Contractbook

CoreRisk Consulting
Governance | Risk | Compliance

DIN EBOG OM PERSONDATAFORORDNINGEN

GDPR

for moderne virksomheder

AF CONTRACTBOOK OG CORERISK CONSULTING

Contractbook

GDPR
for moderne virksomheder

Din første ebog om **persondataforordningen**

Prolog

Den 25. maj 2018 trådte EU's Databeskyttelsesforordning (GDPR) i kraft. Hermed har EU-borgerne fået væsentlig bedre kontrol over deres personlige oplysninger, mens virksomheder mødes af en række nye krav, herunder en væsentlig mængde dokumentationskrav.

EU-parlamentet har besluttet at persondataforordningen træder i kraft den 25. maj, 2018. (Kilde: wikipedia.com)

Vi ved endnu ikke, hvordan forordningen vil blive håndhævet eller hvor mange resurser EU-medlemslandende vælger at afsætte til at styrke myndigheder som Datatilsynet. Loven vil ikke desto mindre kræve væsentlige forandringer i arbejdskulturen, og man kan godt forvente, at loven bliver en milepæl for datasikkerheden i den digitale tidsalder. Allerede nu bevirker forbrugernes øgede

bevidsthed om privatlivssikkerhed, at alle databehandlende virksomheder må overveje deres praksis.

Loven er kompleks og vidtrækkende, som EU-forordninger nu engang er. Derfor tager du sandsynligvis fejl, hvis du ikke tror dig omfattet af reglerne. Når det så er sagt, er der ingen grund til at gå i panik, hvis du driver en ærlig forretning. GDPR er ikke lavet for at gøre livet surt for virksomheder – den er lavet for at regulere den uhæmmede brug og salg af personlige oplysninger og for at tvinge virksomheder til at udvikle en datapolitik.

At forordningen er trådt i kraft, betyder ikke, at løber er kørt. At være GDPR-compliant kræver, at man kontinuerligt reviderer og optimerer sine praksis, at man altid er åben for at finde nye, bedre løsninger. Hvis du endnu ikke er på plads, er det første vigtige skridt på vejen mod at efterkomme forordningen, at du indser nødvendigheden af at handle. Det andet er rent faktisk at handle. Det tredje er så at dokumentere handlingen.

I den følgende tekst vil vi skitsere nogle af den nye forordnings mest grundlæggende elementer. Vi vil derefter også gennemgå forordningens nye dokumentationskrav – med en guide til hvert enkelt dokument.

Vi er ikke advokater, så vores tekst skal ikke læses som en

fyldestgørende juridisk guide. Denne E-bog er en letlæselig introduktion, og kan ikke erstatte eventuel juridisk vejledning. Her vil vi i stedet henvise til Datatilsynets udførlige vejledninger eller CoreRisk Consultings kyndige rådgivning. Til trods for dette forbehold lover vi, at du med denne guide vil være bedre rustet til de kommende frokostpauser.

E-bogen er blevet til i samarbejde mellem Contractbook og erhvervsjurist Bjørn L. Erichsen fra CoreRisk Consulting. Vores forhåbning er, at alle virksomheder (store som små) lykkes med at efterleve databeskyttelsesforordningens krav til datasikkerhed. Ønsker du at vide mere, finder du mere end 2 timers foredrag om forordningen samt en udførlig praktisk guide til at skabe den gode databehandleraftale på dette link.

Indhold

KAPITEL 1.

Introduktion

Introduktion

Vi benytter af pædagogiske årsager den mundrette og ikke mindst læsbare danske titel Databeskyttelsesforordningen. Da vi ønsker at virke som folk med sans for detaljen, skal lovens officielle titel dog for god ordens skyld nævnes:

> *Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse).*

Forordningen blev ratificeret af EU's medlemslande i april 2016, og fungerer som erstatning for Persondataloven og et EU-direktiv fra 1995. Efter en toårig transitionsperiode trådte forordningen i kraft den 25. maj 2018.

Det oprindelige direktiv indeholdt mange af de samme elementer som Databeskyttelsesforordningen, men de nye regler og dokumentationskrav udgør en væsentlig udvidelse af privatpersoners rettigheder.

