ALEXANDRA INSTITUTTET

# GDPR I PRAKSIS

## Når forordningen rammer virkeligheden

Danske virksomheders implementering af
EU's nye persondataforordning

# Indhold



DCSC
Danish Cyber Security Clusters

infinit
Innovationsnetværk for it

INNOVATIONSAGENTERNE

# Indledning

# Baggrund

Den 25. maj 2018 træder den nye EU persondataforordning (på engelsk: *General Data Protection Regulation*, forkortet: GDPR) i kraft som lov i hele EU og dermed også i Danmark. Forordningen har fokus på at sikre bedre håndtering af persondata og databeskyttelse og giver bedre muligheder for at sanktionere virksomheder, der ikke lever op til lovgivningen. Følgelig er der i virksomhederne opstået et behov for at få styr på håndteringen af persondata i en grad, der ikke tidligere har været nødvendig.

Denne rapport er resultatet af en kvalitativ undersøgelse af, hvor danske virksomheder står i forhold til implementeringen af forordningen. Formålet med rapporten er – udover at beskrive hvilke udfordringer danske virksomheder har med persondataforordningen – at pege på områder, hvor virksomheder og udbydere af konsulentydelser omkring forordningen med fordel kan sætte ind. Rapporten er således primært tiltænkt rådgiver og løsningsudbydere inden for it.

I forbindelse med undersøgelsen har vi gennemført en række kvalitative interviews med nøglepersoner i 10 store og mellemstore danske virksomheder, hvor vi har talt med dem om de indsatser, de har gennemført i forhold til persondataforordningen. Disse 10 interviews er blevet fulgt op af 5 telefoninterviews med mindre virksomheder.

Under analysen blev det klart, at de adspurgte virksomheder var godt i gang med at forholde sig til forordningen og havde en forståelse af samt plan for, hvad der skal til at komme i mål (dvs. blive *GDPR-compliant*). Dette resultat stod i nogen kontrast til det billede, man møder i medierne, og hvad forskellige konsulenter skriver på de sociale medier. Vi besluttede derfor at supplere vores interviewundersøgelse med 5 telefoninterviews med mindre virksomheder, for at få et indtryk af, om deres udfordringer var de samme, eller om de stod med nogle andre udfordringer.

Resultaterne viser, at der er stor forskel på store og mellemstore kontra de mindre virksomheder. Hvor de store virksomheder har væsentlige ressourcer sat af til implementering og har en plan for, hvad de skal gøre, ender opgaven i mindre virksomheder ofte hos en enkelt person og er derfor i større risiko for forsinkelser.

De centrale resultater af undersøgelsen blandt *store og mellemstore* virksomheder er, at:

- **De adspurgte personer er generelt positivt stemt** over for forordningen – især fra et værdimæssigt standpunkt. Samtidig peger de på, at forordningen er et stort og omkostningstungt projekt for virksomhederne, og at det vil vanskeliggøre nogle arbejdsprocesser fremadrettet.
- **Virksomhederne har en oplevelse af at vide, hvad de skal gøre** for at leve op til forordningen. Der er enkelte tvivlspørgsmål, men det er ikke noget, der skaber stor uro eller handlingslammelse hos de adspurgte.

- **Opfattelsen af forordningen har stor betydning** for, hvor langt virksomhederne er i arbejdet med forordningen. Hvor nogle ser den 25. maj som en hård deadline for implementeringen, opfatter andre det mere som en flydende proces, der kommer til at ske over tid.

- **Forordningen kræver et nyt mindset i virksomhederne**, fordi der dels kommer større fokus på informationssikkerhed i det daglige arbejde, dels skal foretages en vurdering af den risiko, databehandlingen medfører for den registrerede – en analyse der tidligere har begrænset sig til risiko for forretningen.

De centrale resultater af undersøgelsen blandt de *mindre* virksomheder er, at:

- **Forordningen kan hæmme digitaliseringen**, fordi det kan være for uigennemskueligt eller krævende for virksomhederne at indføre de nødvendige systemer og procedurer. I yderste konsekvens kan det derfor betyde, at digitale projekter rulles tilbage.

- **De mindre virksomheder er meget afhængige af eksterne kilder til viden.** Her læner de sig primært op ad de organisationer, de plejer at søge viden hos, idet de har en oplevelse af, at de på den måde får de mest konkrete, handlingsanvisende råd og samtidig undgår unødvendige informationer og ”støj”.

- **Implementeringsarbejdet er mere personbåret i mindre** virksomheder, hvilket kan medføre en risiko for forsinkelse. Derudover bliver valget af løsninger i højere grad afhængigt af, hvilke kompetencer der er til stede i den givne virksomhed.

# Implementering af persondataforordningen i danske virksomheder

# Hvor langt er virksomhederne?

Dette afsnit beskriver, hvor langt virksomhederne er i processen med at implementere persondataforordningen. Vi ser på, hvordan virksomhederne har organiseret indsatsen, hvordan de personer, vi har interviewet i de enkelte virksomheder, overordnet ser og opfatter forordningen, hvad virksomhedernes mål er med implementeringen, samt hvorvidt de regner med at nå i mål. Afsnittet afsluttes med en liste af opmærksomhedspunkter.

## ORGANISERING AF INDSATSEN

Generelt er de adspurgte virksomheder godt i gang med implementering af forordningen, men det varierer, hvor længe arbejdet har stået på. Hvor nogle virksomheder gjorde de indledende øvelser for halvandet år siden, er enkelte først gået i gang for nylig og er stadig i opstartsfasen.

Opgaven med at gøre virksomheden *GDPR-compliant* løftes i høj grad internt – et forhold, der især kan forklares med, at de adspurgte alle er it-virksomheder, hvorfor de nødvendige tekniske kompetencer har været til stede i organisationen. I de tilfælde, hvor der er blevet hentet eksterne konsulenter ind til opgaven, har det som oftest været for at yde juridisk bistand, såsom at vurdere virksomhedens indledningsvise compliance-niveau.

Organisatorisk er der i mange større virksomheder blevet nedsat en central gruppe til at varetage indsatsen omkring forordningen på tværs af virksomheden og ned i de enkelte afdelinger. Gruppen består typisk af ledere for forskellige afdelinger og én eller flere jurister – evt. en Data Protection Officer (DPO), hvor det er relevant (mere om denne funktion senere).

For at planlægge og gennemføre et compliance-projekt har det været nødvendigt for virksomhederne at foretage en indledende kortlægning af deres datasituation: Hvordan opsamles data, hvordan opbevares data, hvordan analyseres og bruges data, hvornår slettes data, hvordan flyder data etc.? Denne proces er der to forskellige tilgange til: Nogle laver en bred kortlægning af arbejdet med personoplysninger i hele virksomheden, mens andre starter fokuseret med at gennemføre en granskning af de områder, som de ved kan være problematiske. Ligeledes ruller nogle virksomheder den efterfølgende indsats ud i etaper, mens andre sætter bredt ind og kører sideløbende spor i hele virksomheden på én gang.

Generelt sker planlægningen af indsatsen ud fra vurderinger af, på hvilke områder det er bydende nødvendigt at gøre noget, og om løsningen på problemet er teknisk, organisatorisk eller juridisk. Samtidig tænkes det ind, om det er opgaver, virksomheden selv kan og vil håndtere, eller om det er noget, der skal overlades til eksterne leverandører. Ud over det grundlæggende fokus på virksomhedens daglige drift, arbejdes der i indsatserne med beredskabsplaner og dokumentation. Virksomhederne fortæller, at de med forordningen har fået en ny bevidsthed om, at de skal være klar, hvis der sker datalæk, eller Datatilsynet kommer på besøg.

## OPFATTELSE AF FORORDNINGEN

Alle de personer vi har talt med i undersøgelsen tilkendegiver at have en positiv opfattelse af forordningen – især fra et værdimæssigt standpunkt, men også som en organisatorisk og forretningsmæssig force. En teknologi- og sikkerhedsdirektør mener eksempelvis, at lovgivningen er med til at sende et vigtigt budskab til slutbrugerne af de teknologiske produkter:

> *"Digitalisering kan potentielt give os en massiv værditilvækst. Det kræver selvfølgelig, at det er lavet ordentligt, men det kræver også, at vi kan have tillid – både til, at systemerne virker, som de skal, men også at vores data beskyttes, og at vi selv har kontrol over dem. Derfor er det væsentligt med en lovgivning, der forsøger at definere nogle elementer, der kan give os den her tillid til den digitale databehandling."*

Omvendt peger mange også på, at forordningen gør nogle ting mere besværlige og medfører en øget administrativ byrde for virksomhederne. De adspurgte er spændte på, om forordningen reelt vil få den effekt, der sigtes efter, eller om den i højere grad vil blive noget, som efterleves på symbolsk niveau – sådan som det i manges øjne er sket med cookie-direktivet. Dog ses bødestørrelsen som et signal fra myndighedernes side om, at forordningen tages meget alvorligt.

