Europa-Kommissionen

Den generelle forordning om databeskyttelse: nye muligheder, nye forpligtelser

Alt, hvad enhver virksomhed behøver at vide om EU's generelle forordning om databeskyttelse

Retlige Anliggender og Forbrugere

Printed by Bietlot in Belgium

Luxembourg: Den Europæiske Unions Publikationskontor, 2018

Print	ISBN 978-92-79-79422-3	doi:10.2838/592942	DS-01-18-082-DA-C
PDF	ISBN 978-92-79-79450-6	doi:10.2838/75901	DS-01-18-082-DA-N

INDHOLD

KAPITEL 1

EN FORRETNINGSMULIGHED

Den generelle forordning om databeskyttelse regulerer, hvordan virksomheder skal behandle og forvalte personoplysninger. Den træder i kraft den 25. maj 2018 og gælder for alle virksomheder og organisationer (f.eks. hospitaler, offentlige forvaltninger osv.). Det er den største ændring af EU's databeskyttelsesregler i over 20 år.

Den generelle forordning om databeskyttelse giver ikke blot borgerne bedre kontrol med, hvordan deres personoplysninger anvendes. Den harmoniserer i høj grad også de lovgivningsmæssige rammer for virksomheder. Det sker ved at oprette en ensartet ramme for databeskyttelseslovgivning i hele EU. I stedet for at hvert land har sine egne databeskyttelseslove, er hele EU med andre ord nu underlagt en enkelt forordning. En virksomhed, der er aktiv i forskellige lande, behøver således ikke længere at overholde flere — ofte forskellige — regelsæt. Den skal nu alene overholde den generelle forordning om databeskyttelse for at tilbyde dens tjenester i hele EU.

Hvordan kan jeres virksomhed få gavn af den generelle forordning om databeskyttelse?

- **Én union, én lovgivning:** Et enkelt sæt regler gør det enklere og billigere for virksomheder at drive forretning i EU.
- **Et enkelt kontaktpunkt:** I de fleste tilfælde skal virksomheder kun være i kontakt med én datatilsynsmyndighed.
- **Europæiske regler på europæisk jord:** Virksomheder, der er etableret uden for EU, skal anvende de samme regler som europæiske virksomheder, når de tilbyder deres varer eller tjenesteydelser til fysiske personer i EU.
- **Risikobaseret tilgang:** Den generelle forordning om databeskyttelse går udenom en besværlig »one-size-fits-all«-forpligtelse og tilpasser i stedet forpligtelser i henhold til de respektive risici.
- **Regler, der passer til innovation:** Den generelle forordning om databeskyttelse er teknologineutral.

Det handler om tillid

Beskyttelse af personoplysninger er en stor bekymring for mange mennesker. Deres tillid til digitale miljøer er derfor fortsat lav. Af en Eurobarometerundersøgelse fremgår det:

- at otte ud af ti mennesker ikke føler, de har fuldstændig kontrol over deres personoplysninger
- at seks ud af ti siger, at de ikke har tillid til internetvirksomheder
- at over 90 % af europæerne siger, at de ønsker samme databeskyttelsesrettigheder i alle EU-landene.

»Virksomheder, som ikke i passende grad beskytter fysiske personers personoplysninger, risikerer at miste forbrugernes tillid, som er afgørende for at tilskynde mennesker til at anvende nye produkter og tjenesteydelser.«

Den generelle forordning om databeskyttelse er en ny mulighed for jeres virksomhed for at øge forbrugernes tillid gennem risikobaseret forvaltning af personoplysninger.

KAPITEL 2

OVERBLIK OVER DEN GENERELLE FORORDNING OM DATABESKYTTELSE

Gælder den generelle forordning om databeskyttelse for jer?

Kort sagt gælder den generelle forordning om databeskyttelse for ***alle*** virksomheder, der:

behandler personoplysninger ved hjælp af **automatisk** eller **manuel** behandling (forudsat at dataene er struktureret i henhold til kriterier).

Selv om jeres virksomhed alene behandler data på vegne af andre virksomheder, skal I stadig overholde reglerne.

Den generelle forordning om databeskyttelse gælder, hvis:

- jeres virksomhed behandler personoplysninger og er etableret i EU, uanset hvor den faktiske databehandling finder sted, eller
- jeres virksomhed er etableret uden for EU, men tilbyder varer eller tjenesteydelser eller overvåger fysiske personers adfærd i EU.

