



Avdeling for økonomi og organisasjonsvitenskap

Sverre Holm

Masteroppgave

Personvern, europeisering og norske
kommuner

Data Privacy, Europeanization, and Norwegian Municipalities

Master i offentlig ledelse og styring (MPA)

2018

Samtykker til tilgjengeliggjøring i digitalt arkiv Brage JA

Forord

Kunnskap er et privilegium. Det er et særlig privilegium å få anledning til å dukke ned i nye fagområder også i moden alder. Høgskolen i Lillehammer var ukjent for meg fram til jeg startet på «Helse og omsorg i plan» høsten 2012. Motivasjonen for å fortsette som student kan jeg i stor grad takke alle de dyktige foredragsholderne, veilederne og kurslederne som jeg har møtt på Campus Lillehammer for. Ingen nevnt, ingen glemt.

En særlig takk allikevel til min veileder, professor Noralv Veggeland som med konstruktive tilbakemeldinger og gode spørsmål hjalp meg med å finne retning og struktur i starten og hele tiden har vært på tilbudssiden. Jeg burde nok vært flinkere til å be om veiledning også underveis.

Takk også til mine medstudenter for gode faglige diskusjoner, hyggelig og givende sosialt samvær og ikke minst hjelp og tilbakemeldinger på utkastet til spørreundersøkelsen. 102 anonyme medarbeidere i kommuner og fylkeskommuner, som satte av tid i en travel hverdag til å besvare enda en spørreundersøkelse fortjener også en takk.

Kjell-Ivar, tusen takk for de diskusjonene vi har hatt og fortsatt vil ha og tusen takk for at du hjalp til med korrektur og språkvask.

Mari, Lina og Anders, de målene dere har satt dere for egen faglig utvikling har vært til inspirasjon også for meg. Selv om det ikke har vært naturlig med lange og dype faglige diskusjoner har de i flere tilfelle vært det lille som skulle til for at jeg skulle komme meg videre med oppgaven.

Sist, men ikke minst, tusen takk til Marte for at jeg fikk anledning til å forfølge målet om å fullføre denne utdanningen. De siste par årene har jeg vært mye «borte», både mentalt og fysisk. Jeg får prøve å ta igjen det forsømte.

Skotterud 14. mai 2018

Sverre Holm

Innhold

Forord	i
Innhold	iii
Tabeller	vi
Figurer	vii
Sammendrag	viii
Abstract	ix
Forkortelser	x
1 Innledning	1
1.1 Bakgrunn og tema	1
1.2 Problemstilling	2
1.3 Avgrensinger	4
1.4 Oppgavens struktur og oppbygging	5
2 Teori og tidligere forskning	7
2.1 EU, EØS og europeisering av forvaltningen	7
2.1.1 Generelt om europeisering	7
2.1.2 Europeisering av Norge	8
2.1.3 Aktører på nasjonalt nivå	10
2.1.4 EØS-avtalen, fylker og kommuner	11
2.2 Personvern	13

2.2.1	Om personvern	13
2.2.2	Datatilsynet	14
2.2.3	Øvrige aktører på personvernområdet	16
2.2.4	Internkontroll og informasjonssikkerhet	17
2.2.5	Modenhet og måling	18
2.3	Teorien om oversettelse	20
2.3.1	Translasjonsteori	20
2.3.2	Virusteori	22
3	Metode og data	25
3.1	Metode	25
3.2	Datatilsynets undersøkelse i 2010	26
3.3	Spørreundersøkelse høsten 2017	27
3.3.1	Design	27
3.3.2	Gjennomføring og representativitet	28
3.3.3	Målemodell for modenhet	31
3.4	Data fra øvrige kilder	32
3.4.1	Supplerende datamateriale	32
3.4.2	Folketall og egenskaper ved kommunene	33
3.4.3	Øvrige kilder til eksterne data	33
3.5	Forskningsetikk	34
3.6	Reliabilitet og validitet	35
3.6.1	Reliabilitet	35
3.6.2	Validitet	36
4	Europeisering, kommunene og personopplysninger	37
4.1	Europeisering av kommunenes personvern	37
4.2	Behovet for endringer	38
4.3	Ovenfra-ned europeisering	39
4.4	Nedenfra-opp europeisering	40
4.4.1	Høringsinstansenes synspunkter	41
4.4.2	Norsk behandling	42
4.4.3	Spesielt om overtredelsesgebyr	44
4.5	Forordningen i hovedtrekk	45

4.6	Synspunkter fra fra undersøkelsen	46
4.6.1	Felles europeisk regelverk	46
4.6.2	Lokale endringer	47
4.6.3	Informasjonskanaler	47
5	Behandling av personopplysninger i kommunesektoren	49
5.1	Om de kvantitative analysene	49
5.2	Respondentene	50
5.3	Modell for påvirkningsfaktorer	50
5.4	Sammensatt mål på modenhet	52
5.4.1	Indikatorer	52
5.4.2	Testing av modellen	54
5.4.3	Fullføring av modellen	57
5.5	Faktorer som påvirker modenhetsnivået	59
5.5.1	Om modellene og enkelte faktorer	59
5.5.2	Ytre faktorer	61
5.5.3	Indre faktorer	65
5.6	Sammenligning mellom 2010 og 2017	70
5.6.1	Internkontroll i 2010	70
5.6.2	Internkontroll – utvikling fra 2010 - 2017	72
6	Er personvern smittsomt?	77
6.1	Europeisering	77
6.2	Hva gjør forordningen med kommunen	79
6.3	Teori og praksis	82
7	Oppsummering og konklusjon	85
	Litteraturliste	89
	Vedlegg	97
A	Spørsmål til kommunene	97

B	Svar avgitt på spørsmålene 4, 18 og 20	107
B.1	Spørsmål 4 – Synspunkter på felles europeisk regelverk	107
B.2	Spørsmål 18 – Lokale endringer (kvalitativt)	110
B.3	Spørsmål 20 – Andre kommentarer	115
C	Utvalgt deskriptiv statistikk	119
C.1	Respondentene	119
C.1.1	Kommunestørrelse	119
C.1.2	Geografisk fordeling	119
C.1.3	Rolle i kommunen/fylkeskommunen	120
C.1.4	Kommunestørrelse som indre faktor	120
C.2	Modenhet	122

Tabeller

3.1	Svarprosent i undersøkelsen	29
4.1	Tidspunkt og kanaler for informasjon om nytt regelverk . . .	48
5.2	Deskriptiv statistikk av egenvurdert modenhet	54
5.3	Faktoranalyse av indikatorer for modenhet	55
5.4	Modenhet – reliabilitetsanalyse.	56
5.5	Modenhet – korrelasjon mellom indikatorene. N = 85	58
5.6	Modenhetsnivå – Frekvensfordeling.	59
5.7	Deskriptiv statistikk av ytre faktorer	62
5.8	Ytre påvirkningsfaktorer. Lineær regresjon	64
5.9	Deskriptiv statistikk – indre faktorer	67
5.10	Indre faktorer - lineær regresjon	69
5.11	Deskriptiv statistikk – internkontroll 2010	70
5.12	Andel med internkontroll etter innbyggertall 2010. Prosent. .	71
5.13	Internkontroll og kommunestørrelse i 2010	73
5.14	Kommuner med internkontroll i 2010 og 2017. N = 92	74
B.1	Synspunkter på EUs ambisjon om felles personvernregler N = 28	107
B.2	Spm 18 – Lokale endringer som følge av forordningen N = 54	110
B.3	Spm 20 – andre kommentarer N = 15	115
C.1	Antall svar (n) i forhold til kommuner (N) etter folketall . . .	119
C.2	Fylkesvis oversikt over svarandel	121
C.3	Fordeling av respondentenes roller. N = 102	122

C.4 Modenhet vs kommunestørrelse. Lineær regresjon	123
--	-----

Figurer

2.1	Begrepsmodell – Europeisering av personvernet	10
2.2	Modell for modenhet (Nasjonal sikkerhetsmyndighet, 2015) .	20
4.1	Beslutningsprosessen i EU (European Commission, udatert) .	41
5.1	Variabelmodell over ytre og indre påvirkningsfaktorer	51
5.2	Modenhet – personvern i kommunene	52
5.3	Skreddiagram for modenhet	54
5.4	Modenhetsfordeling	58
5.5	Internkontroll i kommunene 2010 og 2017. N = 92	75
C.1	Svarfordeling i undersøkelsen (venstre bilde) sammenlignet med alle kommuner (høyre bilde)	120
C.2	Egenvurdering av modenhet – svarfordeling	124
C.3	Egenvurdering av modenhet – spredning	125

Sammendrag

Samtidig med at EU-kommisjonen var i gang med å utarbeide et nytt personvernregelverk, i 2011, slo Datatilsynet alarm om kommunesektorens behandling av personopplysninger. Denne masteroppgaven er en case-studie som undersøker om lovarbeidet i Brussel og praktisering av loven i kommunene – to sider av samme sak – møttes på noe tidspunkt i årene etter. Og, blir innbyggernes personopplysninger bedre ivaretatt i 2018 enn de var i 2011?

EUs personvernforordning følges med norske øyne og kommunenivået som perspektiv fram til den ble vedtatt i mai 2016. Åpne kilder om norske aktørers deltakelse, nasjonal koordinering og norske posisjoner har få indikasjoner på at man fra norsk side har brukt mulighetene til å påvirke innholdet i forordningen. Det er heller ingen formelle spor etter konsultasjoner med kommunene eller sektorinnspill til nasjonale posisjoner.

Kommunenes egen vurdering av status for personvernet i 2017 er innhentet gjennom en undersøkelse og et rammeverk til en modenhetsskala er utviklet. Resultatene er gyldige for den femtedel av kommunene som deltok, men kan ikke generaliseres på grunn av skjevfordeling både geografisk og i folketall.

Statistiske analyser av svarene er tolket ved hjelp av virusteorien (Røvik, 2011) og målt mot en modenhetsskala som er utviklet. Kommuner som gjennomgår styringssystemet årlig anser seg mer modne i å behandle personopplysninger enn andre. Lokale hendelser, medieoppslag, ressurser og medarbeideres vilje til å følge regelverket ser også ut til å påvirke hvor modne kommunene oppfatter seg. Om kommunen har personvernombud eller ikke syntes derimot ikke å ha noen innvirkning på egenvurderingen.

70 % svarte at de har internkontroll, en svak økning (3 %) fra 2011. I Datatilsynets undersøkelse fra 2011 var det dobbelt så stor sannsynlighet for at de største kommunene hadde internkontroll i forhold til de minste. Denne forskjellen fant vi ikke i 2017. Hver femte kommune som hadde internkontroll i 2011 hadde det ikke lenger høsten 2017.

Abstract

In 2011, with the first draft General Data Protection Regulation yet to be published by the EU Commission, the Norwegian Data Protection Authority raised grave concern on the processing of personal data by local government. This master's thesis investigates possible interfaces between two means to the same end, preparatory legislative work in Brussels and lawful processing of personal data by Norwegian counties and municipalities – it takes two to tango.

The development of the GDPR is reviewed from the perspective of the local government level into participation, co-ordination, and positions taken by Norwegian officials in the process. Sources accessible to the public show little evidence of active Norwegian interventions in EU deliberations, and no traces of national consultations between central government bodies and the counties or the municipalities, or any formal positions taken on their behalf.

An update on the status of current processing of personal data, conducted as a survey, received responses from one fifth of the regional and local authorities. Scewness in size and geographical distribution prevents generalization; yet, the results are valid for the group of participating bodies.

Statistical analyses were conducted on the responses, measured against a developed maturity scale, and interpreted by means of the virus theory (Røvik, 2011). Municipalities conducting yearly assessment of their system for internal control are likely to consider themselves more mature in handling personal data than those who are not. Other significant (within the group) findings were that local incidents, media, resources, and co-operation of staff had likely impacts on the self-assessment of maturity.

The survey could reveal that 70 % of the participating bodies had a system for internal control of their personal data, a meagre 3% increase from 2010. In 2011, the group of largest municipalities were 50% more likely to have such a system than the group of smallest municipalities, a difference not evident in 2017. Furthermore, nearly one out of five of the systems in 2010 were no longer in use in 2017.

Forkortelser og sentrale begrep

Artikkel 29-gruppen	= EU-kommisjonens rådgivende organ i personvernspørsmål
Behandlingsansvarlig	= Virksomhetens leder (Rådmannen i en kommune)
CEMR	= Council of European Municipalities and Regions
CMMI	= Capability Maturity Model Integration (CMMI Product Team, 2001)
COBIT	= Control Objectives for Information and related Technology
COSO	= Committee of Sponsoring Organizations of the Treadway Commission
DAPIX	= Working Party on Information Exchange and Data Protection – Rådets arbeidsgruppe i bl.a. personvern
Databehandler	= Underleverandører som behandler data på vegne av behandlingsansvarlig
Det europeiske råd	= EUs toppmøte (The European Council), regjeringssjefene representerer nasjonene. Se også «Rådet»
Difi	= Direktoratet for forvaltning og ikt
DPIA	= Data Protection Impact Assessment – vurdering av personvernkonsekvenser
DPO	= Data Protection Officer – personvernombud

eInnsyn	= Innsynsløsning for statlige etater og Oslo kommune
EFTA	= European Free Trade Association
ENISA	= European Union Agency for Network and Information Security
ESA	= EFTA Surveillance Authority
Europautredningen	= NOU 2012:2 «Utenfor og innenfor»
EØS	= Europeisk økonomisk samarbeidsområde
FAD	= Fornyings-, administrasjons- og kirkedepartementet (nedlagt 2014)
FD	= Forsvarsdepartementet
GDPR	= General Data Protection Regulation (Personvernforordningen)
ISO	= International Standardization Organization
ISO 2700x	= Familie av standarder for informasjonssystemssikkerhet
IKT	= Informasjons- og kommunikasjonsteknologi
JD	= Justis- og beredskapsdepartementet
KINS	= Foreningen for kommunal informasjonssikkerhet
Kommuneundersøkelsen 2011	= Kommuneundersøkelsen 2010-2011 (Datatilsynet, 2011)
KMD	= Kommunal- og moderniseringsdepartementet
KOSTRA	= Kommune-Stat-Rapportering (SSB, 2018)
KS	= Kommunesektorens organisasjon
MLG	= Multilevel governance
NSM	= Nasjonal sikkerhetsmyndighet
NorSIS	= Norsk senter for informasjonssikring

NOU	= Norges offentlige utredninger
NYPE	= NYe PErsonvernregler – todagers kurs for kommuner med informasjon/opplæring i personvernforordningen (KINS, KS og Datatilsynet)
OLS	= Lineær regresjonsanalyse (Ordinary least squares)
OEP	= Offentlig elektronisk postjournal – innsynsløsning for statlige etater, erstattet av eInnsyn fra 5. februar 2018
PVO	= Personvernombud
ROS-analyse	= Risiko- og sårbarhetsanalyse. Metode for å etterkomme krav i personopplysningsforloften § 2-4 om risikovurdering.
Rådet	= Rådet for den Europeiske Union (Council of the European Union) – Fagstatsrådene fra EU-landene, sammensetning etter saker som behandles. Se også «Det europeiske råd».
Subsidiaritetsprinsippet	= Nærhetsprinsippet, beslutninger i EU skal fattes på et lavest mulig effektivt nivå
UD	= Utenriksdepartementet

1 Innledning

1.1 Bakgrunn og tema

Denne oppgaven handler om kommunesektorens behandling av personopplysninger. Den handler også om europeisering og hvordan sentrale, regionale og lokale norske forvaltningsnivå samhandler med det overnasjonale nivået som EU representerer. Bakgrunnen er at EUs personvernforordning trer i kraft den 25. mai 2018 i EU.

Kommuner og fylkeskommuner behandler store mengder personopplysninger om innbyggerne, i alle aldersgrupper og fra alle sosiale lag. Tidligere undersøkelser og studier har konkludert med at kommuner og fylkeskommuner ikke ansees for å behandle de personopplysningene de er tiltrodd på en tilfredsstillende måte (Datatilsynet, 2011, Datatilsynet, 2016 og Tranvik, 2009c).

Forordningen gir borgerne nye rettigheter og setter nye og strengere krav til hvordan personopplysninger behandles. Den omfattes av EØS-avtalen og skal implementeres som ny personopplysningslov i Norge. Den er EUs bidrag til å gjøre lovverket i stand til å håndtere utfordringene som den teknologiske utviklingen og økende bruk av personopplysninger i samfunnet bringer med seg.

En annen og mindre profilert årsak til at det kommer nytt regelverk er å finne i utviklingen av EUs digitale indre marked. Et harmonisert lovverk og høy tillit til digitale tjenester er sentrale rammefaktorer for at næringslivet og det offentlige skal få utnyttet de innovasjonsmulighetene som ligger i digitale tjenester, produkter og løsninger.

Som EØS-medlem skal Norge innarbeide alle rettsakter som EU vedtar og som omfattes av EØS-avtalen i norsk lov. EØS-medlemmer har ikke sete i EUs lovgivende organ, Rådet for den europeiske union og EU-parlamentet. Norske myndigheter og interesseorganisasjoner er allikevel ikke uten mulighet til å påvirke. Spørsmålet er om vi fra norsk side benytter de mulighetene vi har, og eventuelt hvordan de benyttes.

1.2 Problemstilling

For å belyse disse temaene i masteroppgaven legges følgende problemstillinger til grunn:

- I hvilken grad har sentrale norske myndigheter og organisasjoner formidlet synspunkter fra regionalt og lokalt nivå inn i EUs arbeid med personvernforordningen?
- Er det mulig å finne systematiske forskjeller mellom kommunene som kan forklare status og forskjeller i regeletterlevelse av EU-initiert lovverk?

Disse kan i utgangspunktet fremstå som to separate problemstillinger med ulike tilnærminger. Samtidig er de to sider av samme sak. Kommunene representerer det lokale nivået av offentlig myndighet som iverksetter offentlig politikk overfor innbyggerne og leverer tjenester på alle de store velferdsområdene. Det innebærer at kommunene er unike organisasjoner også når det gjelder behandling av personopplysninger. Undertegnede påstand er at det ikke er noen statlige eller private virksomheter som har et tilsvarende spenn i oppgaver og kompleksitet i hvilke personopplysninger som behandles.

Dette spennet og denne kompleksiteten innebærer at det offentlige i særlig grad burde ta sektoren med på råd når det utformes regelverk som kommunene skal implementere. Regelverket må være hensiktsmessig utformet for at implementering av det i kommunal sektor skal gå mest mulig smertefritt. Denne ambisjonen burde omfatte både nasjonale lover og rettsakter fra EU som kommunene skal implementere.

Nasjonal lovgivningsprosess har strukturerte systemer for innspill, høringer og koordinering. Norge, som EØS-medlem, har mere begrensede muligheter for å øve innflytelse på nye rettsakter i EU. Mulighetene er imidlertid til stede gjennom den offisielle norske delegasjonen til EU og gjennom en rekke organisasjoner som er representert med egne kontorer i Brussel.

Sjansen for å få gjennomslag for nasjonale syn er størst i en tidlig fase og reduseres etterhvert som kompromisser fra tidligere forhandlingsrunder er innarbeidet i utkastet. Når et direktiv eller en forordning er gjort gjeldene i EU og skal innarbeides i norsk lov som del av EØS-avtalen er det i praksis ikke mulig å gjøre endringer. Mulighetene ligger da i å tolke hvilket handlingsrom rettsakten gir og utforme norsk lov på en måte som er mest mulig hensiktsmessig for de som skal implementere dem.

For å besvare den første problemstillingen følges personvernforordningen med norske øyne fra det ble lansert som forslag av kommisjonen i 2012, til det ble vedtatt i 2016. Hensikten er å finne ut om det har vært noen dialog eller koordinering med norsk regionalt og lokalt nivå i den perioden hvor det var muligheter for å gi innspill til forordningen.

Det teoretiske grunnlaget for at dette er et tema av betydning ligger i teoriene om overføring av organisasjonsideer mellom ulike organisasjoner slik den er fremstilt i Røviks «Trender og translasjoner» (Røvik, 2007). Konkret er utgangspunktet kontekstualisering – EUs regler om personvern skal introduseres som praksis i norske kommuner.