Et kritikpunkt, som mange af deltagerne i undersøgelsen rejser, er, at formuleringerne i forordningen sine steder er meget vage, og at der mangler konkrete anvisninger til den tekniske og organisatoriske implementering. Hvornår er noget fx *'tilstrækkeligt anonymiseret'*, eller hvor hurtigt skal virksomheden reagere for at leve op til kravet om *'undue delay?'* [red.: at rapportere et datalæk indenfor 72 timer]. En it-konsulent påpeger, at det i nogle tilfælde er meget op til den enkeltes tolkning, hvordan kravene i forordningen efterkommes:

> *"Det gør vores job nemmere, at ting er specificeret – men der mangler nogle konkretiseringer, for at den kan overføres til praksis."*

Uklarhederne gør det altså svært for virksomhederne at vide, om de arbejder i den rigtige retning, og om de mål, der sigtes efter, faktisk er gode nok. Som en it-chef udtrykker det:

> *"Hvad hvis man gør noget, som man tror, er det rigtige, og så ender med at få en bøde?"*

Ved at spørge ind til både holdninger og praksis i virksomhederne er det gennem interviewene blevet klart, at opfattelsen af forordningen har stor indflydelse på den indsats, virksomhederne gør for at blive klar til den 25. maj. Eksempelvis er det forskelligt, hvor langt virksomhederne mener, de skal være i indsatsen. Hos nogle af de adspurgte ses ikrafttrædelsesdatoen som den absolutte deadline for, hvornår man skal være færdig med implementeringen – ellers kan forretningen lide skade, og virksomheden få bøder. Som det fremgår af nedenstående udsagn fra en teknisk chef, handler det i denne optik om at gå så tidligt i gang, at der er plads til uforudsete problemer:

> *"Timing er altafgørende i det her. Vi går i gang nu, og så regner vi med at have styr på det midt-slut januar, hvor vi så kan gøre status; er der mangler, vi skal have styr på? Den indledende proces skal være afsluttet inden Q1 – ellers er det for sent."*

I andre virksomheder ses kravene og forordningen som noget mere flydende – noget man hverken kan eller skal leve op til den 25. maj. Denne holdning hænger bl.a. sammen med de mange uklarheder og en opfattelse af, at forordningen skal ud at leve, før det kan siges mere præcist, hvordan den skal udmøntes i praksis. Derudover er det så stort et forandringsprojekt for virksomhederne, at der forventes at være forståelse for, at alt ikke er i mål på den pågældende dato. De adspurgte inden for denne gruppe mener, det vil være tilstrækkeligt, at man som virksomhed er opmærksom på sine problemer og arbejder på at udbedre dem. Realistisk set kommer der altså mere til at være tale om en glidende overgang end om en hård bagkant, mener en teknologi- og sikkerhedsdirektør:

> *"Det er en utopi at tro, at alle er compliant til en bestemt dato næste år. Der vil jo være tilfælde, hvor folk ikke er nået i mål eller har overset forskellige risici – eller bare ikke var klar over, hvilke dataflows de havde i virksomheden. Så vil der helt sikkert også være nogen, som bare ignorerer det – eller ikke har hørt om det. Og det er da bekymrende, men det handler jo også om, at man ikke har givet klar nok eller tilstrækkeligt balanceret vejledning."*

Fordelen ved den mere flydende tilgang er, at der åbnes for at tage arbejdet med forordningen mere oppefra og ned. Som det påpeges, er der en risiko for, at det bliver for uoverskueligt, hvis forordningen opfattes som et *"all or nothing*-projekt" – og at det kan betyde, at virksomhederne ganske enkelt giver op på forhånd.

## MÅLET MED INDSATSEN

Det er forskelligt fra virksomhed til virksomhed, hvilken målsætning der sigtes efter i arbejdet med forordningen. Grundlæggende opfattes det som et stort, ambitiøst og ressourcekrævende projekt at få forordningen ind i alle aspekter af virksomhedens drift – også hos de virksomheder, som allerede har den grundlæggende tilgang til data, der lægges op til med forordningen. Hertil kommer, at der altid vil være noget, som kunne være bedre. Ergo er man som virksomhed nødt til at prioritere – dels hvor compliant man vil være, dels hvilke områder det er vigtigst at få gjort noget ved. Som det fremgår af dette citat fra en DPO, hænger det at nå i mål også sammen med, hvor ambitiøse succeskriterierne er:

> *"Vi bliver ikke 100% færdige til maj. Det er en stor opgave – også fordi forretningen udvikler sig så hurtigt, som den gør, og vi ikke kun stiller os tilfredse med compliance."*

Umiddelbart kunne spørgsmålet om compliance fremstå som enten eller: enten lever du op til forordningen, eller også gør du ikke. I praksis er billedet dog et andet. Nogle virksomheder vælger at fokusere på det allermest nødvendige, mens andre ser det som forretningskritisk at

gå ekstra meget ind i forordningen og måske endda nå til et højere niveau end det, forordningen kræver. Den øgede indsats skyldes ikke så meget et ønske om at have en særligt etisk tilgang til data, men om at undgå datalæk – og dermed bøder, tab af kunder og dårlig medieomtale – eller i hvert fald have deres ryg så fri som muligt, hvis skaden alligevel skulle ske. Som en CTO/DPO opstiller det:

> *"Vi har ikke råd til en Version2-forside med, at vi har mistet eller lækket data. Men det er måske mere et spørgsmål om, hvornår end om hvorvidt det kommer til at ske. Men vi prøver at begrænse det."*

En anden faktor som spiller ind i målsætningen for virksomhedernes arbejde med forordningen er, hvor omfangsrigt det skal være ift. organisationens drift og arbejdsgange. For mange er persondataforordningen et implementeringsprojekt: virksomheden skal leve op til nogle nye krav, og når der er styr på det, vil det automatisk være en del af virksomhedens praksis. Dog opfattes det i nogle virksomheder som et forandringsprojekt, hvor organisationen kontinuerligt vil arbejde med og videreudvikle databeskyttelsen – et aspekt som derved kommer til at spille en ny og større rolle i virksomhedens drift.

Et andet perspektiv på forordningen er de afledte gevinster, den kan medføre for virksomheder. De fleste steder er det primære fokus lige nu at blive klar til 25. maj, men i enkelte tilfælde ser virksomhederne deres løsninger omkring forordningen som en mulighed for at være i front og differentiere sig fra andre i markedet. De kan fx bruge deres erfaringer som afsæt for at undervise eller rådgive om forordningen, eller de kan sælge ydelser, hvor forordningen er tænkt ind fra starten, så kunden ikke selv behøver at bekymre sig om det. Indadtil peger flere også på, at arbejdet med forordningen betyder, at virksomheden får strammet op på procedurerne og ryddet op i sine data – en øvelse der både kan spare serverplads og give et overblik, som er befordrende for at analysere og bruge data aktivt i forretningen.

## NÅR VIRKSOMHEDERNE I MÅL TIL MAJ?

Som nævnt er det forskelligt, hvor langt virksomhederne er nået i deres proces. De fleste er færdige med afdækningen og står nu over for selve indsatsen. Det er en tidskrævende opgave, hvor mange forskellige aspekter skal tænkes sammen, og hvor alle detaljer ikke nødvendigvis kan planlægges på forhånd. Eksempelvis skal den tekniske udvikling tænkes ind i projektet – et aspekt, en af de adspurgte it-chefer ikke mener, hans ledelse har taget tilstrækkeligt højde for:

> *"Vi er ret langt i analysearbejdet. For mig er det nok den letteste del; den svære del er at få det i produktion, få det tænkt – få fundet den rigtige løsning. Som med al anden software kommer der til at være fejl i det […] Så kan jeg ikke nå det ift. den udviklertid, jeg skal bruge på at nå i mål. Jeg kunne godt tænke mig, at det var mere agilt. Vi kommer til at skulle implementere et monster af en elefant […]"*

I nogle virksomheder er der planlagt ud fra, at processen vil blive tidskrævende, og at der kan opstå uforudsete udfordringer undervejs. Hos andre er det kommet som en overraskelse, hvor stort et arbejde der ligger i at gøre virksomheden GDPR-compliant, hvilket kan føre til forsinkelser og mangel på ressourcer. En jurist i en mellemstor virksomhed fortæller om udfordringen ved at skulle balancere mellem forordningen og andre opgaver:

> *"Men det overrasker mig, hvor lang tid det tager. Jeg havde regnet med maksimum tre uger til hvert område, men bare området med jobansøgninger har taget snart seks uger. Men det er jo også fordi, jeg har andre opgaver udover GDPR."*

En væsentlig, men ofte overset udfordring, ligger i at få medarbejderne med på vognen, så ændringerne bredes ud til hele organisationen og de nye procedurer for datahåndtering og -sikkerhed bliver en naturlig del af den enkelte medarbejders daglige arbejde.

Dog har de færreste virksomheder udformet en decideret indsats på denne front. I nogle tilfælde fordi de endnu ikke er nået til den del af processen, i andre tilfælde fordi det ikke anses for at være relevant. Der er ofte en standardholdning om, at den slags kan løses med politikker og guidelines for, hvordan medarbejderne skal håndtere data og irettesættelser, hvis det viser sig, at de ikke overholder disse retningslinjer.

