

EVA JARBEKK | SIMEN SOMMERFELDT



# PERSONVERN OG GDPR I PRAKSIS

2. UTGAVE

CAPPELEN DAMM AKADEMISK

Eva Jarbekk og Simen Sommerfeldt

# Personvern og GDPR i praksis

ÇAPPELEN DAMM AKADEMISK

© CAPPELEN DAMM AS, Oslo, 2024

ISBN 978-82-02-72596-9

2. utgave, 1. opplag 2024

Materialet i denne publikasjonen er omfattet av åndsverklovens bestemmelser. Uten særskilt avtale med Cappelen Damm AS er enhver eksemplarfremstilling og tilgjengeliggjøring bare tillatt i den utstrekning det er hjemlet i lov eller tillatt gjennom avtale med Kopinor, interesseorgan for rettighetshavere til åndsverk. Enhver bruk av hele eller deler av utgivelsen som input eller som treningskorpus i generative modeller som kan skape tekst, bilder, film, lyd eller annet innhold og uttrykk, er ikke tillatt uten særskilt avtale med rettighetshaverne.

Bruk av utgivelsens materiale i strid med lov eller avtale kan føre til inndragning, erstatningsansvar og straff i form av bøter eller fengsel.

#### Lisenser

Contains public sector information licensed under the Open Government Licence v3.0

Maler og sjekklister basert på materiale fra ICO er underlagt følgende lisens: <http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/>

Omslagsdesign: Kristin Berg Johnsen

Sats: Bøk Oslo AS

Trykk og innbinding: AIT Grafisk AS

[www.cda.no](http://www.cda.no)

[akademisk@cappelendamm.no](mailto:akademisk@cappelendamm.no)



## Forord til 2. utgave

Vi er glade for å konstatere at den første utgaven av denne boken ble godt mottatt og vi har fått flere forespørsler fra lesere – og forlegger – om å oppdatere den. Det har utvilsomt skjedd mye innen personvern siden den første utgaven, og deler av teksten trengte en revisjon. Noe av det mest påfallende er hvor internasjonalt fagfeltet er blitt. Det kommer mange dommer fra Europa som har umiddelbar og stor betydning for virksomheter i Norge. Det er både spennende og utfordrende. Likeledes kommer det en stor mengde veiledere fra Personvernrådet (EDPB) som gir føringer for hva som er riktige tolkninger av regelverket. Det er mer enn nok å holde seg oppdatert på, men man skal også huske at de store hovedlinjer ligger fast.

I forkant av den første utgaven av boken, var personvern et felt for «spesielt interesserte» og vi må vel kunne si at regelverket som fantes før GDPR ikke alltid ble etterlevd. Så ble plutselig personvern noe «alle» måtte forholde seg til, og vi opplevde en enorm etterspørsel etter praktiske råd, foredrag og opplæring. Etterlevelsen har nok også tatt seg opp, selv om det (alltid) vil være ting å arbeide mer med.

Etter hvert har nok mange også innsett at personvern er en kontinuerlig øvelse som ikke tok slutt da det første personvernprosjektet i 2018 var ferdig eller når en innleid konsulent hadde levert noen rutiner som bedriften skulle følge. Nå ser vi at mange virksomheter bemanner opp sine personvernsteam. Det er rett og slett mangel på flinke personvernfolk. Det er også en mye større forståelse for at personvernombudet skal ha en uavhengig posisjon og en gjennomgående profesjonalisering av faget.

Heldigvis har personvern blitt en langt mer integrert del av hva folk oppfatter som almen digital dannelse, men det er en krevende kompetanse å tilegne seg. Forklaringen på dette går vi litt inn på i innledningen og dette henger sammen med vår motivasjon for å skrive denne boken og for å revidere den: Folk trenger en guide som ikke bare forteller hva *teorien* rundt personvern er, men som også gir nyttige tips til *hvordan* en skal innrette seg med både teknologi, dokumentasjon og organisasjon.

En annen trend er at flere regelverk enn bare personvernforordningen, griper inn i hvordan man kan forvalte personopplysninger. Et åpenbart eksempel er AI Act som ennå ikke er inkorporert i norsk rett, men som nok blir det i løpet av kort tid. Regelverket griper inn i hvordan personopplysninger kan forvaltes, samtidig som GDPR ligger fast som en bærebjelke i bunn.

Vi er glade for at Torgeir Waterhouse igjen har villet skrive en introduksjon. Torgeir er en av samtidens mest iherdige debattanter innenfor personvern og han er kunnskapsrik om hva som er reelle problemer for individer, privat virksomhet og forvaltning. Hans betraktninger er høyst lesverdige.

