Europa-Kommissionen

Syv trin til virksomheder

for at blive klar til den generelle forordning om databeskyttelse

Retlige Anliggender og Forbrugere

Hvem er vejledningen til?

Formålet med vejledningen er at hjælpe de virksomheder, hvis primære forretningsaktiviteter ikke er behandling af personoplysninger. Det er for eksempel SMV'er, som hovedsageligt behandler personoplysninger om deres medarbejdere, eller som har lister over kunder. Det kan være forhandlere og butikker såsom bagere eller slagtere eller tjenesteudbydere såsom arkitekter. Vejledningen gennemgår de få trin, der er nødvendige for at blive klædt på til at overholde reglerne i den generelle forordning om databeskyttelse.

Personoplysninger er alle oplysninger, som vedrører en fysisk levende person (ikke juridiske enheder). Det er for eksempel: navn, efternavn, hjemmeadresse, e-mailadresse eller lokaliseringsdata fra kortet på en mobiltelefon. Det vil normalt sige de oplysninger, du eventuelt opbevarer om dine medarbejdere, kunder eller leverandører.

Jo færre risici, der er forbundet med personoplysningerne i forbindelse med dine aktiviteter, jo mindre skal du gøre

Anvend centrale principper:

- **indsaml personoplysninger med et klart defineret formål, og brug ikke oplysningerne til noget andet** (hvis du beder kunder om at give dig deres e-mailadresse, så de kan modtage nye tilbud eller kampagner, må du ikke bruge den e-mailadresse til noget andet eller sælge den til en anden virksomhed)
- **indsaml ikke flere oplysninger, end du har brug for** (hvis du leverer varer til en hjemmeadresse, har du f.eks. brug for en adresse og navnet på dørskiltet, men du har ikke brug for at vide, om personen er gift eller ugift). Du skal ganske enkelt være opmærksom på, hvilke personoplysninger du har ansvaret for.

TRIN 1 — KONTROLLÉR DE PERSONOPLYSNINGER, DU INDSAMLER OG BEHANDLER, FORMÅLET MED INDSAMLINGEN OG BEHANDLINGEN SAMT RETSGRUNDLAGET

Hvis du har **medarbejdere**, behandler du deres personoplysninger på baggrund af deres ansættelseskontrakt og på baggrund af retlige forpligtelser (f.eks. indberetninger til skattemyndigheder/sociale ordninger).

Du vedligeholder måske en liste over **individuelle kunder**, for eksempel for at sende meddelelse til dem om særtilbud/reklamer, hvis du har indhentet samtykke fra disse kunder.

Du skal ikke altid indhente et samtykke. Der er tilfælde, hvor enkeltpersoner må forvente, at du behandler deres personoplysninger.

Som pizzabager kan du f.eks. anvende leveringsadressen til at reklamere for et af dine nye produkter. Dette kaldes en legitim interesse. Du skal informere enkeltpersoner om din påtænkte anvendelse og ophøre med at behandle personoplysningerne, hvis de beder dig om det.

Hvis du vedligeholder en liste over **leverandører** eller **erhvervskunder**, gør du det på baggrund af de aftaler, du har med dem. Disse aftaler er ikke nødvendigvis skriftlige.

TRIN 2 — INFORMER DINE KUNDER, MEDARBEJDERE OG ANDRE ENKELTPERSONER, NÅR DU INDSAMLER DERES PERSONOPLYSNINGER

Enkeltpersoner skal vide, at du behandler deres personoplysninger og til hvilket formål.

Der er dog ikke noget behov for at informere enkeltpersoner, hvis de allerede har oplysninger om, hvordan du vil bruge oplysningerne, f.eks. når en kunde anmoder dig om en levering til en hjemmeadresse.

Du skal også efter anmodning informere enkeltpersoner om de personoplysninger, du opbevarer om dem, og give dem adgang til deres oplysninger. Hold styr på oplysningerne, således at du, hvis en medarbejder f.eks. spørger dig, hvilken type oplysninger du har, nemt kan svare uden noget ekstra besvær.

TRIN 3 — OPBEVAR KUN PERSONOPLYSNINGERNE, SÅ LÆNGE DET ER NØDVENDIGT

Oplysninger om dine medarbejdere: så længe ansættelsesforholdet og de dertilhørende retlige forpligtelser varer.

Oplysninger om dine kunder: så længe kundeforholdet og de dertilhørende retlige forpligtelser varer (f.eks. skattemæssige forpligtelser).

Slet dataene, når de ikke længere er nødvendige til det formål, de blev indsamlet til.

TRIN 4 — SØRG FOR SIKKERHEDEN FOR DE PERSONOPLYSNINGER, DU BEHANDLER

Hvis du opbevarer oplysningerne i et **it-system**, skal adgangen til filerne med oplysningerne begrænses, f.eks. med en adgangskode. Systemets sikkerhedsindstillinger skal opdateres regelmæssigt.

(Bemærk, at databeskyttelsesforordningen ikke foreskriver brug af noget specifikt it-system)

Hvis du opbevarer fysiske dokumenter med personoplysninger, skal du sørge for, at uautoriserede personer ikke har adgang til dem. De skal låses inde i et pengeskab eller et skab.

TRIN 5 — OPBEVAR DOKUMENATION OM DINE DATABEHANDLINGSAKTIVITETER

Udarbejd et kort dokument, der redegør for de personoplysninger, du opbevarer, og årsagen til det. Du kan blive afkrævet at stille dokumentationen til rådighed for den nationale datatilsynsmyndighed, når denne anmoder om det.

Disse dokumenter bør indeholde de oplysninger, der er anført herunder.

