

Innhold

Introduksjon ved Torgeir Waterhouse	21
1. Innledning	25
Bokens inndeling.....	25
Hvorfor er personvern viktig – og hvorfor er det viktigere nå enn før?.....	27
Bakgrunn for de nye reglene	31
Sanksjonsapparat og gruppesøksmål	32
Risikobasert implementering	32
Personvern i oppkjøpsituasjoner	33
Egne vurderinger blir viktigere	34
2. Kilder om personvern	35
Personopplysningsloven og GDPR.....	35
Veiledning til å lese forordningen.....	36
Veiledninger fra artikkel 29-gruppen, WP29, EDPB	38
Veiledning fra tilsynsmyndighetene	39
Litteratur.....	39
3. Sentrale begreper	41
Når gjelder personvernforordningen?.....	41
Hva er en personopplysning?	42
Særlige kategorier av personopplysninger	44
Roller og ansvar.....	45
Behandlingsansvarlig.....	45
Databehandler.....	45
Underdatabehandler	45
Generelle grunnleggende prinsipper	46
Sjekkliste for om grunnleggende prinsipper er ivaretatt	48
Lovlighet.....	48
Rettferdighet.....	48
Åpenhet.....	48
Formål.....	48

Nøyaktighet	49
Lagringstid	49
4. Personvernets rolle for IT-porteføljen	50
Virksomhetsarkitektur – hva er det?	50
Personvern og sikkerhet prioriteres ikke alltid	51
Felles forståelse for grunnleggende prinsipper innen sikkerhet og personvern	52
Forholdet mellom kunde og leverandør	53
5. Behandlingsgrunnlag	55
Innledning	55
Plikt til å presisere behandlingsgrunnlaget for hvert formål, endring av behandlingsgrunnlag	55
Hjemmel for å behandle alminnelige personopplysninger	56
Hjemmel for å behandle særlige kategorier av personopplysninger	59
Om konsern og behov for å dele personopplysninger mellom organisasjonsnumre	60
Samtykker	62
Generelt om samtykker	62
De enkelte kravene til samtykker	63
Sjekkliste for samtykker	70
Om avtaler	71
Om berettiget interesse	73
Hovedregler	73
Utføring av vurderingen	75
Sjekkliste for berettiget interesse	77
Om lov	78
Gjenbruk av personopplysninger til andre formål	79
6. Individets rettigheter	81
Innledning	81
Hvordan kan rettigheten fremsettes?	81
Hvordan sikre at den som krever noe er rette vedkommende?	82
Informasjon, åpenhet	84
Retningslinjer fra WP29 om informasjonsplikten	87
Generelt	87
Klart språk	87
Informasjon i ulike kanaler	88
Brukerpaneler	90
Informasjon til barn	90
Endringer i personvernerklæringer	90
Unntak fra informasjonsplikten	91

Når skal de registrerte få informasjonen?	91
Noen særlige tilfeller	92
Sjekkliste om informasjonsplikten	93
Innsyn	95
Innledning	95
Hva har den registrerte rett til?	95
Egne skjema for innsynsbegjæring?	96
Hvordan skal opplysningene formidles til de registrerte?	97
Må man forklare informasjonen som sendes til den registrerte?	97
Hva med forespørsler om store mengder personopplysninger?	98
Hva med forespørsler som er gjort på andres vegne?	98
Hva med informasjon som inneholder personopplysninger om andre? ..	98
Innsyn og bruk av databehandlere	99
Unntak fra innsynsrett.....	99
Retting.....	100
Hva består rettekravet i?.....	100
Hvordan håndheves retten?.....	100
Når er data uriktige?.....	101
Hva med personopplysninger som viser en feiltakelse?.....	101
Hva med vurderinger som er omstridt?	101
Hva skjer mens man vurderer om noe er uriktig?.....	101
Hva om virksomheten mener at personopplysningene er riktige?..	102
Hva om personopplysningene er delt med andre virksomheter? ...	102
Sletting	102
Når gjelder retten til å bli glemt?	105
Hva om personopplysningene er delt med andre virksomheter? ...	105
Unntak fra retten til å bli glemt.....	105
Begrensning	106
Innledning	106
Når gjelder retten til begrensning av behandling?	107
Hvordan begrenser man en behandling?.....	107
Kan man gjøre noe med personopplysningene som skal behandles begrenset?	108
Plikt til å informere andre virksomheter om begrensningen av personopplysninger	108
Når kan begrensningen avsluttes?	108
Rett til å protestere.....	109
Må man informere de registrerte om retten til å protestere?.....	109
Når gjelder retten til å protestere?	109
Må personopplysninger slettes for å respektere en protest?	111
Dataportabilitet.....	111
Innledning	111
Når gjelder retten til dataportabilitet?	112