Hvad er personoplysninger?

Personoplysninger er alle oplysninger, der vedrører en identificeret eller identificerbar levende fysisk person. Disse oplysninger kan omfatte:

- navn
- adresse og telefonnummer
- placering
- sundhedsjournaler
- oplysninger om indtægter og bankoplysninger
- kulturelle præferencer
- ... med mere.

Personoplysninger, der er blevet afidentificeret eller pseudonymiseret, men som stadig kan anvendes til at identificere en person, falder også under den generelle forordning om databeskyttelses anvendelsesområde.

Personoplysninger, som uigenkaldeligt er gjort anonyme på en sådan måde, at personen ikke længere kan identificeres, anses ikke for at være personoplysninger og er derfor ikke omfattet af den generelle forordning om databeskyttelse.

Den generelle forordning om databeskyttelse er desuden teknologineutral, dvs. at den beskytter personoplysninger, uanset hvilken teknologi der anvendes, og uanset hvordan personoplysningerne opbevares. Uanset om jeres virksomhed behandler og opbevarer personoplysninger ved hjælp af et komplekst IT-system eller via papirbaserede arkiver, er I underlagt den generelle forordning om databeskyttelse.

»Uanset om jeres virksomhed behandler og opbevarer personoplysninger ved hjælp af et komplekst IT-system eller via papirbaserede arkiver, er I underlagt den generelle forordning om databeskyttelse.«

Vær ekstra opmærksom på særlige (følsomme) kategorier af personoplysninger

Hvis de personoplysninger, I indhenter, omfatter oplysninger om en fysisk persons helbred, race, seksuel orientering, religion, politisk overbevisning eller medlemskab af faglige organisationer, anses de for følsomme. Jeres virksomhed må kun behandle disse oplysninger under særlige omstændigheder, og I bliver eventuelt nødt til at indføre yderligere sikkerhedsforanstaltninger, såsom kryptering.

Hvad omfatter behandling af personoplysninger?

I henhold til den generelle forordning om databeskyttelse er handlinger såsom indhentning, anvendelse og sletning af personoplysninger omfattet af definitionen på behandling af personoplysninger.

Overvåger I jeres faciliteter med overvågningskameraer? Slår I op i en database med personoplysninger i forbindelse med jeres forretning? Sender I reklame-e-mails? Sletter I (digitale) medarbejderregistre, eller makulerer I dokumenter? Lægger I et billede af en person op på jeres hjemmeside eller på sociale medier?

Hvis I svarede »ja« til et af disse spørgsmål, behandler jeres virksomhed afgjort personoplysninger.

Hvordan bidrager den generelle forordning om databeskyttelse til at spare omkostninger?

Den generelle forordning om databeskyttelse tager hensyn til virksomhedernes behov. Forordningen har f.eks. til formål at fjerne administrative krav for at reducere omkostninger og minimere den administrative byrde:

- **Ikke flere forudgående anmeldelser:** Reformen afskaffer de fleste forudgående anmeldelser til tilsynsmyndigheder og de dermed forbundne omkostninger.
- **Databeskyttelsesrådgivere:** Virksomheder skal hovedsageligt udpege en databeskyttelsesrådgiver, hvis deres kerneaktiviteter omfatter behandling af følsomme oplysninger i stor skala eller inkluderer omfattende, regelmæssig og systematisk overvågning af fysiske personer. Offentlige forvaltninger skal udpege en databeskyttelsesrådgiver.
- **Konsekvensanalyse vedrørende databeskyttelse:** Virksomheder skal kun udføre en konsekvensanalyse vedrørende databeskyttelse, hvis de har til hensigt at foretage en databehandlingsaktivitet, der indebærer høj risiko for enkeltpersoners rettigheder og frihedsrettigheder.
- **Fortegnelser:** Virksomheder med mindre end 250 medarbejdere er ikke forpligtet til at føre fortegnelser, medmindre databehandling ikke er tilfældig, eller den omfatter følsomme oplysninger.