Den andre problemstillingen tar utgangspunkt i norske kommuner og den mangel på regeletterlevelse på personvernområdet som ble nevnt helt innledningsvis. Sentralt i dagens krav er at kommunene skal ha et internkontrollsystem som skal sikre en systematisk oppfølging av kravene i personopplysningsloven og -forskriften. Kommunene skal også ha et system for informasjonssikkerhet som beskytter opplysningene mot at de misbrukes, sikrer at de er korrekte og at de er tilgjengelig for de som har behov for dem. Disse kravene videreføres ikke direkte, men forordningen vil også kreve en systematikk og tilfredsstillende datasikkerhet hos de som skal behandle personopplysninger. Det hevdes også fra Datatilsynet at de

virksomhetene som følger dagens lovverk er godt rustet til å møte kravene i personvernforordningen.

Systematiske undersøkelser på området er endel år gamle og det ville vært ønskelig med et oppdatert kunnskapsgrunnlag. Som del av oppgaven fikk alle kommuner og fylkeskommuner tilbud om å delta i en spørreundersøkelse (survey) om behandling av personopplysninger i kommunen høsten 2017. Undersøkelsen ble gjennomført i perioden 23. oktober til 17. november 2017. Av 445 som fikk invitasjonen deltok 102 (97 kommuner og 5 fylkeskommuner), 23%.

I undersøkelsen fikk kommunene spørsmål om de mener å ha et styringssystem for informasjonssikkerhet. Egenskaper ved styringssystemet settes sammen til en skala for modenhet som er et sammensatt mål på forankring i kommunens toppledelse, ansvarsfordeling, dokumentasjon, reaksjon ved brudd, kompetanse og hvor systematisk oppfølgingen er.

Skalaen for modenhet er avhengig variabel i regresjonsanalyser for å undersøke om det er samvariasjon mellom den egenvurderte modenheten og variabler for indre og ytre faktorer ved kommunene som kan bidra til å forklare forskjeller i regeletterlevelse. Indre faktorer og egenskaper er for eksempel kommunestørrelse, om kommunen har personvernombud og eventuelt hvor lenge de har hatt det. Ytre faktorer kan være om kommunen deltar i interkommunale samarbeid på IKT-området, om kommunen har hatt tilsyn fra Datatilsynet eller av andre årsaker har vært i kontakt med tilsynet.

Det teoretiske fundamentet for å tolke resultatene fra undersøkelsen er virusteorien, en forklaringsmodell på hvilke mekanismer som er i virksomhet når nye organisasjonsideer skal implementeres i en organisasjon. Teorien er lansert som et alternativ til organisasjonsmoteteorier som har samme ambisjon men et mindre rikt begrepsapparat (Røvik, 2007, Røvik, 2007)

1.3 Avgrensinger

Den viktigste avgrensingen er at undersøkelsen ikke sier noe om årsaksforhold. Analysen av Datatilsynets undersøkelse i 2010 (i avsnitt 3.2 på side 26) viser en signifikant korrelasjon mellom kommunestørrelse og om kommunen

hadde et system for internkontroll. Man kan ikke trekke den konklusjonen at kommunestørrelsen er *årsak* til forskjellene, bare at sannsynligheten øker for at kommunene har internkontrollsystem med økende folketall. Analysene gir heller ikke grunnlag for å trekke konklusjoner for enkeltkommuner. Det vil finnes eksemplarisk utformede internkontrollsystem i en kommunene med få innbyggere og det vil finnes kommuner med mange innbyggere som har langt igjen til å oppfylle lovkravene.

Analysene baseres på kommunenes egenvurdering av hvordan de etterlever utvalgte dokumentasjonskrav og organisatoriske krav. En slik kvantitativ undersøkelse og analyse vil imidlertid ikke fange opp kommunenes praktisering av regelverket.

Spørsmålene vil rettes til dagens kommuner og fylkeskommuner¹. Interkommunale selskaper etter § 27 eller kommunalt eide aksjeselskaper vil ikke omfattes av undersøkelsen, blant annet fordi disse etter høringsnotatet ikke skal betraktes som «offentlige organ» eller «offentlig myndighet» (JD, 2017, s. 67). Problemstillinger relatert til samkommuner vil ikke behandles fordi kommunelovens samkommunemodell ble opphevet i 2016. De to eksisterende samkommunene skal avvikles innen 1. januar 2020. Skulle det komme opp forhold som bare er relevante for kommuner/fylkeskommuner med parlamentarisk styreform vil disse ikke belyses ut over at de kort nevnes.

1.4 Oppgavens struktur og oppbygging

Kapittel 2 er en gjennomgang av tidligere forskning på hvordan kommunesektorens forhold seg til EØS-avtalen og hvilken innvirkning avtalen har på kommuner og fylkeskommuner. Her gjøres det også greie for hva som menes med europeisering, tidligere forskning på europeisering og norske aktører i forholdet til EU. Det legges særlig vekt på aktører og forskning på personvernområdet som er relevante for kommunesektoren. Videre belyses det teoretiske grunnlaget for en modenhetsskala som blir utviklet. Hensikten med den er å kunne fange opp flere fasetter av hvordan personopplysninger behandles enn bare å vurdere styringssystemet. Til slutt i kapittelet gis en

¹<https://www.ssb.no/offentlig-sektor/kommunekatalog/kommunekatalog-2017>

kort introduksjon til de delene av translasjons- og virusteoriene som blir brukt i oppgaven.

Metodene presenteres i kapittel 3 sammen med en innledende presentasjon av utvalgte data fra Datatilsynets undersøkelse (Datatilsynet, 2011), data fra undersøkelsen høsten 2017 samt kilder til eksterne data som blir brukt i oppgaven. Etske vurderinger og vurdering av studiens reliabilitet og validitet inngår også i det kapittelet.

Europeisering er tema for kapittel 4. Etter en innledende beskrivelse av behovet for endringer på personvernområdet og kort om EUs ambisjoner på dette feltet legges hovedvekten på å belyse norske aktørers rolle i de fire årene forordningen var under behandling i EUs lovgivende organer. De av undersøkelsens spørsmål som belyser kommunenes syn på et felles europeisk regelverk og hvordan de fikk kjennskap til det blir gjennomgått til slutt i kapittelet.

I kapittel 5 gjennomføres kvantitative analyser av svarene fra undersøkelsen. Analysene er basert på en modell for indre og ytre påvirkningsfaktorer som presenteres i starten av kapittelet og skalaen for modenhet i behandling av personopplysninger som utvikles på grunnlag av noen av svarene i undersøkelsen.

Kapittel 6 inneholder drøfting av sentrale funn i studien, som avsluttes med en oppsummering og konklusjon i kapittel 7.

2 Teori og tidligere forskning

2.1 EU, EØS og europeisering av forvaltningen

2.1.1 Generelt om europeisering

Gjennom EØS-avtalen har Norge forpliktet seg til å følge de direktiver og forordninger som EU vedtar innen de områdene som omfattes av EØS-avtalen. Om lag tre fjerdedeler av EUs rettsakter blir også norske lover og forskrifter som del av EØS-avtalen (NOU 2012:2, 2012). Formelt sett er det Stortinget som vedtar disse, men har i realiteten liten innflytelse på lovtekstene. Den innflytelsen de kunne hatt på hvordan lovene iverksettes i Norge brukes i noen tilfelle, men det diskuteres i hvor stor grad det nasjonale handlingsrommet utnyttes (Veggeland, 2010, Austvik og Claes, 2011).

Europeisering er et begrep med mange fasetter og har gitt grobunn til mye forskning. EU har manifestert seg som en overnasjonal organisasjon med en autoritet over medlemsnasjonene som ikke ligner noen annen internasjonal organisasjon. Bruk av begrepet europeisering og hva det inneholder har imidlertid vært problematisert, blant annet har konseptet blitt fremstilt som uoversiktlig (Olsen, 2002, Olsen, 2006).

På overordnet nivå er en vanlig tilnærming til europeisering at påvirkningen har to komponenter. Beslutninger i EU legger rammer for nasjonal politikktutforming i medlemsstatene og hos nære samarbeidspartnere. Dette gir begrepet en ovenfra-ned komponent. Samtidig har nasjonene også påvirkningsmuligheter på EUs institusjoner og politikk. Her går påvirkningen motsatt vei og gir en nedenfra-opp komponent (Börzel og Panke, 2016). Gjennom en rekke tiltak for å styrke demokratiet (eller redusere demokra-

tiunderskuddet) i EU har borgerne, regionene, de nasjonale parlamentene og EU parlamentet fått økt innflytelse over beslutninger i EU (Smismans, 2016). I denne sammenhengen er det naturlig å ta utgangspunkt i samspillet mellom ulike forvaltningsnivå, fra EUs styrende organ til kommunenivået som skal iverksette de rettsaktene som besluttes i EU.

Claes og Førland har formulert europeisering som «endring i nasjonal politikk som skyldes beslutninger eller beslutningsprosesser i EU» (2015, s. 44). Den dekker våre begrensede mulighet til å øve innflytelse på EUs beslutninger, manglende innpass i beslutningsprosessen og liten vilje til å utvikle politikk for å utnytte det handlingsrommet som finnes. De trekker fram tre europeiseringsmekanismer som er viktige: Påvirkning gjennom regler, gjennom beregning av interesser og gjennom læring og overføring av ideer. De to siste elementene er vesentlige fordi EØS-avtalen gir oss, inklusive norske kommuner, adgang til arenaer og informasjon vi ellers ville vært avskåret fra.

2.1.2 Europeisering av Norge

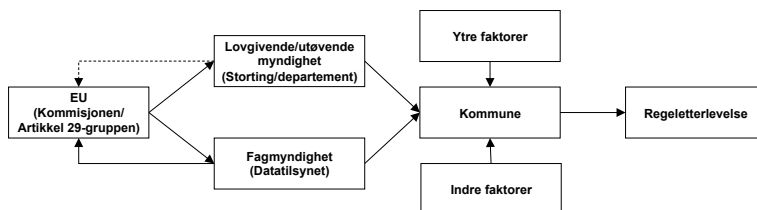
Europautredningen (NOU 2012:2, 2012) er en bred og grundig vurdering av EØS-avtalen og Norges øvrige avtaler med EU. En av hovedkonklusjonene er at EØS-avtalen, selv om det er en utenrikspolitisk avtale, har minst like stor betydning for innenrikspolitiske forhold. Begrepet *europeisering* er brukt gjennom hele dokumentet og bl.a. viet et eget kapittel.

Påvirkning gjennom regler er den dominerende mekanismen for europeisering av Norge og den som i særlig grad gjelder for personvernregelverket. I de 20 årene fra 1992 til 2011 hadde Norge implementert 3/4 av EU-retten sammenlignet med EU-medlemmene (NOU 2012:2, 2012, s. 807). Dette endrer norsk rett for alle politikkområder og griper inn i alle forvaltningsnivå. En gjennomgang av kommunestyre- og fylkestingssaker viste bl.a. at 73% av sakene var relatert til EU/EØS (Indset og Hovik, 2008, s. 60). Det store omfanget av rettsakter som vedtas i EU er en type hard regulering som bidrar sterkt til at regulerings- og oppfølgingsystemer innsnevrer det nasjonale politiske handlingsrommet og virkeområde (Veggeland, 2010).

Norge er en av de nasjonene som mest lojalt implementerer EUs rettsakter i norsk lov. Kommisjonen utarbeider en årlig status for «transposition deficit» – andel direktiver som ikke er innarbeidet i nasjonalt lovverk. Gjennomsnittlig etterslep i EU er på 1,5 % (European Commission, 2018b). EØS-avtalens overvåkingsorgan ESA (European Surveillance Authority) utarbeider en tilsvarende oversikt for EØS-landene. I november 2017 var Norges etterslep på 0.5 % (ESA, 2018), en promille bak Malta som hadde 0.4 % og det laveste etterslepet blant EU-nasjonene. Det er grunn til å reflektere over om vi er mere lojale enn vi behøver å være.

Selv om Norge ikke er EU-medlem har vi allikevel mulighet for å øve innflytelse på nye direktiver og forordninger. EØS-medlemmene har har anledning til å delta i fora som bistår kommisjonen i arbeidet med utkast til lovtekster. Mye tyder på at denne muligheten for å øve innflytelse ikke brukes på en systematisk måte. Det finnes ingen fullstendig oversikt over norsk deltakelse i slike fora. Forskning innen veterinær- og næringsmiddelområdet har også vist at deltakerne «hverken gis klare politiske mandat eller lyttes til når de kommer hjem» (Claes og Førland, 2015, s. 214). I delstudier til lokaldemokratiutredningen (Veggeland, 2005a) og til europautredningen (Egeberg og Trondal, 2011, s. 8) bekreftes dette synet. Utenriksdepartementets håndbok i EU/EØS-arbeid beskriver hvor viktig det er at norske representanter i ekspertgrupper kjenner EUs konsultasjonsprosedyrer, men gir ingen anvisninger om nasjonal koordinering eller rutiner for forankring og rapportering (Utenriksdepartementet, 2009).

I mange tilfelle vil Norge måtte forholdt seg til eksterne regler og reguleringer helt uavhengig av EØS-avtalen. Dette er åpenbart tilfelle i spørsmålet om personvernets stilling i dagens samfunn, hvor globalisering og teknologisk utvikling er dominerende. EU har imidlertid tatt en ledende rolle globalt for å regulere personvern og styrke rettighetene til «de registrerte» gjennom personvernforordningen. Den gjelder i prinsippet innenfor EU og EØS-området. Alle virksomheter som driver virksomhet innen dette området, uavhengig av hvor virksomhetene har sin formelle forretningsadresse, må følge forordningens bestemmelser. For eksempel vil personvernforordningen regulere forholdet mellom store internasjonale



Figur 2.1: Begrepsmodell – Europeisering av personvernet

aktører som Facebook, Amazon og Google og de enkeltpersoner i EU som er registrert i deres systemer.

Personvernforordningen er ikke en rettsakt som er politisk kontroversiell, slik for eksempel datalagringsdirektivet var det. Den styrking av individets rettigheter som forordningen fører med seg blir i hovedsak godt mottatt både i det politiske miljø og hos allmennheten. Allikevel er det grunn til å spørre om det er handlingsrom i forordningen som man fra norsk side burde vurdere å utnytte. I figur 2.1 skisseres en begrepsmodell for forholdet mellom det overnasjonale nivået og kommunesektoren for utvikling og regeletterlevelse av personvernforordningen.

Den venstre delen av modellen, hvilken innflytelse Norge har hatt, eller kunne ha hatt, på utviklingen av forordningen drøftes nærmere i kapittel 4. Høyre del av modellen, faktorer som påvirker kommunenes regeletterlevelse er tema i kapittel 5. Modellen drøftes samlet i kapittel 6.

2.1.3 Aktører på nasjonalt nivå

EU-nasjonenes parlamenter skal etter Lisboa-traktaten forelegges nye lover som berøres av subsidiaritetsprinsippet eller nærhetsprinsippet. Dette er et traktatfestet prinsipp som innebærer at lovgivning i EU skal gis på et lavest mulig nivå, men så høyt at det blir effektivt (Veggeland, 2005b). Forslagene til nye forordninger eller direktiver skal legges fram for de nasjonale parlamentene så tidlig at de har en reell påvirkningsmulighet (Grønnestad, 2012). Stortinget har ikke en tilsvarende konstitusjonell rett overfor EU til å uttale seg om forslag til forordninger eller direktiver på et stadium som gir reell innflytelse. En spissformulering er at europapolitikk i

Stortinget «tjener først og fremst til å legitimere regjeringens politikk, ikke til selvstendig parlamentarisk maktutøvelse» (NOU 2012:2, 2012, s. 822).

Navet for norsk dialog med EU er Norges delegasjon til EU som er Norges største utenriksstasjon. Delegasjonen hører til Utenriksdepartementet (UD), men består av medarbeidere etter politikkområder som dekker de fleste departementene. Disse rapporterer på faglinjer til respektive departementer i tillegg til at delegasjonen som helhet rapporterer til UD². I delegasjonen er personvern angitt som ansvarsområde både for en justisråd og for delegasjonens IKT- og forvaltningsråd. Personvernforordningen skal innarbeides i norsk lovverk av Justis- og beredskapsdepartementet (JD), mens det er Kommunal- og moderniseringsdepartementet (KMD) som er moderdepartement for kommunesektoren og regjeringens IKT-politikk. På personvernområdet synes det derfor å være samsvar mellom organisatorisk ansvar på departementsnivå og fagansvar i delegasjonen, med parallelle kanaler for rapportering.

Norge har med EØS-avtalen anledning til å delta med nasjonalFle eksperter i arbeidsgrupper, råd og utvalg som rapporterer til kommisjonens generaldirektorater. I Norge er Datatilsynet medlem i *Artikkel 29-gruppen*. Det er få formelle spor av hvilken rolle tilsynet har spilt i denne gruppen, ut over den presentasjonen de gir på sine hjemmesider (Datatilsynet, 2018) og i Artikkel 29-gruppens arkiver som er tilgjengelige på kommisjonens nettsider (European Commission, 2018a)

2.1.4 EØS-avtalen, fylker og kommuner

Det lokale nivået iverksetter nasjonal politikk og nasjonalt lovverk, inklusive de delene av EU-retten som er gjort til del av norsk lov. Som beskrevet i avsnitt 2.1 på side 7 kan begrepet europeisering inneholde både en ovenfra- ned og en nedenfra-opp komponent. Nedenfra-opp komponenten mellom norske kommuner og EU er det ikke helt lett å få øye på. Rent teknisk vil en finne at norske kommuner deltar i Interreg-prosjekter, regionale samarbeid over grensene og noen er med på å finansiere regionkontorene som er etablert i Brussel.

²Egne notater fra et studiebesøk ved delegasjonen i september 2017

Gjennom mange av sine forskningsbidrag har Veggeland vist hvordan EUs styring ved regulering gjennom EØS-avtalen legger føringer for kommunal utvikling, styring og handlingsrom (Veggeland, 2000, 2003, 2005b, 2010, 2012). Samtidig trekker han frem at det er handlingsrom som kommunene kunne utnytte. Tjenester som drives i egenregi av kommunene behøver for eksempel ikke å konkurransesettes og EUs konkurranseregler vil i så fall ikke komme til anvendelse.

Baldersheim (Baldersheim, 2014, s. 66) nevner fire teoretiske retninger som arbeider med å forklare hvordan faktorene på nivå over det lokale påvirker styringsstrukturene og maktforholdene lokalt. Disse er *reguleringsteori*, *globaliseringsteori*, *flernivåanalyse* og *nettverksteori*. I en kort gjennomgang av disse konkluderer han med at alle teoriens styrker ligger på «det overlokale» mens det lokale perspektivet i en europeisert og globalisert verden er fraværende.

I en empirisk studie utført for KS 2008 om kommunesektoren og EØS-avtalen var en av hovedkonklusjonene at «... en konsekvens av EØS-avtalen for kommunesektoren er en svekket samfunnsmessig forankring av politikken innhold (Indset og Hovik, 2008, s. 8). Dette begrunnes med at kommunesektoren i liten grad medvirker i den politikktutformingen som skjer i EU. Til tross for at det er god kompetanse i sektoren om muligheter og begrensninger for å realisere politiske mål, legger de politiske prosessene ikke til rette for slik deltakelse fra det lokale nivået.

Ett interessant poeng i Europautredningen er at mens kommunene i stor grad er det utførende organ når EUs rettsakter skal gjennomføres som del av EØS-avtalen, er fylkeskommunenes rolle konsentrert om EUs utviklingsprogram (NOU 2012:2, 2012, s. 148). Dette nyanseres noe av Indset (2008, s. 101) som formidler inntrykket av at regionkontorene involverer seg i EUs policyarbeid, riktignok uten at dette begrunnes.

Det regionale og lokale nivåets interesser ivaretas av regionkomiteen i EU (Committee of the Regions – CoR). Dette er et rådgivende for kommisjonen organ som ble etablert med Maastrichttraktaten og sammensatt av valgte representanter for regionene i EU. Som EØS-land har Norge ikke sete i denne komiteen og det er heller ikke et tilsvarende organ i EFTA.