Hva kan kreves portert?	112
Anonyme eller pseudonyme personopplysninger	113
Hva hvis personopplysningene inneholder informasjon om andre?	113
Om overføring direkte til en annen behandlingsansvarlig	113
Hvordan skal personopplysningene overføres?	114
Hva skjer hvis en virksomhet mottar personopplysninger om et individ som har begjært personopplysninger portert til virksomheten?	115
Rettigheter knyttet til automatiserte beslutninger og profilering	115
Hva er automatiserte beslutninger og profilering?	115
Hovedregel om automatiserte individuelle beslutninger og profilering	117
Når kan automatiserte beslutninger og profilering utføres?	118
Særlige krav	118
Enkelte felles forhold for alle rettighetene	119
Kan man nekte å imøtekomme en forespørsel?	119
Kan det tas gebyr for å gjennomføre rettighetsforespørselen?	119
Hvor raskt må forespørsler etterkommes?	120
Sjekkliste for individets rettigheter	121
Generell sjekkliste som gjelder for alle begjæringer	121
Sjekkliste for sletting	121
Sjekkliste for retting	121
Sjekkliste for innsyn	121
Sjekkliste for begrensning	122
Sjekkliste for dataportabilitet	122
Sjekkliste for retten til å protestere	122
Sjekkliste for automatiserte behandlinger	122
Oversikt over behandlingsgrunnlag og rettigheter	123
7. Innledende risikovurderinger (ROS)	126
Innledning	126
Hva skal vurderes i en personvernfokusert ROS-analyse?	128
Innhold i en ROS-analyse	129
Innledning	129
Klassifisering av risiko	131
Mal for ROS-analyse og identifikasjon av uønskede hendelser	133
Andre sikkerhetsvurderinger	137
Kommuniser vurderingene til de som skal lage løsninger	137
8. Vurdering av personvernkonsekvenser (DPIA)	138
Innledning	138
DPIA erstatter meldeplikt og konsesjon	138
Kriterier for å gjennomføre en DPIA	139
Unntak	142
Tidspunkt for gjennomføring og revurdering	142

Overordnet gang i DPIA-prosessen	142
Hvordan virksomheten må arbeide med DPIA.....	144
Nyutvikling: En DPIA eller flere?.....	145
Minimumsinnhold og mal	145
Steg 1: Identifiser behovet for en DPIA.....	146
Steg 2: Beskriv behandlingen av personopplysninger	146
Steg 3: Innhenting av synspunkter og ekspertise.....	147
Steg 4: Vurdering av nødvendighet og proporsjonalitet	148
Steg 5: Risikoanalyser og korrigerende tiltak	148
Steg 6: Godkjenning og arkivering.....	149
«Informasjonsreisen» – en metode for informasjonskartlegging.....	149
9. Forankring av informasjonssikkerhet	154
Innledning.....	154
Store mørketall.....	155
Invester i opplæring.....	155
Grunnsikring, og spesifikk sikkerhet.....	155
Sikkerhet krever kontinuerlig oppfølging	156
Sikkerhetskultur.....	156
Noen sikkerhetsrelaterte aktiviteter forbundet med forordningen...	157
Råd: Utfør alltid risiko- og sårbarhetsanalyser.....	157
Metoder og oppfølging.....	158
Et eksempel	160
Fire typer kompetanse og tiltak for personvern og sikkerhet.....	160
Lovverk, forskrifter og bransjestandarder	161
Rutiner, prosedyrer, opplæring.....	161
Infrastruktur og tilgangssystemer.....	161
Virksomhetsarkitektur og løsningsarkitektur	161
Rutiner og dokumentasjon	162
ISO 27000-serien og andre standarder.....	162
Sertifisering garanterer ikke god sikkerhet.....	163
NIS-direktivet	163
Forholdet mellom sikkerhet og personvern i virksomheten	164
Krav til leverandører	165
Spørsmål som kan stilles til leverandører	165
Andre veiledninger på nettet	166
10. Personvernombud og andre roller med ansvar for personvern.....	167
Innledning.....	167
Hvem må ha personvernombud	168
Hvilke virksomheter omfattes av «offentlig myndighet og organ?»	168
Plikt til å ha personvernombud i privat sektor	168
Databehandlere og personvernombud.....	170