»Forordningen har til formål at fjerne administrative krav for at reducere omkostninger og minimere den administrative byrde.«

KAPITEL 3

JERES FORPLIGTELSER IFØLGE DEN GENERELLE FORORDNING OM DATABESKYTTELSE

Den generelle forordning om databeskyttelse tillægger virksomheder direkte forpligtelser vedrørende databehandling, der gælder for hele EU. I medfør af den generelle forordning om databeskyttelse må en virksomhed *kun* behandle personoplysninger under visse betingelser. Behandlingen skal f.eks. være rimelig og gennemsigtig, ske med henblik på et bestemt og legitimt formål og være begrænset til de oplysninger, der er nødvendige for at opfylde dette formål. Behandlingen skal også være baseret på et af følgende retsgrundlag:

- **samtykke** fra den berørte fysiske person
- en **kontraktlig forpligtelse** mellem jer og den fysiske person
- opfyldelse af en **retlig forpligtelse**
- beskyttelse af en fysisk persons **vitale interesser**
- udførelse af en **opgave, som er i samfundets interesse**
- i forbindelse med virksomhedens **lovlige interesser**, men kun efter at have kontrolleret, at det ikke i væsentlig grad påvirker rettigheder og frihedsrettigheder for den fysiske person, hvis oplysninger behandles. Hvis personens rettigheder går forud for jeres interesser, må I ikke behandle oplysningerne.

Fokus: indhentning af samtykke til at anvende personoplysninger

Den generelle forordning om databeskyttelse anvender strenge regler for behandling af oplysninger baseret på samtykke. Formålet med reglerne er at sikre, at den fysiske person forstår, hvad han eller hun giver sit samtykke til. Det betyder, at samtykket skal afgives **frivilligt, specifikt, informeret** og **utvetydigt** i form af en anmodning fremsat i et klart og enkelt sprog. Samtykket skal desuden gives i form af en **klar bekræftelse**, såsom at afkrydse et felt på en internetside eller underskrive en formular.

Hvis I behandler personoplysninger vedrørende et **barn** baseret på et samtykke, er forældrenes samtykke obligatorisk. Eftersom aldersgrænsen er mellem 13 og 16 år afhængigt af land, anbefales det, at I konsulterer national lovgivning.

»Husk! Hvis en person giver samtykke til behandling af vedkommendes personoplysninger, må I kun behandle oplysningerne i forbindelse med de formål, samtykket blev givet til. I skal desuden give personen mulighed for at trække sit samtykke tilbage.«

Fastsættelse af jeres rolle og ansvar

Når I har afgjort, at den generelle forordning om databeskyttelse finder anvendelse på jeres forretningsaktiviteter, og at der finder behandling af personoplysninger sted, er næste skridt at fastslå jeres rolle.

Databeskyttelsesreglerne skelner mellem dataansvarlig og databehandler, og der gælder forskellige forpligtelser for de to. Den dataansvarlige fastlægger formål og hjælpemidler i forbindelse med behandling af personoplysninger, hvorimod databehandleren alene behandler personoplysninger på vegne af den dataansvarlige. Det betyder dog ikke, at databehandleren blot kan skjule sig bag den dataansvarlige.

Den generelle forordning om databeskyttelse kræver, at den dataansvarlige kun må benytte en databehandler, der stiller tilstrækkelige garantier. Disse garantier skal fremgå af en skriftlig aftale mellem den dataansvarlige og databehandleren. Denne aftale skal også indeholde en række obligatoriske bestemmelser, herunder bl.a. en bestemmelse om, at databehandleren kun behandler personoplysninger efter dokumenteret instruks fra den dataansvarlige.

Forpligtelser, der beskytter fysiske personers rettigheder

Den generelle forordning om databeskyttelse omfatter en række forpligtelser, der har til formål at beskytte en fysisk persons ret til at have kontrol over sine egne personoplysninger.

Jeres forpligtelse: at tilbyde gennemsigtige oplysninger

Virksomheder skal tilbyde fysiske personer oplysninger om, hvem der behandler hvad og hvorfor. Oplysningerne skal tydeligt som minimum oplyse:

- hvem I er
- hvorfor I behandler oplysningerne
- på hvilket retsgrundlag
- hvem der modtager oplysningerne (hvis det er relevant).