Vi har også igjen bedt et knippe av personvernombud og andre som har mye erfaring med å arbeide med personvern om å dele sine erfaringer som ombud med oss. De er spesielt valgt ut til å gi innspill fordi de dels har lang erfaring og dels fordi de kommer fra ulike bransjer og representerer både privat og offentlig sektor. Dette har vi gjort ved at vi har stilt dem en rekke spørsmål, som de har besvart, og resultatet har blitt et eget kapittel. En stor takk til alle som bidro.

Kapittelet om personvernkonsekvensvurderinger (PVK) ble justert som et resultat av en workshop som vi organiserte sammen med Tone Hoddø Bakås. Vi retter selvfølgelig en takk til alle som var med på denne.

Vi ønsker også å rette en stor takk til Johan Paramanathan, som har hjulpet oss med en gjennomgang av kapittelet om smidig utvikling med innebygd personvern.

Til slutt ønsker vi å takke Hans A. Tvedt som har vært en førsteklases og hyggelig forlegger for begge utgavene.

# Forord til 1. utgave

De siste årene har de av oss som har arbeidet med personvern gnidd oss i øynene annenhver dag. Hvordan i alle dager har det hatt seg at «alle» nå er opptatt av personvern. Det er selvfølgelig de nye reglene fra EU som er årsaken til dette – og for å være realist er det nok mer faren for gebyrer og erstatningssøksmål som har vært en driver, heller enn en klar interesse for prinsippene bak. Det er greit det. Det blir personvern ut av det også.

Det har vært en ganske liten gruppe mennesker, teknologer og jurister, som har vært opptatt av personvern de siste 10–20–40 årene. Eva er en av dem som har arbeidet med personvern de siste 20 årene, helt fra før hun var utdannet jurist. Dette har gjort at hun veldig tidlig så at de nye EU-reglene ville få en enorm betydning. Simen var i 2014 i gang med et rådgivningsoppdrag der han hyret inn Eva for å bistå med juridiske betraktninger om personvern og databehandleravtaler. Han forstod raskt hvilke konsekvenser den kommende forordningen ville få, og ble en av de første i IT-bransjen til å skrive artikler og holde foredrag om forordningen.

Etter hvert begynte vi å holde foredrag sammen, fordi vi så at spørsmålsstillingene er tverrfaglige. Det nytter ikke å være enten teknolog eller jurist for å svare på de praktiske spørsmålene som dukker opp rundt personvern. Det er kombinasjonen av disse bakgrunnene som kan skape forståelse og verdifulle løsninger. Det merker vi da også på tilbakemeldingene vi får når vi jobber sammen på prosjekter.

Eva har skrevet bøker om personvern tidligere og da Hans Andreas Tvedt i Cappelen Damm spurte om hun ville skrive en håndbok for personvernombud, var det åpenbart for Eva at det ikke er tilstrekkelig med personvernkompetanse for å lage en bra bok, men at teknologisk kompetanse må med. Simen sa ja til å være medforfatter og noen måneder senere leveres nå bokens manus. Vi gir en varm takk til Hans Andreas som har vært en førsteklasses og hyggelig forlegger og ikke minst for alle de mange gode spørsmål han har stilt til manuskriptet underveis.

Mye i boken er bygget på foredragene vi har holdt sammen, men det er lagt til betydelig mer detaljert informasjon enn hva man rekker å gå gjennom på kursene våre.

Som et mal-apropos kan nevnes at vi innledningsvis optimistisk trodde at vi kunne få et automatisk talegjenkjenningsprogram til å transkribere lydopptakene fra kursene vi har holdt. Vi trodde vi skulle spare tid. Det var en smule teknologioptimistisk. Under står noen fragmenter av hva vi fikk ut av programmet.

Kan du har fått en mengde innspill til det såkalte tekniske endring men det viste seg at det er nok noen virksomheter som fortelle litt mer strimler til seg selv. okser og en veldig vanskelig for deg så har du sittet og sett på Stortinget blir sagt at den prompen som kommer nå til jul

Det er stadig vekk får høre folk som har blitt fortalt at ikke alle ansatte Google Metallica for tørre samtykke til bruk av overføring av data til Nei Nei Nei hvis du søker om podcasten som kommer fra det som kom fra hvis det er greit å oversette.

Underholdningsfaktoren var stor da vi leste materialet, vi lo så vi hadde tårer i øynene. Men teksten var jo ikke brukbar. Det var bare å skrive selv. Vi har derfor brukt det meste av ledig tid til på relativt kort tid og i et lite format, å gi en innføring i hva de fleste må forholde seg til når personvern nå er blitt en del av ordinær forretningsdrift og forvaltning.