Antall ombud	171
Eksterne eller interne ombud	171
Personvernombudets kvalifikasjoner	171
Offentliggjøring av ombudets kontaktinformasjon	172
Personvernombudets rolle og oppgaver	172
Hvordan ombudet bør prioritere	175
Ombudets uavhengighet og rolleforståelse i virksomheten	176
Taushetsplikt for personvernombud	177
Praktiske råd fra erfarne personvernombud	178
Hvordan personvern og sikkerhet kan og bør håndteres av andre roller	178
Ledelsen	179
Personvernrådgiver og Chief Privacy Officer, CPO	180
IT-sikkerhetsansvarlig	180
Forretningsutvikling	181
Brukeropplevelse (UX)	181
Virksomhetsarkitekt	181
IT-ansvarlig	182
IT-utvikling og forvaltning	182
Data scientist og andre som arbeider med rapportering og stordata	183
11. Anonymisering og pseudonymisering	184
Innledning	184
Felles holdning til pseudonymisering og anonymisering i virksomheten	185
Noen anvendelsesområder	186
Anerkjente metoder	186
Tokenization	187
Kryptering med en kjent nøkkel	187
Hashing	188
Bruk av støy (noise)	188
Erstatning (substitution)	188
Permuteringer	189
Aggregering: «K-anonymity»	189
Aggregering: «L-diversity»	189
Generalisering	189
Differential privacy	190
Periodevis håndtering er ofte nødvendig for å oppnå anonymisering	190
To kilder til statistikk – fortløpende og oppsummert	190
12. Smidig systemutvikling med innebygd personvern	191
Innledning	191
De syv grunnleggende prinsippene for innebygget personvern	191
1. Vær i forkant, forebygg fremfor å reparere	191
2. Gjør personvern til standardinnstilling	192

3. Bygg personvern inn i designet	192
4. Skap full funksjonalitet.....	193
5. Ivareta informasjonssikkerheten i hele kundereisen	193
6. Vis åpenhet	193
7. Vis respekt for den registrerte	193
Valg av behandlingsgrunnlag har stor betydning.....	193
Unike forutsetninger for hvert system	194
Betydning for tilgang, lagringstid, pseudonymisering og anonymisering	194
Smidige utviklingsprosesser og personvern	195
Begreper som blir brukt i smidig utvikling.....	196
Hvor lite ekstra formalisme kan man slippe unna med?.....	197
Fra DevOps til DevSecPrivOps?.....	198
En intern leverandør er også en leverandør	198
Datatilsynets veileder	199
Design for sikkerhet	200
Noen gode sikkerhetsprinsipper	200
Design for personvern.....	201
Databasesdesign og informasjonsflyt	201
Tilgangskontroll	202
Gjem og skjul: Skill person og prosess	202
Etabler livssyklusoversikter for personopplysningene	202
Audit trail?	202
Personopplysninger kan forekomme mange steder.....	202
Teknologier som en bør være varsom med	203
Tiltak på tvers av prosjekter.....	203
Etabler en logisk modell med personopplysninger	203
Identifiser hjemmel for hver type behandling i hvert system	204
Zero trust (ingen tillit).....	204
Logg-analysatorer gjør en i stand til oppdage angrep	204
Håndtering av sikkerhetshendelser.....	205
Dokumentér og sikre dataflyt for hele utviklingsløpet.....	205
Tiltak for hvert prosjekt/team	205
Kravhåndtering.....	205
Interaksjonsdesign for innebygget personvern.....	206
Sørg for at teamet samlet kan nok om sikkerhet og personvern	207
Planlegging og bemanning.....	207
Sikkerhet og personvern må inn i arkitekturen på et tidlig tidspunkt	208
Kodestandarder og konvensjoner.....	208
Bruk av komponenter og åpen kildekode	208
Kvalitetssikring	209
Testing	209
Aspekter knyttet til forvaltning.....	210
Avvikshåndtering	210