I nogle tilfælde skal oplysningerne også angive:

- kontaktoplysninger for databeskyttelsesrådgiveren
- den legitime interesse (når den legitime interesse er retsgrundlaget for behandling)
- grundlaget for overførsel af oplysninger til et land uden for EU
- hvor længe oplysningerne bliver opbevaret
- fysiske personers databeskyttelsesrettigheder (dvs. retten til indsigt, berigtigelse, sletning, begrænsning, indsigelse, portabilitet osv.)
- hvordan samtykket kan tilbagetrækkes (når samtykket er retsgrundlaget for behandling)
- om der er en lovmæssig eller aftalemæssig forpligtelse til at meddele oplysningerne
- når der er tale om automatiske afgørelser, oplysninger om logikken i afgørelsen, betydningen og konsekvenserne af afgørelsen.

»Virksomheder skal tilbyde fysiske personer oplysninger om, hvem der behandler hvad og hvorfor.«

Jeres forpligtelse: retten til indsigt og retten til dataportabilitet

Fysiske personer har ret til at bede om at få indsigt i deres personoplysninger uden beregning og i et format, de kan bruge. Hvis I modtager en sådan anmodning, skal I:

- fortælle den fysiske person, om I behandler vedkommendes personoplysninger
- informere vedkommende om behandlingen (bl.a. om formålet med behandlingen, kategorier af berørte personoplysninger, hvem der modtager oplysningerne osv.)
- udlevere en kopi af de personoplysninger, der bliver behandlet.

Derudover kan den fysiske person, når behandlingen er baseret på samtykke eller en aftale, anmode om, at personoplysningerne tilbageleveres eller overføres til et andet selskab. Dette kaldes retten til dataportabilitet. Oplysningerne skal meddeles i et almindeligt anvendt og maskinlæsbart format.

Selv om disse to rettigheder hænger tæt sammen, er der tale om to særskilte rettigheder. I skal derfor sørge for, at der ikke sker sammenblanding af de to rettigheder, og oplyse den fysiske person i overensstemmelse hermed.

Jeres forpligtelse: retten til sletning (retten til at blive glemt)

I nogle tilfælde kan en fysisk person anmode den dataansvarlige om at slette vedkommendes personoplysninger, såsom når der ikke længere er behov for oplysningerne til at opfylde formålet med databehandlingen. Jeres virksomhed er imidlertid ikke forpligtet til at efterkomme en anmodning fra en fysisk person, hvis:

- behandlingen er nødvendig for at respektere ytrings- og informationsfriheden
- I skal opbevare personoplysningerne for at opfylde en retlig forpligtelse
- andre hensyn til samfundsinteresser berettiger til at opbevare personoplysningerne, såsom folkesundhed eller videnskabelige eller historiske forskningsformål
- I er nødt til at opbevare personoplysningerne for at gøre et retskrav gældende.

Jeres forpligtelse: retten til berigtigelse og retten til at gøre indsigelse

Hvis en fysisk person mener, at vedkommendes personoplysninger er forkerte, ufuldstændige eller unøjagtige, har vedkommende ret til at få dem berigtiget eller fuldstændiggjort uden unødig forsinkelse.

En fysisk person kan også til enhver tid gøre indsigelse mod behandling af vedkommendes personoplysninger til et bestemt formål, hvis virksomheden behandler dem på baggrund af dens legitime interesse eller med henblik på udførelse af en opgave i samfundets interesse. Medmindre I har en legitim interesse, der går forud for den fysiske persons interesse, skal I ophøre med at behandle personoplysningerne. En fysisk person kan ligeledes anmode om, at behandlingen af vedkommendes personoplysninger begrænses, mens det afgøres, om jeres legitime interesse går forud for den fysiske persons interesse. For så vidt angår direkte markedsføring er I dog altid forpligtede til at ophøre med behandlingen af personoplysninger efter anmodning fra den fysiske person.

En advarsel om automatiske afgørelser og profilering

Fysiske personer har ret til ikke at blive genstand for en afgørelse, der alene er truffet på grundlag af automatisk behandling. Der er imidlertid nogle undtagelser fra denne regel, såsom når den fysiske person eksplicit har givet sit samtykke til automatiske afgørelser. Medmindre automatiske afgørelser er baseret på en lov, skal jeres virksomhed:

- underrette den fysiske person om de automatiske afgørelser
- give den fysiske person ret til at få den automatiske afgørelse gennemgået af en person
- give den fysiske person mulighed for at bestride den automatiske afgørelse.