2.2 Personvern

2.2.1 Om personvern

Personvernet slik vi kjenner det i dag har sine røtter i traktater om menneskerettigheter. De viktigste er FNs verdenserklæring om menneskerettigheter fra 1948, FN-konvensjonen om sivile og politiske rettigheter fra 1966 og den europeiske menneskerettskonvensjon fra 1950 (Schartum & Bygrave, 2016). I 1967 utga den amerikanske jusprofessoren Alan F. Westin boken «Privacy and Freedom» hvor rettsvernet for personopplysninger ble knyttet sammen med utviklingen i bruk av elektronisk databehandling. Dette var starten på en debatt i store deler av den vestlige verden. Forfatteren selv begrunnet styrken i den amerikanske debatten med at den var «et symptom på en tillitskrise mellom offentlig forvaltning og store selskaper på den ene siden, og det amerikanske folk på den annen side» (Bing, 1991, s. 14-15).

Endringer i av personvernlovgivingen de siste tiårene har bakgrunn i en økende elektronisk behandling av personopplysninger som følge av IKT- og internettutviklingen. Personopplysningsloven og forordningen setter krav til internkontroll, sikkerhetsorganisasjon og andre organisatoriske tiltak for virksomheter som behandler personopplysninger og plasserer det innen organisasjonskunnskapens domene. I denne oppgaven er det organisatoriske forhold som er hovedtema.

Beskyttelse av personopplysninger omhandler flere fagområder. Med en egen lov som regulerer behandling av personopplysninger er juridiske problemstillinger åpenbare. I det norske akademiske miljøet har fagområdene rettsinformatikk og forvaltningsinformatikk ved Juridisk fakultet, Universitetet i Oslo vært toneangivende i forskning på personvern. Fagområdene er tverrfaglige, og selv om det juridiske perspektivet synes å dominere i volum har miljøene bidratt med forskning som også dekker organisatoriske og teknologiske sider ved personvernet.

For personvern i kommunesektoren er det særlig grunn til å trekke fram arbeidene til Tranvik i perioden 2009 til 2012 (Tranvik, 2009a, Tranvik, 2009b, Tranvik, 2009c, Tranvik, 2011, Tranvik, 2012). Disse arbeidene stammer fra en undersøkelse av hvordan 19 større norske kommuner i

østlandsområdet etterlevde personopplysningslovens krav. Studien omfattet også Datatilsynets virkemiddelbruk overfor kommunene.

En av hovedkonklusjonene var at kommunene gjennomgående hadde god vilje, men lav evne til å følge regelverket. De var også bedre til å utarbeide dokumentasjon enn til å implementere systemene og iverksette organisatoriske tiltak. Tranvik kalte dette for en «etterlevelsillusion», hvor «atferdsendring [blir] ... mindre nødvendig: papirene og dokumentene gjør mangelen på endring mindre synlig og vanskeligere å oppdage» (Tranvik, 2009c, s. 116). I en nyere masteroppgave har Andersen (2017) trukket samme konklusjon i en studie av Datatilsynets virkemiddelbruk og hvordan to kommuner arbeidet med å følge opp avvikene som ble påpekt ved tilsyn.

Forordningen setter krav til alle offentlige og en rekke private virksomheter om at de må utnevne personvernombud. Et personvernombud vil bli kommunens ressurs innen personvern og ha flere roller hovedoppgaver. Kommunens kontaktpunkt for «de registrerte» hvis de har personvernrelaterte spørsmål, støtte for rådmannen som behandlingsansvarlig og intern ressurs for kommunens medarbeidere er de viktigste. I høringsutkastet til ny personopplysningslov brukte JD (JD, 2017) betegnelsen personvernrådgiver om denne funksjonen, men etter mange innspill er begrepet personvernombud beholdt i selve lovforslaget.

2.2.2 Datatilsynet

Lovgrunnlaget i Norge for elektronisk behandling av personopplysninger har også fulgt den teknologiske utviklingen. Siden 1978 har behandling av personopplysninger og personregistre vært regulert i lov, først ved personregisterloven (1978) og tilhørende forskrifter. Personopplysningsloven (2000) og personopplysningsforskriften (2000) erstattet personregisterloven i år 2000. Den bygger på EUs personverndirektiv (European Council, 1995) og er implementert som del av EØS-avtalen.

Datatilsynet, som forvalter personopplysningsloven har over tid vært bekymret for om kommunene etterlever personopplysningsloven med forskrifter. Tilsyn, undersøkelser og forskning har vist at kommunene gjennomgående har lav evne til å iverksette de tiltakene som loven krever. I 2010 kartla

Datatilsynet kommunenes egne vurderinger av hvordan de oppfylte personopplysningslovens dokumentasjonskrav og organisatoriske tiltak (Datatilsynet, 2011). Resultatene bekreftet inntrykket fra tidligere tilsyn. En streng tolking av svarene tilsa at bare syv % av kommunene hadde dokumentasjon i henhold til lovens krav, selv om halvparten oppga at de hadde det. Undersøkelsen vil bli grundigere behandlet i kapittel 5.

I de påfølgende årene har Datatilsynet brukt kommuneundersøkelsen som grunnlag for sine tilsyn. Det er ikke gjennomført noen ny kommuneundersøkelse etter 2011, men i 2016 skriver tilsynet at det er indikasjoner på en svak bedring i kommunenes internkontroll, datasikkerhet og etablering av databehandleravtaler i sin årsmelding (Datatilsynet, 2016).

Datatilsynet bruker både instrumentelle og institusjonelle virkemidler i å forvalte personopplysningsloven og personopplysningsforskriften. Loven og forskriftens bestemmelser er i sin natur instrumentell, med klare krav til ansvar, oppgaver og organisering av hvordan personopplysninger behandles i virksomheter. Tilsyn og vedtak er instrumentelle virkemidler som tilsynet har brukt i økende grad, se bl.a. (Tranvik, 2009a, Datatilsynet, 2016). Bruk av overtredelsesgebyr og politianmeldelse er andre instrumentelle virkemidler som tilsynet rår over, men som tidligere ikke har vært brukt overfor kommunesektoren. Fra 2014 har imidlertid overtredelsesgebyr vært brukt som administrativ sanksjon overfor enkelte kommuner (Datatilsynet, 2014b). Politianmeldelse har ikke vært brukt overfor kommuner, og dette sanksjonsnivået vil også falle bort i ny personvernforordning.

Bruken av institusjonelle, «harde» virkemidler balanseres ved at Datatilsynet i utstrakt grad formidler informasjon om personvern, deltar i samfunnsdebatten, gjennomfører utredninger og kartlegginger, utarbeider veiledere, gir veiledning og besvarer henvendelser om forståelse og praktisering av loven og forskriften. Datatilsynet dialog med KINS og KS er viktige kanaler for å markedsføre personvernlovgivingen overfor kommunesektoren. Siden ordningen med personvernombud ble etablert på 2000-tallet har Datatilsynet utdannet og utnevnt ombud i den enkelte virksomhet. De vil trolig få en annen rolle overfor ombudene etter at personvernforordningen trer i

kraft, uten at denne foreløpig er fastlagt³. I perioden november 2017 til mars 2018 gjennomførte tilsynet, i samarbeid med KINS og KS, åtte todagers kurs/seminarer i forskjellige deler av landet som et tilbud til kommunene om informasjon om ny personvernforordning.

Tilsynet driver også egen forskning og generelle undersøkelser. I 2013/2014 fokuserte tilsynet på personvern i opplæringssektoren og dokumenterte funn og anbefalinger i rapporten «Personvern i skole og barnehage» (Datatilsynet, 2014a). Siden 2013 har Datatilsynet utarbeidet årlige rapporter «Personvern – tilstand og trender» i samarbeid med Teknologirådet, i tillegg til at de har publisert en rekke temarapporter⁴. Datatilsynets årsrapporter er utfyllende kilder som årlig rapporterer resultatene fra tilsyn, sanksjoner som er tatt i bruk, generelle utviklingstrekk og andre aktuelle tema.

2.2.3 Øvrige aktører på personvernområdet

Øvrige aktører nevnes kort og har ikke som siktemål å være en uttømmende liste over aktører innen personvernområdet. Hvilken rolle og ressurs de kan utgjøre for kommunene vil utdypes hvis det er naturlig i senere kapitler.

KINS – Foreningen for kommunal informasjonssikkerhet er en frivillig organisasjon med medlemmer fra kommunene og private virksomheter som arbeider med informasjonssikkerhet i kommunal sektor. Det er et faglig nettverk hvor medlemskommunene kan utveksle erfaringer. Foreningen har hatt sterk vekst i antall medlemmer etter at forordningen trådte i kraft og består i skrivende stund av 296 kommuner, fylkeskommuner og driftsselskap.

KS – Kommunesektorens organisasjon vedlikeholder en rullerende kommunal digitaliseringsstrategi, arrangerer årlige eKommunekonferanser og har etablert KommIT-rådet som et rådgivende utvalg om digitalisering i sektoren. De har gjennomført kartlegginger av digitaliseringsstatus i kommunene

³Egne notater fra NYPE-kurs på Gardermoen 19 mars 2018

⁴Interesserte henvises til tilsynets nettsider <https://www.datatilsynet.no/om-personvern/rapporter-og-utredninger/>

ved «eKommunekartlegginger» i 2011 og 2014. Nylig har de publisert et oppdatert kunnskapsgrunnlag på digitaliseringsområdet (Rambøll, 2018b) og en kvantitativ undersøkelse av digital modenhet (Rambøll, 2018a).

Difi – Direktoratet for forvaltning og ikt (Difi) er underlagt KMD, men har sektorovergripende oppgaver i digitaliseringen av offentlig sektor. Hovedinnsatsen er overfor statlige virksomheter, men med kommunene som en viktig målgruppe ved samordning av forvaltningsnivåene (KMD, 2018). Difi har utviklet kurs og veiledere i informasjonssikkerhet som også kan være anvendelige i kommunesektoren.

NSM – Nasjonal sikkerhetsmyndighet overvåker og koordinerer alvorlige dataangrep nasjonalt. Ansvarsområdet dekker kritisk infrastruktur i offentlig og privat sektor.

NorSIS – Norsk senter for informasjonssikring er et rådgivingscenter for offentlige og private virksomheter. De er med på å gjennomføre «Nasjonal sikkerhetsmåned» som arrangeres i oktober hvert år. I samarbeid med Lillehammer og Gjøvik kommuner utga de en rapport om behovet for, og mulig organisering av, et senter for forebygging, varsling og støtte ved cybersikkerhetshendelser i kommunesektoren (NorSIS, 2015). Forslaget er til behandling i KommIT-rådet.

2.2.4 Internkontroll og informasjonssikkerhet

Kravet til internkontroll og informasjonssikkerhet følger av gjeldende personopplysningslov §§ 13 og 14 (Personopplysningsloven, 2000) og blir videreført, men med andre formuleringer, i den nye loven. Offentlige myndigheter, inklusive kommunesektoren, har også krav om internkontroll i blant annet eForvaltningsforskriftens §15 (eForvaltningsforskriften, 2004).

Informasjonssikkerhet og internkontroll i de aktuelle forskriftene er beskrevet med egenskaper som er hentet fra internasjonale standarder og rammeverk. For informasjonssikkerhet er ISO/IEC 27000 den dominerende familien av standarder (se Daler, Gulbrandsen, Høie, og Sjølstad, 2010,

s. 121-129 og Disterer, 2013). De egenskapene som forskriftene setter til internkontroll bygger på rammeverkene COSO⁵ og COBIT⁶. Rammeverkene inneholder en rekke kjennetegn på egenskaper som må eller bør være til stede for at organisasjonen kan sies å ha tilfredsstillende informasjonssikkerhet og internkontroll.

I denne studien tas det utgangspunkt i de faktorene som standardene 27001 og 27002 anser som vesentlige og egenskaper som kan utledes av forordningen. Disse finnes i den uoffisielle oversettelsen av artikkel 32 og fortalepunktene, 75 - 79 og 83 Justis- og beredskapsdepartementet, 2017. Det vil blant annet belyses hvor mange av kommunene som mener å ha et styringssystem for informasjonssikkerhet. Aktuelle faktorer er ledelsesforankring, dokumentasjon på styringssystemet og gjennomføring av risikovurderinger.

2.2.5 Modenhet og måling

Begrepet modenhet brukes i denne studien om organisasjoners utviklingsnivå i forhold til det potensialet de har. Modenhet blir i denne studien brukt som et felles mål på hvor vel utviklet kommunene er i å ivareta personopplysningene som de behandler. Formålet med et slikt felles mål er å fange et bredere spekter av indikatorer på regeletterlevelse enn hva vurderingen av et internkontrollsystem kan gi.

Indekser og skalaer er sammensatte mål hvor en variabel representerer verdiene på flere indikatorer. Hensiktene med å bruke sammensatte mål kan være å forenkle modeller ved å redusere antallet variabler samtidig som mest mulig av meningsinnholdet beholdes, redusere målefeil og at flere sider ved et begrep tas med i modellen (Ringdal, 2013, s. 94). Indekser og skalaer måler begge latente variabler eller egenskaper, teoretiske begrep som ikke kan måles direkte. Det som skiller er at skalaer settes sammen av effektindikatorer hvor den latente variabelen påvirker svarene på hver enkelt

⁵Committee of Sponsoring Organizations of the Treadway Commission - <https://www.coso.org>

⁶Control Objectives for Information and related Technology - <http://www.icasa.org>

indikator. Indekser settes sammen av årsaksindikatorer, det er de samlede svarene på indikatorene som leder til verdien på indeksvariabelen.

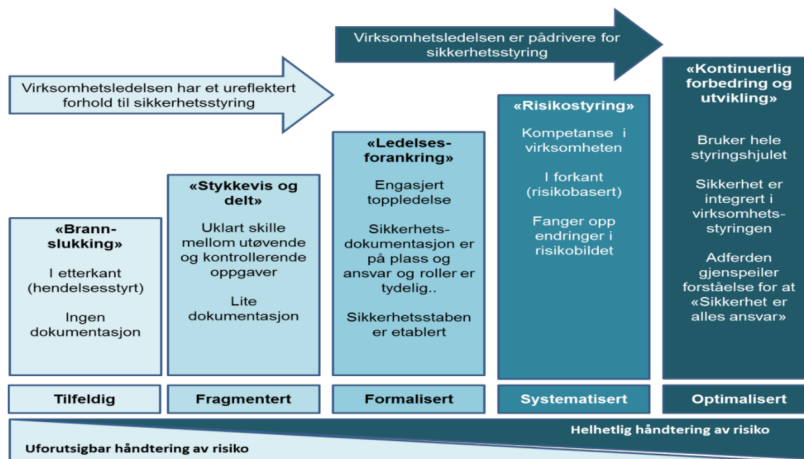
Det har ikke lyktes å finne vitenskapelige arbeider som har utviklet et slikt sammensatt mål for modenhet i å behandle personopplysninger. Begrepet modenhet er imidlertid brukt i flere typer vurderinger av hvor langt offentlig virksomhet er kommet i digitalisering av tjenester og myndighetsutøvelse.

Riksrevisjonen gjennomførte en undersøkelse av digitaliseringen i kommunene hvor «modenhet» er hyppig brukt i beskrivelsene av status, men selve begrepet er ikke definert i rapporten (Riksrevisjonen, 2016). KS utga i mars 2018 en kartlegging av digital modenhet i kommunesektoren (Rambøll, 2018a). I den offentlig tilgjengelige oppsummeringen er begrepet modenhet ikke definert ut over at det representerer et gjennomsnitt av svarene på utvalgte spørsmål. Difi har oversatt et verktøy for å måle digital modenhet i organisasjoner. Verktøyet er utviklet for Government of South Australia av KPMG Australia (Difi, 2017) og opererer med fem modenhetsnivå. Difi sitt verktøy er godt beskrevet, men det presiseres at verktøyet ikke er et vitenskapelig måleinstrument.

Nasjonal sikkerhetsmyndighet bruker en modell som deler virksomheters sikkerhetsstyring inn i fem modenhetsnivå (Nasjonal sikkerhetsmyndighet, 2015, s. 26). Denne har utgangspunkt i modellen Capability Maturity Model Integration (CMMI) fra Carnegie Mellon University (CMMI Product Team, 2001). Her deles modenhet inn i fem nivå. Denne synes å ha den sterkeste vitenskapelige forankringen og er valgt som utgangspunkt for å utvikle et mål for modenhet i behandling av personopplysninger. Figur 2.2 på neste side visualiserer egenskapene for organisasjoner på de ulike trinnene⁷.

I det laveste nivået av modenhet mangler organisasjonen strukturerte, formaliserte og dokumenterte prosesser for styring av risiko. Hendelser som oppstår løses «der og da» ut fra beste skjønn hos medarbeiderne, men uten at det er gitt retningslinjer for hvordan de skal håndteres og rapporteres. På nivået over finnes noen rutiner og prosedyrer, men har avgrenset virkeområde

⁷Figuren har også mange likhetstrekk med en illustrasjon fra den daværende danske Økonomistyrelsens veileder i risikostyring (Eide og Nagell-Erichsen, 2007, s. 22).



Figur 2.2: Modell for modenhet (Nasjonal sikkerhetsmyndighet, 2015)

og dekker heller ikke hele organisasjonen. Ledelsen tar en aktiv rolle i å legge til rette for organisasjonens sikkerhetsstyring fra det midlere nivået og over. Nederst i figuren indikeres en glidende overgang fra at risikohåndteringen skjer på ad hoc basis til en systematisk og gjennomgripende systematisk tilnærming til risiko.

2.3 Teorien om oversettelse

2.3.1 Translasjonsteori

Pragmatiske institusjonalisme og translasjonsteori har sitt utgangspunkt i overføring av organisasjonsideer. Dekontekstualisering benyttes som begrep for prosessen med å hente ut organisatorisk praksis fra ett miljø og klargjøre begrepene og praksiselementer slik at de kan tas i bruk i andre organisasjoner. Prosessen med å innføre ideene i andre virksomheter kalles kontekstualisering. Overføring kan skje vertikalt mellom forvaltningsnivåer og horisontalt mellom enheter på samme forvaltningsnivå (Røvik, 2007). I denne studien behandles personvernforordningen som en organisasjonsidé.

Det kan diskuteres om det rimelig å anvende teorien på en EU-forordning som skal bli norsk lov. Når myteperspektivet presenteres i

«Organisasjonsteori for offentlig sektor» er EU trukket fram som en av de store skaperne av organisasjonsoppskrifter. Senere i samme kapittel brukes Di Maggio og Powells begrep *tvangsmessig adoptering* om oppskrifter som pålegges ved lov eller forskrift (T. Christensen, Egeberg, Læg Reid, Roness, og Røvik, 2015, s. 83, 91).

Forordningen har også egenskaper som Røvik bruker som kjennetegn på organisasjonsideer. GDPR, den engelskspråklige forkortelsen for personvernforordningen, er blitt et *allestedsnærværende* begrep. Forkortelsen er mer vanlig i bruk enn begrepet også i norske medier⁸. Det blir ikke riktig å hevde at selve forordningen har en *uklar historie*, men mange av elementene den består av er hentet fra andre organisasjonsoppskrifter. En forordning er åpenbart *gjennomtrengende* i EU/EØS-området, men også i USA er GDPR satt på dagsorden og blitt et tema for advokater, rådgivere og organisasjoner. Reglene vil gjelde for all næringsvirksomhet rettet mot EU/EØS-området og vil også påvirke de globale store selskapene på internett. De *Reformutløsende* aspekten illustreres av tilsynsmyndighetenes oppfordringer til virksomhetene om å skaffe seg oversikt, gjennomgå rutiner og forberede nytt lovverk. Kommunene er det siste året blitt jevnlig kontaktet av firma som skal selge produkter, tjenester eller columbi egg som skal «løse utfordringen med GDPR» for dem. Forordningen har også *tvetydige virkninger*. Den har vært presentert, og er akseptert, som en nødvendig modernisering av lovgivingen for å håndtere press på personvernet som følge av internettets utvikling. Den andre, og like viktige begrunnelsen for EU er å bruke forordningen for å harmonisere lovverket og skape best mulige rammefaktorer for det digitale indre markedet.