Med den nye forordning går EU's persondatapolitik fra at være et mål til at blive en juridisk bindende lov i alle EU-lande – vel og mærket uden at medlemslandende først skal vedtage loven i

deres respektive parlamenter.

EU præsenterer to overordnede mål med forordningen:

- At beskytte EU-borgernes privatliv ved at give dem øget kontrol over deres persondata. Hermed sigter EU mod at styrke forbrugeres tillid til den digitale økonomi.
- At harmonisere EU-landenes persondatalove, således at det bliver enklere og mere gennemsigtigt for virksomheder at operere i EU. De estimerer selv, at det kan spare virksomhederne op mod 2.3 milliarder euro om året.

Hvad er persondata og hvad er sensitive personoplysninger?

Forordningen definerer persondata som: ”enhver form for information om en identificeret eller identificerbar fysisk person.” Pointen er, at data bliver persondata, hvis det kan ledes tilbage til og være med til at identificere en fysisk person. Det kan være alt fra navn, fotografier, IP-adresse eller fysiologiske, kulturelle og sociale karakteristika - listen er for så vidt uudtømmelig.

Bemærk dog, at det samme type data ikke altid vil gælde som

personoplysninger for forskellige personer. Firkantet sagt vil man være identificerbar ved sit køn, hvis man er den eneste mand i en forsamling, mens ”Mand, København” næppe gør en person identificerbar.

Forordningens Artikel 9 nævner en række særlige kategorier af personoplysninger, som er sensitive. Listen af sensitive data er udtømmelig, og det er en god idé, at man om muligt indgår at behandle den salgs data, da det kræver en særlig lovhjemmel og nogle skrappere sikkerhedskrav. Det lyder i forordningen:

”Behandling af personoplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetisk data, biometrisk data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering er forbudt.”

Det er relevant, hvis du registrerer dine ansattes tilknytning til fagforeninger eller hvis du eksempelvis har en kundedatabase, der indeholder oplysninger om, hvem der er homoseksuelle eller hvem der af religiøse årssager ikke spiser særlige råvarer.

Strafferammen

Forordningens strafferamme har fået en del opmærksomhed. EU truer nemlig med bødestraffe på op mod 4 % af den årlige omsætning i det foregående år eller 20 millioner euro, afhængigt af hvad er er højest. Man skal have sig for øje, at det kun gælder for de mest alvorlige forbrydelser, og at det er maksimumstraffen.

Den slags tilfalder sandsynligvis kun virksomheder, der har databehandling som kerneaktivitet, ikke den lokale pizzamand med rod i ansættelseskontrakterne. Det er dog ikke noget, man bør spekulere i.

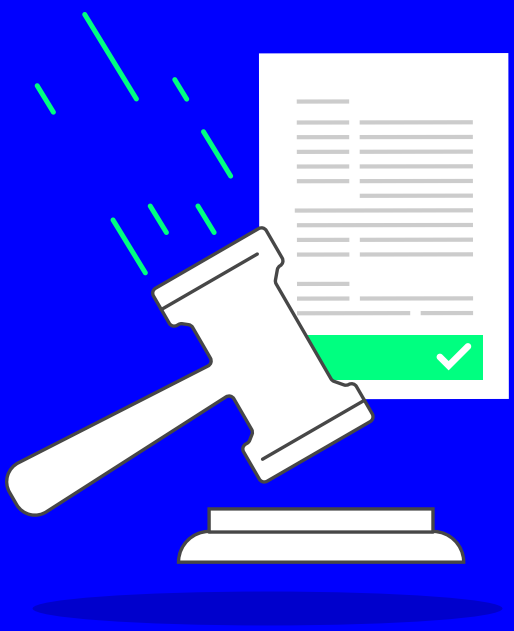
Mindre brud kan nemlig stadig blive straffet med bøder på op mod 2 % af den årlige omsætning i det foregående år eller 10 millioner euro (hvad end der er højest).

Det lyder skræmmende, og det er seriøst. Vi skal dog have for øje, at det er maksimumstraffen og at vi endnu ikke ved, hvilken linje domstolene vælger at lægge. Vi ved heller ikke, hvor mange resurser Datatilsynet afsætter til at kontrollere og retsforfølge virksomheder - om de handler med ond vilje eller ej.