Samtidig innser vi at boken kan og bør utdypes enda mer fordi vi på noen områder egentlig bare har skrapet i overflaten. Som på alle felt er det slik at jo mer man undersøker, jo mer forstår man at det er mye igjen å lære og å lære bort. I denne runden har vi prioritert å få den mest sentrale informasjonen ut til ikke bare personvernombud, men til alle som nå må forholde seg til regelverket i det praktiske og daglige liv. Både jurister, programmerere, systemarkitekter, HR-medarbeidere, ledere og andre som må ta et ansvar for personopplysninger fremover. Vi tror behovet er stort.

Dessverre er virkeligheten slik at det vil komme praksis den nærmeste tiden som blir viktig for hvordan ulike ting skal tolkes. Det er derfor viktig å følge med på denne og det kan ikke utelukkes at tolkninger vi kommer med i denne boken vil måtte justeres. Vi skal følge med på rettsutviklingen og teknologisk praksis, men er takknemlige dersom en leser som ser at noe bør beskrives annerledes sier fra. Vi er heller ikke blinde for at noen tolker reglene annerledes enn hva vi mener er riktig, og tar også gjerne slike innspill.

Står lykken oss bi, kommer det en revidert og utvidet utgave om et stykke tid. Vår jobbhverdag er slik at vi ser nye eksempler og problemstillinger som burde tas med i boken hver eneste dag.

Vi er glade for at Torgeir Waterhouse har villet skrive et forord. Torgeir er en av samtidens mest iherdige debattanter innenfor personvern og han er kunnskapsrik om hva som er reelle problemer for individer, privat virksomhet og forvaltning. Vi synes han kommer med gode betraktninger. Og det er lett å være enig i at det viktigste er ikke compliance-problematikken – det viktigste er å fortjene og å oppnå tillit hos kunder og brukere.

En del av sjekklisterne i boken er basert på arbeid som er gjort av det engelske Datatilsynet, det som heter ICO (Information Commissioner's Office). Noen sjekklister er oversatt og brukt nærmest uendret, andre har vi gjort tilpasninger i. Vi har fått lov av ICO til å bruke dem mot å oppgi dem som kilde. ICO har en meget god nettside som gir mye bra og praktisk rettet informasjon for de som er komfortable med å lese engelsk tekst.

Vi har bedt et knippe av personvernombud om å dele sine erfaringer som ombud med oss. De er spesielt valgt ut til å gi innspill fordi de dels har lang erfaring og dels fordi de kommer fra ulike bransjer og representerer både privat og offentlig sektor. Dette har vi gjort ved at vi har stilt dem en rekke spørsmål som de har besvart og svarene er samlet i et vedlegg bak i boken. En stor takk til Anders Holt, Anna Forseback, Kjetil Rognsvåg, Tone Hoddø Bakås, Anne-Marie Østgaard og Øyvind Røst. Dere har gitt mange nyttige tips.

Eva ønsker å takke kollega Inge Brodersen for å ha lest gjennom de juridiske delene av manus og for å ha kommet med mange gode innspill underveis. Det må også sendes en varm takk til en familie som har stilt opp og tålt at mor har arbeidet med bok både tidlig og sent. Det er et privilegium å ha en ektemann som Thomas Nygaard som oppmuntrer til å stå på og som støtter når det har vært krevende å håndtere både jobb og bokskriving. Til slutt må det også sendes en stor takk til mine store barn, Mathias Nygaard Jarbekk og Mathea Nygaard Jarbekk som har hjulpet med både tekster, korrekturlesing og kildesøk underveis. Det er en glede å se hvordan de har blitt unge voksne som er gode og reflekterte diskusjonspartnere.

Simen sender sin takk til Rune Schumann og Benita Haftorn Hildonen for bistand med informasjonssikkerhet og DPIA, gjennomlesning, og tips om «Informasjonsreisen». Videre takkes Knut Haakon Tolleshaug Mørch for mange gode innspill til kapittelet om informasjonssikkerhet, og oversikter i kapittelet. Kjetil Stallemo takkes for innspill til kompetansekrav for utviklere. Jeg ønsker å rette en spesiell takk til kona mi An-Magritt Eide. Hun og de tre barna mine har vært tålmodige i de helgene og ettermiddagene der jeg har sittet inne og skrevet bok i stedet for å være ute sammen med familien.