For den vertikale overføringen, fra EU via nasjonale lovgivende myndigheter til kommunesektoren vil oppgaven avgrensnes til å behandle kontekstualisering av de kravene som kommunene må oppfylle i henhold til forordningen. Når forordningen skal implementeres vil den tas forskjellig i mot fra kommune til kommune og etter teorien kunne møte tilnærmingene eller

⁸Et oppslag i Atekst 4/5-18 gir 108 treff på *personvernforordning* i norske medier i løpet av de siste to årene, mens tilsvarende søk på *GDPR* ga 247 treff.

oversettelsesreglene *reproduserende*, *modifiserende* og *radikale* modus. Disse vil lede til ulik implementering av forordningen.

Også horisontal overføring mellom kommuner kan ha betydning for regeletterlevelse og implementering av ny personopplysningslov. En arbeidshypotese er at i kommuner som tilfredsstiller ett eller flere av kriteriene har personvernombud, er medlem av KINS og/eller deltar i interkommunale samarbeid innen IKT vil ha en regeletterlevelse som er bedre enn kommuner som ikke deltar i slike samarbeid.

2.3.2 Virusteori

Virusteorien (Røvik, 2007) er lansert som et alternativ og en mellomting mellom de instrumentelle og institusjonelle teoritradisjonene. Som en metafor benyttes virusets egenskaper for å forstå hvordan organisasjonsideer, i dette tilfellet organisasjonsoppskrifter som lovkrav, oppfører seg når de forsøkes implementert i en organisasjon. Elementene i denne teorien er det teoretiske grunnlaget for å tolke resultatene av de kvantitative analysene.

Form, innhold og opprinnelse for forordningen adskiller seg fra virusets form, og populære organisasjonsideer ved at den ikke kan betraktes som enkel. Det er heller ikke noen uklarheter om opprinnelsen. Sett under ett er det få likhetspunkter mellom dette elementet i virusteorien og personvernforordningen.

Smitte omhandler spredningen av organisasjonsideer og har klare likheter med virus i måten de spres på. Spørsmålet som må undersøkes nærmere er om behandling av personopplysninger «smitter» mellom kommuner i samme region eller som samarbeider i nettverk som for eksempel KINS eller interkommunale IKT samarbeid.

Immunitet innebærer at organisasjonsideer ut fra teorien vil kunne utløse organisatoriske forsvarsmekanismer eller møte annen indre motstand som gjør at ideen ikke finner fotfeste i organisasjonen. Argumentasjonen bygger på at organisasjonsideen enten truer eksisterende rutiner eller strukturer, at ideen ikke ansees som relevant eller at ideen av ulike årsaker ikke når inn til de delene av organisasjonen som kan sette dem ut i livet. Hvis dette elementet fra virusteorien skal være relevant må det være å avdekke

indre motstand eller manglende evne til å etterleve regelverket. Tranviks forskning tyder på manglende evne til å følge regelverket snarere enn aktive forsvarsmekanismer. Hvilke barrierer kommunene selv oppgir som de viktigste hindrene mot å praktisere personvernlovgivningen etter lovens intensjon vil derfor undersøkes nærmere.

Inkubasjonstid og *Fra smitte til symptomer* omfatter at det kan ta tid fra en ny lov blir vedtatt og til den er gjennomført i de organisasjonene som skal forholde seg til den. Dette bryter med instrumentell oppfatning av kommunene som lojale og lovlydige verktøy for styringsnivåene over. Realitetene på personvernområdet i kommunesektoren er allikevel at de fleste tilsyn avdekker avvik (Datatilsynet, 2016). Endring i regeletterlevelse i 2017 sammenlignet med 2010 vil kunne knyttes til dette elementet av virusteorien.

Lov og forskrift samt praktisering av disse kan neppe *mutere* eller *usynliggjøres* i kommunene. Det som kan være tilfelle er at kommunenes praktisering er i tråd med lovverket ved at personopplysninger er sikret og behandles slik de skal, men uten at formkrav og dokumentasjon tilfredsstiller kravene til tilsynsmyndighetene. Vil kommunenes egenvurderinger og modenhet gi indikasjoner på om det å ha vedtatt et internkontrollsystem er et godt mål på kommunenes behandling av personopplysninger?

Inaktivering og reaktivering ser en eksempler på i disse dager. Oppmerksomheten rundt ny personopplysningslov har bragt en rekke rådmenn og andre kommunale ledere som deltakere på KINS, Datatilsynet og KS sine todagers NYPE-kurs. Vil tilsyn, uheldige episoder i kommunen, forvaltningsrevisjoner og medieoppslag også ha bidratt til å reaktivering av personopplysningslovens krav til behandling av personopplysninger?

Virusteori har vært brukt som teoretisk grunnlag i noen norske og skandinaviske masteroppgaver. Hellsaa (2013) drøftet endringsledelse og bruk av kvalitetsrammeverket ISO9001 i kommuner og fant symptomer som tilsvarte Tranviks «etterlevelsessillusjon», blant annet med virusteorien som forklaringsmodell. En studie av balansert målstyring (Østby, 2016) fant også virusteorien egnet til å belyse hvordan dette styringsverktøyet hadde utviklet seg over 15 år i det norske forsvaret.

3 Metode og data

3.1 Metode

Oppgaven er en casestudie utarbeidet ved en kombinasjon av kvantitativ og kvalitativ forskningsstrategi. En definisjon av casestudie er «å se caser som tilfeller av en bestemt type teoretisk fenomen» (Ringdal, 2013, s. 170). Sammenhengen mellom de teoretiske fenomenene *europisering* og *regeletterlevelse* som studien omfatter er skjematisk fremstilt i figur 2.1 på side 10.

Personvernforordningen representerer ett element i europiseringen av kommunal forvaltning. Europisering drøftes med norske øyne og fra det lokale nivået som perspektiv i kapittel 4, i hovedsak på grunnlag av dokumentstudier fra åpent tilgjengelige kilder. Behandlingen bygger også i noen grad på de delene av undersøkelsen hvor respondentene hadde anledning til å gi egne vurderinger.

Regeletterlevelse operasjonaliseres ved å utvikle en modenhetsskala på grunnlag av respondentenes egenvurdering av hvordan kommunen etterlever personopplysningsloven med forskrift. Ambisjonen er å avdekke egenskaper ved kommunene som kan være med på å forklare forskjeller regeletterlevelse mellom kommunene. Hovedinnholdet i inneværende kapittel er en presentasjon av den kvantitative delen av studien og den metodiske tilnærmingen til de statistiske analysene i kapittel 5. Først beskrives de data som det har vært mulig å gjenbruke fra kommuneundersøkelsen 2011 (Datatilsynet, 2011) samt andre kilder som utfyller bildet av den undersøkelsen. Deretter presenteres undersøkelsen høsten 2017 med design og gjennomføring. Videre gjøres det rede for data som er innhentet fra andre

kilder . Til slutt, i avsnitt 3.5 og 3.6 vurderes henholdsvis etiske forhold og undersøkelsens reliabilitet og validitet.

Analysemetodene som er valgt tar sikte på å identifisere om det er statistisk sammenheng mellom det teoretiske begrepet regeletterlevelse og variablene som er hentet inn gjennom undersøkelsen og andre kilder. Begge undersøkelsene som er brukt ble gjennomført i hele populasjonen av norske kommuner.

En forutsetning for å kunne teste statistisk signifikans er at dataene som brukes representerer et tilfeldig utvalg av populasjonen. Signifikanstesting kan derfor ikke begrunnes i designbasert statistisk teori, som er det mest brukte teoretiske grunnlaget for bruk av statistiske tester. Thrane (2017, s. 83) viser til at modellbasert statistisk teori er et alternativ, og henviser i den forbindelse til Aaberge & Laake (1984) og Hoem (2008). Storstad (2010) har også brukt den samme argumentasjonen i en større undersøkelse av lokalt kulturliv for Norsk kulturråd. Modellbasert statistisk teori innebærer at det er forholdet mellom variablene som generaliseres. Det er denne begrunnelsen og ambisjonen om å finne eksterne og interne faktorer som kan indikere forskjell i regeletterlevelsen i kommunesektoren som er rasjonalet for signifikanstesting som metode.

Bearbeiding av data og analyser er i hovedsak gjennomført i statistikkprogrammet R (R Core Team, 2017) og utvalgte tillegg. De viktigste tilleggene har vært *Tidyverse* (Wickham, 2017) for datamanipulering, *Likert* (Bryer & Speerschneider, 2016) for visualisering og analyse av data på Likert-format, *Ordinal* (R. H. B. Christensen, 2015) for analyse av ordinale data samt *Stargazer* (Hlavac, 2018) og *xtable* (Dahl, 2016) for de fleste av tabellene. Faktoranalysen ble gjort i SPSS. Data fra eksterne kilder er hentet ned og behandlet i Excel før de ble hentet inn i statistikkprogrammene.

3.2 Datatilsynets undersøkelse i 2010

Datatilsynets kommuneundersøkelse ble gjennomført blant annet for å kontrollere om forutsetningene i personopplysningsloven var fulgt av kommunesektoren. 429 kommuner og fylkeskommuner, 96 %, deltok.

Deltakende kommuners svar på hovedspørsmålet, om kommunen hadde et system for internkontroll, er gjengitt i vedlegg til rapporten (Datatilsynet, 2011). For noen kommuner er det bare oppgitt hvilket fylke de tilhører. Enkelte av disse kunne identifiseres ved at navn manglet på en kommune i fylket eller at alle de «navnløse» kommunene hadde avgitt samme svar. 9 kommuner i tre fylker måtte tas ut av datasettet fordi det ikke var mulig å identifisere dem.

Det fulle datasettet fra undersøkelsen i 2010 har ikke vært tilgjengelig. Ut over spørsmålet om internkontroll folketallet i kommunene i 2010 hentet fra SSB. Det har også vært mulig å identifisere hvilke kommuner som hadde personvernombud i 2010 ved hjelp av uttrekk fra Offentlig elektronisk postjournal sammenholdt med en oversikt over personvernombud som lå på Datatilsynets hjemmesider fram til høsten 2017.

Datasettet fra 2010 som er brukt i studien består av 420 kommuner og fylkeskommuner. Det inneholder kommunenes folketall i januar 2010 og to kategoriske variabler som viser om kommunen/fylkeskommunen hadde internkontroll og om den hadde personvernombud. Sammenlignende analyser mellom 2010 og 2017 er avgrenset til om kommunene mener å ha system for internkontroll.

3.3 Spørreundersøkelse høsten 2017

3.3.1 Design

Studien ble innledet med å gjennomføre en spørreundersøkelse (survey) i perioden 23. oktober til 16. november 2017. De viktigste formålene med undersøkelsen har vært å få respondentenes egen vurdering av hvor godt forberedt kommunen er på de endringene som kommer med ny personvernforordning, synspunkter på europeisering av det lokale forvaltningsnivået og forhold internt og i kommunenes omgivelser som kan påvirke regeletterlevelsen. Siden forordningen i stor grad bygger på at kravene i dagens personopplysningslov med forskrift er oppfylt er de fleste av spørsmålene knyttet til plikter etter dagens lovverk.

Utgangspunktet for å konstruere spørsmål var kommuneundersøkelsen 2010. Europeisering av det lokale forvaltningsnivået eller mekanismer som kan tenkes å forsterke eller svekke regelletterlevelse i kommunene inngikk ikke som tema i denne. Høsten 2017 var det usikkert om bestemmelsene om internkontroll ville videreføres i ny personopplysningslov. De to undersøkelsene skiller seg derfor på vesentlige punkter og det er bare enkelte deler som vil kunne sammenlignes. For det etterfølgende brukes begrepet «undersøkelsen» om dette prosjektets kommuneundersøkelse, med mindre det er eksplisitt vist til en annen undersøkelse eller det fremgår av sammenhengen.

Undersøkelsen ble konstruert med innlagte faktaopplysninger om kommunene (kommunennummer, navn og fylke) for å redusere feilkilder og unngå at respondentene skulle bruke tid på slike spørsmål. For øvrig ble spørsmål utledet av forskningsspørsmål fra studiens problemstillinger. De data som kunne hentes eller utledes fra andre kilder ble identifisert. Før undersøkelsen ble sendt ut ble et utkast testet ut på mine medstudenter. Tilbakemeldingene fra denne testen førte til at enkelte av spørsmålene justert. Endringene bidro til å forbedre språket og redusere faren for at spørsmålene skulle misoppfattes.

Den endelige undersøkelsen består av 20 spørsmål. Tre av spørsmålene er rent åpne spørsmål med tekstfelt for synspunkter og kommentarer. De øvrige er en kombinasjon av vurderings- og adferdsspørsmål. Spørsmålene i undersøkelsen er gjengitt i vedlegg A.

3.3.2 Gjennomføring og representativitet

Invitasjonen til å delta i undersøkelsen gikk til alle kommuner⁹ og ble sendt til kommunens postmottak på epost den 23 oktober 2017. Verktøyet Questback ble brukt for undersøkelsen fordi Høgskolen i innlandet har lisenser til disposisjon for blant annet studentoppgaver. I løpet av undersøkelsesperioden ble det sendt to purringer til de kommunene som til da ikke hadde svart. Den første etter ca. en uke, 29. oktober, og den andre 13.

⁹De som var registrert i SSBs standarder for kommuneinndeling og fylkesinndeling pr januar 2017 (SSB, 2017b, 2017a), til sammen 445 henvendelser

Tabell 3.1: Svarprosent i undersøkelsen

	Antall	Svar	Andel svar	Andel respondenter
Kommuner	426	97	22.8%	95.1%
Fylkeskommuner	19	5	26.3%	4.9%
Sum	445	102	22.9%	100%

november, fire dager før undersøkelsen lukket. Begge puringene resulterte i en økning av svarandelen. Personer jeg tidligere har hatt kontakt med i noen av kommunene som ikke hadde svart ble også kontaktet og anmodet om å oppfordre kommunen til å svare. En presentasjon av undersøkelsen ble publisert på KINS sine hjemmesider (KINS, 2017) og republisert på foreningens og min egen facebookside.

Ved undersøkelsens slutt den 16. november hadde det kommet inn 102 svar, fra 97 kommuner og 5 fylkeskommuner. Tabell 3.1 viser andel svar i forhold til totalt utsendte henvendelser og forholdet mellom svar fra kommunene og fylkeskommunene.

Deltakelsen er lav sammenlignet med Datatilsynets undersøkelse hvor 96% av kommunene fullførte undersøkelsen. Også Direktoratet for samfunnsikkerhet og beredskap har hatt svarprosent på over 90 i sine årlige spørreundersøkelser om kommunenes samfunnsikkerhetsarbeid (DSB, 2017). Samtidig er lav svarprosent en gjennomgående utfordring som diskuteres i fagmiljøene internasjonalt, særlig for personundersøkelser med utvalgsdata (Hellevik, 2015). Årsakene til at Datatilsynet hadde såvidt høy svarprosent var at de brukte systemplikten etter § 14 i personopplysningsloven og satte på vesentlige ressurser for å følge opp kommuner som ikke svarte (Datatilsynet, 2011). For DSBs vedkommende har de et regionalt ledd i Fylkesmennesens beredskapsavdelinger som ble brukt for å følge opp kommunene.

I KS sin undersøkelse var det 32% som besvarte hele undersøkelsen og en noe høyere andel som besvarte deler av den, og hadde samme målgruppe. Det antas også at undersøkelsene ble gjennomført noenlunde samtidig, selv om det ikke fremgår av den dokumentasjonen som er publisert. Konsulentselskapet som gjennomførte KS sitt prosjekt kunne bruke KS sin

autoritet. De satte ekstra ressurser på for å følge opp kommunene som ikke svarte og fikk derfor en høyere svarprosent (Rambøll, 2018a).

Totalt sett hadde det vært ønskelig med en høyere svarandel enn 23% også i denne studien. Det ville trolig vært mulig med en omfattende oppfølging mot enkeltkommuner. Dette kunne vært gjort ved å kontakte kommunene på forhånd og identifisere kontaktperson og i etterkant ved å kontakte kommunene som ikke hadde svar, direkte. Det er imidlertid usikkert hvor mye høyere svarandelen kunne blitt og om det ville være verd innsatsen.

Fordelingen av kommunene som deltok i undersøkelsen avviker betydelig fra populasjonen med hensyn til folketall, geografisk representasjon og andelen med personvernombud. Tabell C.1 på side 119 viser kommunestørrelsen til de kommunene som har svart sammenlignet med alle kommunene i landet, inndelt i 6 grupper etter folketall. Mer enn hver femte av landets kommuner har under 2 000 innbyggere, men de utgjør bare en sjuendedel av deltakerne. Den samme tendensen gjelder også geografisk. over halvparten av kommunene i Akershus svarte på undersøkelsen, mens bare en av kommunene i Nord-Trøndelag deltok. Antallet kommuner med personvernombud er også overrepresentert. 37% av de som deltok i undersøkelsen hadde personvernombud pr 1. januar 2017, mot 19% for alle kommuner og fylkeskommuner. Utfyllende tallmateriale og grafikk ligger i vedlegg C.

Disse skjevhetene vil kunne gi et for optimistisk resultat for kommunesektoren som helhet og er en utfordring å korrigere fordi det ikke finnes data som kan brukes som referanse. Konsekvensen er at undersøkelsens funn ikke kan generaliseres til kommunesektoren som helhet. De konklusjonene som trekkes i undersøkelsen vil være gyldige for de kommunene som deltok i undersøkelsen.

Ambisjonsnivået med studien er å redegjøre for prosessen for å analysere status for regeletterlevelse, modenhet i behandling av personopplysninger og beskrive faktorer som innvirker på modenheten. Prosessen eksemplifiseres med resultater som vil være gyldige for de som har besvart undersøkelsen. I de tilfelle det vil være naturlig kommenteres hvilke vurderinger som vil avvike for en analyse som gjelder hele kommunesektoren (populasjonen) eller et tilfeldig utvalg.

3.3.3 Målemodell for modenhet

I avsnitt 2.2.5 på side 18 er det gjort rede for det teoretiske grunnlaget for sammensatte mål, indekser og skalaer. Modenhet som sammensatt mål viser om virksomheten har en systematisk og strukturert tilnærming til hvordan personopplysninger behandles. Det ble også gjort rede for hvorfor denne studien bygger på NSM sin modell for modenhetsnivå i sikkerhetsstyring (Nasjonal sikkerhetsmyndighet, 2015), som igjen bygger på CMMI (CMMI Product Team, 2001). Den videre konstruksjonen av det sammensatte målet for modenhet følger trinnene *valg av målemodell (skala eller indeks), velge ut indikatorer, testing av skalaen og ferdiggjøring* (Ringdal, 2013, s. 347).

Det er ikke umiddelbart intuitivt hvordan en kommunes modenhet i behandling av sine personopplysninger som latent variabel best kan representeres. En indeks settes sammen av indikatorer som samlet gir verdi til den latente variabelen, mens i en skala er verdien på indikatorene en effekt av verdien på den latente variabelen (Ringdal, 2013, s. 346). En av indikatorene som inngår i det sammensatte målet er ledelsens rolle. Er det rådmannen som viser vei og ved sine prioriteter og tiltak er med på å gi verdi til kommunens modenhet, eller er det slik at i en moden kommune vil interne prosesser og organisasjonskultur føre til at viktige aktiviteter blir forankret hos ledelsen? Dette er et spørsmål som griper inn i kjernen av forskjellene mellom et institusjonelt og et instrumentelt perspektiv på offentlige organisasjoners virkemåte (T. Christensen mfl., 2015). Tranviks (2009c) studier konkluderer blant annet med at viljen til å følge regelverket er god, mens evnen i mange kommuner svikter. Det er en indikasjon på at modenhetsnivået er en latent variabel som påvirker ledelsesforankringen. Det er det også rimelig å anta at interne prosesser og organisasjonskultur er med på å avgjøre kvaliteten på dokumentasjonen, om ansvarsfordelingen i kommunen er kjent, medarbeidernes kompetanse og om det er etablert og gjennomføres jevnlig kontroll. I denne studien legges det til grunn og det sammensatte målet for modenhet i å behandle personopplysninger utvikles som en modenhetsskala.

Ideelt sett burde skalaen vært utviklet med en forundersøkelse med statistiske analyser av svarene for å sjekke dimensjonalitet og reliabilitet.