Hvad skal du så gøre? Du skal indledningsvist lave en fortegnelse over, hvilke oplysninger du behandler, hvilken typer der er tale om og hvad er formålet med behandlingen er?

KAPITEL 2.

Databeskyttelsesforordningens anvendelse



Databeskyttelsesforordningen gælder for alle firmaer, som behandler eller opbevarer persondata på fysiske personer, der er bosiddende i EU. Det gælder uanset virksomhedens placering. Forordningen har altså det, EU på klassisk advokatnonsens kalder ekstraterritorial anvendelse. Det betyder på dansk, at forordningen også gælder for amerikanske, afrikanske og asiatiske virksomheder, der behandler EU-borgeres personlige oplysninger. Det hjælper i dette tilfælde ikke at have sin virksomhed placeret i Panama.

Virksomhedens størrelse har en betydning, da selskaber med mere end 250 ansatte skal efterleve højere krav end dem under. Det er også afgørende, om en virksomhed har systematisk og omfattende databehandling som kerneaktivitet. Da vil der være øgede krav.

Generelt skal man have sig for øje, at forordningen fungerer efter et proportionalitetsprincip, der tager virksomhedens størrelse og resurser med i vurderingen af krav og en eventuel straf. Generelt anbefaler vi dog, at alle virksomheder uanset størrelse forholder sig til forordningens krav.

Databehandlere og dataansvarlige

Forordningen skelner mellem dataansvarlige og databehandlere.

Den dataansvarlig er den, som indsamler data og bestemmer formålet hermed. Det kunne eksempelvis være et firma, som indsamler persondata på deres ansatte for at kunne udbetale dem løn. Databehandlere er dem, der opbevarer, bruger eller analyserer data på vegne af den dataansvarlige. Det kunne eksempelvis være Contractbook, der opbevarer persondata i ansættelseskontrakter.

Hvis man videregiver data til en tredjepart, skal datasubjektet (den fysiske person, dataet omhandler) gøres opmærksom på det. I nogle tilfælde skal man have vedkommendes tilladelse. Hvis en tredjepart selv definerer, hvordan dataet skal benyttes, vil denne også være dataansvarlig.

Databehandleraftale

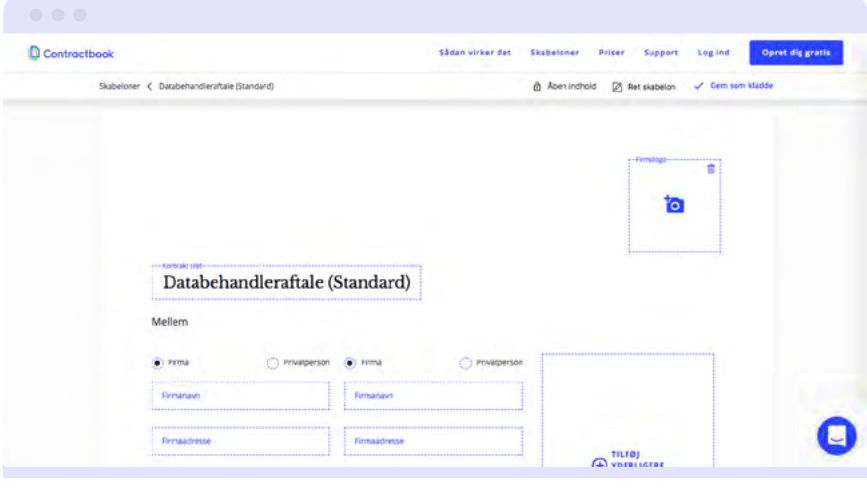
Databehandleren agerer altså efter instruks fra en dataansvarlig. Dette forhold skal reguleres af en databehandleraftale, der definerer, på hvilken baggrund databehandleren opbevarer eller behandler data.

Aftalen skal sikre, at de oplysninger databehandlere har, behandles i overensstemmelse med loven, og derfor hverken misbruges, deles, fortabes eller forringes. Her skal desuden være beskrivelser af underdatabehandlere, oversigt over eventuel

overførsel af persondata til tredjelande og en beskrivelse af procedure for underretning i tilfælde af et brud.