## OPMÆRKSOMHEDSPUNKTER

- **Forankring og ledelsesopbakning:** Hvis indsatsen omkring forordningen skal få fodfæste i organisationen, er det vigtigt, at den både er forankret i organisationen og har opbakning fra den øverste ledelse; der skal være nogen, som står i spidsen for arbejdet, og som har mandat og ressourcer til at føre ændringerne igennem i de enkelte afdelinger. Hvis virksomheden har en DPO, ligger forankringen oplagt her. De virksomheder som ikke har en DPO, kan med fordel udpege en hovedansvarlig for projektet.

- **Sparring:** For SMV'er kan det være en stor opgave at overskue konsekvenserne af persondataforordningen i deres virksomhed, ligesom der ikke er så mange midler til at hyre eksterne ressourcer ind. Det kan være en stor hjælp at få sparring på området, fx gennem ERFA-grupper, som også kan gå sammen om at betale for konsulentbistand. ERFA-grupper kan findes eller efterspørges hos lokale erhvervsråd og væksthuse eller i brancheorganisationer. Brancheorganisationer har endvidere mulighed for at udarbejde branchespecifikke adfærdskodeks og eventuelt certificeringsordninger, som kan hjælpe med at gøre afklaringsarbejdet mindre for den enkelte virksomhed. Endelig kan det være givet godt ud at søge råd og vejledning hos leverandører, revisorer, advokater, uafhængige it-konsulenter, it-revisorer m.m. og indgå aftale om et format og omfang, der er til at betale for en mindre virksomhed.

- **Datakultur:** Erfaringer viser, at tiltag som guidelines, nedskrevne politikker og online kurser man skal klikke sig igennem kun i ringe grad skaber en sikker adfærd blandt medarbejdere. Skal der ske en reel ændring er man som virksomhed nødt til at arbejde med kulturen og lave tiltag, som tager afsæt i den måde, medarbejderne i forvejen arbejder på. Et eksempel på denne tilgang er en virksomhed, hvor det er op til den enkelte medarbejder selv at vurdere, hvor følsomme data er og dernæst klassificere dem som enten røde, gule eller grønne. Systemet er simpelt og letforståeligt, og medarbejderne forstår, hvorfor de forskellige typer af data er klassificeret, som de er – alt sammen noget, som gør det mere naturligt for medarbejderne at følge de procedurer og politikker, der er forbundet med de tre kategorier. I eksemplet skulle medarbejderne klassificere forretningskritisk data, men konceptet kunne sagtens overføres til personfølsomme data.

# Virksomhedernes udfordringer

I dette afsnit vil vi gennemgå de konkrete udfordringer, virksomhederne står overfor: opbevaring og dataflow; kategorier af persondata; databehandling; rollefordeling i databehandling og sletning. Inden for hvert afsnit er der en beskrivelse af, hvad forordningen siger om emnet, og hvad virksomhederne har sagt om udfordringen. Desuden opstiller vi en række opmærksomhedspunkter, man som virksomhed eller konsulent med fordel kan kigge på.

## OPBEVARING OG DATAFLOW

Så længe data om EU-borgere opbevares inden for EU's grænser, i et EØS-land (Island, Liechtenstein og Norge) eller i et sikkert tredjeland (p.t. Andorra, Argentina, Færøerne, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Schweiz og Uruguay), er der ingen problemer ved at have data i et andet land. Skal data derimod overføres til andre lande end disse, skal virksomheden sikre sig, at der eksisterer valide garantier i forhold til forordningen. En sådan garanti kan fx findes i EU-US Privacy Shield-aftalen som sikrer ordnede forhold, når personhenførbar data overføres fra EU til USA.

Udover selve opbevaringen af data, flyder data rundt i virksomhedernes forskellige systemer og muligvis ud til underleverandører og andre eksterne parter. Her skelnes der mellem, hvorvidt data *overlades* til en databehandler eller *videregives* til en ekstern dataansvarlig – nærmere herom senere. Hvis man som virksomhed overlader data til en databehandler skal man sikre, at man fortsat har fuld tilgang til data. Hvis man som virksomhed videregiver data til en ekstern dataansvarlig, skal man sikre, at man har hjemmel til videregivelsen.

### ERFARINGER: HVAD SIGER VIRKSOMHEDERNE?

For de fleste virksomheder er spørgsmålet om opbevaring ikke et problem, da deres eksisterende serverløsninger er i overensstemmelse med forordningen, fx ved at være hostet inden for EU/EØS. Dog ser vi også en stigende orientering imod cloud-løsninger, hvilket kan skabe udfordringer ift. internationale selskaber og *safe harbour*-reglen, som forhindrer overførsel af persondata til lande med mindre striks privacy-lovgivning. Virksomhederne peger på, at det er besværligt og tidskrævende at skifte udbyder, hvorfor de kan have en modvilje mod at skulle skifte cloud-leverandør trods usikkerhed ift. informationssikkerheden.

Når vi taler med virksomhederne om, hvor data flyder i og uden for virksomheden, bliver billedet straks mere komplekst. Flere fortæller, at de er blevet forbavsede over, hvor mange forskellige softwaresystemer, der findes i virksomheden – og at det derfor kan være svært at danne sig et overblik over, hvilke data de egentlig har, og hvor mange steder der eksempelvis ligger data på den enkelte kunde.

En anden udfordring er, at den enkelte virksomhed har begrænset mulighed for at styre, hvad der sker med de data, som sendes til samarbejdspartnere, underleverandører og

kunder. De kan indgå aftaler om, hvordan data skal behandles eller bede om at få dem slettet, men de kan aldrig vide sig sikre på, at det faktisk sker. Eksempelvis peger en it-chef på, at han deler oplysninger om kunder i sin webshop med den fragtmand, der skal levere ordren. Selvom virksomheden selv kan slette data om kunden fra sit eget system, når en ordre er udført, kan de ikke forhindre, at fragtmanden stadig har dem. Når først data er sendt ud af huset, er de i praksis ude af virksomhedens hænder. I nogle tilfælde søges problemstillingen udbedret ved, at deling af data holdes til et minimum, eller at data kun deles med eksterne parter i anonymiseret form. Dog er der tilfælde, hvor dette ikke er en mulighed.

At få styr på hvor data ligger, og hvor de kommer hen, kræver ikke blot en forståelse af virksomhedens systemer og samarbejder, men betyder også, at der skal sættes ind på det menneskelige plan, både internt i virksomheden og i eksterne forhold.

Internt kan der være arbejdsgange, som er problematiske fra et informationssikkerhedsmæssigt perspektiv – fx hvis en medarbejder henter tal ud fra et cloud-baseret system og dernæst arbejder lokalt med dem i Excel, så de kommer til at ligge lokalt på vedkommendes computer og dermed uden for de sikkerhedsforanstaltninger, der er opsat i systemet.

På den eksterne side fortælles der om, at kunder og brugere uden at tænke over det kan sende data på en måde, som reelt udgør et problem for virksomheden – fx ved at indtaste fortrolige oplysninger i supportsager eller sende data via mails som vedhæftede Excel-ark. En it-chef fortæller, at problemet både består i at få kunderne til at forstå, hvad de må sende til virksomheden, og i at håndtere det, når virksomheden får data ind på uhensigtsmæssige måder:

> *”Hvad gør jeg, når en kundeservicemedarbejder har modtaget kreditkortoplysninger fra en kunde – skal han slette mailen? Den forsvinder jo ikke. Folk sender os alt muligt.”*

I deres arbejde med at leve op til den nye persondataforordning står virksomhederne altså ikke bare over for en systemmæssig og teknisk udfordring, men også – som de selv kalder det – en udfordring med at ”opdrage” kunder og medarbejdere.

Den eksisterende datakultur i virksomhederne varierer meget og følger ikke nødvendigvis følsomheden af de data, der arbejdes med. Det handler i højere grad om, hvorvidt der hidtil har været eksplicit fokus på datasikkerhed og -etik i organisationen. Nogle steder har der eksempelvis været træning og dialog på området, og det er blevet italesat som en del af virksomhedens DNA.

Det påpeges i den forbindelse, at det ikke bare handler om at have det rette mindset, men også om at have den nødvendige viden for at kunne håndtere data rigtigt. Det kan fx kan være en udfordring med de medarbejdere, der ikke så ofte har med personoplysninger at gøre. Et andet aspekt er, at man i nogle virksomheder ikke har tænkt over følsomheden af de

data, man ligger inde med – eller i det hele taget ikke har betragtet dem som data, som det fx kan være tilfældet med CV'er, der ligger i en skuffe.

