Digitaliseringsstyrelsen

Guide til virksomheder: Dataetik i anvendelsen af tredjepartstjenester

Tag stilling til jeres deling af brugeres data gennem tredjepartstjenester i fx jeres app eller på jeres hjemmeside.

Tredjepartstjenester på hjemmesider og i apps anvendes typisk til at tilføje komponenter, forbedre designet eller analysere brugeradfærd.

Brug af tredjepartstjenester kan både give brugervenlighed og være omkostningseffektivt. Samtidigt kan det dog indebære en omfattende deling af dine brugeres og kunders data, for at tredjepartstjenesterne fungerer.

Idet en bruger besøger en hjemmeside eller app med integrerede tredjepartstjenester, sendes der typisk data til de eksterne virksomheder, som ejer tjenesten. Nogle tredjepartstjenester indsamler mere omfattende personlige oplysninger, mens andre begrænser sig til anonymiserede eller aggregerede data. Denne datadeling sker ofte automatisk, og kan være uigennemskuelig for brugeren.

Omfattende datadeling

Langt de fleste apps og hjemmesider anvender tredjepartstjenester. En undersøgelse fra Digitaliseringsstyrelsen af over 11.000 danske hjemmesider viser, at 89 pct. anvender en eller flere tredjepartstjenester, og at data deles med især tech-giganter som fx Alphabet (Googles koncern) og Meta.

En anden undersøgelse fra Digitaliseringsstyrelsen af de 25 mest populære gratis spilapps til iPhone viser samtidigt, at alle deler data med Meta, 95 pct. med Alphabet og 40 pct. med TikTok. Brugeren accepterede kun nødvendige vilkår og det understreger, at tredjepartstjenester stadig kan indsamle data, selvom brugere afviser dataindsamling.

Opmærksomheden hos danskerne vokser

Digitaliseringsstyrelsen og Danmarks Statistik har undersøgt danskernes tillid til virksomheders datahåndtering. Her ses det, at 6 ud af 10 har fravalgt et produkt eller en tjeneste pga. bekymring for datahåndtering, og 8 ud af 10 mener, det er vigtigt, at virksomheder tydeligt oplyser, hvis de tjener penge på kundernes persondata.

Dette understreger vigtigheden af, grundigt at overveje valget og implementeringen af de specifikke tredjepartstjenester for både at beskytte dine brugeres og kunders privatliv.

Digitaliseringsstyrelsen

I de følgende tre trin, gennemgås det, hvordan du dataetisk kan tage stilling til anvendelsen af tredjepartstjenester i din virksomhed:

1. Kortlæg hvilke tredjepartstjenester du anvender og hvilken data du deler

Der er stor forskel på tredjepartstjenester, både hvad angår deres anvendelse, men også i, hvordan de teknisk fungerer og de kontraktuelle vilkår, herunder hvem der i sidste ende ejer tjenesterne, og hvor de indsamlede data sendes hen.

Et godt sted at starte er derfor at danne et overblik over, hvilke tredjepartstjenester du anvender, hvilke data der deles, og med hvem.

Hvilke tredjepartstjenester anvender du?

Nogle af de elementer på hjemmesider og apps, hvor tredjepartstjenester oftest anvendes er blandt andet:

- Analysetjenester
  Bruges til at spore og analysere brugeraktivitet
- Cookiebanneret i sig selv
  Bruges til at indhente samtykke til indsamling af data
- Betalingsløsninger
  Bruges til sikre betalinger
- Markedsføring og annoncering
  Bruges til målrettede annoncer
- Integrationer til sociale medier
  Bruges til at tillade login med sociale mediekonti
- Medieafspillere
  Bruges til at integrere videoer, musik og podcasts direkte på hjemmesiden eller appen
- Captcha og sikkerhedsvalidering
  Bruges til at beskytte mod bots og spam
- Live chat og kundesupport
  Bruges til at tilbyde kundeservice direkte på hjemmesiden
- Skrifttyper og ikonbiblioteker
  Bruges til at integrere eksterne skrifttyper og tilføje ikoner uden at hoste dem lokalt
- Layout og skabeloner
  Bruges til at strukturere og designe hjemmesider ved hjælp af prædefinerede skabeloner