Det er et krav, at alle firmaer (uanset størrelse) kan dokumentere, at virksomheden har databehandleraftaler på plads med alle sine databehandlere. Disse skal kunne fremvises ved et tilsyn. Du finder en gratis skabelon til en sådan aftale her.

For at blive klar, skal du altså finde ud af, om du er dataansvarlig eller databehandler. Derefter skal du lave en fortegnelse over, hvilke databehandlere du bruger og sørge for, at der kommer en databehandleraftale på plads.



KAPITEL 3.

Dokumentationskrav

Persondataforordningen rækkevidde

Det væsentligste nye i forordningen er dokumentationskravene. Virksomheder skal nu kunne dokumentere, hvordan de behandler data, hvilket data de indsamler, samt hvilke systemer der bruges i behandlingen.

Det fremgår direkte af forordningen, at man skal have udfyldt en databehandleraftale og en fortegnelse over behandlingsaktivitet. Derudover er der en række dokumenter, som ikke direkte er beskrevet, men som stadig er en naturlig del af et godt setup.

Dokumentation sikrer dig dog ikke 100 %. At efterkomme forordningen kræver naturligvis, at man gør, som man selv skriver. Derfor fordrer den nye forordning en kulturændring med hensyn til, hvordan vi behandler og opbevarer data fornuftigt.

Baggrund for bestyrelsens eller ledelsen beslutninger

Man skal kunne bevise, hvem der har taget virksomhedens beslutninger. Derfor vil det være en god idé, at man udarbejder skriftlig dokumentation, som beviser, at bestyrelsen og/eller ledelsen har taget stilling til virksomhedens dataskik.

Der er ingen formkrav til dette dokument, da det kan være alt fra en udførlig bestyrelsesbeslutning til to linjer i et referat. Det vigtigste er, at man viser, at man har taget stilling til emnet og at man behandler det som en prioritet. Dokumentet kan samtidig bruges til at bevise overfor myndighederne, at man forholde sig til spørgsmålet løbende.

Det er desuden en god anledning til at få afklaret principper og procedurer en gang om året. Det er nemlig ledelsen og/eller bestyrelsens ansvar, at virksomheden har styr på databehandlingen. De kan tilmed gøres personligt ansvarlige, hvilket har stor betydning i en eventuel forsikringssag.

Gap-analyse

Det er ikke noget krav, at man laver en gap-analyse. Det er dog en forudsætning for god databehandling, at man kender de data, man behandler og at man ved, hvad man skal gøre.

Gap-analysen er altså en metodisk overvejelse til at finde ud af, hvad man gør og hvad man mangler for at efterkomme forordningen.

Først kan man stille sig selv spørgsmålet om, hvilket data man

behandler. Er det normal eller sensitiv data? Hvad er formålet med at opbevare data? Hvor opbevares det? Og har man databehandleraftaler på plads?

Det er en øvelse, der tager lidt tid, men det er et godt grundlag for at finde ud af, hvad man mangler.

Databeskyttelsespolitik

Ifølge Artikel 24 i forordningen skal en virksomhed have beskrevet, hvordan man behandler data, så man kan påvise sin ret overfor myndigheder, forsikringsselskaber eller tredjeparter. Det vil være virksomhedens databeskyttelsespolitik.

Det kan være to til fire siders tekst, hvor man beskriver de forskellige kategorier, man behandler og hvordan de behandles, slettes og opbevares. Der er som sådan ingen formkrav, for dokumentet bruges mest til at danne et overblik.

Forordningen efterlader nemlig meget til virksomhederne selv at definere. Vi anbefaler, at man har så simple regler og så vidde rammer som muligt. Man kan godt beslutte sig for eksempelvis at have meget strikse sletteregler, men det kan være svært at overholde.

En god måde til at skabe en overskuelig databeskyttelsespolitik vil være at arbejde med det som en procesbeskrivelse. De fleste virksomheder vil eksempelvis have fem områder, hvor de behandler data: 1. Kunder. 2. Leverandører. 3. Rekruttering. 4. Ansatte. 5. Tidligere ansatte.

Indenfor hvert område vil en virksomhed behandle forskellige typer data og bruge forskellige systemer til at håndtere den data. I rekrutteringsprocessen vil man modtage CV'er, man vil have nogle til samtale og i sidste ende vælger man den rette kandidat. Hvordan behandler virksomheden ansøgernes data og hvordan slettes disse? Beskriv det kort og præcist for alle fem kategorier. Der vil du have et godt overblik.