# Innholdsoversikt

1. Innledning.....	29
2. Kilder om personvern.....	41
3. Sentrale begreper.....	47
4. Personvernets rolle for IT-porteføljen .....	58
5. Behandlingsgrunnlag .....	63
6. Individets rettigheter.....	99
7. Innledende risikovurderinger (ROS) .....	144
8. Personvernkonsekvensvurdering (PVK) .....	156
9. Forankring av informasjonssikkerhet.....	170
10. Personvernombud og andre roller med ansvar for personvern.....	189
11. Anonymisering og pseudonymisering.....	208
12. Smidig systemutvikling med innebygd personvern.....	218
13. Kunstig intelligens, maskinl�ring og stordata .....	256
14. Databehandleravtaler .....	262
15. Skytjenester og databehandlere i tredjeland .....	281
16. Dokumentasjon og rutiner.....	296
17. Atferdsnormer .....	309
18. Avvik, sikkerhetsbrudd.....	311
19. Typiske behandlinger for mange virksomheter .....	319

# Innhold

Introduksjon ved Torgeir Waterhouse.....	25
<b>1. Innledning.....</b>	<b>29</b>
Bokens inndeling .....	29
Hvorfor er personvern viktig – og hvorfor er det viktigere nå enn før? .....	31
Bakgrunn for GDPR .....	35
Sanksjonsapparat og gruppesøksmål.....	36
Risikobasert implementering .....	36
Personvern i oppkjøpsituasjoner.....	37
Egne vurderinger blir viktigere.....	38
Personvern kan være utfordrende.....	38
<b>2. Kilder om personvern.....</b>	<b>41</b>
Personopplysningsloven og GDPR .....	41
Veiledning til å lese forordningen .....	42
Veiledninger fra EDPB/Personvernrådet og artikkel 29-gruppen .....	44
Formelle avgjørelser fra datatilsyn og domstoler .....	45
Veiledning fra tilsynsmyndighetene .....	45
Litteratur.....	46
<b>3. Sentrale begreper .....</b>	<b>47</b>
Når gjelder personvernforordningen? .....	47
Hva er en personopplysning? .....	48
Særlige kategorier av personopplysninger .....	50
Roller og ansvar .....	51
Behandlingsansvarlig.....	51
Felles behandlingsansvar .....	51
Databehandler .....	53
Underdatabehandler.....	53
Generelle grunnleggende prinsipper.....	53
Sjekkliste for om grunnleggende prinsipper er ivaretatt.....	55
Lovlighet.....	55

## INNHold

Rettferdighet .....	56
Åpenhet.....	56
Formål.....	56
Nøyaktighet .....	56
Lagringstid.....	57
<b>4. Personvernets rolle for IT-porteføljen.....</b>	<b>58</b>
Et av mange premisser.....	58
Personvern og sikkerhet prioriteres ikke alltid .....	60
Felles forståelse for grunnleggende prinsipper innen sikkerhet og personvern.....	60
Forholdet mellom kunde og leverandør .....	61
<b>5. Behandlingsgrunnlag .....</b>	<b>63</b>
Innledning.....	63
Plikt til å presisere behandlingsgrunnlaget for hvert formål, endring av behandlingsgrunnlag.....	63
Hjemmel for å behandle alminnelige personopplysninger .....	64
Hjemmel for å behandle særlige kategorier av personopplysninger.....	66
Om konsern og behov for å dele personopplysninger mellom organisasjonsnumre .....	67
Samtykker.....	69
Generelt om samtykker.....	69
De enkelte kravene til samtykker .....	71
Sjekkliste for samtykker .....	77
Om avtaler.....	78
Generelt.....	78
Særlig om avtaler for tjenester på nett.....	82
Om personalisert reklame (ofte kalt retargeting) .....	82
Om personalisert innhold .....	83
Om berettiget interesse.....	83
Hovedregler.....	83
Utføring av vurderingen.....	85
Sjekkliste for berettiget interesse .....	88
Om lov.....	89
Gjenbruk av personopplysninger til andre formål.....	90
Særlig om retargeting av brukere i sosiale media .....	91
Typetilfeller av retargeting.....	92