**OPMÆRKSOMHEDSPUNKTER**

- **Uden for EU/EØS**: Vær opmærksom på, om data bevæger sig uden for EU/EØS-området og sikre tredjelande. Undgå det, hvis det kan lade sig gøre, eventuelt ved skift af leverandør. Kan det ikke lade sig gøre, vil det være en god ide at søge vejledning.
- **Minimering af systemer**: Jo færre systemer, jo færre steder at holde styr på data, og jo nemmere er det at skabe overblikket – tænk det ind næste gang I gentænker jeres it-setup.
- **Data der flyder:** Sørg for at data ikke ligger og flyder på medarbejderes devices og i mapper og systemer rundtomkring i virksomheden. Er det nødvendigt at hente data ud, skal der være procedurer for, at de bliver slettet igen, og at medarbejderne tager ansvar for dette.
- **E-mails:** Tilbyd dine medarbejdere og kontakter andre muligheder end at sende personoplysninger i e-mails og "opdrag" dem til at bruge dem.

## KATEGORIER AF PERSONDATA

Persondataforordningen dækker data, der kan henføres til en fysisk person, og som er let og hurtigt søgbare ved enten at være på elektronisk format eller på anden måde indeholdt i et register. Man må som udgangspunkt ikke have noget med persondata at gøre, medmindre man har en gyldig grund til det (mere herom nedenfor).

Persondata deles op i *almindelige* og *særligt personfølsomme* oplysninger. Almindelige data kan fx være navn og adresse, oplysninger om økonomiske forhold, kundeforhold eller andre lignende ikke-følsomme oplysninger. Følsomme oplysninger er defineret som oplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold, genetiske data, biometriske data, helbredsoplysninger, seksuelle forhold eller seksuel orientering. Data vedrørende strafbare forhold samt CPR-numre er op til medlemslandenes individuelle lovgivning.

For at have lov til at behandle personoplysninger skal formålet med behandlingen beskrives sammen med en saglig begrundelse for proportionaliteten mellem risikoen for den registrerede og værdien af behandlingen. Der skal også argumenteres for, at data er nødvendige for opfyldelsen af formålet, og det skal beskrives, hvordan data sikres, hvem der har adgang til data samt hvor længe disse opbevares. Hjemmel til at behandle personoplysninger kan enten findes i behov for at overholde lovgivning eller kontraktlig forpligtelse eller i et samtykke. Samtykke skal vælges, når der ikke er anden hjemmel. Det er vigtigt, at samtykket sker som en frivillig, specifik, informeret og utvetydig viljestilkendegivelse.

## ERFARINGER: HVAD SIGER VIRKSOMHEDERNE?

Blandt de adspurgte virksomheder er det meget forskelligt, hvilke typer af data, der håndteres. Nogle samler ikke videre følsomme personoplysninger, mens det for andre er en kerneydelse at behandle netop denne type af data. I en virksomhed, hvis systemer retter sig mod det offentlige, fortæller en it-konsulent om omfanget af data:

> *"Basalt set har vi data på dig, fra du bliver undfanget, til du dør."*

Kravene om, at den registrerede skal informeres og give samtykke til databehandlingen er ikke noget, der bekymrer virksomhederne. Opgaven ligger her i at få lavet samtykker, der er specifikke nok til at leve op til kravet om informeret samtykke, hvor brugeren skal indvillige i databehandlingen frem for aktivt at melde den fra. Derudover skal det være muligt at trække sit samtykke tilbage. I den forbindelse er det et vurderingsspørgsmål, hvordan tilbagetrækningen skal foregå, og hvor let det skal være for den registrerede at gøre denne ret gældende. Skal det ske via en selvbetjeningsside, et opkald til kundeservice eller en mail til administrationen?

Virksomhederne har generelt hjemmel til at samle og behandle data, som de gør, og kan derfor forsætte som hidtil efter 25. maj. Dog betyder forordningen, at der i flere virksomheder sker en stigende orientering mod minimering af data – og dermed et skift væk fra den tilgang, der har fulgt med det store fokus på big data. Hvor alting her er blevet samlet og gemt med tanke på, at det muligvis kunne vise sig at være værdifuldt på sigt, begynder virksomhederne nu at forholde sig mere kritisk til, hvilke data der samles op og opbevares. Fra at være et spørgsmål om diskplads, bliver dataindsamling i højere grad et spørgsmål om nødvendighed, hvilket stemmer godt overens med *privacy-by-design* tankegangen fra forordningen (mere herom nedenfor). Som en jurist fortæller, giver forordningen anledning til at få gået virksomhedens data efter:

> *"Persondataforordningen kommer til at betyde, at vi får ryddet op på en positiv måde. Vi har mange oplysninger, der bare ligger, uden vi bruger dem."*

Mange virksomheder har ikke tidligere forholdt sig til "levetiden" på data – altså at data har en livscyklus og skal slettes på et tidspunkt. Dels har der ikke været en struktureret tilgang for at sikre, at data blev slettet med bestemte intervaller, eller når et projekt afsluttes. Dels kan det være angstprovokerende at slette data. Som en it-chef formulerer det:

> *"Det kræver utrolig meget mod at turde slette noget."*

Flere virksomheder fortæller, at de nu vil skabe større disciplin omkring sletning af data ved at gøre det til en del af virksomhedens procedurer – procedurer der skal følges op på fra centralt hold, fremfor at lade det være op til den enkelte afdeling, projekt eller person, hvad der skal ske med data, når de ikke længere er nødvendige.

**OPMÆRKSOMHEDSPUNKTER**

- **Få overblik og beskriv:** Hvilke kategorier af data behandler vi? Til hvilket formål? Hvilken hjemmel har vi til det? Hvordan sikrer vi, at data kun bruges til det, der er beskrevet og kun så længe, det er nødvendigt?
- **Dataminimering:** Overvej om formålet kan opfyldes med mindre indgriben, specielt når det handler om følsomme data. Er CPR-nummer f.eks. nødvendigt, eller kan der bruges en anden nøgle, som mindsker konsekvensen ved et evt. datalæk?
- **Specifikke samtykker:** Det er ikke længere lovligt at indhente samtykke til at behandle en given type data. Der skal nu opnås et samtykke til hvert formål, data anvendes til.

## DATABEHANDLING

Begrebet 'behandling af data' dækker over enhver håndtering af data. Det kan være opbevaring, overførsel, overgivelse, at se på data eller at analysere data. Databehandling er altså både noget, der sker automatisk i systemer, og som bliver udført af mennesker med adgang til data. Dermed er det vigtigt at have styr på, hvilke processer der sker rundt omkring i virksomheden, samt hvad der sker i de systemer, der anvendes.

### ERFARINGER: HVAD SIGER VIRKSOMHEDERNE?

Der er stor forskel på, hvordan de virksomheder der har deltaget i undersøgelsen behandler data; nogle analyserer slet ikke de data, de håndterer, nogle har dataanalyse som grundlag for deres produkter og ydelser, nogle laver analyser til andre, nogle udleverer data til kunder, og nogle stiller værktøjer til rådighed for kunder, så de selv kan analysere data. Med enkelte undtagelser lægger forordningen ikke noget til hinder for, at de adspurgte virksomheder kan fortsætte disse databehandlinger som hidtil.

Dog kan forordningen vanskeliggøre nye måder at bruge data på. Fx fortæller en virksomhed, at de med henblik på at levere nye og bedre services til deres kunder ønsker i højere grad at koble deres data på de enkelte brugere af et system. Men er nu i tvivl om, hvorvidt dette vil være i strid med persondataforordningen.

Et problem flere virksomheder peger på er brugen af data til test. Som det er nu, bruges der ofte ægte data – eksempelvis om borgere eller kunder – i udviklingen af nye systemer, fordi kvaliteten af syntetiske data ikke er høj nok. En DPO fortæller om dilemmaet mellem produktudvikling og datasikkerhed:

> *"Vores udviklere vil gerne have rigtige kundedata, men det er ulovligt. Problemet er, at det er svært at lave gode testdata. Men det ville jo være forfærdeligt, hvis en testserver blev hacket, og der lå ægte data på den!"*

En anden virksomhed har fået grønt lys fra deres jurister til fortsat at bruge produktionsdata til test, så længe det sker i en pseudonymiseret form. Dog er virksomheden i tvivl om, hvornår data er tilstrækkeligt pseudonymiseret, idet de finder forordningens definition for overordnet og ukonkret til at være operationaliserbar.

Det kan være en udfordring at få privacy og datasikkerhed arbejdet ind i virksomhedernes udviklingsprocesser, fordi det ofte ikke er udviklernes førsteprioritet. De ønsker i højere grad frihed til at være kreative, og her kan datasikkerhed ses som en barriere. Omvendt bliver det sværere at få privacy og datasikkerhed ind i produktet, jo senere i processen det bliver tilføjet. Problematikken søges bl.a. imødegået gennem tjeklister, som skal gennemgås, når der laves nye projekter eller udvikles produkter.

En problematik, som virksomhederne ikke nødvendigvis selv er opmærksomme på, er brugen af visse tredjepartsværktøjer som fx Google Analytics. Med den nye persondataforordning kan brug af disse gratis services blive problematisk, da det kan være svært at gennemskue, hvad der egentlig sker med data.