Omfanget av sikkerhetstesting må stå i stil til leveransene.....	210
Livssyklus-håndtering av komponenter	210
Ha gode rutiner for oppfriskning av ROS-analyser og DPIA	211
Ha et personvernvennlig regime for feilretting.....	211
Artikkelens påvirkning på kravene til IT-systemene og forvaltningen...	211
Artikkel 7: Samtykke.....	211
Artiklene 12, 13 og 14: Transparens	212
Artikkel 15: Retten til innsyn	213
Artikkel 16: Rett til korrigerings	214
Artikkel 17: Retten til å bli glemt	214
Artikkel 18: Rett til å nekte behandling, begrensning	215
Artikkel 19: Underretningsplikt	215
Artikkel 20: Rett til dataportabilitet	215
Artikkel 22: Profilering og automatiske avgjørelser.....	216
Artikkel 32: Sikkerhet ved behandlingen	216
Artikkel 35: Vurdering av personvernkonsekvenser og forhåndsdrøftelser.....	217
Test på produksjonsdata	218
Innledning	218
Tekniske forhold	218
Behandlingsgrunnlag	219
Informasjonsplikt.....	220
Gjennomføring av test.....	220
Utviklingsrelatert dokumentasjon	220
Økede krav til sikkerhet krever ny kompetanse	221
Økede krav trenger økt fokus	221
Måter å tilegne seg kunnskap innen sikkerhet på.....	222
Personvernkompetanse for utviklere og systemarkitekter	222
Kompetanse for de som jobber med interaksjonsdesign og kundereiser	224
Stordata, kunstig intelligens og maskinlæring.....	226
Innledning	226
Behandlingsgrunnlag og rettighetsspørsmål knyttet til grunndata..	227
Beslutninger basert på KI	228
Transparens, åpenhet.....	228
Sjekkliste for innebygget personvern og personvern som standardinnstilling	229
13. Databehandleravtaler	231
Innledning.....	231
Én eller flere databehandleravtaler eller en standardavtale?.....	232
Når kreves en databehandleravtale?	233
Grensesituasjoner.....	234
Sjekkliste for grensesituasjoner.....	234

Typetilfeller for IT-systemer	235
Krav til databehandleren.....	236
Innhold i en databehandleravtale	237
Databehandleravtalen må beskrive selve behandlingen.....	237
Behandlingens art, formål og varighet	237
Kategorier av registrerte som omfattes, samt hva slags personopplysninger som behandles	238
Behandlingsansvarliges plikter og rettigheter	238
Databehandlerens forpliktelser	239
Særlig om kostnader.....	244
Særlig om erstatning og overtredelsesgebyrer	245
Konserndatabehandleravtaler	249
Skytjenester og databehandlere i tredjeland	250
Innledning	250
Særlig om overføring av personopplysninger til tredjeland	251
Overføringsgrunnlag.....	252
Kritikk mot overføringsgrunnlagene	253
Andre generelle forhold om skytjenester.....	254
BCR – bindende virksomhetsregler	255
14. Dokumentasjon og rutiner	256
Innledning.....	256
Krav til å dokumentere etterlevelse, protokoll	257
Er kravet til protokoll nødvendig og tilstrekkelig?.....	258
Kartlegging	258
Annen dokumentasjonsplikt.....	259
Særlig om personvernerklæringer	261
Om utforming av dokumentasjonen.....	262
Styrende dokumentasjon.....	262
Gjennomførende dokumentasjon.....	263
IT-instruks for ansatte	263
Sikkerhetskopier, back-up.....	267
15. Atferdsnormer	269
Innledning.....	269
Hvordan lager man en atferdsnorm?.....	269
16. Avvik, sikkerhetsbrudd	271
Innledning.....	271
Hovedregel.....	271
Vurdering av alvorligheten	272
Rutine for håndtering av brudd.....	276
Intern håndtering og varsling til Datatilsynet.....	276

Hva skal varselet til Datatilsynet inneholde?	276
Særlige unntak	277
17. Typiske behandlinger for mange virksomheter	279
Innledning	279
HR-opplysninger	279
Rekruttering	279
Personvernerklæring for søkere	280
Hvilke personopplysninger kan lagres etter avsluttet rekrutteringsprosess?	281
Rekrutteringsbyråer og jobbsøkerportaler	281
Hvor lenge kan personopplysninger om søkere og ansatte lagres?..	283
Kundedata, markedsføringshenvendelser og nyhetsbrev	284
Juridiske utgangspunkter	284
Et mulig scenario: En nettbutikk før og etter forordningen	286
Når krever markedsføringsloven samtykke?	287
Når trenger man ikke samtykke?	287
Ehandelslovens bestemmelser	290
Særlig om potensielle kunder	290
Informasjonsplikt	290
Cookies	291
Generelt	291
Ulike typer informasjonskapsler	291
Juridiske rammer	291
Ny lovregulering – ePrivacy-forordningen	292
Personvern og offentlig anbud	293
Vedlegg	295
Råd fra erfarne personvernombud	295
Personvernombudet i NAV	295
DPO i Schibsted Media Group AS	297
DPO i Telenor Norge ASA	299
Personvernombud i Oppland fylkeskommune og Hedmark fylkeskommune	301
DPO i Basefarm ASA	303
Personvernombud i Finans Norge Forsikringsdrift	305
Eksempler på sikkerhetskrav til leverandører	307
Innsynsbegjæring	312
Litteratur og kilder	317
Kilder	317
Viktige veiledninger fra EDPB/WP29	318
Stikkord	321