, og den dataansvarlige er pålagt at foretage en konkret vurdering af, om barnet er tilstrækkeligt moden til at forstå de risici og konsekvenser, der kan være forbundet med indsamlingen af data. Som udgangspunkt vil et barn fra og med 15 år på egne vegne kunne give et gyldigt samtykke.

### 3.2.4 Utvetydig viljestilkendegivelse

Et samtykke kræver en *utvetydig viljestilkendegivelse* ved en erklæring eller klar bekræftelse fra brugerne. Samtykke skal dermed gives ved en aktiv handling eller erklæring.

Dette betyder, at du ikke kan bruge cookies eller lignende teknologier på baggrund af, at brugerne fortsat anvender din tjeneste. Dette vil ikke udgøre et gyldigt samtykke, eftersom det ikke vil udgøre en aktiv handling, at brugeren fortsat bruger tjenesten. Samtykket vil dermed være ugyldigt, og din anvendelse af teknologierne vil være ulovlig.

Samtykket er heller ikke udtryk for utvetydig viljestilkendegivelse, hvis du f.eks. anvender forudafkrydsede felter og on-sliders i din samtykkeløsning, idet brugerne ikke giver samtykke ved en aktiv handling. Samtykket vil derfor i sådanne tilfælde heller ikke være gyldigt.

Generel accept af dine almindelige betingelser og vilkår kan heller ikke opfattes som en utvetydig viljestilkendegivelse, da brugeren let vil kunne overse anmodningen om samtykke.<sup>5</sup>

### 3.2.5 Adgang til at trække samtykke tilbage

Du skal sikre dig, at det til enhver tid er lige så let for brugerne at trække deres samtykke tilbage, som det var at give det. Brugere skal samtidig have mulighed for at trække deres samtykke tilbage, uden at det er til skade for dem. Det betyder bl.a., at brugerne let skal kunne tilbagekalde samtykket uden betaling af gebyrer.

I praksis kan du sikre adgangen til at trække samtykke tilbage ved f.eks. at placere et tydeligt og sigende link i toppen eller bunden af din hjemmeside, eller ved at have et fast ikon, som kan tilgås fra alle undersider på hjemmesiden.

#### Eksempel 7: Mulighed for at trække samtykke tilbage

I dette eksempel fremgår der både på hjemmesidens hovedside og undersider et fast ikon, hvor brugerne ved et enkelt klik kan tilgå samtykkeløsningen og ændre sine valg.



Hvis du indhenter samtykke f.eks. ved et klik, swipe eller tryk, skal brugerne kunne tilbagekalde deres samtykke på en tilsvarende enkel måde. Har du f.eks. indhentet samtykke via en app, bør brugerne også kunne trække sit samtykke tilbage via lettilgængelige indstillinger i appen.

### 3.3 Hvordan kan jeg indhente samtykke?

I tillæg til de specifikke krav ovenfor gælder der også nogle helt generelle krav til, hvordan du skal opbygge din samtykkeløsning.

#### *Krav til informationens tilgængelighed*

Visse informationer skal være tilgængelige f.eks. i første lag af samtykkeløsningen, mens andre oplysninger kan fremgå af en fold-ud menu, privatlivspolitik eller lignende, som du henviser til gennem et link i samtykkeløsningen. Andre midler såsom pop-up meddelelser eller "mouse-

<sup>5</sup> For nærmere herom henvises til Datatilsynet afgørelse vedrørende [tilsyn med Dating.dk \(datatilsynet.dk\)](https://www.datatilsynet.dk/tilsyn-med-dating.dk)

over"-meddelelser kan også benyttes ud over den lagdelte information med henblik på at gøre informationen mere tilgængelig for brugeren.

I første lag af din samtykkeløsning skal du som minimum oplyse om:

- Organisationens og dine eventuelle samarbejdspartneres identitet
- Formålet med at indsamle (person)oplysninger gennem anvendelsen af cookies og lignende teknologier
- Hvilke(n) typer(r) af personoplysninger der vil blive indsamlet og behandlet
- Hvorvidt der indsamles eller videregives oplysninger af/til tredjeparter
- At brugerne har ret til at trække samtykket tilbage

Med hensyn til din og dine eventuelle samarbejdspartneres identitet – f.eks. annonceringspartnere – vil der være tale om et gyldigt samtykke, hvis informationen om eventuelle samarbejdspartnere fremgår af en liste eller en oversigt, f.eks. ved en fold-ud menu (som er "et-klik-væk") i første lag af samtykkeløsningen.