Dimensjonalitet angir om spørsmålene er endimensjonale, om de måler ett og samme fenomen. Reliabiliteten sier noe om hvor pålitelig indikatoren er og indikerer hvor store målefeil de inneholder. For store målefeil vil svekke gyldigheten av undersøkelsen fordi resultatene vil variere for mye på grunn av feilene. Også ferdiggjøring av skalaen (før bruk) burde omfattet utprøving på ulike grupper av kommuner for å teste om dimensjonaliteten og reliabiliteten er gyldig for hele spekteret. Skalaens validitet, om den måler det man ønsker å måle burde også ideelt sett vært testet som forberedelser til en undersøkelse. Det har hverken vært tid eller ressurser til en slik omfattende testing i denne studien. For det videre arbeidet med konstruksjon av skalaen er det riktigst å betrakte undersøkelsen som en stor forundersøkelse. De statistiske testene gjennomføres på innkomne svar og kan eventuelt danne grunnlag for en videreutvikling av en modenhetsskala for behandling av personopplysninger i kommunesektoren.

3.4 Data fra øvrige kilder

3.4.1 Supplerende datamateriale

Data for visse variabler er hentet fra ulike åpne kilder. Dette for å holde antall spørsmål i undersøkelsen lavest mulig, hente data som respondentene ikke har forutsetninger for å besvare, redusere feil på grunn av misforståelser eller erindringsforkyving hos respondentene og for å dra nytte av den kvalitetssikringen som gjøres for åpne offentlige datasett. Kilder har vært Statistisk sentralbyrå, OEP¹⁰, opplysninger på Datatilsynets og KINS sine hjemmesider samt data hentet ut fra rapporter og vitenskapelige arbeider. Kommunenummeret ble brukt som koblingsnøkkel mellom svarene fra undersøkelsen og data fra øvrige kilder. Under redegjøres det kort for de eksterne data og hvordan de er innhentet. Bakgrunnen for at de ansees relevante vil diskuteres når de brukes i modellene i kapittel 5.

¹⁰Offentlig elektronisk postjournal – erstattet av eInnsyn fra 5. februar 2018.

3.4.2 Folketall og egenskaper ved kommunene

Samlet folketall i alle kommunene er hentet fra SSB sin statistikkbank for januar 2017 (SSB, udatert). Selv om folketall er en kontinuerlig variabel er det hensiktsmessig for noen analyser å dele inn kommunene i grupper etter kommunestørrelse. Det brukes forskjellige inndelinger, også i SSB. I de kommunegruppene som benyttes i KOSTRA ¹¹ er kommunestørrelsene delt inn i tre grupper, 0 – 4999, 5000 – 19999 og 20000 og over. Denne inndelingen dekker ikke alle kommuner, de fire største byene og de ti kommunene med høyest frie disponible inntekter per innbygger er skilt ut i en egen gruppe (Langørgen, Løkken, & Aaberge, 2015).

Når SSB publiserer statistikk som er basert på inndeling av kommuner etter befolkningsstørrelse benyttes «Standard for klassifisering av kommuner etter innbyggertall» (1998). I denne deles kommunene i følgende grupper: 1) Under 2000 innbyggere. 2) 2 000 - 4 999 innbyggere. 3) 5 000 - 9 999 innbyggere. 4) 10 000 - 19 999 innbyggere. 5) 20 000 - 49 999 innbyggere. 6) 50 000 eller flere innbyggere. Gruppe 5 og 6 er videre delt inn i to undergrupper, men det gir ikke bedre innsikt å bruke flere enn seks grupper.

3.4.3 Øvrige kilder til eksterne data

Deskriptiv statistikk for de eksterne variablene finnes i tabell 5.7 på side 62. Offentlig data om dialoger og kontakter med Datatilsynet inneholder en oversikt over skriftlig dialog mellom Datatilsynet og kommunene i perioden 2010 til 2016. Disse dialogene og enkeltkommuner ble kategorisert etter tema og koblet til kommunenummeret. Tilsyn omfatter brevkontroll, stedlig tilsyn og etterkontroller i kommunen. Tilsynsobjektene har vært kommunen sentralt, en sektor eller en institusjon. Disse er slått sammen til en dikotom variabel som angir om kommunen har hatt tilsyn fra Datatilsynet eller ikke. På samme måte er det registrert en variabel som angir om kommunene har hatt dialog med Datatilsynet vedrørende avvik.

Fram til medio 2017 vedlikeholdt tilsynet en oversikt over hvilke kommuner og fylkeskommuner som hadde personvernombud. Denne listen

¹¹KOmmune-STat-RApportering

ble hentet ned i mars 2017. I tillegg var hvert personvernombud utnevnt av Datatilsynet, slik at i eInnsyn er det søkbart hvilke kommuner som har fått utnevnt, endret eller avvirket personvernombud fra 2010. Ut fra disse to kildene kunne det konstrueres ett datasett med alle kommuner som hadde ombud pr januar 2017, samt hvilket år det første gang ble etablert. Noen interkommunale IKT-samarbeid har også personvernombud, men disse er ikke tatt med i datasettet. Bakgrunnen er at ombudet utnevnes for kommunen og ville i så fall vært eksplisitt angitt som personvernombud for eierkommunene.

Oversikt over KINS-medlemmer er hentet ut fra KINS sin hjemmeside (KINS, 2017) tidlig i 2017. I løpet av 2017 og 2018 har veksten i medlemmer vært spesielt sterk samtidig som det er tvilsom hvilken effekt et medlemskapet har hatt etter bare noen måneder. De som er tatt med i oversikten er derfor bare kommuner/fylkeskommuner som var registrert som KINS medlemmer 1. januar 2017, til sammen 160 eller 36%. Blant de som responderte på undersøkelsen var 52 av 102 kommuner medlem av KINS.

I 2015 gjennomførte konsulentselskapet PwC en rapport over interkommunale samarbeid på IKT-området. Som vedlegg til rapporten er det en detaljert oversikt over alle IKT-samarbeid i kommunesektoren da rapporten ble utgitt (PwC, 2015, s. 58-62), med navn, deltakerkommuner og årstall for når det ble opprettet samt type interkommunalt samarbeid.

3.5 Forskningsetikk

I følgebrevet til undersøkelsen er det presisert at prosjektets tema ikke var status i enkeltkommuner, men å gi en samlet oversikt over status og forberedelser til ny personvernforordning for sektoren som helhet. Dette er fulgt opp ved at det ikke er mulig å identifisere hva hver enkelt kommune har svart i denne rapporten.

Respondentene i undersøkelsen ble ikke spurt om navn, bare funksjon i kommunen. Ut fra funksjonen kan det være mulig for undertegnede å identifisere noen enkeltpersoner, som for eksempel i de kommunene hvor rådmannen selv har svart på undersøkelsen. Disse vil imidlertid ikke kunne

identifiseres ut fra denne rapporten eller vedleggene. For å unngå at tekstfelt i de kvalitative spørsmålene som er gjengitt i vedlegg B skulle kunne knyttes til en kommune er alle navn tatt ut og erstattet med tegnet <...>.

For øvrig er det med ett unntak brukt åpne kilder. Unntaket er masteroppgaven til Andersen (2017) som har begrenset tilgang på grunn av lovpålagt taushetsplikt. Det er ikke referert materiale fra den rapporten som bryter taushetsplikten i denne rapporten.

3.6 Reliabilitet og validitet

3.6.1 Reliabilitet

Reliabiliteten til studien, hvor pålitelige studiens konklusjoner er henger nøye sammen med datagrunnlaget og feilkilder ved innsamlingsmetode og bearbeiding. Kildene til den kvalitative delen av undersøkelsen er åpne data og i hovedsak offentlig informasjon som holder god kvalitet. Det kan allikevel ikke utelukkes at vesentlig informasjon ikke er innhentet. Det finnes også skjernet informasjon som kunne nyansere bildet og som kunne gitt andre konklusjoner.

Undersøkelsen som ble gjennomført er ny og ikke basert på gjennomprøvde spørsmål fra flere tidlige undersøkelser. Faren er derfor større for at enkelte spørsmål er utformet slik at de oppfattes forskjellig av den enkelte respondent. Dette er forsøkt håndtert ved en prøveundersøkelse blant mine kolleger. Elektroniske undersøkelser minimaliserer faren for prosesseringsfeil, men ikke for at respondenten avgir et annet svar enn tiltenkt. Data fra spørreundersøkelsen er hentet inn i statistikkprogrammet fra de originale filene som ble levert av Questback for å redusere faren for konverteringsfeil.

Data som er hentet fra vedlegg til tidligere undersøkelser måtte gjennom flere konverteringsprosesser siden de i utgangspunktet ikke var på et maskinlesbart format. Disse konverteringene kan ha ført til at data er blitt feilregistrert. Majoriteten av disse er trolig luket ut ved teknikker for å sortere og krysse data fra forskjellige tabeller. Data som er hentet ned fra SSB er av god kvalitet og systematiske feil i prosesseringen av dem er lite sannsynlig.

3.6.2 Validitet

Validitet – om studiens resultater gjelder eller om det er feil som gjør at svarene som er funnet ikke er dekkende eller gyldige for forskningsspørsmålene. En forutsetning er reliabilitet. Sunn fornuft, argumentasjon og tidligere forskning sier Thrane (2017, s. 47). Ringdal bruker begrepene umiddelbar validitet (face validity), innholdsvaliditet, kriterievaliditet og nomologisk validitet fra Netemeyer, Bearden, & Sharma (2003) som aktuelle perspektiver. Sunn fornuft og teori har vært brukt for å konstruere å ta fram problemstillingen, formulere forskningsspørsmål og i studiens design. Det utelukker ikke at feil kan forekomme.

Umiddelbar validitet, innholdsvaliditet og sunn fornuft fremstår som flere sider av samme sak. Er forskningsdesignet egnet til å besvare problemstillingene, og er svarene dekkende slik at ikke vesentlige momenter ikke blir belyst vil drøftes i avslutningen.

Kriterievaliditet kreves et sett kriterier å sammenligne med. Aktuelle kriterier kan være om funnene stemmer med tidligere undersøkelser og tidligere forskning om personvern i kommunesektoren. Skjevhetene blant deltakerne vil svekke verdien av en slik sammenligning, når utvalget av respondenter ikke er representative for sektoren kan det heller ikke ventes at svarene/synspunktene deres er sammenfallende med representative undersøkelser.

Nomologisk validitet er en vurdering av om studiens svar gir bidrag til å forstå temaet som belyses. Er det slik at kommuner med lav score på modenhet, i praksis ikke behandler personopplysningene slik de burde? Målet med å konstruere en skala som dekker flere aspekter enn dokumentasjonen var å komme nærmere slik validitet.

En kilde til systematiske målefeil er *enighetssyndromet*, at enkelte respondenter har en tendens til å gi like svar uavhengig av spørsmålet. Slike feil er problematiske hvis de blir systematiske. Noen av spørsmålene/indikatorne burde vært snudd, for eksempel ved at samme svar, for eksempel «helt enig», gir motsatt indikasjon på modenheten. Det ble ikke gjort i undersøkelsen og kan bidra til å svekke studiens validitet. Resultatene vil ikke ha gyldighet ut over de kommunene som deltok, av årsaker som er drøftet i avsnitt 3.3.2.

4 Europeisering, kommunene og personopplysninger

4.1 Europeisering av kommunenes personvern

EUs personvernforordning ble vedtatt i mai 2016 og gjøres gjeldende i EU fra 25 mai 2018 (EU, 2016). Forordningen skal også innlemmes i EØS-avtalen, en prosedyre som i skrivende stund ikke er fullført, og vil da gjelde EU/EØS-området. I dette kapitlet drøftes spørsmålet om hvordan EUs personvernforordning påvirker europeiseringen av kommunal forvaltning ut fra europeiseringens to komponenter, ovenfra-ned som beskriver hvordan EUs rettsakter legger rammer for nasjonal politikkutforming og nedenfra-opp om hvordan nasjonale aktører påvirker EU.

Historikk og bakgrunn for forordningen presenteres og vil belyses fra et ovenfra-ned perspektiv. Hvordan føyer personvernforordningen seg inn i det større bildet av europeisk integrasjon? Det gis også en kortfattet presentasjon av hvordan forordningen innlemmes i EØS-avtalen og status i denne prosessen.

Nedenfra-opp perspektivet representeres ved innvendinger som ble reist mot forslaget av, eller på vegne av, regionalt og lokalt nivå. Ut fra åpne kilder eller det som kan utledes fra disse redegjøres det for de rollene norske myndigheter og andre sentrale norske aktører har hatt i utviklingen av og informasjon om forordningen frem til 2016. Eventuelle spor av dialog mellom nasjonalt og regionalt/lokalt nivå i Norge i denne perioden vil også belyses. Hovedtrekk fra respondentenes synspunkter på nytt regelverk og virkninger for egen kommune sammenfattes til slutt i kapitlet.

4.2 Behovet for endringer

Arpanet, internettets forløper, ble utviklet på 1960-tallet og var i starten forbeholdt forskningsmiljø og militære formål. Først på begynnelsen av 1990-tallet ble det åpnet for kommersiell bruk (Nordal, Liseter, & Rossen, 2016). I samme tidsrom ble GSM-systemet, teknologien som blant annet gir mulighet for internett på mobiltelefoner, lansert i Europa (Hansen, 2017). Det var også i løpet av første halvdel av 1990-tallet at personverndirektivet (European Council, 1995) ble utviklet i EU. I 2017 var 48% av verdens befolkning regnet som internettbrukere, hvorav 81 % i I-landene (ITU, 2017).

Overgangen fra prosessering på lokale datamaskiner og servere til skytjenester har skapt nye strukturer for hvor personopplysninger lagres og hvordan de behandles for øvrig. For den enkelte har veksten i sosiale medier og smarttelefonenes mulighet til alltid å være «på nett» medført endrede bruksmønstre. Personverndirektivet har imidlertid en teknologinøytral form som har bidratt til at det i stor grad har kunnet fylle funksjonene det var tiltenkt, selv om lovgiverne neppe kunne ane rekkevidden av endringene som kom (Blume, 2015).

De siste årene har det vært en økende bruk av personopplysninger som samles inn på grunnlag av de sporene vi etterlater oss på nettet til bruk i reklameøyemed eller annen type rettede henvendelser mot sluttbrukere. Denne forretningsmodellen er en dominerende del av den globale digitale økonomien, ikke bare for sosiale medier som Facebook og Twitter, men også for mediekonsern verden over. Et annet felt som er i ferd med å modnes er profilering av adferdsdata for å kunne tilby differensierte priser på for eksempel bil- og helseforsikringer hvor en defensiv kjøreadferd eller et sunt og aktivt liv belønnes med lavere forsikringspremier.

For offentlige virksomheter vil for eksempel løsninger av typen velferds-teknologi¹² være systemer som kommer til å behandle store mengder personopplysninger på andre områder enn tidligere. Det er også mulig å se

¹²Teknologisk assistanse som bidrar til økt trygghet, sikkerhet, sosial deltakelse, mobilitet og fysisk og kulturell aktivitet, og styrker den enkeltes evne til å klare seg selv i hverdagen til tross for sykdom og sosial, psykisk eller fysisk nedsatt funksjonsevne (NOU 2011:11, 2011).

konturene av selvbetjente systemer for myndighetskontakt og automatiserte avgjørelser hvor vedtak om tildeling av tjenester eller offentlig myndighetsutøvelse ikke lengre fattes av saksbehandlere, men er resultat av algoritmer¹³ i dataprogrammer.

Kommisjonens viktigste begrunnelse for forslaget om å erstatte direktivet med en forordning var at den må innarbeides ordrett i lovverket til alle landene i EU/EØS området. Bakgrunnen var store variasjoner i hvordan nasjonene hadde implementert personverndirektivet. Et direktiv skisserer målsettinger, men hvordan dette skal implementeres i lovverket er opp til den enkelte nasjon. Variasjonene hadde etter kommisjonens oppfatning ført til et fragmentert regime for behandling av personopplysninger innad i EU som ga manglende forutsigbarhet for næringsdrivende og virket hemmende på veksten i den digitale økonomien. En forordning skal innarbeides ordrett i medlemslandenes lovverk og det argumenteres med at denne vil virke som katalysator for fortsatt vekst i det digitale indre markedet.

EUs interesse i å ivareta innbyggernes tillit til digitale tjenester har følgelig to ulike begrunnelser. Det er en følge av at EU sluttet seg til den europeiske menneskerettskonvensjon gjennom Lisboaatraktaten i 2009, et av fundamentene som europeisk personvern hviler på. Det er også et strategisk grep for å bidra til den videre utviklingen av det digitale indre markedet i EU, tilliten til digitale tjenester er ansett for å være en forutsetning for fortsatt vekst. Tilliten til sikkerhet og at personopplysninger behandles forsvarlig vil også bidra til at løsninger for velferdsteknologi kan tas i bruk i offentlig helseomsorg.

4.3 Ovenfra-ned europeisering

Da EU kommisjonen fremmet forslaget til ny personvernforordning i januar 2012 knyttet de forslaget til ny lovgiving opp i vedtak fra Kiev- toppmøtet i 2009. versendeslesbrevet fra kommisjonen formidlet tre overordnede begrunnelser for å fornye regelverket (European Commission, 2012):

¹³... en fullstendig og nøyaktig beskrivelse av fremgangsmåten for løsning av en beregningsoppgave eller annen oppgave (SNL, 2018)

- Den teknologiske utviklingen fører til et sterkere behov for at den enkelte har kontroll over egne personopplysninger
- En erkjennelse av at det fortsatt var et fragmentert regelverk på personvernområdet og at harmonisering av disse vil skape den forutsigbarheten som næringsliv og offentlige organ trenger
- Innbyggernes tillit til digitale tjenester er en nødvendig forutsetning for vekst i den digitale økonomien i EU

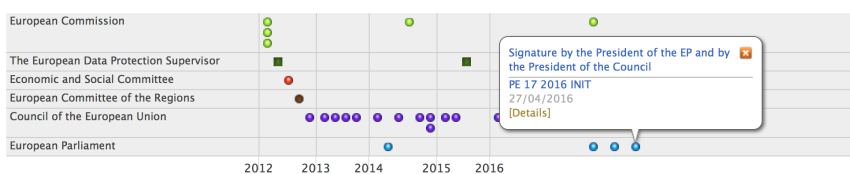
Begrunnelsene innebærer ingen endring i forhold til de overordnede mål i personverndirektivet, innbyggernes rett til personvern og fri flyt av data i EUs indre marked. Den første begrunnelsen over er knyttet til enkeltpersoners rett til i størst mulig grad å styre hvordan egne opplysninger brukes, både av det offentlige og av private aktører. Den andre handler om rammefaktorer for utviklingen av det digitale indre markedet¹⁴ i EU og for digital handel. Begrunnelsen om innbyggernes tillit er en kombinasjon av personvern hensyn og hensynet til å skape best mulig rammefaktorer for det digitale indre markedet i Europa.

4.4 Nedenfra-opp europeisering

Behandlingen av forordningen i EUs institusjoner pågikk i over fire år, prosessen er grovt gjengitt i figur 4.1 på neste side. Som det fremgår av figuren er rådet, EU-parlamentet og regionkomiteen (Committee of the Regions – CoR) de sentrale institusjonene som har behandlet forslaget. CoR har en konsultativ rolle ved at de har rett til å uttale seg om forslaget, men det er parlamentet og rådet som har beslutningsmyndighet.

Da forslaget ble lagt fram av kommisjonen ble det gjennomført konsultasjoner med de nasjonale parlamentene. De har rett til å uttale seg om nye EU-lover etter EUs subsidiaritetsprinsipp (nærhetsprinsipp), prinsippet om at all lovgiving skal skje på et lavest mulig nivå, men allikevel et så høyt nivå at lovgivingen blir effektiv. Regionene og kommunene i Europa

¹⁴EUS strategi for å dra nytte av den teknologiske utviklingen, fjerne digitale handelshindere samt bidra til best mulig tilgang til digital infrastruktur EU-borgerne



Figur 4.1: Beslutningsprosessen i EU (European Commission, udatert)

har en interesseorganisasjon, CEMR (Council of European Municipalities and Regions), som også spilte en aktiv rolle.

Det ligger utenfor denne studien å redegjøre for alle sider som ble diskutert i EU i den tiden utkastet til forordning var til behandling i EUs lovgivende organ. De som trekkes frem er enkelte innvendinger som ble reist mot forordningen og som er av betydning også for norsk kommunesektor.