- Software Development Kits (SDK) (specifikt for apps)
  Et værktøj som bruges til at bygge apps til en specifik platform eller tjeneste

Desuden anvendes der ofte såkaldte ”tracking pixels” til at dele data med tredjepartstjenester især til analyser på hjemmesider og i apps. Tracking pixels er små, usynlige billeder på en hjemmeside eller app, der anvendes til at spore brugeradfærd, indsamle data som fx IP-adresse, enhedstype og interaktioner. De hjælper oftest med at analysere brugermønstre og målrette reklamer. Pixels har lignende formål som cookies, men der gemmes ikke data direkte på brugerens enhed. Pixels og cookies bruges ofte i samspil med hinanden.

En anden metode, som anvendes til at spore brugeradfærd online er fingerprinting (fingeraftryk). Det er en nyere teknik, der anvendes til at identificere en bruger ved at indsamle oplysninger om deres enhed, som fx browser, skærmopløsning, og operativsystem. Ved at kombinere disse data skabes et unikt "fingeraftryk", der kan bruges til at spore brugeren på tværs af hjemmesider, selv uden cookies. Fingerprinting sker oftest uden brugerens samtykke, og er derfor svært at blokere.

Hvilke data deler du med tredjepartstjenesterne?

Efter at du har dannet dig et overblik over, hvilke tredjepartstjenester din virksomhed anvender på din hjemmeside eller app, kan du undersøge hvilken data, der deles med dine tredjepartstjenester. Nogle af de typer af data, der oftest deles er:

- IP-adresse: Oplysninger om brugerens lokation og enhed, som sendes automatisk ved anmodning om indhold fra tredjepartsservere.

- Reklame-ID: En unik identifikator, som især anvendes på smartphones og bruges til at spore brugernes adfærd til markedsføringsformål uden at afsløre personlige oplysninger.

- Browserinformation: Oplysninger om fx brugerens browser, enhed, styresystem eller platform.

- Besøgs- og adfærdsdata: Information om brugerens adfærd på hjemmesiden eller appen, herunder klikspor og tid brugt på forskellige indholdssider.

- Cookiedata: Informationer gemt i cookies, som kan spore brugeren på tværs af hjemmesider og apps.

- Login-oplysninger til sociale medier: Afhængigt af tilladelse, kan dette inkludere navn, køn og alder, samt oplysninger om venner mv.

- App-version og fejlmeddelelser: Informationer om versionen af brugerens app og hvilke fejl der opleves i anvendelsen.

Hvem deles data med?

Når din virksomhed anvender tredjepartstjenester, kan tjenesten både ejes fra tech-giganter som fx Alphabet (Google), Meta eller Amazon, men den kan også ejes af en mindre virksomhed, som udbyder en service enten gratis eller mod betaling. Selvom du anvender en tjeneste der *ikke* er ejet af en af de store aktører, kan der stadig være risiko for, at data deles med dem. Mange tredjepartstjenester integrerer med større platforme ved hjælp af fx API'er, annonceværktøjer eller hosting. Mange mindre tredjepartstjenester hoster fx deres data og applikationer på cloud-platforme, der ejes af tech-giganterne som fx Amazon Web Services (AWS) eller Google Cloud. Det betyder, at selvom du anvender en mindre tredjepartstjeneste, kan dataene i sidste ende alligevel blive lagret og behandlet hos større aktører. Dermed kan data utilsigtet ende med at blive delt med dem.

Derudover kan nogle tredjepartstjenester vælge at sælge eller dele data som en del af deres forretningsmodel. Dette er særligt udbredt blandt gratis tjenester. Disse tredjepartstjenester agerer dermed datamæglere ved at samle og derefter videresælge data. I sidste ende kan det dermed være svært at spore, hvem der har adgang til dine kunder og brugeres data.

2. Tag dataetisk stilling til dine tredjepartstjenester

Som forbruger er det svært at gennemskue og forholde sig til hvilken data, der indsamles og deles, når man besøger hjemmesider og apps. Hvis du og din virksomhed tager nogleaktive valg, kan I give forbrugerne større tryghed og derigennem styrke jeres brand. Her kan dataetik være en ramme for at afveje forskellige hensyn.