Hvis f.eks. en bank automatisk træffer afgørelse om, hvorvidt den vil give en bestemt fysisk person et lån, skal den pågældende person underrettes om den automatiske afgørelse og have mulighed for at bestride afgørelsen og anmode om menneskelig medvirken.

Forpligtelser baseret på risici

Ud over de forpligtelser, der har til formål at beskytte fysiske personers rettigheder, indeholder den generelle forordning om databeskyttelse også en række forpligtelser, hvor anvendelsen af dem afhænger af risikoen.

Jeres forpligtelse: udpegning af en databeskyttelsesrådgiver

En databeskyttelsesrådgiver er ansvarlig for at føre tilsyn med, om I overholder den generelle forordning om databeskyttelse. En af databeskyttelsesrådgiverens vigtigste opgaver er at informere og rådgive medarbejdere, der udfører den faktiske behandling af personoplysninger, om deres forpligtelser. Databeskyttelsesrådgiveren samarbejder desuden med datatilsynsmyndigheden og fungerer som kontaktpunkt mellem datatilsynsmyndigheden og de fysiske personer.

Virksomheden er forpligtet til at udpege en databeskyttelsesrådgiver, når:

- den regelmæssigt og systematisk overvåger fysiske personer eller behandler særlige kategorier af oplysninger
- behandlingen er en central forretningsaktivitet, og
- den gør det i stort omfang.

Hvis I f.eks. behandler personoplysninger for at målrette markedsføring gennem søgemaskiner baseret på menneskers adfærd på internettet, er det et krav i den generelle forordning om databeskyttelse, at I udpeger en databeskyttelsesrådgiver. Hvis I derimod kun sender reklamemateriale til jeres kunder én gang om året, behøver I ikke udpege en databeskyttelsesrådgiver. Hvis der er tale om et lægehus, der indsamler oplysninger om patienters helbred, er der sandsynligvis heller ikke behov for en databeskyttelsesrådgiver. Hvis I derimod behandler personoplysninger om genetik og helbred for et hospital, skal I udpege en databeskyttelsesrådgiver.

Jeres forpligtelse: databeskyttelse gennem design og standardindstillinger

Den generelle forordning om databeskyttelse indfører to nye principper: databeskyttelse gennem design og databeskyttelse gennem standardindstillinger.

Databeskyttelse gennem design hjælper med at sikre, at en virksomhed tager højde for databeskyttelse i de tidlige faser i planlægningen af en ny metode til at behandle personoplysninger. I henhold til dette princip skal den dataansvarlige træffe alle nødvendige tekniske og organisatoriske skridt til at gennemføre databeskyttelsesprincipperne og beskytte fysiske personers rettigheder. Disse skridt kan for eksempel omfatte brug af pseudonymisering.

Databeskyttelse gennem design minimerer risici vedrørende privatlivets fred og øger tilliden. Ved at fokusere på databeskyttelse i udviklingen af nye varer og tjenesteydelser er det muligt at forebygge alle eventuelle problemer om databeskyttelse på et tidligt tidspunkt. Denne praksis hjælper desuden med at øge opmærksomheden på databeskyttelse på tværs af alle afdelinger og niveauer i en virksomhed.

Databeskyttelse gennem standardindstillinger skal sikre, at virksomheden altid anvender de indstillinger, der beskytter privatlivets fred mest muligt, som standardindstillinger. Hvis der for eksempel er to mulige indstillinger for datafortrolighed, og en af indstillingerne forhindrer andre i at få adgang til personoplysningerne, skal denne anvendes som standardindstilling.

»Databeskyttelse gennem design minimerer risici vedrørende privatlivets fred og øger tilliden.«

»Databeskyttelse gennem standardindstillinger skal sikre, at virksomheden altid anvender de indstillinger, der beskytter privatlivets fred mest muligt, som standardindstillinger.«

Jeres forpligtelse: at give en passende meddelelse i tilfælde af brud på persondatasikkerheden

Der er tale om et brud på persondatasikkerheden, når de personoplysninger, som I har ansvaret for, videregives, enten ved et hændeligt uheld eller ulovligt, til uautoriserede modtagere, eller hvis de gøres midlertidigt utilgængelige eller bliver ændret.