En række informationer kan f.eks. fremgå i andet lag af samtykkeløsningen, herunder:

- Identiteten på dem, der står bag de anvendte teknologier, herunder navnet på teknologierne, teknologiernes formål og – hvis der f.eks. er tale om cookies – udløbsdato (funktionsvarighed).
- Instruktioner i, hvordan brugeren trækker sit samtykke tilbage (og eventuelt sletter allerede placerede cookies eller lignende).

Derudover skal samtykkeløsningen generelt være klar og kortfattet og være adskilt fra f.eks. dine almindelige vilkår og betingelser. Det betyder, at anmodningen om samtykke ikke må være skjult eller generelt fremgå af dine betingelser, vilkår eller lignende.

#### *Krav til samtykkeløsningens opbygning*

Du skal derudover være opmærksom på, hvordan din samtykkeløsning designes og implementeres. Løsningen skal bl.a. være lettilgængelig, uanset hvilken enhed, som tjenesten tilgås fra. Dette kunne f.eks. være via mobiltelefon, tablet eller computer.

Samtykkeløsninger skal ikke være unødvendigt forstyrrende. Det kan dog være nødvendigt, at samtykkeløsningen til en vis grad forstyrrer brugeroplevelsen, hvis anmodningen skal være effektiv. Du skal derfor vælge en løsning, som sikrer den rigtige balance. Eksempelvis vil der ikke være den rigtige balance i tilfælde, hvor en bruger, som tilgår en hjemmeside eller app flere gange dagligt, bliver præsenteret for samtykkeløsningen på ny hver gang siden eller appen tilgås.

Hvis løsningen er svært tilgængelig, kan det betyde, at det indhentede samtykke ikke er gyldigt.

Du skal endelig være opmærksom på, at en af udfordringerne ved samtykkeløsninger også kan være, at brugerne kan overse eller bevidst ignorere disse meddelelser og hurtigt fortsætte deres videre gang på hjemmesiden mv. Brugere som ikke interagerer med samtykkeløsningen, kan dog ikke, som nævnt ovenfor, siges at have givet et gyldigt samtykke.

#### *Krav til sproget*

Når du udformer din samtykkeløsning, er det vigtigt, at du er opmærksom på det sprog, som du anvender. Du skal give de nødvendige informationer i et klart og enkelt sprog. Undgå derfor komplekse sætnings- og sprogstrukturer samt unødvendigt brug af teknisk eller juridisk sprog. Informationen skal formuleres klart og konkret, og du bør derfor ikke formulere den i abstrakte eller tvetydige vendinger.

Du bør i vidt omfang udforme din samtykkeløsning på samme sprog som resten af din tjeneste. Hvis du udbyder en dansksproget tjeneste (eksempelvis app eller hjemmeside), bør din samtykkeløsning og privatlivspolitik eller lignende derfor også være på dansk.

### 3.4 Hvor ofte skal jeg opdatere et samtykke?

Cookiereglerne og databeskyttelsesreglerne fastsætter ikke en specifik tidsgrænse for, hvor ofte et samtykke skal opdateres.

Når du vurderer hvor ofte du skal indhente et samtykke skal du lægge vægt på til hvilke formål behandlingen af oplysningerne sker, karakteren af behandlingen, herunder om den må anses for særligt ingribende for brugerne og brugerenes berettigede forventninger.

Det vil ofte være passende at opdatere samtykket en gang årligt. Ligeledes vil det også være mest passende, at genanmode en bruger, som har afslået at give samtykke, en gang årligt.

Hvis der sker en betydelig ændring af din tjenestes anvendelse af cookies eller lignende teknologier, vil det samtykke, som brugerne har givet, ikke altid være tilstrækkeligt til at dække den nye behandling. I disse tilfælde, skal du altid indhente et nyt samtykke. Det kan f.eks. være tilfældet hvis du indsamler oplysninger gennem cookies eller lignende teknologier til statistik, men du fremadrettet ønsker at indsamle oplysninger til markedsføring. Det oprindelige samtykke vil i denne situation ikke dække det nye behandlingsformål, og du skal derfor indhente et nyt samtykke, før du igangsætter denne behandling.