## INNHold

<b>6. Individets rettigheter</b> .....	99
Innledning.....	99
Særlig om manipulativ design.....	99
Hvordan kan rettigheten fremsettes? .....	100
Hvordan sikre at den som krever noe er rette vedkommende? .....	101
Informasjon, åpenhet.....	102
Retningslinjer om informasjonsplikten.....	105
Generelt.....	105
Klart språk .....	106
Informasjon i ulike kanaler.....	107
Brukerpaneler .....	108
Informasjon til barn.....	108
Endringer i personvernerklæringer.....	108
Unntak fra informasjonsplikten.....	109
Når skal den registrerte få informasjonen? .....	110
Noen særlige tilfeller .....	110
Sjekkliste om informasjonsplikten .....	111
Innsyn.....	113
Innledning .....	113
Hva har den registrerte rett til?.....	114
Egne skjema for innsynsbegjæring? .....	115
Hvordan skal opplysningene formidles til de registrerte? .....	115
Må man forklare informasjonen som sendes til den registrerte?.....	115
Hva med forespørsler om store mengder personopplysninger?.....	116
Hva med forespørsler som er gjort på andres vegne? .....	116
Hva med informasjon som inneholder personopplysninger om andre? .....	117
Innsyn og bruk av databehandlere.....	117
Unntak fra innsynsrett.....	117
Retting.....	118
Hva består rettekrevet i?.....	118
Hvordan håndheves retten? .....	119
Når er data uriktige?.....	119
Hva med personopplysninger som viser en feiltakelse? .....	120
Hva med vurderinger som er omstridt? .....	120
Hva skjer mens man vurderer om noe er uriktig? .....	120
Hva om virksomheten mener at personopplysningene er riktige? ..	120
Hva om personopplysningene er delt med andre virksomheter? ...	120
Sletting.....	121
Når gjelder retten til å bli glemt?.....	123
Hva om personopplysningene er delt med andre virksomheter? ...	123

## INNHold

Unntak fra retten til å bli glemmt .....	124
Begrensning .....	125
Innledning .....	125
Når gjelder retten til begrensning av behandling? .....	125
Hvordan begrenser man en behandling? .....	126
Kan man gjøre noe med personopplysningene som skal behandles begrenset? .....	126
Plikt til å informere andre virksomheter om begrensningen av personopplysninger.....	127
Når kan begrensningen avsluttes?.....	127
Rett til å protestere .....	127
Må man informere de registrerte om retten til å protestere? .....	128
Når gjelder retten til å protestere? .....	128
Må personopplysninger slettes for å respektere en protest? .....	129
Dataportabilitet .....	130
Innledning .....	130
Når gjelder retten til dataportabilitet? .....	131
Hva kan kreves portert? .....	131
Anonyme eller pseudonyme personopplysninger .....	131
Hva hvis personopplysningene inneholder informasjon om andre? .....	132
Om overføring direkte til en annen behandlingsansvarlig .....	132
Hvordan skal personopplysningene overføres?.....	132
Hva skjer hvis en virksomhet mottar personopplysninger om et individ som har begjært personopplysninger portert til virksomheten? .....	133
Rettigheter knyttet til automatiserte beslutninger og profilering .....	134
Hva er automatiserte beslutninger og profilering? .....	134
Hovedregel om automatiserte individuelle beslutninger og profilering.....	135
Når kan automatiserte beslutninger og profilering utføres? .....	136
Særlige krav .....	137
Enkelte felles forhold for alle rettighetene .....	137
Kan man nekte å imøtekomme en forespørsel? .....	137
Kan det tas gebyr for å gjennomføre rettighetsforespørselen? .....	138
Hvor raskt må forespørsler etterkommes? .....	138
Sjekkliste for individets rettigheter.....	139
Generell sjekkliste som gjelder for alle begjæringer .....	139
Sjekkliste for sletting .....	139
Sjekkliste for retting.....	139
Sjekkliste for innsyn.....	139
Sjekkliste for begrensning.....	139

## INNHold

Sjekkliste for dataportabilitet .....	140
Sjekkliste for retten til å protestere .....	140
Sjekkliste for automatiserte behandlinger .....	140
Oversikt over behandlingsgrunnlag og rettigheter.....	141
<b>7. Innledende risikovurderinger (ROS) .....</b>	<b>144</b>
Innledning.....	144
Hva skal vurderes i en personvernfokusert ROS-analyse? .....	146
Innhold i en ROS-analyse.....	147
Innledning .....	147
Klassifisering av risiko.....	149
Mal for ROS-analyse og identifikasjon av uønskede hendelser.....	151
Andre sikkerhetsvurderinger .....	155
Kommuniser vurderingene til de som skal lage løsninger.....	155
<b>8. Personvernkonskvensvurdering (PVK).....</b>	<b>156</b>
Innledning.....	156
Hva er rettigheter og friheter .....	156
Forhåndskontroll på eget ansvar.....	157
Kriterier for å gjennomføre en PVK.....	157
Unntak.....	160
Tidspunkt for gjennomføring og revurdering.....	160
Overordnet gang i PVK-prosessen .....	161
Anbefalinger for arbeid med PVK-er.....	162
Én PVK eller flere? .....	165
Minimumsinnehold og mal.....	165
Steg 1: Identifiser behovet for en PVK.....	166
Steg 2: Beskriv behandlingen av personopplysninger .....	166
Steg 3: Innhenting av synspunkter og ekspertise .....	167
Steg 4: Vurdering av nødvendighet og proporsjonalitet .....	168
Steg 5: Risikoanalyser og korrigerende tiltak .....	168
Steg 6: Godkjenning og arkivering.....	169
<b>9. Forankring av informasjonssikkerhet .....</b>	<b>170</b>
Innledning.....	170
Store mørketall .....	171
Invester i opplæring .....	171
Sikkerhetsstyring.....	171
Sikkerhet krever kontinuerlig oppfølging .....	172
Sikkerhetskultur.....	172
Noen sikkerhetsrelaterte aktiviteter forbundet med forordningen .	173