Præcis hvad brugen af Google Analytics kommer til at betyde for virksomhederne, når forordningen er trådt i kraft, er stadig uafklaret. Viser det sig at være et problem, er problemet stort, da langt de fleste virksomheder har Google Analytics kørende på deres hjemmeside. Virksomhederne er typisk enten ikke opmærksomme på, at det kan udgøre en problematik, eller ved ikke, hvordan de skal løse det og forholder sig afventende i håbet om, at Google selv kommer med en løsning.

**OPMÆRKSOMHEDSPUNKTER**

- **Databeskyttelse som prioritet:** Databeskyttelse er ikke altid en prioritet for udviklere. Understøtter jeres nuværende datakultur databeskyttelse, er eller det noget, I skal blive bedre til at tænke ind?
- **Privacy-by-design:** Forordningen er baseret på principperne for *privacy-by-design* som er lavet for at sikre at privacy tænkes ind i processen fra start til slut. Man kan med fordel kigge på Rådet for Digital Sikkerheds vejledning.
- **Hjemmel til databehandling:** Er der hjemmel til databehandlingen, eller er det noget den registrerede implicit har samtykket til? Hvis det sidste er tilfældet, er databehandling ikke længere lovlig og vil kræve et eksplicit samtykke for at kunne fortsætte.
- **Tredjepartsværktøjer:** Bliver der brugt tredjepartsværktøjer som en del af databehandlingen bør man undersøge, hvorvidt disse selv behandler data eller sender data videre. Er det tilfældet, bør man have en databehandleraftale. Dette er beskrevet i næste afsnit.

## ROLLEFORDELING I DATABEHANDLING OG SLETNING

Forordningen definerer dataansvarliges og databehandleres roller og ansvar tydeligere end tidligere. Overordnet set er den dataansvarlige den, der definerer med hvilke formål og hjælpemidler en behandling foretages, mens databehandler ikke tager selvstændige beslutninger men udelukkende handler efter instruks fra den dataansvarlige. Denne skelnen er yderligere belyst i Datatilsynets vejledning om dataansvarlige og databehandlere.

Den dataansvarlige har hovedansvaret for data, for at definere formål, sikre at der er hjemmel til behandlingen, at den registreredes rettigheder overholdes, og at der foreligger en databehandleraftale med databehandleren, hvori instrukser til behandlingen er anført. Den dataansvarlige skal endvidere føre opsyn med, at databehandleraftalen overholdes. Datatilsynet har udgivet en skabelon til databehandleraftaler, som findes på deres hjemmeside: https://www.datatilsynet.dk/vejledninger/vejledninger-databeskyttelsesforordningen/

### ERFARINGER: HVAD SIGER VIRKSOMHEDERNE?

For nogle virksomheder står det endnu ikke klart, om de er databehandler eller dataansvarlig. Men det er ofte også tilfældet, at virksomheden har forskellige roller, alt efter hvilke relationer og ydelser der er tale om. Som en del af rolleafklaringen må virksomheden vurdere ansvar og risiko i de værdikæder, den indgår i, og træffe de nødvendige forholdsregler for at sikre en databehandling, der lever op til persondataforordningen, såsom at vælge de rette leverandører og samarbejdspartnere. En DPO fortæller, at GDPR-compliance vil veje tungt i virksomhedens valg af partnere fremadrettet:

> *"Vi kommer til at vælge partnere på en anden måde i fremtiden. Det er billigere for os at betale mere for ydelsen hos nogen, der har styr på dokumentationen."*

At have rollen som dataansvarlig indebærer generelt et større ansvar for databehandlingen – og dermed også en større risiko. Nogle virksomheder ønsker derfor ikke at indtage rollen som dataansvarlig, og placeringen af ansvaret kan til tider blive en varm kartoffel mellem samarbejdspartnere.

Rollen som dataansvarlig medfører, som virksomhederne udtrykker det, en forpligtelse til at gå forrest i arbejdet med at sikre, at der er den nødvendige sikkerhed og de rette procedurer omkring databehandlingen. Et første skridt har for mange virksomheder været at få styr på databehandleraftalerne, fx i forbindelse med, at de gamle alligevel skulle opdateres. Næste skridt er at begynde at føre tilsyn med databehandlerne, sådan som forordningen kræver det. Der peges fra virksomhedernes side på, at der altid har været en dialog med databehandlerne, men at det nu skal formaliseres, og tiltagene skal dokumenteres. Som en DPO påpeger:

> *"Når man laver tilsyn, skal det have karakter af tilsyn – ikke bare erfaringsudveksling."*

Generelt er det ikke så meget selve tilsynene, der skaber bekymring hos virksomhederne, men i højere grad det at skulle håndhæve dem og fx opsige samarbejder, fordi en databehandler ikke lever op til kravene. En it-chef reflekterer omkring sin e-shop:

> *"Skal jeg fx smide min eneste service provider på betaling ud?? Det kan jeg ikke gøre fra den ene dag til den anden."*

**OPMÆRKSOMHEDSPUNKTER**

- **Databehandler/dataansvarlig:** Gør dig klart, om du er databehandler eller dataansvarlig. Du vil ofte have forskellige roller i forskellige sammenhænge.
- **Databehandleraftale:** Er du dataansvarlig eller har underdatabehandlere, sørg da for databehandleraftaler, fx efter Datatilsynets skabelon.
- **Databehandleren ved ofte mest:** I de tilfælde hvor databehandleren er leverandør af system(er) til den dataansvarlige, vil databehandleren ofte være den der ved mest og kan rådgive den dataansvarlige om, hvilke løsninger der skal vælges. Det anbefales derfor at have en god dialog mellem parterne ved som leverandør at tage initiativet på området og som dataansvarlig at søge råd hos sine leverandører.

## ANONYMISERING OG PSEUDONYMISERING

Forordningen gælder for alle virksomheder, der har med persondata at gøre. En måde at sikre persondata er gennem pseudonymisering, hvor *identificerende* data, som fx navn og personnummer, erstattes med et af virksomheden kendt ID, som for udenforstående ikke kan henføres til personen. Dette gør, at man kan sammenligne data om et individ, uden nødvendigvis at vide hvem individet er.

Et eksempel kan være, at man gerne vil vide, hvordan en specifik person bevæger sig i et indkøbscenter ved hjælp af WIFI-signaler. I stedet for at gemme en unik *identifier* som fx en MAC-adresse kan man i stedet hashe den og gemme et pseudonym. På den måde kan man kæde forskellige WIFI-målinger sammen, uden at kende MAC-adressen. Pseudonymiserede data er stadig persondata, men metoden kan anvendes som et middel til dataminimering.

Vil man sikre data endnu mere, kan man vælge kun at gemme anonymiseret data. Det betyder, at man ikke længere har med persondata at gøre, og dermed gælder forordningen ikke for denne type data. Et eksempel kunne være at man, modsat eksemplet før, ikke er interesseret i at vide, hvordan en specifik person bevæger sig, men i stedet bare vil vide, hvor mange personer der er i et givent område på et bestemt tidspunkt. Ved anonymisering er det vigtigt, at en person ikke kan gen-identificeres.

I vurderingen af, om personer kan genidentificeres, skal der tages højde for alle rimelige hjælpemidler. Har man fx en løberute på et kort med start- og slutsted ved samme bolig, vil der ofte kunne udledes information om den pågældende person, til trods for at det kun er

ruten, der fremgår. Det kan fx gøres ved at sammenkæde informationen med krak.dk og dermed finde ud af, hvem der løber denne rute.

### ERFARINGER: HVAD SIGER VIRKSOMHEDERNE?

Anonymisering og pseudonymisering kan for virksomhederne være et redskab til at bruge følsomme data på en sikker måde – eksempelvis til at lave test i udviklingen af nye systemer, eller når data deles med eksterne parter. Dog kan det være uklart for virksomhederne, hvornår der er tale om hhv. anonymisering eller pseudonymisering, og udtrykkene bruges af og til forkert. Samtidig hersker der en vis tvivl om, hvor meget data skal anonymiseres eller pseudonymiseres for at være tilstrækkeligt sikret. Som en konsulent forklarer, fremgår det ikke helt tydeligt af forordningen:

> *"Problemet er, at det er enormt ukonkret, hvornår noget er pseudonymiseret. Der står, at personer ikke må kunne identificeres ved hjælp af 'rimelige sekundære kilder' – hvad er det?"*

I nogle virksomheder bruges pseudonymisering også som alternativ til sletning. Eksempelvis kan der være tilfælde, hvor en kunde ønsker at blive slettet fra et system – men hvor det pga. anden lovgivning (fx revisorloven) er påkrævet, at disse data opbevares i 5 år. Her vil kunden stadig findes i systemet, men i en deaktiveret, pseudonymiseret form, så vedkommende ikke kan søges frem af medarbejderne

### OPMÆRKSOMHEDSPUNKTER

- **Anonymisering eller pseudonymisering:** Find ud af, hvilken metode der er tale om, eller hvilken metode du har brug for. Det kan være svært at få styr på, men det er meget vigtigt, da forordningen forholder sig meget forskelligt til anonymisering og pseudonymisering.
- **Anonymisering og pseudonymisering er svært:** Det kan være svært at finde ud af, hvornår oplysninger er tilstrækkeligt anonymiseret eller pseudonymiseret. Hent eventuelt hjælp udefra til at finde ud af, hvordan I kan gøre. Som minimum bør I dokumentere, hvorfor I mener, I har foretaget tilstrækkelige foranstaltninger.