INFORMATION	EKSEMPLER
Formålet med databehandling	Fortælle kunder om særtilbud/tilbyde levering til en hjemmeadresse, betaling af leverandører, løn og sociale sikringsydelser til medarbejdere
Typer af personoplysninger	Kunders kontaktoplysninger, leverandørers kontaktoplysninger, medarbejderes personoplysninger
Kategorier af berørte registrerede	Medarbejdere, kunder, leverandører
Kategorier af modtagere	Arbejdsmyndigheder, skattemyndigheder
Opbevaringsperioder	Medarbejderes personoplysninger skal opbevares, indtil udløbet af ansættelseskontrakten (og tilhørende retlige forpligtelser), kunders personoplysninger skal opbevares, indtil kunde-/aftaleforholdet ophører
De tekniske og organisatoriske sikkerhedsforanstaltninger til beskyttelse af personoplysningerne	It-systemer skal opdateres løbende, aflåst skab/pengeskab
Oplysning om, hvorvidt personoplysningerne overføres til modtagere uden for EU	Brug af databehandling uden for EU (f.eks. lagring af data i skyen)

TRIN 6 — SØRG FOR, AT DINE UNDERLEVERANDØRER OVERHOLDER REGLERNE

Hvis du udliciterer behandling af personoplysninger til en anden virksomhed, skal du kun bruge en tjenesteudbyder, som garanterer en behandling, der overholder kravene i databeskyttelsesforordningen (f.eks. sikkerhedsforanstaltninger). Før du indgår en kontrakt, skal du kontrollere, om de allerede har ændret og tilpasset deres procedurer til databeskyttelsesforordningen. Skriv det ind i kontrakten.

TRIN 7 — TJEK, HVIS DU HAR SPØRGSMÅL OM BESTEMMELSERNE HERUNDER

> For bedre at beskytte personoplysninger kan det være nødvendigt for virksomheder at udpege en databeskyttelsesrådgiver. **Det er dog ikke obligatorisk at udpege en databeskyttelsesrådgiver**, hvis behandling af personoplysninger ikke er en central aktivitet i din forretning, ikke er en risikofyldt behandling, og aktiviteten ikke er i stor skala.

Hvis din forretning f.eks. kun indsamler oplysninger om kunder med henblik på levering på deres hjemmeadresse, behøver du ikke udpege en databeskyttelsesrådgiver.

Hvis du skal udpege en databeskyttelsesrådgiver, kan det være en eksisterende medarbejder, der får denne opgave ud over vedkommendes øvrige opgaver. Det kan også være en ekstern konsulent, på samme måde som mange organisationer benytter eksterne rådgivere.

> **Du vil normalt ikke være pålagt at foretage en databeskyttelsesvurdering**

Organisationer, der bringer personoplysninger i fare, skal foretage en databeskyttelsesvurdering, f.eks. hvis de i stort omfang foretager overvågning af et offentligt tilgængeligt område (såsom videoovervågning).

Hvis du er en mindre virksomhed, der varetager medarbejderes løn og en kundeliste, behøver du ikke foretage en databeskyttelsesvurdering for disse operationer.

Bøder

Datatilsynsmyndigheder har bemyndigelse til at sanktionere overtrædelser af databeskyttelsesreglerne. De kan vedtage korrigerende foranstaltninger (såsom en ordre eller midlertidig suspension af behandlingen) og/eller pålægge en bøde.

Deres afgørelse om at pålægge en bøde skal stå i rimeligt forhold til overtrædelsen og være baseret på en vurdering af alle omstændighederne ved den enkelte sag.

Hvis de beslutter at pålægge en bøde, afhænger bødens størrelse også af sagens omstændigheder, herunder hvor alvorlig overtrædelsen er, samt om overtrædelsen er forsætlig eller uagtsom. De tager desuden din holdning og dine intentioner i betragtning.

Hvis du ønsker flere oplysninger:

1. **Gå ind på Europa-Kommissionens internetvejledning om reformen af databeskyttelsesreglerne — den er tilgængelig på alle EU-sprog:**

   europa.eu/dataprotection/da

2. **Kontakt den nationale databeskyttelsesmyndighed:**

   edpb.europa.eu/about-edpb/board/members_da

VIGTIG MEDDELELSE

Formålet med oplysningerne i denne vejledning er er at give en bedre forståelse af EU's databeskyttelsesregler.

Den er udelukkende ment som en vejledning – det er kun teksten i den generelle forordning om databeskyttelse, der har retlig gyldighed. Det er derfor kun den generelle forordning om databeskyttelse, der kan indebære rettigheder og forpligtelser for enkeltpersoner. Denne vejledning indebærer ingen rettigheder eller krav, der kan håndhæves.

EU-Domstolen har enekompetence til bindende fortolkning af EU-retten. De holdninger, der gives udtryk for i denne vejledning, har ingen indflydelse på den holdning, som Europa-Kommissionen måtte antage foran EU-Domstolen.

Hverken Europa-Kommissionen eller en person, der handler på vegne heraf, kan drages til ansvar for brug af oplysningerne i vejledningen.

Da dette dokument afspejler den tilgængelige viden på tidspunktet for udarbejdelsen, skal det anses for at være et dokument i udvikling, som løbende kan forbedres, og indholdet kan ændres uden varsel.

Publikationskontoret

Luxembourg: Den Europæiske Unions Publikationskontor, 2018

Print	PDF
ISBN 978-92-79-85375-3	ISBN 978-92-79-85392-0
doi:10.2838/627113	doi:10.2838/868153
DS-02-18-544-DA-C	DS-02-18-544-DA-N