## INNHOOLD

Råd: Utfør alltid risiko- og sårbarhetsanalyser .....	173
Zero Trust som hovedprinsipp .....	174
Man kan aldri være 100 % sikker, men minimere skade .....	174
«Skygge-IT». Sterk sikkerhet kan gi dårlig sikkerhet .....	175
Metoder og oppfølging .....	175
Et eksempel .....	177
«Informasjonsreisen» – en metode for informasjonkartlegging .....	178
Fire typer kompetanse og tiltak for personvern og sikkerhet .....	182
Lovverk, forskrifter og bransjestandarder .....	182
Rutiner, prosedyrer, opplæring .....	182
Infrastruktur og tilgangssystemer .....	183
Virksomhetsarkitektur og løsningsarkitektur .....	183
Rutiner og dokumentasjon .....	183
ISO 27000-serien og andre standarder .....	183
Sertifisering garanterer ikke god sikkerhet .....	184
Relevante lover og forskrifter – og økende ansvar for ledelsen .....	184
Forholdet mellom sikkerhet og personvern i virksomheten .....	186
Krav til leverandører .....	186
Spørsmål som kan stilles til leverandører .....	187
Andre veiledninger på nettet .....	188
<b>10. Personvernombud og andre roller med ansvar for personvern .....</b>	<b>189</b>
Innledning .....	189
Hvem må ha personvernombud .....	190
Hvilke virksomheter omfattes av «offentlig myndighet og organ»? .....	190
Plikt til å ha personvernombud i privat sektor .....	190
Databehandlere og personvernombud .....	193
Antall ombud .....	193
Eksterne eller interne ombud .....	193
Personvernombudets kvalifikasjoner .....	194
Offentliggjøring av ombudets kontaktinformasjon .....	194
Personvernombudets rolle og oppgaver .....	195
Hvordan ombudet bør prioritere, årshjul .....	198
Ombudets uavhengighet og rolleforståelse i virksomheten .....	199
Taushetsplikt for personvernombud .....	201
Praktiske råd fra erfarne personvernombud .....	202
Hvordan personvern og sikkerhet kan og bør håndteres av andre roller .....	202
Ledelsen .....	203
Personvernrådgiver og Chief Privacy Officer, CPO .....	204
IT-sikkerhetsansvarlig .....	204

## INNHOOLD

Forretningsutvikling.....	205
Brukeropplevelse (UX) .....	205
Virksomhetsarkitekt.....	205
IT-ansvarlig .....	206
IT-utvikling og forvaltning .....	206
Data scientist og andre som arbeider med rapportering og stordata .....	207
<b>11. Anonymisering og pseudonymisering.....</b>	<b>208</b>
Innledning.....	208
Definisjoner .....	208
Felles holdning til pseudonymisering og anonymisering i virksomheten.....	209
Noen anvendelsesområder.....	210
Anerkjente metoder .....	210
Tokenization.....	211
Kryptering med en kjent nøkkel.....	211
Hashing.....	212
Bruk av støy (noise) .....	212
Erstatning (substitution).....	213
Permuteringer.....	213
Aggregering: «K-Anonymity».....	213
Aggregering: «L-Diversity» .....	214
Generalisering.....	216
Differential Privacy .....	216
Periodevis håndtering er ofte nødvendig for å oppnå anonymisering .....	217
To kilder til statistikk – fortløpende og oppsummert .....	217
<b>12. Smidig systemutvikling med innebygd personvern .....</b>	<b>218</b>
Innledning.....	218
Andre relevante veiledninger .....	218
De syv grunnleggende prinsippene for innebygget personvern .....	220
1. Vær i forkant, forebygg fremfor å reparere.....	220
2. Gjør personvern til standardinnstilling.....	220
3. Bygg personvern inn i designet .....	221
4. Skap full funksjonalitet .....	221
5. Ivareta informasjonssikkerheten i hele kundereisen .....	221
6. Vis åpenhet.....	221
7. Vis respekt for den registrerte .....	221
Valg av behandlingsgrunnlag har stor betydning.....	222