## DOKUMENTATION

Et af de væsentlige nye elementer i persondataforordningen er kravet om dokumentation. Tidligere har der været krav om indberetning til Datatilsynet i visse tilfælde. Dette krav bortfalder, mens der til gengæld kræves dokumentation for, hvilke data der behandles, om hvem, til hvilket formål, samt hvem data videregives eller overlades til, og hvilke foranstaltninger der er taget for at sikre data og den registreredes rettigheder. Se Datatilsynets vejledning om fortegnelse for yderligere information.

### ERFARINGER: HVAD SIGER VIRKSOMHEDERNE?

Noget af det der er nyt for virksomhederne er det øgede fokus på dokumentation. Nu er det ikke længere er nok i sig selv at arbejde med informationssikkerhed – det skal også dokumenteres. Som Dansk Industri formulerer det i deres vejledning om persondataforordningen:
*"Hvis noget ikke er dokumenteret, er det ikke gjort."*

I nogle virksomheder ses dokumentationskravet som værende meget ligetil, idet det opfattes som et spørgsmål om blot at dokumentere de tiltag, der allerede findes i virksomheden. En DPO forklarer, at arbejdet for dem består i at nedfælde de tanker, de har gjort sig på området:

> *"Der er jo ikke noget nyt i det her, men du skal nu kunne dokumentere, at du har nogle strukturer og processer på plads i forhold til det her."*

Hos de mere usikre virksomheder ses dokumentationskravet som en meget stor, administrativ arbejdsbyrde, og de kan være i tvivl om, hvornår dokumentationen er tilstrækkelig – hvor meget skal dokumenteres, og i hvilken form?

### OPMÆRKSOMHEDSPUNKTER

- **Accountability:** Hensigten med dokumentationen er at kunne påvise ansvarlighed ('accountability').
- **Form:** Der er ingen eksplicitte krav til formen på dokumentationen, og det anses for tilstrækkeligt med et eller flere Word-dokumenter og/eller Excel-ark.
- **Indhold:** I forhold til indholdet er kravene beskrevet i Datatilsynets vejledning om fortegnelse, og man kan tage udgangspunkt i et regneark udarbejdet af Henning Mortensen, tidligere chefkonsulent i Dansk Industri (DI).

## DATA PROTECTION OFFICER

Persondataforordningen kræver i visse tilfælde, at virksomheder ansætter en Databeskyttelsesrådgiver – på engelsk *Data Protection Officer* (DPO) – som skal understøtte, at den dataansvarlige overholder persondataforordningen. DPO'en skal rådgive virksomheden om databeskyttelse og være kontakten til Datatilsynet på virksomhedens vegne, og virksomheden skal sørge for, at DPO'en inddrages rettidigt og tilstrækkeligt i spørgsmål om beskyttelse af persondata. Inddragelsen bør ske på øverste ledelsesmæssige niveau.

De færreste private virksomheder skal have en DPO – kravet gælder kun, hvis disse tre forhold gør sig gældende: 1) behandling af personoplysninger er virksomhedens kerneaktivitet, 2) der behandles personoplysninger i et stort omfang og 3)

behandlingsaktiviteten består i regelmæssig og systematisk overvågning af personer eller vedrører følsomme oplysninger eller oplysninger om strafbare forhold.

### ERFARINGER: HVAD SIGER VIRKSOMHEDERNE?

Der er i praksis meget forskellige tolkninger af DPO'ens rolle, samt hvilke funktioner og kompetencer vedkommende skal have. Blandt de adspurgte virksomheder har der både været DPO'er med teknisk og juridisk baggrund. Hvor nogle har det at være DPO som deres primære funktion, er det for andre en tillægstitel, de har fået ved siden af deres job som eksempelvis jurist eller leder for en afdeling. Der ses også eksempler på, at der i større organisationer er en overordnet DPO, som hjælper lokalafdelingerne i arbejdet med forordningen, og som fremadrettet vil komme og føre tilsyn. En lignende konstellation findes også, hvor DPO'en er en ekstern person, der fungerer som DPO for flere forskellige organisationer.

Uvildighed er en grundlæggende forudsætning for, at DPO'en reelt kan lave de vurderinger og tilsyn, der ligger i opgaven. Det kan være svært for især mindre virksomheder at finde en person i organisationen, som kan indtage denne position. En DPO, der i sin egenskab af jurist for virksomheden både skal udføre og overvåge arbejdet med at leve op til forordningen, fortæller om udfordringen i at holde tingene adskilt:

> *"Det kan være svært i en virksomhed som vores. Fordi vi ikke er så mange, har vi jo alle sammen lidt skiftende kasketter på. […] Ift. compliance er det jo også mig, der i praksis laver meget af det udførende arbejde, så jeg skal finde ud af at skille tingene ad, så jeg ikke overvåger mit eget arbejde."*

En anden DPO fortæller, at han i sin egenskab af CTO måske kunne ses som værende uegnet til rollen:

> *"Men i og med, at jeg har et vist medejerskab, er jeg ikke så nervøs for det. Og så er vores virksomhed jo også startet på bløde værdier."*

DPO'en får ansvaret for virksomhedens GDPR-proces og er på forskellig vis med til at gennemføre implementeringen. Hun kan fx udstikke de overordnede retningslinjer, som afdelingerne hver især skal arbejde ud fra, eller hun kan komme ud i de enkelte afdelinger og være aktivt med i deres del af arbejdet. Uanset hvordan DPO-rollen gribes an, er det afgørende, at DPO'en har den nødvendige indflydelse og opbakning til at gøre ændringer og nye procedurer gældende. Sådan er det fx hos denne DPO, der fortæller, at beslutningerne omkring data i sidste ende ligger hos hende:

> *"Hvis ikke vi kan blive enige, så træffer jeg beslutningen. Med DPO-rollen følger også betydeligt mandat – i hvert fald hos [os]. Ellers ville det være en umulig opgave."*

**OPMÆRKSOMHEDSPUNKTER**

- **Forankr ansvaret hos én person:** Selvom det ikke er påkrævet, at din virksomhed har en DPO, er det en god ide at sørge for, at der er en forankring af ansvaret for håndtering af persondata hos en enkelt person, og at denne person har mandat til at træffe beslutninger på området. Vælger I frivilligt at have en DPO, skal vedkommende leve op til samme krav som en lovpligtig DPO. Derimod kan man som virksomhed selv definere, hvad der ligger i fx en 'compliance-rådgiver's rolle.
- **DPO'ens faglige kompetencer:** Der er stor variation i fagligheden hos de personer, der varetager DPO-rollen. Der er ingen krav til uddannelsesmæssig baggrund, men vedkommende skal udpeges ud fra sine faglige kvaliteter og kan eventuelt videreuddannes på områder, som ligger ud over disse.
- **Hvem kan være DPO:** DPO'en kan både være intern og ekstern (fx en advokat, revisor, it-rådgiver mm.). En intern DPO skal være uafhængig og må ikke have det øverste ansvar, ergo bør det altså ikke være it-chefen eller HR-chefen, men det kan godt være en anden ledende medarbejder, som påtager sig dette arbejde på deltid.

## REGISTREREDES RETTIGHEDER

### KORT OM FORORDNINGEN

Persondataforordningen giver den registrerede ret til at få indsigt i, rettet og udleveret de data, der er indsamlet om vedkommende. Udleveringen af data skal yderligere gøres i et maskinlæsbart format, så det er nemt for den registrerede at bruge data igen. Dette betyder, at virksomheden skal have en procedure for at kunne ændre i data, for at finde alt data om en registreret på tværs af systemer samt for at udlevere denne data på en standardiseret måde.

Se generel vejledning om forordningen på datatilsynets hjemmeside. I skrivende stund er vejledningen om Registreredes rettigheder endnu ikke udgivet.

### ERFARINGER: HVAD SIGER VIRKSOMHEDERNE?

Med den nye persondataforordning får den registrerede ret til at få indsigt i, rettet og udleveret de data, der er indsamlet om vedkommende. Dog regner virksomhederne ikke med at få nogen videre efterspørgsel på dette område, eftersom de arbejder med data, de enten ikke mener, at folk har ret til eller interesse i at få udleveret. Som denne udtalelse fra en it-konsulent viser, er det derfor ikke et område, der får nogen særlig opmærksomhed i virksomhedernes GDPR-projekter:

> *"Det er ikke en problematik i sig selv at trække data ud – ganske enkelt fordi jeg ikke tror, at mange kommer til at bede om det."*

De fleste regner således med at foretage udtrækningen manuelt, hvis der mod forventning skulle komme henvendelser fra personer, som ønsker at få deres data. Dog ses der også eksempler på selvbetjeningsløsninger, hvor registrerede kan gå ind og søge om at få deres data udleveret. En projektleder fortæller, at de har valgt denne løsning for at være på den sikre side:

> *"Vi kan jo ikke vide, hvor mange der beder om det – hvis der kommer 500 på en måned, bliver vi lagt ned. Så det er en risikoafdækning i forhold til kravet om at levere inden for 30 dage."*

Han peger i den forbindelse på, at der kan komme mange forskellige typer af henvendelser, og at de som en større virksomhed fx kan opleve, at der er en del journalister, der i forordningens første måneder vil afprøve, om virksomhederne faktisk kan opfylde de registreredes rettigheder.