4.4.1 Høringsinstansenes synspunkter

I de formelle tilbakemeldingene til beslutningstakerne var høringsinstansene enige i behovet for at lovverket måtte revideres som følge av den teknologiske utviklingen. Innvendingene gikk i hovedsak på om det var ønskelig og nødvendig å vedta en forordning eller om et revidert direktiv ville være det beste, og om det er riktig å likebehandle kommersielle og offentlige aktører.

Flere nasjoner stilte spørsmål ved om subsidiaritetsprinsippet ble fulgt når det reviderte regelverket ble fremmet som en forordning. Riksdagens innvendinger er representative: De hevdet at en forordning ville snevre inn den nasjonale handlefriheten og redusere nasjonenes muligheter for å ta hensyn til nasjonale og lokale forhold ved implementeringen. Kommisjonens fullmakter til å utgi forskrifter («delegated acts») var etter riksdagens syn for vide. De reiste også spørsmål ved om det var hensiktsmessig å detaljregulere satsene for overtredelsesgebyr. Generelt var de skeptiske til omfanget og reiste spørsmål ved et så omfattende og detaljert regelverk var hensiktsmessig eller om det kunne virke kontraproduktivt for nasjonalt gjennomslag og god implementering (Riksdagen, 2012).

Regionkomiteen og CEMR reiste innvendinger mot at en forordning skulle omfatte offentlig sektor. De foreslo at et revidert direktiv burde

utgis for det offentliges behandling av persondata, mens en forordning kunne gjelde for næringslivet. De var også kritiske til at forslaget ville gi kommisjonen anledning til å utstede tillegg («delegated acts»). (CoR, 2012, CEMR, 2012).

CEMR viste også til at en begrunnelse for høye overtredelsesgebyr er relevant for næringsdrivende som kan ha økonomisk gevinst av å tøye lovverket. Det offentlige har ikke kommersielle formål med sin behandling, det er derfor urimelig at de samme prinsippene og satsene for overtredelsesgebyr gjelder for offentlige virksomheter. Videre hevdet de at de administrative kostnadene for å overholde nytt regelverk i offentlige virksomheter ikke sto i et rimelig forhold til effekten for innbyggerne. Storbritannia opererte med et anslaget på nesten 300 millioner euro pr år, Finland 200 millioner mens Danmarks anslag var i størrelsesorden 80 millioner euro for kommunene (CEMR, 2015).

Samlet kan innvendingene mot det opprinnelige forslaget fra nasjonalt, regionalt og lokalt nivå grupperes i fire hovedinnvendinger. 1) Kommisjonen får for store fullmakter til å utgi supplerende bestemmelser. 2) En forordning gir for liten handlefrihet til nasjonal tilpassing av reglene, særlig for offentlige virksomheter. 3) Kostnadene ved å gjennomføre bestemmelsene i offentlig virksomhet står ikke i forhold til gevinsten for borgerne. 4) De høye overtredelsesgebyrene bør ikke gjelde offentlige virksomheter. De to første innvendingene er begrunnet i ulik tolking og vektlegging av subsidiaritetsprinsippet, mens de to siste begrunnes i forskjeller mellom offentlig og kommersiell virksomhet.

4.4.2 Norsk behandling

EFTA har ikke en tilsvarende konsultasjonsprosedyre som EU. Regjering og Storting tar derfor først formelt stilling til EØS-relevant lovverk når det er vedtatt i EU. Den norske EU-delegasjonen følger imidlertid med på hva som publiseres av forslag til nye rettsakter og holder nasjonale myndigheter orientert. Gjennomgangen under er avgrenset til om forordningens virkninger for regionalt og lokalt nivå, herunder andre effekter av at det lokale forvaltningsnivået europeiseres, har vært tema.

Utkastet ble sendt på høring i 2012 (Justis- og beredskapsdepartementet, 2012). Høringen ble trolig gjennomført for å gi innspill til den norske representanten i rådets arbeidsgruppe for personvernspørsmål (Working Party on Information Exchange and Data Protection – DAPIX). Høringen ser ikke ut til å ha resultert i offisielle nasjonale dokumenter. Til sammen kom det inn 57 uttalelser, hvorav 14 uten kommentarer. Kommunesektoren ble ikke nevnt blant høringsinstansene ut over at Riksarkivet støttet forslaget om obligatorisk personvernombud for offentlige virksomheter og begrunnet det med helhetsinntrykket fra tilsyn i offentlig sektor. En rekke av høringsinstansene advarte om at forslaget ville gi kommisjonen vide fullmakter til å utgi supplerende rettsakter.

KS var høringsinstans, men ikke fylkeskommuner eller kommuner. Kommunene synes ikke å ha blitt konsultert av KS, som heller ikke ga innspill i høringen. Under en diskusjon om årsakene til dette viste lederen for KS sitt Europakontor til at de hadde gitt sine innspill gjennom CEMR¹⁵.

Datatilsynet er trolig den instans i Norge som har vært tettest involvert i utviklingen av forslaget til forordning. Som observatør i Artikkel 29-gruppen og medlem i arbeidsfora under denne gruppen har de deltatt i å utforme uttalelser til kommisjonens arbeid med ny forordning. De har i årsrapportene for de aktuelle årene (2012-2015) oppgitt å ha bistått Fornyings-, administrasjons- og kirkedepartementet(FAD)/KMD, uten at bistanden er konkretisert. Videre har de deltatt i Justisdepartementets referansegruppe for departementets arbeid i DAPIX samt deltatt i møter med norske representanter i Brussel.

Stortinget ble holdt jevnlig orientert i perioden fram til forordningen ble vedtatt, hovedsakelig gjennom stortingsmeldinger og de halvårslige møtene i stortingets EU/EØS-utvalg. Stortingsmeldingen «Personvern – utsikter og utfordringer» (Meld. St. 11 (2012–2013), 2012) orienterte Stortinget om forslaget til ny personvernforordning i meldingens avsnitt 3.2.3. Orienteringen var på et relativt overordnet nivå om virkningene for Norge, men konsentrerte seg om å begrunne behovet, nevne samordningstiltak for datatilsynene og skissere konkrete endringstiltak for rettighetene til den

¹⁵Egne notater fra KS kurset «EØS/EU på 1-2-3» i Brussel 20-21 september 2017

enkelte borger. Det ble også på side 23 hevdet at «[t]anken med framlegga er å lette dei administrative byrdene for dei behandlingsansvarlege».

Forordningen ble sendt på høring sommeren 2017 (Justis- og beredskapsdepartementet, 2017) og regjeringen la fram forslag til ny personopplysningslov i mars 2018 (Justis- og beredskapsdepartementet, 2018). Innstillingen fra Justiskomiteen til Stortinget har frist samme dag som denne oppgaven leveres, 15. mai 2018.

4.4.3 Spesielt om overtredelsesgebyr

Nivået for overtredelsesgebyr som kan ilegges er vesentlig øket, inntil 4% av global omsetning eller 20 millioner euro. Det er også en ambisjon om at gebyrsatsene for overtredelser skal harmoniseres. I norsk sammenheng og i denne studiens tema er det flere forhold som er interessante. Hvorvidt det skal være anledning til å ilegge overtredelsesgebyr for offentlige virksomheter er overlatt til nasjonale myndigheter. Hvilke overtredelser som skal sanksjoneres med gebyr er gitt i forordningens artikkel 83, men JD foreslår en nasjonal utvidelse ved at brudd på ytterligere to artikler gir grunnlag for å ilegge overtredelsesgebyr. Datatilsynet er medlem¹⁶ av en arbeidsgruppe under Artikkel 29-gruppen som lager harmoniserte retningslinjer for bruk av sanksjoner i EU/EØS (Art 29 WP, 2017) og arbeider med å tilpasse disse til forordningen.

I ny personopplysningslov (Justis- og beredskapsdepartementet, 2018) foreslås at offentlige virksomheter skal kunne ilegges overtredelsesgebyr. Det begrunnes det med at dette er etablert rettspraksis i Norge og at få av høringsinstansene hadde innvendinger. Av høringsinstansene¹⁷ var det ingen som motsatte seg generell bruk av overtredelsesgebyr for offentlige organ. KS reiste et (forsiktig) spørsmål om det var hensiktsmessig, og sammen med Oslo kommune anbefalte de at en skulle være tilbakeholden med å bruke overtredelsesgebyr i starten.

¹⁶Egne notater fra Datatilsynets seminar om ny personvernregler 27. april 2018

¹⁷Høringsinstansenes svar er samlet på <https://www.regjeringen.no> Høringssvarene som det er referert til kan finnes der, men er ikke tatt med i referanselisten

I proposisjonen foreslås det også at hjemlene for hvilke overtredelser som skal kunne sanksjoneres med overtredelsesgebyr utvides i forhold til forordningen (Justis- og beredskapsdepartementet, 2018, s. 135-142). De to artiklene er artikkel 10 om straffedommer og lovovertridelser samt artikkel 24 om internkontroll. Innvendinger som ble reist i høringen var at det er diskutabelt om forordningen hjemler en nasjonal utvidelse for de aktuelle artiklene, at det er uhensiktsmessig å ha særnorske regler for hvilke sanksjoner som brukes og at de aktuelle artiklene er så uklare til at de ikke bør kunne sanksjoneres.

Samlet tegner dette bildet av en norsk implementering hvor vi pålegger norske aktører en strengere praksis enn i EU-nasjonene for øvrig. De som «treffes» av denne praksisen er blant annet kommunesektoren.

4.5 Forordningen i hovedtrekk

Fundamentet i personopplysningsloven endres ikke når forordningen trer i kraft. Virksomhetens øverste leder, rådmannen i kommunene, vil fortsatt være behandlingsansvarlig. Alle kommuner må ha oversikt over hvilke personopplysninger som de behandler og ikke behandle andre opplysninger enn de har hjemmel for. De må fortsatt ha systemer, organisasjon og prosedyrer for å behandle opplysningene korrekt etter lovverket. Dette innebærer at personopplysninger må sikres mot at de kommer på avveie, sikres mot utilsiktede endringer og være tilgjengelige når det er behov for dem. I tillegg fører forordningen med seg noen nye plikter. Under følger et utvalg plikter og tiltak som påvirker kommunene spesielt.

Av organisatoriske tiltak blir det obligatorisk for alle offentlige virksomheter å utnevne personvernombud. Hittil har dette vært en frivillig ordning som kommunene har kunnet benytte seg av for å unngå visse meldinger til tilsynet. Det vil trolig også gjelde interkommunale selskaper som kommunene deltar i. Ved årsskiftet 2016/2017 deltok bare hver sjettede kommune i ordningen, så det må utnevnes og utdannes flere hundre nye ombud i kommunene og deres selskaper.

«De registrerte» – innbyggere, ansatte og andre som er i dialog med kommunen får mer definerte rettigheter til å bestemme over egne personopplysninger. Samtykke, en av de mest brukte behandlingshjemplene skal det være enkelt å trekkes tilbake. Retten til innsyn i hvilke opplysninger kommunen behandler om den enkelte er blitt utvidet og styrket. Informasjon om behandlingen skal være enkelt og tilpasset målgruppen. Endringer i rettighetene innebærer at alle kommuner må gjennomgå ekstern informasjon og interne rutiner og etablere systemer for å kunne oppfylle rettighetene.

«Privacy by design and by default» – personvern skal bygges inn i system fra bunnen og de mest personvernvennlige innstillingene skal være standardinnstillinger – er nye krav til systemløsninger. Når nye løsninger skal anskaffes eller eksisterende erstattes må slike krav spesifiseres av kommunene overfor leverandørene.

Datatilsynet skal varsles innen 72 timer etter at alvorlige sikkerhetsbrudd ble oppdaget. Selv om bruddet skjer hos en av kommunens databehandlere (underleverandører) så er det rådmannen som behandlingsansvarlig som er ansvarlig for at Datatilsynet blir varslet. Oversittes denne fristen vil det kunne føre til overtredelsesgebyr.

Det blir også et krav om at kommunene utarbeider en vurdering av personvernkonsekvenser (DPIA – Data Protection Impact Assessment) hvis behandlingen kan medføre «høy risiko for fysiske personers rettigheter og friheter» (Justis- og beredskapsdepartementet, 2018, s. 305).

4.6 Synspunkter fra fra undersøkelsen

4.6.1 Felles europeisk regelverk

Respondentene i spørreundersøkelsen ble bedt om synspunkter på et felles europeisk regelverk: «Har du noen synspunkter på EUs ambisjon om å etablere et felles europeisk regelverk for behandling av personopplysninger?» Svarene er vedlagt i tabell B.1 på side 107.

De fleste uttrykte forståelse for at det er nødvendig med et nytt regelverk. Den gjennomgående trenden i svarene er at det er positivt og nødvendig å tilpasse reglene til teknologiske endringer og en virkelighet hvor

personopplysninger er i utstrakt bruk som handelsvare. Med felles regler vil Europa også stå sterkere overfor globale selskap.

Innvendinger gikk ut på at regelverket er komplisert, det er krevende å få oversikt over alt som må gjøres og at det vil være utfordrende å gjennomføre det før forordningen trer i kraft. Enkelte trakk fram det «unorske» nivået for overtredelsesgebyr. Det var også noen som hevdet at et felles regelverk blir så komplisert at det hemmer godt personvern i kommunene, framfor å fremme det.

4.6.2 Lokale endringer

På slutten av undersøkelsen fikk respondentene anledning til å uttale seg om hva de trodde at forordningen ville medføre av lokale endringer. Flere enn halvparten hadde synspunkter på spørsmålet «Tror du at EUs personvernforordning vil føre til endringer i organisasjon, prosedyrer og/eller prosesser i din kommune/fylkeskommune?» Svarene finnes i tabell B.2 på side 110.

Selv om to av svarene er et klart nei, er majoriteten like klare på at forordningen vil endre måten kommunen behandler personopplysninger på. Begrunnelsen som går igjen er at den nasjonale oppmerksomheten rundt nye regler virker som en katalysator og har ført til at eksisterende prosedyrer og rutiner gjennomgås på nytt. Dette fører til bedre kompetanse og flere som kjenner regelverket i kommunene. Videre nevnes kravet om å opprette personvernombud som en faktor som vil fremme personvernarbeidet.

I tillegg til de som kun svarte nei på spørsmålet, var det også noen som mente at de over tid har hatt gode rutiner, oppdatert dokumentasjon og et kontinuerlig fokus på temaet. Disse anså arbeidet som en justering for å tilpasse seg nye regler. Også på dette spørsmålet var det en som nevnte bøter (overtredelsesgebyr) som drivende faktor.

4.6.3 Informasjonskanaler

To innledende spørsmål i undersøkelsen handlet om når og hvordan respondenten ble kjent med at det vil komme en ny personvernlov

på bakgrunn av EUs personvernforordning. Det ble også åpnet for respondentenes synspunkter på et felles europeisk regelverk. Formålet med disse spørsmålene var å få indikasjoner på hvor bevisst respondenten var at EU-regelverk legger rammen for nasjonale lover og om de hadde noe forhold til høringen i 2012 (Justis- og beredskapsdepartementet, 2012). Drøyt

Tabell 4.1: Tidspunkt og kanaler for informasjon om nytt regelverk

	Kanaler								Sum
	Media	Konf	KS	Nettv	Brev 17	JD 17	JD 12	Nå	
Før 2015	2	4	1	1	1	1	3	0	13
I 2015 eller 2016	16	27	17	10	20	7	3	0	100
Første halvår 2017	9	18	23	11	20	6	0	0	87
Siste kvartal	1	1	3	0	0	1	0	0	6
I denne undersøkelsen	0	0	0	0	0	0	0	4	4
Sum	28	50	44	22	41	15	6	4	210

Note: Media: Artikler i media – Konf: Foredrag på konferanser – KS: Informasjon fra KS – Brev17: Datatilsynets brev om reformen våren 2017 – JD 17: Høring om forordningen i 2017 – JD 12: Høring om forordningen i 2012 – Nå: I denne undersøkelsen (4). Flere kanaler kunne oppgis

halvparten av respondentene kjente til forordningen før 2017, men bare 13 var klar over arbeidet i EU før 2015. Det lave antallet (3) som kjente til høringen fra JD i 2012 er ikke overraskende fordi det bare var KS som var høringsinstans. Høringen ble så vidt vites heller ikke formidlet videre fra KS til kommunene, og KS ga som tidligere nevnt ikke høringsinnspill.

Konferanser, informasjon fra KS og brevet fra Datatilsynets direktør til alle landets ordførere og rådmenn er de tre viktigste kanalene for informasjon til kommunene og står for nesten to tredjedeler av de avgitte svarene på dette spørsmålet. Til sammenligning er det bare 7 % som oppgir høringen sommeren 2017 som en kanal til informasjon om ny forordning. Dette tross for at det er i denne høringen at de praktiske konsekvensene for sektoren er grundigst beskrevet og hvor sektoren hadde mulighet til å påvirke hvordan handlingsrommet i forordningen kunnen utnyttet.

Bildet av at norske aktører har sittet på gjerdet mens EU utviklet et nytt regelverk og at regionale og lokale forvaltningsnivå ikke er konsultert er entydig. Om disse allikevel er forberedt på personvernforordningen er tema for neste kapittel.

5 Behandling av personopplysninger i kommunesektoren

5.1 Om de kvantitative analysene

Dette kapittelet inneholder studiens kvantitative analyser. Gjennomføring av – og svarandel for undersøkelsen ble gjennomgått i kapittel 3. Konklusjonen var at svarandelen er for lav og skjevhetene for store til at undersøkelsen kan sies å være representativ for kommunesektoren. Resultatene i modellene som presenteres i dette kapittelet vil beskrive sammenhenger som bare er gyldige for de kommunene som deltok i undersøkelsen. Signifikanstesting er begrunnet i modellbasert statistisk teori.

Teoretisk interessante variabler er gjennomgående presentert i modellene, også der hvor testene indikerer at de ikke har signifikant påvirkning på modellens forklaringskraft. Årsaken er dels at de ved et mere representativt utvalg vil kunne få en annen betydning i modellen, og dels fordi de er del av det større bildet av faktorer som kan være med på å forklare forskjeller i regeletterlevelse. Enkelte variabler som kunne tenkes å ha teoretisk interesse er allikevel tatt ut i noen av modellene. Det er i så fall begrunnet i hvert enkelt tilfelle. I oppbygging og tolking av modellene er utgangspunktet Røviks teorier om overføring av organisasjonsideer (eller i dette tilfellet implementering av en av EUs rettsakter), nærmere bestemt kontekstualisering og virusteori (Røvik, 2007).

Først presenteres svarene på innledende spørsmål fra undersøkelsen som ikke inngår i senere modeller. På grunnlag av en teoretisk modell for påvirkningsfaktorer utvikles en modenhetsskala. Denne representerer

avhengig variabel i regresjonsanalyser av hvordan eksterne og interne faktorer ved en kommune påvirker behandlingen av personopplysninger. De data vi har gir også grunnlag for en sammenligning mellom undersøkelsene i 2010 og 2017 med «Internkontrollsystem» som binær avhengig variabel.

I tillegg til tabeller og figurer i dette kapittelet er det noen steder vist til utdypende eller mer detaljerte tabeller og figurer i vedlegg C.