## INNHold

Unike forutsetninger for hvert system .....	222
Betydning for tilgang, lagringstid, pseudonymisering og anonymisering .....	223
Smidige utviklingsprosesser og personvern .....	223
Begreper som blir brukt i smidig utvikling .....	224
Hvor lite ekstra formalisme kan man slippe unna med? .....	225
Fra DevOps til DevSecPrivOps? .....	226
En intern leverandør er også en leverandør .....	227
Design for sikkerhet .....	227
Noen gode sikkerhetsprinsipper .....	228
Design for personvern .....	229
Databasesdesign og informasjonsflyt .....	229
Tilgangskontroll .....	229
Gjem og skjul: Skill person og prosess .....	229
Etabler livssyklusoversikter for personopplysningene .....	230
Audit trail? .....	230
Personopplysninger kan forekomme mange steder .....	230
Teknologier som en bør være varsom med .....	230
Tiltak på tvers av prosjekter .....	231
Etabler en logisk modell med personopplysninger .....	231
Identifiser hjemmel for hver type behandling i hvert system .....	232
Zero trust (ingen tillit) .....	232
Logg-analysatorer gjør en i stand til å oppdage angrep .....	232
Håndtering av sikkerhetshendelser .....	233
Dokumenter og sikre dataflyt for hele utviklingsløpet .....	233
Tiltak for hvert prosjekt/team .....	233
Kravhåndtering .....	233
Interaksjonsdesign for innebygget personvern .....	235
Sørg for at teamet samlet kan nok om sikkerhet og personvern .....	235
Planlegging og bemanning .....	236
Sikkerhet og personvern må inn i arkitekturen på et tidlig tidspunkt .....	236
Kodestandarder og konvensjoner .....	236
Bruk av komponenter og åpen kildekode .....	237
Kvalitetssikring .....	237
Testing .....	238
Aspekter knyttet til forvaltning .....	239
Avvikshåndtering .....	239
Omfanget av sikkerhetstesting må stå i stil med leveransene .....	239
Livssyklus-håndtering av komponenter .....	239
Ha gode rutiner for oppfriskning av ROS-analyser og PVK .....	239

## INNHold

Ha et personvernvennlig regime for feilretting.....	240
Artikkelens påvirkning på kravene til IT-systemene og forvaltningen ...	240
Artikkel 7: Samtykke.....	240
Artiklene 12, 13 og 14: Transparens .....	241
Artikkel 15: Retten til innsyn.....	242
Artikkel 16: Rett til korrigerings .....	243
Artikkel 17: Retten til å bli glemt .....	243
Artikkel 18: Rett til å nekte behandling, begrensning .....	244
Artikkel 19: Underretningsplikt .....	244
Artikkel 20: Rett til dataportabilitet .....	244
Artikkel 22: Profilerings og automatiske avgjørelser.....	245
Artikkel 32: Sikkerhet ved behandlingen.....	245
Artikkel 35: Vurdering av personvernkonsekvenser og forhåndsdrøftelser.....	246
Test: produksjonsdata eller syntetiske data.....	247
Innledning .....	247
Tekniske forhold .....	247
Behandlingsgrunnlag.....	248
Informasjonsplikt .....	249
Gjennomføring av test.....	249
Utviklingsrelatert dokumentasjon.....	249
Økede krav til sikkerhet krever ny kompetanse .....	250
Økede krav krever økt oppmerksomhet .....	250
Måter å tilegne seg kunnskap innen sikkerhet på .....	250
Personvernkompetanse for utviklere og systemarkitekter .....	251
Kompetanse for de som jobber med interaksjonsdesign og kundereiser.....	252
Sjekkliste for innebygget personvern og personvern som standardinnstilling.....	254
<b>13. Kunstig intelligens, maskinlæring og stordata.....</b>	<b>256</b>
Innledning.....	256
Ny lovgivning fra Europa: AI Act .....	258
Behandlingsgrunnlag og rettighetsspørsmål knyttet til treningsdata ...	259
Generativ KI byr på egne utfordringer.....	259
Beslutninger basert på KI.....	260
Transparens, åpenhet .....	261