Der er to praktiske udfordringer forbundet med den registreredes ret til at få indsigt i, rettet og udleveret data. Den ene handler om at finde frem til og have overblik over data om den enkelte, som kan ligge spredt i virksomhedens forskellige systemer. Den anden er, at der hersker tvivl om, i hvilket format data skal og bør udleveres. Dels peges der på, at der i forordningen optræder forskellige formuleringer, såsom 'machine readable' og 'standard technical format', dels efterlyses der konkrete forklaringer på, hvad disse begreber dækker over. Er det en CSV-fil, er det tilstrækkeligt med rå data, eller skal de være bearbejdede, hvordan skal de forskellige databaser og filformater køres sammen etc.?

**OPMÆRKSOMHEDSPUNKTER**

- **Er der understøttelse i nuværende systemer:** Find ud af, om de nuværende systemer understøtter registreredes rettigheder. Hvis ikke, er det vigtigt at få set på, hvordan I gør det muligt.
- **Hvor stor bliver efterspørgslen:** Overvej i hvor høj grad rettighederne vil blive efterspurgt. Er det noget, der kommer til at ske en sjælden gang, kan det være tilstrækkeligt at have procedurer for, hvordan en medarbejder laver udtrækket manuelt. Er det derimod noget, som vil ske tit, kan det med fordel understøttes i systemerne.

## SLETNING

Retten til at blive slettet er et vigtigt element i forordningen. Det nye her er, at den registrerede har ret til få alle data om sig selv slettet, medmindre dataansvarlig har særlig lovpligtig ret til at gemme oplysninger. Et oplagt eksempel på dette er kriminalregisteret, hvor man ikke uden videre kan bede om at få sin straffeattest slettet.

## ERFARINGER: HVAD SIGER VIRKSOMHEDERNE?

Sletning er et af de emner, hvor der hos virksomhederne er en del tvivlsspørgsmål og tekniske problematikker, som er svære at løse. Det største er, hvornår noget er slettet tilstrækkeligt.

Et emne herunder er håndtering af backups. At slette i en backup kan i praksis kræve, at man tager alle backups, gendanner dem, sletter den registrerede og så gemmer backuppen igen. Ligger backuppen på bånd, vil det i praksis være i bedste fald besværligt og i værste fald umuligt at fjerne registreredes data fra backups. En alternativ løsning kunne være at holde styr på, hvilke registrerede der ønsker at blive slettet og så sørge for, at denne liste gennemføres, hver gang en backup gendannes. Dvs. at den registrerede stadig eksisterer på fx båndene, men at der er mekanismer, som sørger for at slette de berørte brugere ved gendannelse. Der er heller ikke klarhed over, om det faktisk er et krav i forordningen, at data skal slettes fra backuppen med det samme, eller om det er tilstrækkeligt, at de bliver det, når backuppen rutinemæssigt destrueres med bestemte tidsintervaller.

Et lavpraktisk forhold der i første omgang kan være en udfordring, men som på sigt vil være en hjælp for virksomhederne, er selve overblikket over, hvilke data der findes om den enkelte i organisationen, samt hvor de ligger. Virksomheder har ofte mange forskellige systemer med dataopsamling, og da de ikke nødvendigvis er kørt sammen, kan der ligge et stort arbejde i at opspore data, hvis en registreret beder om at blive slettet. Hertil kommer de tilfælde, hvor data deles med eksterne.

I forhold til selve sletningskravet påpeger flere, at det ikke nødvendigvis kommer til at gælde for dem, fx pga. anden lovgivning – såsom Revisorloven – eller fordi de arbejder med data, som tilhører det offentlige. En teknologi- og sikkerhedsdirektør påpeger, at man som virksomhed bør have for øje, at der vil være en del undtagelser:

> *"Det er jo ikke sådan, at man ALTID har retten til dataportabilitet – eller ALTID har retten til at "be forgotten." [...] Specielt i den offentlige sektor – der er masser af de her rettigheder, der ikke kommer i spil i eksempelvis den offentlige sektor."*

Registrerede har derfor ikke altid ret til at få slettet sine data.

**OPMÆRKSOMHEDSPUNKTER**

- **Sletning i backups:** Det er vigtigt, at I forholder jer til, hvordan I håndterer sletning i forbindelse med backups. Hvis ikke det er praktisk muligt at slette i selve backuppen, er det nødvendigt at have procedurer, der sørger for, at personer som har bedt om sletning også stadig er slettet efter en gendannet backup.
- **Lovmæssige krav:** Der kan være lovmæssig hjemmel for, at I ikke må slette en person, selvom vedkommende beder om det, som fx i kriminalregisteret. Få styr på, hvorvidt I har lovmæssig hjemmel for ikke at skulle slette data. Findes denne hjemmel ikke i loven, kan I ikke nægte folk at blive slettet.

## RISIKOVURDERING OG KONSEKVENSANALYSE

Persondataforordningen kræver, at dataansvarlige træffer passende foranstaltninger med henblik på at sikre registreredes rettigheder og frihedsrettigheder. Det er derfor nødvendigt at lave en vurdering af, hvor stor risiko der er for datamisbrug, og hvad konsekvensen for den registrerede kan være. Det er den dataansvarliges ansvar at sørge for, at de foranstaltninger der foretages for at nedsætte risikoen for datalæk er tilstrækkelige i forhold til konsekvensen af et datalæk.

I skrivende stund, arbejder Datatilsynet på en vejledning om konsekvensanalyse. Når denne er færdig vil den være at finde på Datatilsynets hjemmeside. Indtil da henvises til vejledningen fra artikel 29 gruppen.

### ERFARINGER: HVAD SIGER VIRKSOMHEDERNE?

De fleste af virksomhederne er endnu ikke gået i gang med risikoanalyser – bl.a. fordi der er nogle usikkerheder på området. Dels kan der være tvivl om, hvornår vurderingerne skal foretages, dels mangler der en metode at lave dem efter. Selve det at foretage risikovurderinger er ikke nødvendigvis nyt for virksomhederne, men med forordningen sker der en ændring i fokus. Hvor det hidtil har handlet om risikoen for, at forretningen kunne lide skade, handler risikovurderingerne nu om de potentielle konsekvenser for den registrerede og kræver dermed et helt nyt mindset hos virksomhederne.

**OPMÆRKSOMHEDSPUNKTER**

- **Skal der laves en konsekvensanalyse?** For at vurdere om der skal laves en konsekvensanalyse, kan der skeles til vejledningen fra artikel 29 gruppen, specielt eksemplerne på side 13-14.
- **Er I i tvivl?** Det anbefales at lave en konsekvensanalyse, hvis I er i tvivl, og minimum argumentere for, hvorfor I mener det ikke er nødvendigt.
- **Hvornår laves en konsekvensanalyse?** Idet den skal tilpasses ved ændringer, er det en løbende proces at lave konsekvensanalyse. Det anbefales at starte konsekvensanalysen så tidligt som muligt i projektet, da det kan have stor indflydelse på udformningen og muligheden for at gennemføre projektet.
- **Hvordan laves konsekvensanalysen?** Konsekvensanalysen kan f.eks. tage udgangspunkt i DI's Data Protection Impact Assessment skabelon

# Forordningen og de mindre virksomheder

Det er forskelligt, hvor de små virksomheder er i arbejdet med forordningen. Nogle føler, de "famler i blinde," mens andre fortæller, at de tager det ét skridt ad gangen og selv finder deres vej i det, sådan som de plejer at gøre, når der sker nye ting, de skal forholde sig til.

Brancheorganisationer, lokale erhvervsråd o.lign. spiller en central rolle som det sted, virksomhederne går hen for at få den nødvendige og relevante viden. Dog kan det være svært for virksomhederne at få svar på de specifikke spørgsmål, der opstår, når de selv går i gang med arbejdet, fordi de mangler en juridisk kompetence til at besvare dem. Da der for nogle løsningsudbydere i salgsøjemed kan være en interesse i at blæse forordningen op som et stort, næsten uoverstigeligt projekt, kan det også være svært for virksomhederne at gennemskue, hvad de skal lytte til, hvor de skal sætte ind, og hvilke krav de skal stille til rådgivere etc.