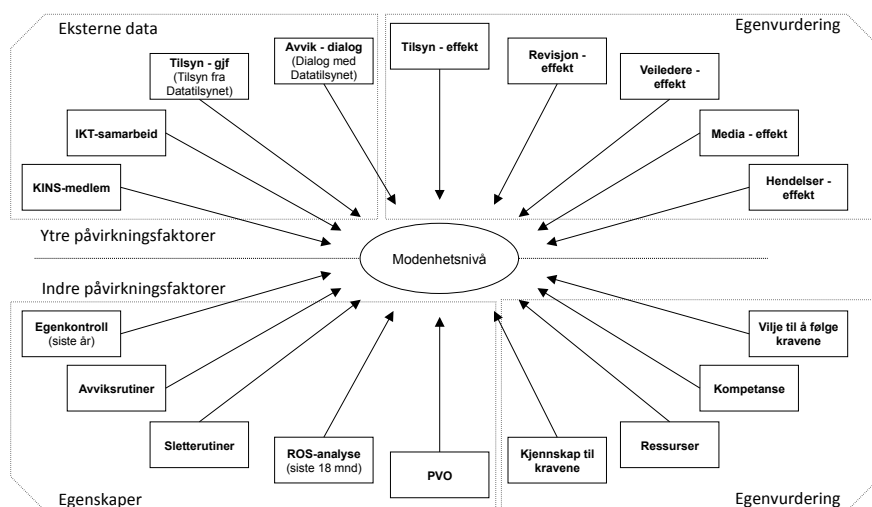
5.2 Respondentene

Innledningsvis ble respondentene bedt om å oppgi hvilken funksjon de har i kommunen. Personvernombud, sikkerhetsansvarlig og kommunalsjefer/tilsvarende er jevnstore grupper og hver av dem representerer om lag 20 %, til sammen 60 % av respondentene. Ledere og medarbeidere i arkiv, IKT-avdelingen og personal/HR utgjør til sammen 30 %, disse gruppene er også jevnstore. De resterende respondentene var rådmenn, jurister og noen enkeltstående funksjoner.

Felles for respondentene er at de har sin funksjon i det som normalt er kommunens sentrale stabsfunksjoner. Synspunkter fra de tjenesteproduserende leddene i kommunen vil derfor ikke være representert direkte i de påfølgende analysene. Hensikten med spørsmålet var å få et overordnet bilde av hvilke funksjoner som behandler generelle personvernspørsmål i kommunene. Respondentenes organisatoriske plassering har for øvrig ingen rolle i de videre analysene.

5.3 Modell for påvirkningsfaktorer

Modellen for påvirkningsfaktorer bygger på begrepsmodellen i figur 2.1 på side 10, vurderingene av undersøkelsen i avsnitt 3.3 på side 27 og eksterne data i avsnitt 3.4 på side 32. Konstruksjonen av en modenhetsskala behandles i sin helhet i avsnitt 5.4. Modellen tar utgangspunkt i at en rekke faktorer i og utenfor kommunene påvirker kommunens modenhet. I figur 5.1 fremstilles faktorene samlet, men det lages separate modeller for regresjonsanalysene av ytre og indre faktorer.

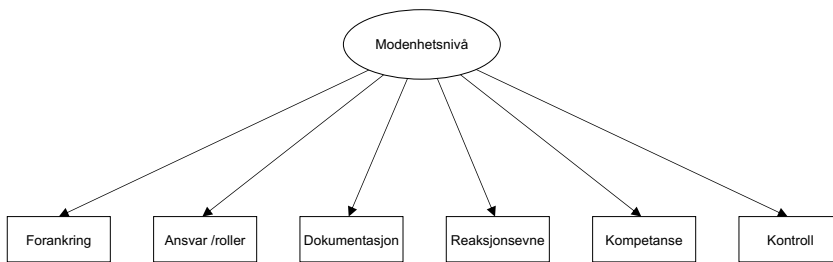


Figur 5.1: Variabelmodell over ytre og indre påvirkningsfaktorer

De ytre påvirkningsfaktorene – faktorer som kan føre med seg «smitte» etter virusteorien – består av *eksterne data* om av IKT-samarbeid, KINS-medlemskap, medieoppdrag om personvern og om kommunen har hatt tilsyn fra eller dialog om avvik med Datatilsynet. Respondentenes *egenvurdering* av hvilke ytre faktorer som bidrar mest til regelleterlevelse regnes også som ytre faktorer.

Indre faktorer er i hovedsak hentet fra undersøkelsen. Spørsmålene om gjennomført egenkontroll, hva som finnes av avvik- og sletterrutiner og gjennomført risikovurdering er gitt fellesbetegnelsen *egenskaper*. Om kommunen har personvernombud er også regnet som en egenskap. *Egenvurderinger* representerer respondentenes oppfatning av de største hindrene for å etterleve regelverket i egen kommune. De gir et mål på indre forsvarmekanismer, immunitet mot idésmitte (å iverksette rettsregler på personvernområdet i denne sammenheng).

Nullhypotesen for alle faktorene i begge modeller er at de ikke påvirker kommunens modenhet. De alternative hypotesene er at de har en unik effekt på kommunens modenhet, kontrollert for øvrige faktorer.



Figur 5.2: Modenhet – personvern i kommunene

5.4 Sammensatt mål på modenhet

5.4.1 Indikatorer

Kommunens modenhet i å behandle personopplysninger er den latente avhengige variabelen. Grunnlaget for valg av indikatorer er NSM sin veileder (Nasjonal sikkerhetsmyndighet, 2015) og rammeverkene ISO 2700x, og COBIT. Det er godt samsvar mellom disse og forhold som er trukket fram i tidligere studier av personvern i kommunene (Tranvik, 2009c, Schartum, Jansen, og Tranvik, 2017) og i Datatilsynets rapporter (Datatilsynet, 2011, Datatilsynet, 2014a).

I undersøkelsen ble indikatorene operasjonalisert ved at respondentene skulle angi i hvor stor grad de var enig i påstander om kommunens behandling av personopplysninger på en Likert skala. Skalaens alternativer var *I svært stor grad (5) – I stor grad (4) – I noen grad (3) – I liten grad (2) – Ikke i det hele tatt (1) og Vet ikke*. For konstruksjon av skalaen ble bare de svar hvor respondentene som hadde tatt stilling til alle spørsmålene benyttet. «Vet ikke» ble betraktet som ikke avgitt svar.

Påstandene som respondentene tok stilling til har det til felles at de ikke er fullstendige i den forstand at de omhandler alle sider ved begrepet. Som eksempel ble ledelsesforankring målt ved at respondentene tok stilling til påstanden «Kommunens/fylkeskommunens ledelse har godkjent alle rutiner». Det er en påstand som er konkret og lukket og som samtidig angir en forventning om at kommunens toppledelse er orientert om hvordan

personopplysninger behandles og har kunnet påvirke praksis. Allikevel er det bare en av mange fasetter i ledelsesforankringen. Rapporteringsrutiner, behandling av avvik og årlig gjennomgang av status er andre sentrale elementer som ikke blir fanget opp. Dette valget ble gjort fordi flere kontrollspørsmål/påstander for å få et mer nyansert bilde ville øke omfanget på undersøkelsen og en ville da risikere et større frafall. De samme vurderingene gjelder også for de øvrige påstandene. Indikatorene i studien er fremstilt i figur 5.2 på forrige side.

Forankring	– Kommunens/fylkeskommunens ledelse har godkjent alle rutiner
Ansvar/roller	– Det er godt kjent hvem som har ansvar for behandlingen av personopplysninger
Dokumentasjon	– Kommunen dokumenterer det som personopplysningsloven krever
Reaksjonsevne	– Kommunen reagerer raskt hvis personopplysninger behandles feil
Ansattes kompetanse	– De ansatte vet godt hvordan personopplysninger skal behandles
Årlig kontroll	– Kontroll av hvordan kommunen behandler personopplysninger gjennomføres hvert år

Deskriptiv statistikk av svarene fremgår av tabell 5.2 på neste side og svarfordelingen er visuelt framstilt i figurene C.2 på side 124 og C.3 på side 125. Svarfordelingen indikerer at respondentene jevnt over har en meget optimistisk vurdering av status i egen kommune. De fleste indikatorene har et gjennomsnitt opp mot 4, altså at kommunene i stor grad forholder seg til regelverket. Unntaket er indikateren for årlige kontroller, som ligger i underkant av 3. Bildet bekreftes av de grafiske fremstillingene. Disse vurderingene avviker fra tidligere studier og undersøkelser (Tranvik, 2009c, Datatilsynet, 2011).

Tabell 5.2: Deskriptiv statistikk av egenvurdert modenhet

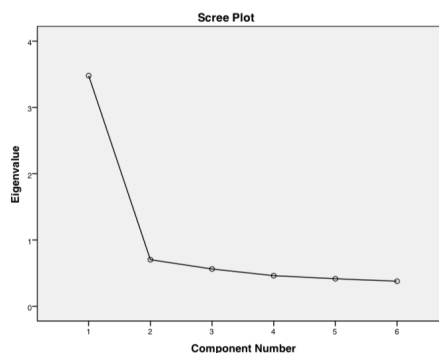
Statistic	N	Mean	St. Dev.	Min	Max
Forankring.	85	3.624	0.963	1	5
Ansvar/roller	85	3.776	0.878	2	5
Dokumentasjon	85	3.565	0.778	2	5
Reaksjonsevne	85	4.024	0.859	2	5
Kompetanse	85	3.494	0.826	2	5
Kontroll	85	2.906	1.109	1	5

5.4.2 Testing av modellen

Dimensjonalitet, om spørsmålene måler ett og samme fenomen, testes ved hjelp av en faktoranalyse (Ringdal, 2013, s. 349 - 354). Faktoranalyser kan være *eksplorerende* eller *bekreftende*. Eksplorerende faktoranalyse innebærer å bruke statistiske metoder for å finne hvor mange faktorer som må til for å representere ett fenomen på grunnlag av en gruppe av variabler. I dette tilfellet er fenomenet modenhet, variablene er indikatorene i tabell 5.2 og metoden er eksplorerende faktoranalyse.

Analysen ble gjennomført i SPSS ved metoden «Principal components» og de vesentlige resultatene fremgår av tabell 5.3 på neste side og figur 5.3. De viktigste kriteriene som vurderes i analysen er faktorens egenverdi, størrelsen på samlet varians som modellen forklarer, faktorladninger og kommunalitet.

Størrelsen på egenverdien (*eigenvalue*) er et mål på hvor mye av den totale variansen som kan forklares av en faktor og må være større enn 1. Den samlede variansen som modellen forklarer bør være over 50 %, mens korrelasjon mellom faktoren og variablene – faktorladningene – bør



Figur 5.3: Skreddiagram for modenhet

Tabell 5.3: Faktoranalyse av indikatorer for modenhet

Variabel	F1	h^2
Forankring	0.72	0.52
Ansvar/roller	0.82	0.67
Dokumentasjon	0.79	0.63
Reaksjonsevne	0.67	0.45
Kompetanse	0.79	0.62
Kontroll	0.77	0.59
Eigenverdi	3.48	
Prosent forklart varians		58.0

Note: F1 – korrelasjon mellom faktoren og variablene
 h^2 – andelen varians i hver variabel

være over 40 %. Kommunaliteten viser hvor stor andel av variansen til den enkelte variabel som forklares av faktoren.

Skredplottet i figur 5.3 viser et klart knekkpunkt etter en faktor. Eigenverdien er 3.5, godt over terskelverdien på 1. Samlet varians er 58 %, også godt over terskelverdien. Faktorladningene er mellom 0.67 og 0.82, over grensen på 0.40. Analysen gir støtte til at spørsmålene er endimensjonale og at en faktor er tilstrekkelig til å representere kommunens modenhet på grunnlag av disse variablene.

Reliabilitetstesting av en skala er å teste hvor nøyaktig skalaen er. En teknisk definisjon på reliabiliteten til et sammensatt mål er «den andelen variansen i de sanne skårene utgjør av den totale variansen til X », hvor X er observert verdi på en indikator og består av den sanne verdien t og en målefeil e (Ringdal, 2013, s. 355). Uttrykt som en formel: $Var(X) = Var(t) + Var(e)$. Reliabilitet = $\frac{Var(t)}{Var(X)}$ og vil ha en verdi mellom 0 og 1 hvor høye tall gir lave målefeil.

Reliabilitetstest av tverrsnittdata gjøres ved å måle den interne konsistensen ved bruk av *Chronbachs alfa* (α). En verdi på over 0.7 regnes

Tabell 5.4: Modenhet – reliabilitetsanalyse.

	Korrelasjon med skala	Felles korrelasjon
Forankring.	0.84	0.52
Ansvar	0.80	0.44
Dokumentasjon	0.80	0.45
Reaksjonsevne	0.84	0.50
Ansattes kompetanse	0.82	0.47
Årlig kontroll	0.81	0.46
Reliabilitet: Chronbachs $\alpha = 0.84$		
Gjennomsnittlig korrelasjon mellom indikatorene = 0.47		
N = 85		

normalt som en nedre grense (Ringdal, 2013, s. 358). Beregningene resulterte i $\alpha = 0.84$, og viser at den indre reliabiliteten i skalaen er god, se tabell 5.4.

Validitet. En forutsetning for at skalaen er valid – at den måler det man ønsker å måle med skalaen – er at den har tilfredsstillende reliabilitet. Den kan imidlertid ha høy reliabilitet uten å være valid. Måleinstrumentet kan være nøyaktig, men det må også brukes slik at det måler alle vesentlige elementer for å gi et korrekt bilde. Validitet kan ikke måles direkte matematisk, men vurderes teoretisk fra ulike perspektiv. Ringdal bruker begrepene umiddelbar validitet (face validity), innholdsvaliditet, kriterievaliditet og nomologisk validitet fra Netemeyer, Bearden, & Sharma (2003) som aktuelle perspektiver. Kriterievaliditet og nomologisk validitet er ikke vurdert fordi det ville kreve at man hadde kriterier som skalaen kunne sammenlignes med eller begrunnede og målbare forventinger til resultatene .

Umiddelbar validitet og innholdsvaliditet innebærer å vurdere om indikatorene samlet synes dekkende for begrepet modenhet ut fra det teoretiske grunnlaget og eget skjønn. Skalaen består av indikatorer som er ansett for å være vesentlige i det teoretiske grunnlaget for skalaen (se avsnitt 2.2.5 på side 18) og i rammeverk for informasjonssikkerhet som COBIT og ISO 27001. Det er også indikatorer som tidligere forskning på

kommunenes regeletterlevelse på området personvern har trukket frem som vesentlige (Tranvik, 2009c).

Kilder til systematiske målefeil er egenskaper ved avgitte svar blant respondentene, «enighetssyndromet» og «sosial ønskelighet» (Ringdal, 2013, s. 358). Enighetssyndromet innebærer at enkelte respondenter har en tendens til å avgi samme svarkategori på alle spørsmål, uavhengig av hva det spørres om. For å motvirke at slike målefeil blir systematiske bør noen av spørsmålene/indikatorne «snus» slik at samme svar, for eksempel «helt enig», på to spørsmål gir motsatt indikasjon på modenheten. Dette er ikke gjort i denne studiens spørsmål, noe som kan bidra til å svekke skalaens validitet. Sosial ønskelighet betyr at respondentene svarer det de tror er de mest akseptable svarene og tegner et for positivt bilde av modenheten, noe som det er vanskelig å korrigere for.

5.4.3 Fullføring av modellen

Frekvensfordelingen for svarene fremgår av figur C.2 på side 124. Fordelingen er beregnet blant de 85 kommunene som hadde avgitt svar på alle spørsmålene. Spredningen rundt gjennomsnittet som vises i figur C.3 på side 125 indikerer en tilnærmet normalfordeling. Som vist i avsnitt 5.4.1 gir svarfordelingen et mere optimistisk bilde av status enn man kunne vente fra tidligere empiriske studier, undersøkelser og tilsyn i sektoren. I en eventuell videreutvikling bør det vurderes å normere skalaen slik at fordelingen i større grad samsvarer med konklusjonene fra empiriske studier. På grunn av skjevhetene i utvalget og at vi ikke har kvalitative analyser av regeletterlevelsen i de kommunene som deltok å forholde oss til er det ikke aktuelt for denne studien.

Korrelasjon mellom indikatorne på en konstruert indeks må være positive og middels sterkt korrelerte, det optimale er om de ligger mellom 0.3 og 0.6 (Ringdal, 2013, s. 359). Korrelasjon mellom de seks indikatorne som skal utgjøre indeksen er gjengitt i tabell 5.5 på neste side. Indikatoren for ledelsesforankring er svakt korrelert med hvor raskt kommunen reagerer på brudd. Videre er indikatoren for kjennskap til hvem som har ansvar for

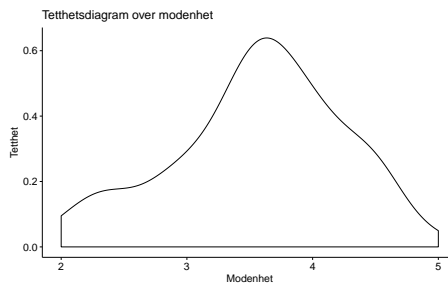
Tabell 5.5: Modenhet – korrelasjon mellom indikatorene. N = 85

	Forankring.	Ansvar	Dok.	Reaksj.	Komp.	Kontroll
Forankring.	1.00					
Ansvar	0.42	1.00				
Dokumentasjon	0.48	0.67	1.00			
Reaksjonsevne	0.27	0.50	0.37	1.00		
Ansattes kompetanse	0.30	0.55	0.51	0.52	1.00	
Årlig kontroll	0.42	0.57	0.60	0.40	0.52	1.00

behandling av personopplysninger noe sterkere korrelert med indikatoren for dokumentasjon. Begge ligger imidlertid svært nær det optimale området. De øvrige indikatorene er optimalt korrelerte.

Reliabilitetsanalysen i tabell 5.4 på side 56 angir korrelasjon mellom den enkelte indikator og skalaen, mellom hver indikator og de øvrige indikatorene (Felles korrelasjon) samt reliabiliteten for skalaen og gjennomsnittlig korrelasjon mellom indikatorene. Korrelasjon med skalaen skal være på over 0.4 og høyest mulig. Med en jevnt høy korrelasjon på over 0.8 tilfredsstillende alle indikatorene dette kravet. Korrelasjonen med øvrige indikatorer er også jevn, men noe lavere. Den gjennomsnittlige korrelasjonen på 0.47 ligger imidlertid godt over kravet på 0.3. Reliabilitet for skalaen målt med Chronbachs α er 0.84, godt over terskelverdien på 0.7.

Analysene viser at indikatorene gir grunnlag for en reliabel skala for sektorens modenhet i behandling av personopplysninger. Gjennomsnittet av indikatorene gir skalaen samme inndeling som spørsmålene i undersøkelsen. Dette gir en skala fra 1 (svært lav) til 5 (svært høy). Figur 5.4 viser fordelingen av kommunenes modenhetsscore grafisk.



Figur 5.4: Modenhetsfordeling

Tabell 5.6: Modenhetsnivå – Frekvensfordeling.

Modenhetsnivå	n	%	Sum %
Svært lav	0	0	0
Lav	2	2.4	2.4
Middels	17	20.0	22.4
Høy	48	56.5	78.8
Svært høy	18	21.2	100.0
Sum	85	100.0	

Note: Mean 3.56; St. Dev. 0.68; Skew -0.39; Kurtosis -0.37

Gjennomsnittet for de 85 som ble brukt for å konstruere indeksen er 3.6 og standardavviket er 0.68. Ingen av kommunene fikk en lavere score enn 2. Skjevheten er -0.39 og kurtosen -0.37. Dette innebærer en fordeling som er svakt venstreskjev, men for øvrig nær en normalfordeling. Fordelingen er imidlertid beregnet ut fra på en skala mellom 2 og 5, siden det ikke er noen av kommunene som har under 2 i score. Totalt sett viser testene av skalaen at den kan brukes som uavhengig variabel i de videre analysene av datasettet. Tabell 5.6 angir fordelingen av modenhet for kommunene.

5.5 Faktorer som påvirker modenhetsnivået

5.5.1 Om modellene og enkelte faktorer

Tester og vurderinger av modellene. Modellene i den resterende delen av dette kapittelet er testet og vurdert for relevante forutsetninger (Thrane, 2017). Testresultatene oppgis bare der det er naturlig eller i de tilfelle testen angir at modellen ligger i nærheten av anbefalte grenseverdier.

Linearitetsforutsetningen er sjekket ved å teste alternative modeller ved mistanke om at den er brutt. Test av multikollinearitet – styrken i korrelasjon/samvariasjon mellom de enkelte faktorene i modellen – er gjort ved å inspisere plott av modellens resultater. Variance Inflation Factor (VIF) er regnet ut i tvilstilfelle og modellen er justert ved en VIF-score på over 2,5.

Modellene er også testet for heteroskedastisitet selv om det ikke er aktuelt å trekke konklusjoner ut over de kommunene som deltok.