Det er afgørende for en virksomhed at indføre passende tekniske og organisatoriske foranstaltninger for at undgå brud på persondatasikkerheden. Skulle der forekomme brud på persondatasikkerheden, og bruddet udgør en risiko for fysiske personers rettigheder og frihedsrettigheder, skal I dog underrette datatilsynsmyndigheden inden for 72 timer, efter I er blevet bekendt med bruddet.

Afhængigt af, om bruddet på persondatasikkerheden udgør en høj risiko for de berørte parter, kan en virksomhed også være forpligtet til at underrette alle berørte fysiske personer om bruddet på persondatasikkerheden.

Overførsler af personoplysninger uden for EU

Den generelle forordning om databeskyttelse finder anvendelse på Det Europæiske Økonomiske Samarbejdsområde (EØS), som omfatter alle EU-landene samt Island, Liechtenstein og Norge. Når personoplysninger overføres uden for EØS, følger beskyttelsen i den generelle forordning om databeskyttelse oplysningerne. Det betyder, at når virksomheder eksporterer oplysninger til udlandet, skal de sikre, at der er indført visse sikkerhedsforanstaltninger.

Den generelle forordning om databeskyttelse indeholder et bredt sæt af værktøjer og mekanismer ved overførsel af oplysninger til tredjelande. I henhold til den generelle forordning om databeskyttelse er sådanne overførsler tilladt, når:

1. EU anser landets beskyttelse for passende
2. virksomheden for eksempel træffer de nødvendige foranstaltninger for at stille passende garantier, såsom ved at medtage specifikke bestemmelser i den aftale, der indgås med importøren af personoplysninger uden for EU, eller
3. virksomheden for eksempel henholder sig til særlige grunde for overførslen (kaldet »undtagelser«), såsom samtykke fra den fysiske person.

Der er flere oplysninger om de regler, der finder anvendelse på internationale dataoverførsler, i Europa-Kommissionens meddelelse om udveksling og beskyttelse af personoplysninger i en globaliseret verden: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017DC0007&from=EN

Skal I gennemføre en konsekvensanalyse vedrørende databeskyttelse?

Det er obligatorisk at udføre en konsekvensanalyse vedrørende databeskyttelse, når behandlingen sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder. Det kan for eksempel forekomme, når der anvendes nye teknologier.

I henhold til den generelle forordning om databeskyttelse forekommer en sådan høj risiko som minimum, når:

- mekanismer til automatisk behandling og profilering anvendes til systematisk og omfattende at evaluere fysiske personer
- et offentligt tilgængeligt område systematisk overvåges i stort omfang (f.eks. overvågningskameraer)
- følsomme oplysninger behandles i stort omfang (f.eks. sundhedsoplysninger).

Formålet med konsekvensanalysen vedrørende databeskyttelse er at afdække eventuelle risici for fysiske personers rettigheder og friheder, før behandlingen af personoplysninger påbegyndes, og før risikoen opstår. Ved at afhjælpe risikoen på forhånd kan skader forebygges, og omkostninger kan minimeres.

Hvis alle afdækkede risici ikke fjernes med den foranstaltning, der fremgår af konsekvensanalysen vedrørende databeskyttelse, skal datatilsynsmyndigheden høres, før den påtænkte databehandling finder sted.

»Det er obligatorisk at udføre en konsekvensanalyse vedrørende databeskyttelse, når behandlingen sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder.«

Hvad skal I gøre?

Imødekommelse af anmodninger

Hvis virksomheden modtager en anmodning fra en fysisk person, der ønsker at udøve sine rettigheder, skal I imødekomme anmodningen uden unødig forsinkelse og under alle omstændigheder inden for en måned efter modtagelse af anmodningen. Svartiden kan dog forlænges til to måneder i forbindelse med komplekse anmodninger eller anmodninger, der indeholder flere anmodninger, såfremt den fysiske person underrettes om forlængelsen. Anmodninger skal desuden behandles **uden beregning**. Hvis en anmodning afvises, skal I informere den fysiske person om årsagerne til dette og om dennes ret til at klage til datatilsynsmyndigheden.