Fortegnelser over behandlingsaktiviteter

Forordningens Artikel 30 definerer klart, at man skal udfærdige en fortegnelse over sine behandlingsaktiviteter. Det er altså et krav, at man har lavet dette dokument.

Her vil det være en god idé at tage udgangspunkt i ens databeskyttelsespolitik og de fem beskrivelser. Man skal nemlig kunne dokumentere, hvilken type personoplysninger man indsamler, og hvad formålet med indsamlingen er. Derefter skal man kunne redegøre for, hvordan man behandler oplysningerne

og hvilke tredjeparter man benytter sig af. De fleste virksomheder bruger en del software og tredjeparter til databehandling, og de skal altså beskrives. Bruger du en mail? Har du et lønsystem? Et CMS? Lejer du serverplads? Alle disse forskellige udbydere skal fremgå af dokumentet sammen med beskrivelser af, hvilket data de behandler og hvorfor.

Dokumentet skal eventuelt også beskrive ens sletteregler og hvilke sikkerhedsforanstaltninger, man har foretaget. Sådan et dokument skal både udfærdiges af dataansvarlige og databehandlere.

Spørgsmålet er så, hvor præcis man skal være i sin beskrivelse? Mange ansættelsesaftaler indeholder en paragraf med ordlyden: ”Virksomheden forbeholder sig ret til at bruge persondata, som den finder hensigtsmæssigt.” Den går ikke længere. I stedet kan man beskrive, at man anvender person data til ”almindelig personaleadministration”. Det vil altid være et skønspørgsmål, hvor meget elastik man har i en sådan formulering.

Baggrund for databrud

I tilfælde af brud på persondatasikkerheden skal du give datasubjektet besked i ordentlig tid. Det kunne være, hvis der har været et hacker-angreb, en medarbejder har mistet en USB-

nøgle eller andre former for læk. Derfor er det en god idé at have et dokument, der beskriver proceduren i tilfælde af et brud.

Tilsynsmyndigheder skal underrettes i løbet af 72 timer efter, du har opdaget bruddet. Hvis sikkerhedsbruddet involverer høj risiko for rettighedsbrud, skal anmeldelsen gives uden forsinkelse. Det kan godt betale sig at være ærlig i denne sag jævnfør strafferammen. Hvis du skønner, at der ikke har været nogen risiko involveret med bruddet, behøver du ikke at indberette det. Du skal dog lave en log over alle brud, som gemmes internt.

Der er et par formkrav til, hvordan man skal reagere og hvad man skal oplyse datatilsynet om i tilfælde af et brud: 1. Hvad er der sket? Hvad er karakteren af databruddet? 2. Hvem har ansvaret? Undlad at bruge titlen DPO fordi det lyder smart. Der er en række ret specifikke krav til en DPO og en sådan er stort set umulig at fyre, så hold dig til persondataansvarlig. 3. Beskriv de sandsynlige konsekvenser. 4. Forklar i prosaform, hvilke foranstaltninger man træffer for at håndtere databruddet.

Det er ikke altid, at man kan beskrive præcist, hvad der er sket, og hvad der kommer til at ske. Det er derfor okay, at man følger op på det løbende, så længe man ikke glemmer det. Altså er det en god idé at have en beredskabsplan.

Samtykkeerklæringer

Et samtykke kan gives mundtligt, men det er meget svært at bevise, hvad der er aftalt. Derfor anbefaler vi, at du udarbejder en skriftlig version af en samtykkeerklæring. Denne skal dog kun bruges, når der ikke er andre muligheder, altså hvis man ikke har hjemmel i et andet behandlingsgrundlag. Det kan du læse mere om i næste kapitel

Da dokumentationskravene er det væsentligte nye i forordningen, vil udfyldelsen af disse dokumenter være et stort skridt på vejen mod at blive compliant.

KAPITEL 4.

Behandlingsgrundlag og samtykke

For at databehandlings kan betragtes som lovligt, skal personoplysninger behandles på baggrund af et samtykke eller et grundlag, som enten er fastsat i love eller som betragtes som den dataansvarliges legitime interesse.