### 3.5 Oplysningspligt

Når du anvender cookies og lignende teknologier skal du være opmærksom på din pligt til at oplyse om behandlingen af brugernes oplysninger.

I praksis kan indhentning af samtykke og opfyldelse af oplysningspligten ske i en integreret løsning. Du skal i den forbindelse sikre, at brugerne får de væsentligste informationer i samtykkeløsningen, samtidigt med at der f.eks. linkes eller på anden vis henvises til mere detaljerede informationer.<sup>6</sup>

Der er hertil krav om, at du informerer brugeren om cookies eller lignende teknologiers funktionsvarighed (udløbsdato). Det vil sige hvor længe teknologien indsamler oplysninger på brugerens terminaludstyr.

### 3.6 Hvem har ansvaret?

Ansvaret for at indhente samtykke, hvis du ønsker at bruge cookies eller lignende teknologier, påhviler dig. Det skyldes, at det er dig, der har ansvaret for, hvilket indhold der integreres på tjenesten og dermed også de cookies og lignende teknologier, som anvendes på tjenesten. Dette gælder også, selvom du vælger at lade en samarbejdspartner eller teknisk leverandør stå for brugen af cookies og lignende teknologier på tjenesten.

Hvis du bruger cookies mv. til at indsamle og behandle personoplysninger, er der yderligere krav, som du skal leve op til efter databeskyttelsesreglerne. Om det er dig eller dine eventuelle samarbejdspartnere, der har ansvaret for at overholde disse krav, afhænger af omstændighederne.

Udgangspunktet er, at du er ansvarlig for at overholde disse krav.

I visse tilfælde kan der være tale om, at din samarbejdspartner kun handler på dine vegne og efter din instruks. Det kan f.eks. være tilfældet, hvis du har antaget en virksomhed til at hjælpe dig med at generere besøgsstatistik på din tjeneste. I givet fald er du fortsat ansvarlig, da din samarbejdspartner handler på dine vegne. Oftest vil du indgå en kontrakt – en databehandleraftale – der fastlægger, hvilke krav samarbejdspartneren skal overholde i jeres indbyrdes relation.

---

<sup>6</sup> Du kan læse mere om, hvilken information du skal give brugerne i afsnit 3 i [Datatilsynets vejledning om de registreredes rettigheder](#).

### **Eksempel 8: Analyseværktøj inhouse**

En virksomhed har opsat et analyseværktøj på sin hjemmeside med henblik på at registrere antallet af besøgende og analysere deres brug af hjemmesiden. I den forbindelse indsamles bl.a. oplysninger om de besøgendes IP-adresse, oplysninger om de besøgendes browser, cookieidentifikatorer, hvilke undersider, de besøger, hvor længe besøget varer m.v.

Virksomheden hoster selv hjemmesiden og analyseværktøjet.

Virksomheden er i dette tilfælde dataansvarlig for behandling af personoplysninger, der sker i forbindelse med de besøgendes brug af hjemmesiden, idet virksomheden selvstændigt fastlægger formålene med og hjælpemidlerne til behandlingen.

Hvis du derimod udliciterer driften af din hjemmeside til en hostingvirksomhed, som hoster hjemmesiden på dine vegne, vil der typisk være tale om en såkaldt databehandlerkonstruktion.

### **Eksempel 9: Udlicitering til hostingvirksomhed**

Virksomheden ønsker ikke længere selv at have udstyr m.v. stående in-house og ønsker derfor at udlicitere driften af sin hjemmeside til en hostingvirksomhed.

Virksomheden indgår en aftale med en hostingvirksomhed om, at hostingvirksomheden fremover skal hoste virksomhedens hjemmeside, herunder analyseværktøjet.

I dette tilfælde vil hostingvirksomheden blive anset som databehandler for virksomheden, idet hostingvirksomheden ikke har et selvstændigt formål med behandlingen af personoplysninger, og behandlingen af oplysninger alene sker på vegne af og efter instruktion fra virksomheden.