## INNHold

<b>14. Databehandleravtaler</b> .....	262
Innledning .....	262
Én eller flere databehandleravtaler eller en standardavtale? .....	263
Når kreves en databehandleravtale? .....	264
Tvilstilfeller .....	265
Sjekkliste for grensesituasjoner .....	265
Krav til databehandleren .....	266
Innhold i en databehandleravtale .....	267
Databehandleravtalen må beskrive selve behandlingen .....	267
Behandlingens art, formål og varighet .....	267
Kategorier av registrerte som omfattes, samt hva slags	
personopplysninger som behandles .....	268
Behandlingsansvarliges plikter og rettigheter .....	268
Databehandlerens forpliktelser .....	269
Særlig om kostnader .....	274
Særlig om revisjon av databehandlere .....	275
Særlig om erstatning og overtredelsesgebyrer .....	275
Konserndatabehandleravtaler .....	280
<b>15. Skytjenester og databehandlere i tredjeland</b> .....	281
Innledning .....	281
Hva er en overføring til tredjeland .....	282
Hvem er ansvarlig for en overføring .....	283
Hovedregel for overføring til tredjeland .....	283
Godkjente tredjeland .....	284
Overføringsgrunnlag – spesielt om samtykke og SCC .....	286
Om Schrems II-dommen og konsekvenser av denne .....	287
EDBPs 6-trinnsvurdering .....	288
Særlig om overføring til USA .....	290
Data Privacy Framework .....	290
Kritikk mot DPF – vil det stå seg i en rettssak? .....	292
Andre generelle forhold om skytjenester .....	293
BCR – bindende virksomhetsregler .....	294
<b>16. Dokumentasjon og rutiner</b> .....	296
Innledning .....	296
Krav til å dokumentere etterlevelse, protokoll .....	297
Unntak fra plikt til å ha behandlingsprotokoll? .....	298
Kartlegging, kjenn dine personopplysninger .....	298
Annen dokumentasjonsplikt .....	299
Særlig om personvernerklæringer .....	300

## INNHOOLD

Om utforming av dokumentasjonen .....	302
Styrende dokumentasjon.....	302
Gjennomførende dokumentasjon .....	303
IT-instruks for ansatte .....	303
Sikkerhetskopier, back-up.....	307
<b>17. Atferdsnormer.....</b>	<b>309</b>
Innledning.....	309
Hvordan lager man en atferdsnorm? .....	309
<b>18. Avvik, sikkerhetsbrudd .....</b>	<b>311</b>
Innledning.....	311
Hovedregel.....	311
Vurdering av alvorligheten, meldeplikt til Datatilsynet og den berørte	312
Rutine for håndtering av avvik.....	316
Hva skal varselet til Datatilsynet og den berørte inneholde?.....	316
Særlige unntak.....	317
<b>19. Typiske behandlinger for mange virksomheter.....</b>	<b>319</b>
Innledning.....	319
HR-opplysninger .....	319
Rekruttering.....	319
Personvernerklæring for søkere.....	320
Hvilke personopplysninger kan lagres etter avsluttet	
rekrutteringsprosess? .....	321
Rekrutteringsbyråer og jobbsøkerportaler.....	321
Hvor lenge kan personopplysninger om søkere og ansatte lagres?..	322
Kundedata, markedsføringshenvendelser og nyhetsbrev .....	323
Juridiske utgangspunkter .....	323
Når krever markedsføringsloven samtykke?.....	325
Når trenger man ikke samtykke?.....	326
Ehandelslovens bestemmelser.....	328
Særlig om potensielle kunder .....	329
Informasjonsplikt .....	329
Cookies.....	329
Generelt.....	329
Ulike typer informasjonskapsler .....	330
Juridiske rammer.....	330
Kort om mulig ny ePrivacy-forordning .....	331
Personvern og offentlig anbud.....	332

## INNHold

<b>Vedlegg</b> .....	335
Råd fra erfarne personvernombud .....	335
Anders Holt – personvernombud i NAV.....	335
Tone Hoddø Bakås – Chief Privacy Officer i SpareBank 1 Østlandet.....	338
Unni Kathe Ottersland – Privacy Compliance Director EMEAP, Abbott .....	340
Morten Haug Frøyen – personvernombud, Oslo kommune .....	342
Chalotte Engø – personvernombud for Eika Gruppen.....	346
Liv Bergliot Simonsen – personvernombud i Lånekassen .....	350
Eksempler på sikkerhetskrav til leverandører.....	354
Etterspurt dokumentasjon.....	354
Sikkerhetsgjennomgang for leverandører.....	356
Innsynsbegjæring .....	358
 <b>Litteratur og kilder</b> .....	 363
 <b>Stikkord</b> .....	 365