Holdningen til forordningen er mindre positiv blandt de små virksomheder end hos de større; den ses af mange som et stort og ressourcekrævende stykke arbejde, som i bund og grund ikke tilfører virksomheden nogen værdi, men bare skaber en masse bøvl. Dette kan bl.a. tilskrives, at virksomhederne selv mener, at de allerede har de rette procedurer omkring data, men også at de ikke ser datahåndtering som en problematik.

Det fortælles i interviewene, at virksomheden allerede passer godt på data ved fx at have password-adgang til computere, eller at sletning af gamle data er unødvendig, da de alligevel ikke går ind og kigger på dem. Hertil kommer, at virksomhederne opfatter sig selv som værende for små og deres data for uinteressante til, at nogen skulle have interesse i at hacke dem. Det betyder dog ikke, at virksomhederne ikke går ind i arbejdet med forordningen, men blot at indsatsen i højere grad begrænses til det nødvendige. Som en virksomhedsejer forklarer, er der en opmærksomhed på, at arbejdet med forordningen ikke må blive for stort:

> *"Vi har besluttet, at vi på ingen måde skal være front runners i det her system. Vi skal bare leve op til det, vi skal leve op til, og på det tidspunkt, hvor det er påkrævet."*

Samtidig er der mindre angst for bøder og tilsyn blandt de små virksomheder – de mener ikke, at de er de første, Datatilsynet vil besøge og regner samtidig med at få en chance for at rette op på tingene, hvis der skulle være fejl og mangler. Qua deres størrelse har de mindre virksomheder ikke adgang til de samme ressourcer, som de større virksomheder. Der er fx ikke altid økonomisk råderum til at inddrage rådgivere, og det fortælles, at det kan være svært at trække folk ud af den daglige drift for enten at drive eller deltage i projektet omkring forordningen. Arbejdet med forordningen hviler dermed på bestemte personer og bliver ofte meget personbåret i de mindre virksomheder.

Det har dels indflydelse på de løsninger, der anvendes, dels kan det skabe en sårbarhed, hvis vedkommende viser sig ikke at have de nødvendige kompetencer, får travlt med andre ting eller forlader virksomheden. En anden udfordring for de mindre virksomheder er, at de er mere afhængige af systemudbyderne end de større virksomheder, der ofte har egen- eller særudviklede systemer. De mindre virksomheder kan heller ikke i samme omfang gøre krav gældende over for systemudbyderne, hvilket fx er udfordrende på de felter, hvor der kun er få systemer at vælge imellem.

**OPMÆRKSOMHEDSPUNKTER**

Der er mange steder at søge information vedrørende persondataforordningen, og det kan være svært at gennemskue, hvem I skal lytte til. Nedenfor er opsummeret nogle gode muligheder:

- **It-kriminalitet kan ramme alle:** Det er vigtigt, at I er opmærksomme på jeres it-sikkerhed, specielt hvis I behandler personoplysninger. Sikkerhedstjekket.dk hjælper med at skabe et overblik over evt. svagheder i virksomhedens it-sikkerhed og giver målrettet vejledning om, hvor der bør sættes ind først for at mindske risikoen for brud. Værktøjet er udviklet af Erhvervsstyrelsen og Rådet for Digital Sikkerhed. https://sikkerhedstjekket.dk/

- **Arrangementer:** Mange aktører inviterer til arrangementer om persondataforordningen. Det kan anbefales at kigge efter hvad DI, DE, væksthuse, erhvervsråd og brancheforeningerne arrangerer.

- **Brancheforeninger:** Flere brancheforeninger har vejledninger, der er tilpasset den enkelte branche, ligesom de kan udarbejde adfærdskodeks eller certificeringer. Det er en god ide at tjekke jeres brancheforenings hjemmeside og ellers kontakte dem for at høre om planerne ift. forordningen.

- **Konsulenter:** Det er en god ide at rådføre sig med sine leverandører, der gerne skal kunne svare på spørgsmålene i forbindelse med deres produkter. Derudover kan uafhængige it-konsulenter hjælpe med at skabe et overblik og sikre de rette investeringer ved nyindkøb, og it-revisorer kan hjælpe med at få overblik, skabe en handleplan og løbende sikre at virksomhedens it lever op til kravene. Organisationsudviklere kan hjælpe med den organisatoriske implementering og sikre, at medarbejderne involveres i de ændringer, der skal foretages.

- **Privacykompasset.dk** – PrivacyKompasset er en online test, der skal hjælpe virksomheder i gang med at efterleve databeskyttelsesreglerne og få svar på helt basale spørgsmål i forhold til ansvarlig datahåndtering. Værktøjet er udviklet af Erhvervsstyrelsen.

- **Vejledninger:** Udover de vejledninger som brancheforeninger udgiver vil Datatilsynet løbende udgive vejledninger på deres hjemmeside. Desuden anbefales Datatilsynets guide "12 spørgsmål som dataansvarlige allerede nu med fordel kan forholde sig til".

# Områder der kan være vanskelige for virksomhederne

Virksomhederne har peget på følgende områder, hvor der opstår vanskeligheder i implementeringen af forordningen – enten fordi det er noget, der indebærer et stort arbejde, virksomheden mangler metoder og teknologi til at udføre opgaven, eller der er uklarheder i forordningen.

- **Overblik:** Det kan være tidskrævende og vanskeligt at få overblik over de softwaresystemer og data, der findes i virksomheden, og virksomhederne kan mangle en metode eller proces for, hvordan det gribes an.
- **Rolle i databehandlingen:** Det er ikke altid gennemskueligt for virksomhederne, om de er databehandler eller dataansvarlig. Hertil kommer en tvivl om, hvilken rolle visse tredjeparter indtager. Det være sig fx Google ved brug af Google Analytics.
- **Deling af data på tværs af grænser:** Der hersker megen tvivl om, hvad reglerne er for deling af data på tværs af grænser, når der er tale om datterselskaber, lokalafdelinger o.lign.
- **Samtykke:** Det ikke tydeligt for virksomhederne, hvor ofte der skal bedes om samtykke, og hvor længe det skal opbevares.
- **Anonymisering og pseudonymisering:** Det er ofte svært for virksomhederne at vurdere, hvornår data er tilstrækkeligt anonymiseret eller pseudonymiseret.
- **Sletning ift. backup:** Grundet backups er det meget vanskeligt for virksomhederne helt at slette en registreret. Virksomhederne efterlyser en uddybning af, hvordan proceduren skal udføres i praksis, og hvad den konkret omfatter.

# Metode

# Interviews med virksomheder

Undersøgelsen er en kvalitativ undersøgelse, som har til formål at få et dybdegående indblik i, hvordan danske virksomheder griber implementeringen af persondataforordningen an. Dette er sket gennem interviews med nøglepersoner om indsatsen i de pågældende virksomheder. Alle virksomheder er blevet udvalgt ud fra et kriterium og en formodning om, at de håndterer personfølsomme data i større omfang end blot i HR- og CRM-sammenhæng.

Virksomhederne er rekrutteret gennem Alexandra Instituttets netværk og er blevet inviteret til at deltage i undersøgelsen via målrettede emails til de virksomheder og personer, vi fandt interessante. I første omgang forsøgte vi at rekruttere både små, mellemstore og store virksomheder, men det var kun mellemstore og store virksomheder, der havde interessen og/eller tiden til at medvirke.

Som forundersøgelse gennemførte vi 4 ustrukturerede telefoninterviews under emnet “den nye persondataforordning”. Formålet med denne del var at udforme spørgeguiden til hovedundersøgelsen. Hovedundersøgelsen bestod af 10 interviews med store og mellemstore virksomheder, og den blev gennemført som semi-strukturerede interviews ude hos virksomhederne, bortset fra to som foregik over Skype. Til interviewene deltog to medarbejdere fra Alexandra Instituttet – en sikkerheds- og privacyekspert og en antropolog. Interviewene blev gennemført i Q3 2017.

Som nævnt var det vanskeligt at rekruttere små virksomheder til on-site interviews, og vi valgte derfor at forsøge at rekruttere små virksomheder til 5 telefoninterviews, hvilket lykkedes. Disse interviews blev gennemført af en antropolog fra Alexandra Instituttet i Q4 2017. Interviewene fra hovedundersøgelsen samt telefoninterviewene med de mindre virksomheder blev efterfølgende kodet af en antropolog og underlagt en tværfaglig analyse. Det er resultaterne af denne analyse, der danner grundlaget for rapporten.

Interviewteamet bestod af sikkerheds- og privacyeksperterne: Mads Schaarup Andersen, Berit Skjernaa og Jonas Lindstrøm samt antropologerne: Laura Lynggaard Nielsen og Mia Kruse Rasmussen.

# Rapportens forfattere

**MADS SCHAARUP ANDERSEN**

Senior IT Consultant, PhD
Alexandra Instituttet

mads.andersen@alexandra.dk

**LAURA LYNGGAARD NIELSEN**

Specialist Anthropologist
Alexandra Instituttet

laura.nielsen@alexandra.dk

**BERIT SKJERNAA**

Senior Security and Privacy Specialist, PhD
Alexandra Instituttet

berit.skjernaa@alexandra.dk