Det kan også være, at du herudover ønsker, at analyseværktøjet også skal drives af en anden ekstern virksomhed, der har flere kompetencer i denne henseende. Det kunne f.eks. være et analysebureau.

### Eksempel 10: Integrering af analyseværktøj fra analysebureau

Virksomheden har vurderet, at den ønsker mere detaljerede analyser af de besøgendes brug af virksomhedens hjemmeside og skal derfor anskaffe sig et andet analyseværktøj.

Virksomheden kontakter et analysebureau, der kan levere det ønskede analyseværktøj. Analyseværktøjet, som bureauet tilbyder, hostes in-house (dvs. hos bureauet). Virksomheden skal blot ændre konfigurationen af sin hjemmeside for at integrere bureauets analyseværktøj. Virksomhedens hjemmeside er fortsat hostet af den tidligere nævnte hostingvirksomhed.

Analyseværktøjet behandler fortsat personoplysninger.

Analysebureauet vil som udgangspunkt – sideløbende med hostingvirksomheden - også være databehandler for virksomheden, idet bureauet behandler personoplysninger i forbindelse med det analyseværktøj, som bureauet leverer, men behandlingen sker dog alene på vegne af og efter instruktion fra virksomheden.

Der kan dog også være tale om, at du er fælles ansvarlig sammen med dine samarbejdspartnere for at overholde reglerne. Det er tilfældet, hvis I i fællesskab fastlægger "formål og hjælpemidler", dvs. i fællesskab beslutter, hvorfor der skal indsamles og behandles oplysninger samt hvordan.

Det vil f.eks. ofte være tilfældet, hvis du integrerer indhold fra tredjeparter f.eks. fra sociale medier, indholdsudbydere og lignende på din tjeneste.<sup>7</sup>

Hvor du og en eller flere tredjeparter i fællesskab bestemmer, hvorfor der skal behandles personoplysninger (formålet), og hvordan oplysningerne skal behandles (hjælpemidlerne), vil der være tale om såkaldt fælles dataansvar.

### Eksempel 11: Fælles dataansvar med et analysebureau

Analysebureauet, der er nævnt i eksempel 10, ændrer sin forretningsmodel og tilbyder nu sit analyseværktøj gratis til virksomheder, herunder til den tidligere nævnte virksomhed. Bureauet behandler dog nu også personoplysningerne til egne formål, navnlig med henblik på bedre at forstå og analysere online adfærd og trends.

Idet både virksomheden og analysebureauet nu hver har et formål med behandling af de omhandlede personoplysninger og begge har indflydelse på hjælpemidlerne til behandlingen, vil parterne i et vist omfang være fælles dataansvarlige.

Omfanget af det fælles dataansvar skal herefter afgøres af parterne ud fra de(n) konkrete behandling(er), der foretages af parterne hver især.

Det nærmere dataansvar skal fastlægges med udgangspunkt i samarbejdet mellem dig og udbyderen af det pågældende plug-in, som du har på din tjeneste. Ansvarsfordelingen skal analyseres på grundlag af de særlige betingelser for samarbejdet med udbyderen af det pågældende plug-in, som kan fremgå af serviceaftalerne.

<sup>7</sup> For nærmere herom henvises til Datatilsynet afgørelse vedrørende [Boligportals brug af Facebook Business Tools](#). For nærmere information om ansvarsfordelingen, når du integrerer indhold fra tredjeparter, se f.eks. [Datatilsynets afgørelse vedrørende DMI's behandling af personoplysninger om hjemmesidebesøgende](#). For nærmere herom henvises til Datatilsynet afgørelse vedrørende [tilsyn med Dating.dk \(datatilsynet.dk\)](#)

I praksis – og navnlig ved brug af større leverandører af it-standardprodukter – er en gennemgang af leverandørens servicevilkår et godt sted at starte. På den måde kan du danne dig et overblik over, hvad det er for et analyseværktøj, som du har med at gøre.