7 overvejelser til dig der bruger tredjepartstjenester

Du kan spørge dig selv:

1. Har du tiltro til de virksomheder, som du deler data med?
   Har du tillid til tredjepartstjenesten, både hvad angår deres anvendelse af den data, du deler med dem, og deres generelle beskyttelse af data.
2. Vedrører den data der deles, særligt udsatte målgrupper?
   Er din virksomheds målgruppe særligt udsatte, herunder fx børn? Udover at sikre, at

Hvad er dataetik?

Dataetik handler om forholdet mellem teknologi og borgernes grundlæggende rettigheder, retssikkerhed og grundlæggende samfundsmæssige værdier, som den teknologiske udvikling giver anledning til at overveje (Kommissorium for Dataetisk Råd 2019).

Det betyder, at dataetik for den enkelte virksomhed handler om at afveje forskellige hensyn, som taler for eller imod en konkret databehandling.

du indhenter samtykke igennem dennes værge/forældre, kan du også overveje, om du bør implementere udvidede tiltag for at beskytte målgruppen.

3. Kan datadelingen begrænses?
   For at beskytte dine kunder og brugere, kan du vælge kun at dele den data, der er nødvendig for, at tredjepartstjenesten kan fungere.
4. Stemmer tredjepartstjenestens dataanvendelse overens med dine egne dataetiske standarder?
   Er tredjepartstjenestens databrug i tråd med din virksomheds etiske retningslinjer og de løfter, du har givet til dine kunder? Du kan gennemgå tjenestens vilkår for at sikre de følger dine egne værdier og principper.
5. Er der alternative tredjepartstjenester med andre vilkår?
   Du kan undersøge, om der findes andre tredjepartstjenester, som kan levere den samme funktionalitet, men under andre betingelser, såsom mindre dataindsamling eller bedre databeskyttelse.
6. Er der behov for en særskilt databehandleraftale?
   Hvis tjenesten involverer behandling af persondata, kan en særskilt databehandleraftale være nødvendig for at sikre, at ansvaret for datahåndtering er klart defineret og ikke utilsigtet anvender dine kunders data.
7. Er tredjepartstjenesten nødvendig for din virksomheds funktionalitet?
   Overvej, om det er nødvendigt for din løsnings funktionalitet at anvende tredjepartstjenesten. Dertil kan det undersøges om der findes interne løsninger, som kan opfylde behovet uden at involvere en tredjepartstjeneste.

   Ovenstående dataetiske overvejelser, skal ikke ses som udtømmende, men som forslag til, hvordan du og din virksomhed, kan vælge at styrke jeres dataetiske tilgang ved anvendelse af tredjepartstjenester. Det kan bidrage til øget gennemsigtighed i forhold til kunder og brugere og samtidigt minimere potentielle risici i forbindelse med datadelingen. Således kan du både imødekomme dine forretningsmæssige behov og samtidig handle dataetisk.

3. Overhold lovgivningen

Du skal sikre, at du overholder lovgivningen i din anvendelse af tredjepartstjenester. Dette er selvom du har taget stilling til, hvordan du agerer dataetisk. I den forbindelse, er der to regelsæt som er særligt relevante: Cookiebekendtgørelsen og GDPR, som begge regulerer datahåndtering, men på forskellige måder.

Digitaliseringsstyrelsen

Cookiebekendtgørelsen regulerer anvendelsen af sporingsteknologier og kræver, at brugere giver et informeret samtykke, før anvendelsen af disse teknologier. Teknisk nødvendige teknologier er dog undtaget for kravet om samtykke.

GDPR omfatter en bredere databeskyttelse og stiller krav til, hvordan persondata behandles af tredjepartstjenester, herunder indhentning af samtykke, gennemsigtighed, dataminimering og formål for dataindsamlingen. I praksis skal du følge begge regelsæt, når du bruger tredjepartstjenester, der både placerer cookies og behandler personoplysninger.

Det anbefales, at du orienterer dig hos de myndigheder, som håndhæver lovgivningen. For cookiebekendtgørelsen, kan du blandt andet orientere dig i artiklen Overhold reglerne for cookies samt på Digitaliseringsstyrelsens temaside om sporingsteknologier. For GDPR, kan du orientere dig i artiklen Sådan behandler og beskytter du personoplysninger eller Datatilsynets vejledning om Cookies og GDPR.