Det er eksempelvis et legitimt grundlag at indsamle kontooplysninger på sine ansatte, da det er betingelsen for, at man kan udbetale dem løn. Det er altså databehandling, som er nødvendig af hensyn til opfyldelse af en kontrakt og som tjener datasubjektets interesser. Databeskyttelsesforordningen skriver endda eksplicit, at behandling af personoplysninger til forebyggelse af svig og direkte markedsføring kan anses for at være en legitim interesse. Det fremgår også, at der kan være andre legitime interesser, så længe de ikke overgår datasubjektets. Der er altså en relativ mange muligheder for at indsamle data på et legitimt grundlag.

Det er dog nødvendigt, at man arbejder i overensstemmelse med god databehandlingsskik ved at leve op til principperne for god databehandling. De lyder, at behandlingen skal være lovlig, retfærdig og gennemsigtig, så formålet både er legitimt og tydeligt angivet.

Det er desuden god skik, at man minimerer databehandlingen, så man kun opbevarer det allermest nødvendige og kun så længe,

det er nødvendigt for at udføre et bestemt formål.

Når man indsamler personlige oplysninger, skal man oplyse formålet med indsamlingen. Hvis du har flere formål, skal de alle angives, og du skal desuden informere folk, hvis formålet ændrer sig undervejs.

Samtykke

Hvis man ikke har umiddelbare legitime interesser, kan man få et behandlingsgrundlag ved at indhente samtykke. Forordningen stiller dog øgede krav til indsamlingen af samtykke.

Et samtykke skal gives frivilligt og være både legitimt, specifikt, informeret og utvetydigt. Derfor skal du informere folk om din identitet samt formål og varighed af behandlingen af de personlige oplysninger, når du indsamler samtykke til at bruge dem. Folk skal i øvrigt informeres om, hvordan de kan tilbagetrække deres samtykke og hvordan de kan klage, hvis de mener, at deres rettigheder er blevet overtrådt. I Danmark varetages klager af Datatilsynet.

Du skal være opmærksom på, at samtykket ikke gælder, hvis du indirekte tvinger en ansat til at afgive samtykke, fordi du sidder i en magtposition. Samtykket skal desuden gives aktivt, så stiltiende

accept gælder ikke. Derfor kan du heller ikke indhente samtykke med førafkrydsede felter.

Når du indhente samtykke, skal det være klart adskilt fra andre emner. Du kan altså ikke gemme anmodningen om samtykke i bunden af række handelsbetingelser på længde med en russisk roman. Anmodningen om samtykke skal skrives i et tilgængeligt, klart og simpelt sprog. Når du skal indhente samtykke fra børn, skal du eksempelvis også skrive anmodningen i et sprog, børn forstår.

Hvis du som dataansvarlig benytter dig af databehandlere, skal det også fremgå tydeligt.

Da det skal være ligeså nemt at trække et samtykke tilbage som at give det, er det en usikker måde at indhente ret til at behandle. Hvis man kan ligge dataindsamlingen ind under legitime interesser, er det klart at foretrække.

Når du har udfyldt de mange dokumenter, er det nødvendigt at se på, om du så har lov til at behandle det data, du gør. Tjek eventuelt, om du har brug for samtykke for at indsamle og opbevare personlige oplysninger, eller om du har et legitimt grundlag.

KAPITEL 5.

Rettigheder og sikkerhed

Forordningen giver borgerne en række nye rettigheder, heriblandt retten til at blive glemt og retten til dataportabilitet. Det bedste råd vi kan give dig for at efterkomme disse rettigheder er, at du etablerer et organiseret, digitalt og sikkert arkiv for det data, du behandler.

Artikel 17 i forordningen beskriver retten til at blive glemt også kendt som retten til sletning. Retten til at blive glemt giver EU-borgere mulighed for at kræve, at deres data bliver slettet, hvis ikke de tjener noget formål (enten fordi de er irrelevante eller forældede) eller hvis oplysningerne kan skade personen. Man kan ligeledes udløse retten til at blive glemt, hvis man oplever, at ens oplysninger bliver behandlet ulovligt.