Du skal i denne forbindelse være særligt opmærksom på, om leverandøren forbeholder sig retten til at behandle personoplysningerne til egne formål, hvilket kan være en integreret del af produktet. Hvis dette er tilfældet, kræver det nøje analyser, før brug af produktet kan ske lovligt.<sup>8</sup>

Fordelingen af jeres roller og ansvarsområder kan ske i hovedaftalen på baggrund af jeres generelle aftaleretlige forpligtelser. Det skal dog ske på en gennemsigtig måde, så det er fuldstændigt klart for brugerne, hvor de med fordel kan henvende sig, hvis de vil gøre deres rettigheder gældende. I skal derfor gøre den "ordning", der ligger til grund for samarbejdet, tilgængelig for brugerne.

Du skal derfor gøre dig en række overordnede overvejelser – ideelt i dialog med leverandøren, f.eks. en udbyder af plug-ins – om, hvordan de forskellige forpligtelser og rettigheder for brugere vil blive håndteret af jer.

For at kunne fastlægge dit konkrete ansvar skal du først og fremmest vide, hvilke cookies og lignende teknologier du benytter på din tjeneste. Du kan med fordel starte med at spørge udvikleren af din tjeneste, hvilke cookies og lignende teknologier tjenesten er "født med", herunder som følge af eventuelle plug-ins.

Når du ved hvilke cookies og lignende teknologier, der benyttes på tjenesten, har du et bedre udgangspunkt for at fastlægge, hvilken rolle du og eventuelle andre parter indtager. Det er vigtigt, at du løbende får lavet en analyse af, hvilke cookies og lignende teknologier, der er integreret på din tjeneste. Når du f.eks. integrerer et plug-in fra et socialt medie, følger der normalt cookies og/eller lignende teknologier med.

Det kan derfor være en god idé løbende at scanne din tjeneste i takt med, at du implementerer nye funktionaliteter eller ændrer på din tjeneste, så du kan danne dig et overblik over hvilke cookies, pixels eller lignende, der benyttes.

---

<sup>8</sup> Se hertil Datatilsynets vejledning om cloud, særligt afsnit 3.2.1. om screening af leverandør(e).

## 4. Dokumentationskrav

---

Har du indhentet samtykke fra brugerne til anvendelsen af cookies og lignende teknologier, skal du kunne dokumentere det, så længe du behandler oplysninger om vedkommende. Dokumentationskravet bør ikke i sig selv medføre yderligere behandling af oplysninger, og du skal derfor ikke indsamle flere oplysninger end nødvendigt for at kunne opfylde dette krav.

Du kan opfylde dokumentationskravet ved såkaldt systemdokumentation. For at opfylde dokumentationskravet om samtykke skal du derfor kunne dokumentere:

- 1) Dine procedurer omkring indhentning af samtykke, herunder hvilke oplysninger brugere blev præsenteret for, da de gav deres samtykke
- 2) At procedurerne opfyldte alle betingelserne for et gyldigt samtykke.

Det betyder for det første, at du skal gemme f.eks. skærmbilleder eller dokumentere på anden vis, hvordan din samtykkeløsning ser ud, og hvilke informationer du giver brugerne, når du beder om deres samtykke. I tvivlstilfælde kan det også være nødvendigt, at du har vurderet og dokumenteret, at din specifikke fremgangsmåde opfylder de betingelser, som er nærmere beskrevet ovenfor.

Du skal også sørge for at opdatere din dokumentation med jævne mellemrum. Det er særligt relevant, hvor du løbende tilpasser samtykkeløsningen. I disse tilfælde kan du eksempelvis gemme skærmbilleder eller lignende dokumentation for hver version af samtykkeløsningen, der er blevet anvendt.

**Brug af cookies og lignende teknologier**

© 2025 Datatilsynet og Digitaliseringsstyrelsen

Eftertryk med kildeangivelse er tilladt

Udgivet af:

Datatilsynet

Carl Jacobsens Vej 35

2500 Valby

T 33 19 32 00

dt@datatilsynet.dk

datatilsynet.dk

og

Digitaliseringsstyrelsen

Landgreven 4

1301 København K

T 33 92 52 00

digst@digst.dk

digst.dk

**Datatilsynet**

Carl Jacobsens Vej 35  
2500 Valby  
T 33 19 32 00  
dt@datatilsynet.dk  
datatilsynet.dk

**Digitaliseringsstyrelsen**

Landgreven 4  
1301 København K  
T 33 92 52 00  
digst@digst.dk  
digst.dk