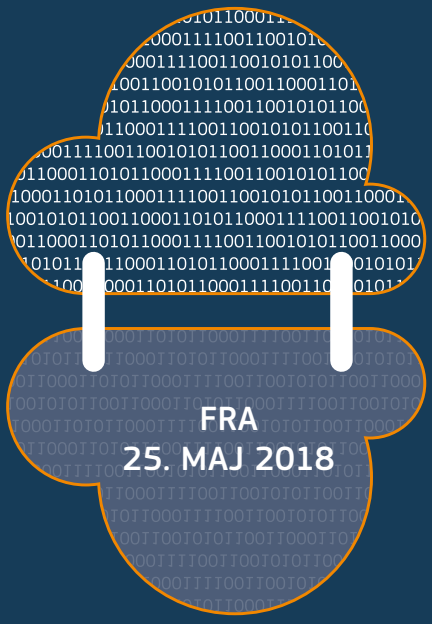
Dokumentation for overholdelse og registrering!

Et af de centrale principper i den generelle forordning om databeskyttelse er at sikre, at virksomheder kan dokumentere, at de overholder reglerne. Det betyder, at I skal kunne dokumentere, at virksomheden handler i overensstemmelse med den generelle forordning om databeskyttelse og opfylder alle gældende forpligtelser — navnlig efter anmodning fra eller kontrol foretaget af datatilsynsmyndigheden.

Dette kan gøres ved at føre detaljerede registre om bl.a.:

- navn og kontaktoplysninger på den del af forretningen, der beskæftiger sig med databehandling
- årsag(er) til behandling af personoplysninger
- beskrivelse af de kategorier af fysiske personer, som leverer personoplysninger
- kategorier af organisationer, som modtager personoplysningerne
- overførsel af personoplysninger til et andet land eller en anden organisation
- opbevaringsperiode for personoplysninger
- beskrivelse af de sikkerhedsforanstaltninger, der anvendes ved behandling af personoplysninger.

Virksomheden skal desuden vedligeholde — og regelmæssigt ajourføre — skriftlige procedurer og vejledninger og formidle dem til medarbejderne.



KAPITEL 4

ER I KLAR TIL AT OVERHOLDE REGLERNE?

For så vidt angår behandling af personoplysninger lægger den generelle forordning om databeskyttelse ansvaret over til jer. Det er så at sige jer, der har bolden. Som første skridt skal I kortlægge de nuværende databehandlingsaktiviteter og evaluere de interne forretningsgange igen. I skal navnlig:

- udpege de oplysninger, I opbevarer, og formålet hermed, samt på hvilket retsgrundlag I opbevarer dem
- vurdere alle indgåede aftaler, navnlig mellem dataansvarlige og databehandlere
- evaluere alle tilgængelige muligheder for internationale overførsler og
- gennemgå virksomhedens overordnede styring (dvs. hvilke IT-foranstaltninger og organisatoriske foranstaltninger der er indført), herunder om I har pligt til eller ønsker at udpege en databeskyttelsesrådgiver.

Et grundlæggende element i denne proces er at sikre, at virksomhedens øverste ledelse er involveret i gennemgangen, kommer med indmeldinger og regelmæssigt holdes ajour og bliver hørt om ændringer i datapolitikken.

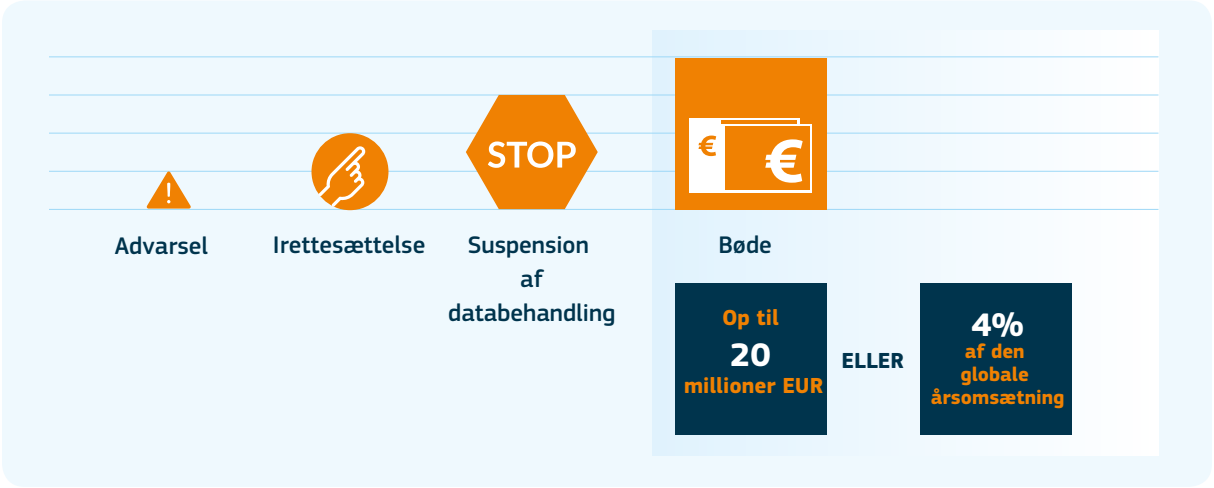
Behandler I oplysninger i mere end ét land?