Det betyder eksempelvis, at en tidligere ansat kan kræve at få sit data slettet fra en virksomheds arkiver efter endt ansættelse. Der er dog mulighed for at beholde dem, hvis de skal bruges til eksempelvis skatteindbetaling. En virksomhed kan endvidere være undtaget, hvis man vurderer, at oplysningerne har særlig historisk eller forskningsmæssig betydning, eller hvis de har offentlighedens interesse.

Retten til at blive glemt er ikke den eneste nye rettighed i forordningen. Artikel 16 beskriver, at EU-borgere har ret til berigtigelse. Altså har man ret til at få sine oplysninger ændret,

hvis de ikke længere er korrekte. Artikel 15 beskriver endvidere retten til indsigt, hvor det fremgår, at man som privatperson har ret til at få indsigt i behandlingen af sine oplysninger. EU-borgere skal altså altid have ret til at vide, om deres data bliver behandlet, hvilke oplysninger der behandles, hvem der behandler dem, hvor de behandles og til hvilket formål de enten opbevares eller behandles. De har desuden ret til at få at vide, hvor de eventuelt kan klage, hvis de oplever brud på sikkerheden eller ikke føler sig ordentligt behandlet. I Danmark varetages klager af Datatilsynet.

Slutteligt beskriver forordningens Artikel 20 retten til dataportabilitet. Denne ret giver EU-borgere ret til at modtage en gratis kopi af deres oplysninger i et struktureret, almindeligt anvendt og maskinlæsbart format. De skal kunne overleveres og transmitteres uden hindring mellem databehandlere og fra et IT-system til et andet. Eksempelvis skal det være muligt at få sin bank til at levere sit persondata til en anden bank. I bedste fald skal det være muligt for datasubjektet selv at downloade sit data.

Det lyder kompliceret, men det er nemt at håndtere med de rette værktøjer. Hvis du opbevarer al din data i et vilkårlig ringbind eller i endeløse e-mailtråde, bliver det svært. Hvis du derimod opbevarer alt data i et organiseret og digitalt rum, vil det være let at administrere retten til at blive glemt og retten til dataportabilitet. Et organiseret arkiv vil desuden gøre det nemmere for dig at

bevise, at du efterkommer forordningens krav. Et sådant arkiv kræver dog, at sikkerheden er på plads.

Sikkerhedsforanstaltninger

Før vi går i detaljer, må vi hellere gøre én ting klart: Alt kan blive hacket. Opbevarer du data digitalt, vil det være sårbart overfor Putins hacker-hær, opbevarer du det fysisk, vil der altid være mennesker, som kan bryde ind. Du kan aldrig være 100 % sikker, hvilket kun understregere vores råd om at minimere databehandling og tage så få risici, som overhovedet muligt.

Forordningen gør klart, at man som dataansvarlig skal implementere tekniske og organisatoriske foranstaltning, som sikrer at "state-of-the-art"-løsninger altid tages i betragtning. Forordningen definerer ikke, hvad det betyder, for det ændrer sig hurtigt i den digitaliserede verden. Gmail og USB-nøgler kan måske være problematiske, hvis det opbevarede data ikke er krypteret.

Hvis du foretrækker at opbevare al dit data på papir, skal du låse papiret inde for at minimere adgangen. Forordningen gør det nemlig klart, at så få som muligt skal have adgang til persondata: det vil sige kun de, der har brug for det for at udfylde det formål, man har bestemt for at indhente oplysningerne. Når du sletter

data i fysisk form, skal papiret shreddes eller brændes, så ingen kan tilgå de følsomme data efterfølgende.

Computere skal have opdaterede firewalls og virus-kontrol installeret. Passwords skal kontrolleres og ændres mindst en gang om året.

Det kan i øvrigt være en god idé at bruge logning-teknologi for at overvåge, hvem der ser hvilken data hvornår. Det vil have en præventiv effekt på indbrud og gøre dig opmærksom på eventuelle sikkerhedsbrud. Systemer der kan gennemskue abnorm trafik eller atypiske mønstrer, kan være en god idé.

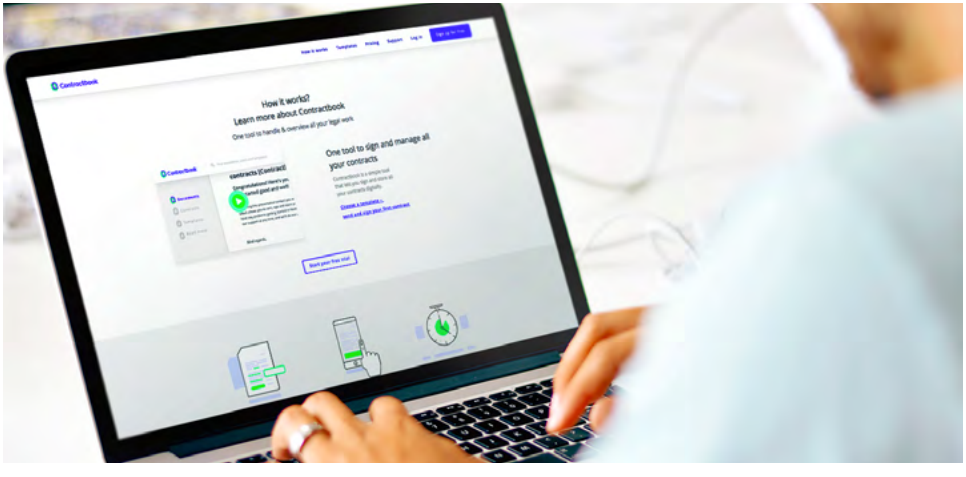
Forordningen introducerer begrebet Databeskyttelse gennem design (Privacy by design). Det betyder, at datasikkerhed skal tænkes ind i design – og ingeniørfasen af digitale systemer. Eksempelvis skal systemer programmeres således, at de kun indsamler det nødvendige data, at det er sletbart og at det kan tilgås i et maskinlæsbart format. Som dataansvarlig har du ansvar for, at databehandleren gør deres bedste for at sikre sig imod brud - organisatorisk som teknisk.

Forordningen opfordrer til pseudonymisering, så dataet ikke gør en person identificerbar. Pseudonymisering er dog ikke i sig selv et nødvendigt træk.

KAPITEL 6.

Contractbook som GDPR-værktøj

Contractbook er et perfekt persondataværktøj for start ups og HR-afdelinger i små og mellemstore virksomheder. Når du har gjort dig klart, hvilket data du behandler og hvorfor, kan vi nemlig hjælpe dig med at skabe organiseret arkiv over dine juridiske dokumenter - det kan være alt fra ansættelseskontrakter til salgsaftaler og fortrolighedsaftaler. Hermed vil du nemt kunne begrænse og dokumentere, hvem der har adgang til det persondata, du besidder.



Contractbook hjælper dig med at skabe et organiseret og sikkert arkiv, som er nemt at navigere i.

Vores digitale værktøj designes til at gøre det nemt at leve op til Retten til at blive glemt, indsigelsesretten og retten til dataportabilitet, da datasubjekter selv kan tilgå deres data, få det slettet og i øvrigt downloade det i et maskinlæsbart format.

Vores gratis skabeloner vil være designet til datasikkerhed, så

du umiddelbart kun indsamler det allermest nødvendige data. Vi vil samtidig give adgang til databehandleraftaler og vi giver dig forslag til korrekte formuleringer, du kan bruge for at sikre at samtykke indhentes korrekt.

Ved at bruge Contractbook viser du, at du gør alt i din magt for at respektere datasikkerheden og efterkomme forordningens krav. Det sætter dig i en langt bedre juridisk position i tilfælde af et brud.

CoreRisk Consulting sørger for, at du kommer til at bruge Contractbook på den bedste og mest korrekte måde. Rådgivningen omfatter blandt andet hjælp til at udfylde dine kontrakter (heriblandt databehandleraftaler) på den mest hensigtsmæssige måde. CoreRisk Consulting leverer desuden strategiske, taktiske og operationelle løsninger relateret til juridisk Governance, Risk & Compliance- aktiviteter i private virksomheder.

Om forfatteren

Bjørn Leth Erichsen er uddannet erhvervsjurist og har mere end 10 års erfaring fra bl.a. 'in-house' juridiske afdelinger i store internationale virksomheder, herunder Deloitte, Adecco Management & Consulting SA samt Sitecore Corporation A/S.

MAY 2018