I forbindelse med grænseoverskridende behandling kan en tilsynsmyndighed i et andet land, og ikke den nationale datatilsynsmyndighed, være den kompetente myndighed. Det vil normalt være datatilsynsmyndigheden i det land i EU, hvor jeres virksomheds hovedkvarter er etableret (hvor beslutninger om metoder til og formål med behandling træffes).

Risici ved manglende overholdelse

Manglende overholdelse af den generelle forordning om databeskyttelse kan medføre store bøder — op til 20 mio. EUR eller 4 % af virksomhedens globale omsætning for visse overtrædelser. Datatilsynsmyndigheden kan pålægge yderligere korrigerende foranstaltninger såsom krav om, at behandling af personoplysninger indstilles. I bør også overveje skader på virksomhedens omdømme i forbindelse med manglende overholdelse.

Omkostningerne ved ikke at overholde den generelle forordning om databeskyttelse er tydeligvis langt større end investeringerne i at overholde den.



Har I spørgsmål? Har I bekymringer? I så fald skal I kontakte den nationale datatilsynsmyndighed.

De nationale datatilsynsmyndigheder kan findes her:

http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm

VIGTIG MEDDELELSE

Formålet med oplysningerne og vejledningen i denne folder 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 brugen af oplysningerne i denne folder.

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

Sådan kontakter du EU

Personligt

Der findes flere hundrede Europe Direct-informationscentre i hele EU. Find dit nærmeste center på: https://europa.eu/european-union/contact_da

Pr. telefon eller e-mail

Europe Direct er en tjeneste, der besvarer spørgsmål om EU. Kontakt Europe Direct:
– på gratisnummer: 00 800 6 7 8 9 10 11 (visse operatører tager betaling for disse opkald)
– på følgende nummer: +32 22999696 eller
– pr. e-mail: https://europa.eu/european-union/contact_da

Sådan finder du oplysninger om EU

Online

Oplysninger om EU er tilgængelige på alle EU's officielle sprog på Europawebstedet: https://europa.eu/european-union/index_da

EU-publikationer

Du kan downloade eller bestille EU-publikationer gratis eller mod betaling fra EU Bookshop på: https://publications.europa.eu/bookshop. Du kan bestille flere eksemplarer af de gratis publikationer ved at kontakte Europe Direct eller dit lokale informationscenter (se https://europa.eu/european-union/contact_da).

EU-ret og relaterede dokumenter

Du kan nemt få adgang til EU's juridiske oplysninger (herunder al EU-ret siden 1952) på alle officielle EU-sprog på EUR-Lex: http://eur-lex.europa.eu

Åbne data fra EU

EU's portal for åbne data (http://data.europa.eu/euodp/da) giver adgang til datasæt fra EU. Dataene kan downloades og genanvendes gratis til både kommercielle og ikkekommercielle formål.

DS-01-18-082-DA-C

Den generelle forordning om databeskyttelse regulerer, hvordan virksomheder behandler og forvalter personoplysninger. Med et enkelt europæisk regelsæt for beskyttelse af personoplysninger skal jeres virksomhed nu primært overholde én lovgivning om databeskyttelse, når I tilbyder varer og tjenesteydelser i EU.

Ved at forenkle de lovgivningsmæssige rammer for virksomheder giver den generelle forordning om databeskyttelse jeres virksomhed mulighed for at forbedre behandlingen af personoplysninger og dermed øge forbrugernes tillid til jeres virksomhed.

Folderen gennemgår jeres virksomheds forpligtelser i medfør af den generelle forordning om databeskyttelse.

europa.eu/dataprotection/da

Publikationskontoret

ISBN 978-92-79-79422-3