Uteliggere er vurdert ut fra grafiske modeller og ekstremverdier er sjekket for å identifisere og korrigere eventuelle feil. Ut over dette er Oslo ikke tatt med i modellene som inneholder folketall. Den ville gi ekstreme utslag hvis den ble betraktet som kommune, som fylke har den ikke kommuner i tradisjonell forstand og Oslo har heller ikke deltatt i undersøkelsen.

Skalaen for modenhet er ordinal, men når modenhet regnes ut for den enkelte kommunen blir verdien et tall på desimalnivå. Dette gir en finmasket verdi på modenhet som går tapt hvis modenhet skulle representeres av en variabel på ordinalnivå i modellene. I arbeidet med studien ble ordinale logistiske modeller sammenlignet med for øvrig like lineære modeller. Ordinal logistisk regresjon syntes å gi høyere signifikansverdier, men endret ikke det innbyrdes forholdet mellom variablene sammenlignet med lineære modeller. De lineære modellene har gjennomgående høyere R^2 enn McFadden pseudo- R^2 for de ordinale modellene. Ut fra en totalvurdering er lineære modeller best egnet i regresjonsanalysene når modenhet er avhengig variabel. For øvrig er annengradsledd, logistisk transformasjon av den avhengige variabelen, samspillsledd og logit-modeller vurdert for å gi modellene best mulig funksjonell form.

Internkontroll. Et av spørsmålene var om kommunen har et system for å behandle personopplysninger. Dette var hovedtema fra kommuneundersøkelsen 2010. Resultatene fra 2010 og 2017 er sammenlignet i avsnitt 5.6 på side 70. For å ta hensyn til usikkerheten om hvordan reglene om internkontroll og informasjonssikkerhet ville videreføres i ny personopplysningslov (Justis- og beredskapsdepartementet, 2017, s. 53, 56) måtte spørsmålsstillingen justeres noe.

Respondentene ble ikke spurt konkret om de har et internkontrollsystem, men om de har et system for hvordan personopplysninger behandles. En innledende tekst til spørsmålet forklarte koblingen til internkontroll i gjeldende personopplysningslov. I de etterfølgende analysene blir internkontroll i visse tilfelle brukt som avhengig variabel som alternativ til modenhetsskalaen, og

konklusjoner er trukket med det forbehold at svarene ikke er direkte sammenlignbare.

Personvernombud. I tillegg til at det er konstruert en oversikt over hvor lenge kommunene har hatt personvernombud ut fra eInnsyn (se avsnitt 3.4.3) fikk respondentene spørsmål om de hadde ombud, organisatorisk plassering og hvor lenge kommunen har hatt ombudet. De som ikke har ombud fikk spørsmål om hvilke planer de hadde og om de hadde tatt stilling til organisatorisk plassering.

Personvernombudet er betraktet som en av flere mulige faktorer som kan påvirke modenhetsnivået. Kravet om at alle offentlige virksomheter skal ha et personvernombud er nytt når forordningen adopteres som norsk lov. Det ville være av interesse om funksjonen har innvirkning på modenhetsnivået i de kommunene som deltok i undersøkelsen. I analysene av modellen for interne faktorer blir personvernombudet behandlet som en kategorisk uavhengig variabel. Mer detaljerte analyser er ikke gjort i denne studien.

5.5.2 Ytre faktorer

Variablene

Med ytre faktorer menes forhold som ikke er egenskaper ved den enkelte kommunen, men egenskaper ved omgivelsene som kan påvirke hvordan kommunene utfører sine oppgaver. Har horisontal og vertikal samordning (Amdam & Veggeland, 2011) effekter som kan indikere at kommunene «smittes», og kan dette spores som en samvariasjon mellom modenhet og ytre faktorer? Faktorene IKT-smarbeid, KINS-medlemskap (Kins-medlem), tilsyn (Tilsyn gjf) fra eller dialoger om avvik (Avvik - dialog) med Datatilsynet er kodet som kategoriske variabler. En kommune har enten hatt tilsyn, eller den har ikke hatt det.

En grundigere analyse av den effekten tilsyn har på modenhet kunne tenkes å skille på brevkontroll, stedlig kontroll og om det er gjennomført etterkontroll. Tiden som har forløpt siden siste tilsyn kan også tenkes å være av betydning. I denne studien har det vært viktigst å finne ut om tilsyn

Tabell 5.7: Deskriptiv statistikk av ytre faktorer

Statistic	N	Mean	St. Dev.	Min	Max
Modenhet	85	3.56	0.68	2.00	5.00
KINS-medlem	85	0.51	0.50	0	1
IKT-samarbeid	85	0.47	0.50	0	1
Tilsyn gjf	85	0.41	0.50	0	1
Avvik - dialog	85	0.07	0.26	0	1
Tilsyn-effekt	83	0.66	0.48	0	1
Revisjon-effekt	83	0.49	0.50	0	1
Veiledere-effekt	83	0.72	0.45	0	1
Media-effekt	83	0.25	0.44	0	1
Hendelser-effekt	83	0.28	0.45	0	1

korrelerer med kommunens modenhet uten å skille på nyansene. Den samme vurderingen ligger til grunn for ikke å ta hensyn til antall avvik eller hvor mange år som er gått siden kommunen hadde dialog om avvik, antall år som KINS-medlem eller som deltaker i et interkommunalt IKT-samarbeid.

Respondentenes svar på spørsmålene om ytre faktorer i undersøkelsen er også kodet som kategoriske, og gir et mål på hvilke kilder til «smitte» som kommunene selv oppfatter som viktigst. Spørsmålet lød: *Hvilke ytre forhold tror du bidrar mest til at kommunen/fylkeskommunen behandler personopplysningene i tråd med lovverket? Flere svar er mulig.* Svaralternativene var (kortformer i parentes): Tilsyn (Tilsyn-effekt), Forvaltningsrevisjoner (Revisjon-effekt), Veiledere fra Datatilsynet (Veiledere-effekt), Medieoppslag nasjonalt (Media-effekt), Uheldige episoder lokalt eller i nabokommunene (Hendelser-effekt).

Tabell 5.7 inneholder deskriptiv statistikk over alle variablene som brukes i analysene.

Halvparten av kommunene er enten KINS-medlemmer, deltar i et interkommunalt IKT-samarbeid eller begge deler. Fire av 10 kommuner har også hatt en eller annen form for tilsyn i løpet av de siste ti årene, mens bare 7 % har hatt dialog omkring avvik siden 2010. Nesten tre fjerdedeler av respondentenes mener at Datatilsynets veiledere virker fremmede på

kommunal regeletterlevelse, mens to av tre angir at tilsyn virker. Hver fjerde deltaker har tiltro til at nasjonale medieoppslag og lokale hendelser påvirker regeletterlevelse positivt.

Modell – ytre faktorer

De hypotesene som er testet er: H_{0yn} – Ytre faktor n har ingen signifikant effekt på hvordan kommunene vurderer egen modenhet. Den alternative hypotesen H_{yn} er at faktor n har signifikant betydning for egenvurdert modenhet i kommunen. Det er ett hypotesepar for hver av faktorene som testes i modellene 1, 2 og 3 i tabell 5.8 på neste side.

Signifikansnivåene er angitt ut fra et 90 % konfidensintervall i tabellen for å få fram de faktorene som synes å peke seg spesielt ut. Modell 2 kontrollerer for respondentenes oppfatning av hvilke ytre faktorer som bidrar til at personopplysninger behandles korrekt mens modell 3 kontrollerer for ytre faktorer som er hentet fra eksterne kilder. Modell 1 kontrollerer for alle faktorer.

Regresjonskoeffisienten til konstantleddet viser til nivået på modenhets-skalaen som variablene skal tolkes i forhold til. Endringene i regresjonskoeffisientene til de uavhengige variablene mellom henholdsvis modell 2 og 1 og modell 3 og 1 er konsistente, det som endres er den relative betydningen av de enkelte variablene.

To variabler peker seg spesielt ut ved størrelsene på regresjonskoeffisientene og signifikansnivåene i modellene. Oppfatningen av at lokale hendelser påvirker regeletterlevelse er signifikant med et 99 % konfidensintervall. Vi kan være 99 % sikre på at nullhypotesen kan forkastes. For nasjonale medieoppslag må vi akseptere ± 10 % usikkerhet for å forkaste nullhypotesen.

Den fjerdedelen av respondentene som mener at lokale hendelser bidrar til en korrekt behandling av personopplysninger vurderer egen kommunes modenhet til å være et halvt poeng lavere enn de andre, kontrollert for øvrige variabler. Effekten av nasjonale medieoppslag kontrollert for andre faktorer har en positiv effekt på et tredjedels poeng i vurderingen av egen modenhet.

Tabell 5.8: Ytre påvirkningsfaktorer. Lineær regresjon

	<i>Dependent variable:</i>		
	Modenhhet		
	(1)	(2)	(3)
Kins-medlem	0.144 (0.156)		0.249 (0.159)
IKT-samarbeid	-0.205 (0.148)		-0.143 (0.156)
Tilsyn gjf	-0.108 (0.150)		-0.251 (0.154)
Avvik - dialog	-0.026 (0.275)		-0.139 (0.289)
Tilsyn-effekt	-0.172 (0.154)	-0.145 (0.149)	
Forvaltningsrevisjoner-effekt	0.076 (0.141)	0.053 (0.139)	
Datatilsynets veiledere-effekt	0.139 (0.158)	0.166 (0.155)	
Nasjonale medieoppslag-effekt	0.305* (0.166)	0.302* (0.165)	
Lokale hendelser-effekt	-0.554*** (0.170)	-0.587*** (0.161)	
Constant	3.701*** (0.233)	3.613*** (0.185)	3.619*** (0.154)
Observations	83	83	85
R ²	0.237	0.195	0.069
Adjusted R ²	0.143	0.143	0.022

Note:

*p<0.1; **p<0.05; ***p<0.01

Totalt sett kan modellen forklare nær 24 % (14 % justert for antallet faktorer) av forskjellene i egenvurdert modenhet blant deltakende kommuner, under ellers like forhold. Deltakernes vurdering av de eksterne faktorene dominerer, mens øvrige eksterne faktorer gir et begrenset bidrag til modellens forklaringskraft.

De fleste av resultatene er ikke signifikante. De gir følgelig ingen svar som er statistisk holdbare og H_y for disse må forkastes og nullhypotesene beholdes. De kan allikevel gi grunn til noen refleksjoner og oppfølgingsspørsmål (som ikke følges opp i denne studien) for gruppen av kommuner som deltok i undersøkelsen. Det er verd å legge merke til at Datatilsynets veiledere under ellers like forhold oppfattes å ha en svakt positiv effekt på kommunenes egenvurdering. Oppfatningen av om tilsyn bidrar er svakt negativ, både for respondentenes oppfatning av effekten og blant de 40 % som har hatt kontroller fra Datatilsynet. Også her vil forklaringen, hvis den tolkes for de kommunene som har deltatt, kunne ligge i en realitetsorientering av egen status.

Den negative påvirkningen av IKT-samarbeid reiser spørsmål om den halvparten av kommunene som ikke deltar i et slikt samarbeid i større grad tar ansvar for egen kommunes behandling av personopplysninger.

5.5.3 Indre faktorer

Variablene

Kjennetegn ved kommunen som kan tenkes å påvirke regeletterlevelse og modenhet er behandlet som indre faktorer. I teorijennomgangen ble flere av virusteoriens elementer knyttet til interne forhold i kommunene som kan utløse forsvarsmekanismer (immunitet), påvirke implementeringstid (inkubasjonstid, fra smitte til sykdom) eller forklare forskjeller i prioritering (inaktivering/reaktivering). De viktigste kildene til slike barrierer mot endring er respondentenes svar på spørsmål i undersøkelsen. Den variabelen som ikke kommer fra undersøkelsen er oversikten over hvem som har personvernombud (PVO).

Respondentenes egne vurderinger av interne barrierer var stilt som et spørsmål hvor de kunne merke av for flere alternativer. Spørsmålet lød: *Hva mener du er de største hindrene i din kommune for å behandle personopplysninger etter kravene i personopplysningsloven? Flere svar er mulig.* Svaralternativene var (kortformer i parentes): Vi kjenner ikke kravene (Kjennskap til kravene), Det er for arbeidskrevende (Ressurser), Vi kan ikke nok om internkontroll (Kompetanse), Det koster for mye (Kostnader), Medarbeideres vilje til følge regler og rutiner (Vilje til å følge kravene).

Om kommunen har etablert et internkontrollsystem eller ikke er vesentlig. Dette representeres ved utvalgte svar fra undersøkelsens spørsmål om egenskaper ved internkontrollsystemet. 61 av kommunene oppga å ha et internkontrollsystem, og det var bare disse som fikk spørsmål om de egenskapene som inngår i modellen.

Jevnlig gjennomgang av internkontrollsystemet er operasjonalisert ved å spørre om hvor lenge det var siden kommunen hadde gjennomført egenkontroll (Egenkontroll siste år). To av spørsmålene om egenskaper ved internkontrollsystemet er av særlig betydning for innbyggerne samtidig som de kan være utfordrende å få implementert. Dette gjelder rutiner for avvikshåndtering (Avvikrutiner) og rutiner for å slette personopplysninger som kommunen ikke lenger har hjemmel for å behandle (Sletterutiner).

En risikobasert behandling av personopplysninger er ett av fundamentene både i gammel og ny lov og inngår i alle rammeverk for informasjonssikkerhet. Dette representeres ved om kommunen har gjennomført risiko- og sårbarhetsanalyse (ROS-analyse) de siste 18 månedene.

Betydningen av kommunestørrelse ble vurdert og testet som som kontinuerlig variabel og på ordinalnivå i seks grupper. Den ble forkastet fordi alle varianter hadde en svært lav og ikke signifikant regresjonskoeffisient. Det ga heller ikke utslag av betydning på modellene om den ble utelatt.

Variablene er kodet om til kategoriske hvor 1 representerer «ja/egenskap tilstede» og 0 representerer «nei/egenskap ikke til stede». Der det var aktuelt ble «vet ikke» regnet som «nei» fordi system eller rutiner som ikke er kjent i organisasjonen ikke kan regnes med som en virksom indre faktor. Det er

Tabell 5.9: Deskriptiv statistikk – indre faktorer

Statistic	N	Mean	St. Dev.	Min	Max
Modenhet	61	3.75	0.55	2.50	5.00
Kjennskap til kravene	61	0.25	0.43	0	1
Ressurser	61	0.38	0.49	0	1
Kompetanse	61	0.28	0.45	0	1
Vilje til å følge kravene	61	0.38	0.49	0	1
Egenkontroll	61	0.51	0.50	0	1
Avviksrutiner	61	0.84	0.37	0	1
Sletterutiner	61	0.48	0.50	0	1
ROS-analyse	61	0.62	0.49	0	1
PVO	61	0.34	0.48	0	1

Note: Modenhet: 1: Svært lav 2: Lav 3: Middels 4: Høy 5: Svært høy

Øvrige variabler: 1: Ja/egenskap til stede – 0: Nei/egenskap ikke til stede

skilt mellom de som har gjennomført egenkontroll siste år (1) og de som ikke har det (0). Deskriptiv statistikk er gjengitt i tabell 5.9.

Andelen personvernombud var høyere for de som oppga å ha internkontrollsystem (34 % mot 27 % for alle som deltok i undersøkelsen og 16 % på landsbasis pr januar 2017). Halvparten hadde gjennomført egenkontroll i løpet av det siste året og nesten to tredjedeler hadde gjennomført risikovurdering i løpet av de siste 18 månedene før undersøkelsen.

Modell – indre faktorer

Hypotesene er formulert som for ytre faktorer: H_{0in} – Indre faktor n har ingen signifikant effekt på hvordan kommunene vurderer egen modenhet. Den alternative hypotesen H_{in} er at faktor i har signifikant betydning for egenvurdert modenhet i kommunen. Det er ett hypoteseepar for hver av faktorene som testes i modellene 1, 2 og 3 i tabell 5.10. Signifikansnivået er også i disse modellene 10 %, med samme begrunnelse som for analysen av de ytre faktorene. Modell 1 i tabell 5.10 kontrollerer for effekten av både de indre påvirkningsfaktorene som respondentene oppgir som interne barrierer, og egenskaper ved internkontrollsystemet. Modell 2 og

3 kontrollerer for effektene av henholdsvis respondentenes oppfatning av barrierer og egenskaper ved internkontrollsystemet samt effekten av å ha et personvernombud.

Regresjonskoeffisientene tolkes i forhold til konstantleddets verdi. I den samlede modellen er årlig gjennomføring av egenkontroll signifikant innenfor et 99 % konfidensintervall kontrollert for øvrige variabler. Nullhypotesen om at egenkontroll ikke har betydning for egenvurdert modenhet kan forkastes. Hypotesene om at ressurstilgang og medarbeidernes vilje til regelletterlevelse har betydning for modenheten under ellers like forhold kan beholdes hvis en aksepterer ± 10 % usikkerhet.

Regresjonskoeffisienten for årlig egenkontroll indikerer at de kommunene som hadde gjennomført slik kontroll det siste året gjennomsnittlig vurderte modenheten til å være to tredjedels poeng høyere enn de øvrige ($3.61 + 0.67 = 4.28$), kontrollert for andre faktorer. Samspillet mellom egenkontroll og ROS-analyse innebærer at for de kommunen som både hadde gjennomført egenkontroll og ROS-analyse har egenkontrollen betydelig lavere betydning ($3.61 + 0.67 - 0.03 - 0.52 = 3.73$). Disse utregningene illustrerer et poeng, men usikkerheten er høy ved at produktleddet har ± 10 % usikkerhet og gjennomført ROS-analyse ikke er signifikant på et 90 % nivå.

I de kommunene hvor det settes spørsmål ved viljen til å følge loven er gjennomsnittlig egenvurdert modenhet et kvart poeng høyere ($3.61 + 0.27 = 3.88$) under ellers like forhold, med et 90 % konfidensintervall. Ressurstilgang som hemmende faktor og samspillet mellom ressurser og kompetanse i organisasjonen har et samspilledd som er signifikant på et 90 % nivå. Det innebærer at de som har vurdert ressurser til å være en begrensende faktor har et snaut tredjedels poeng lavere gjennomsnittlig score enn gjennomsnittet ($3.61 - 0.31 = 3.30$) kontrollert for øvrige faktorer. For de som mener at både ressurser og kompetanse er begrensende faktorer nøytraliserer samspilleddet den negative effekten av regresjonskoeffisientene ($3.61 - 0.31 - 0.28 + 0.64 = 3.66$) og samlet effekt blir nøytral.

Modellen forklarer 31 % (16 % justert for antallet faktorer) av forskjellene i egenvurdert modenhet i blant deltagende kommuner, under ellers like forhold og basert på indre faktorer. Den marginale betydningen

Tabell 5.10: Indre faktorer - lineær regresjon

	<i>Dependent variable:</i>		
	Modenhet		
	(1)	(2)	(3)
Kjennskap til kravene	-0.131 (0.175)	-0.098 (0.181)	
Ressurser	-0.312* (0.161)	-0.313* (0.165)	
Kompetanse	-0.281 (0.206)	-0.291 (0.199)	
Vilje til å følge kravene	0.278* (0.145)	0.236 (0.144)	
Egenkontroll	0.670*** (0.248)		0.695*** (0.253)
Avviksrutiner	0.196 (0.209)		0.186 (0.208)
Sletterutiner	-0.066 (0.155)		0.117 (0.143)
ROS-analyse	-0.027 (0.210)		0.015 (0.209)
PVO	-0.078 (0.149)		-0.140 (0.147)
Ress*Komp	0.646* (0.364)	0.617* (0.362)	
ROS*Egenktrl	-0.521* (0.300)		-0.530* (0.308)
Constant	3.608*** (0.217)	3.845*** (0.128)	3.434*** (0.184)
Observations	61	61	61
R ²	0.310	0.133	0.181
Adjusted R ²	0.155	0.054	0.090

Note: Standardfeil i parenteser.

*p<0.1; **p<0.05; ***p<0.01

Tabell 5.11: Deskriptiv statistikk – internkontroll 2010

Statistic	N	Mean	St. Dev.	Min	Max
<2 000	86	0.34	0.024	0	1
2 000 - 4 999	129	0.48	0.025	0	1
5 000 - 9 999	80	0.56	0.025	0	1
10 000 - 19 999	54	0.61	0.024	0	1
20 000 - 49 999	37	0.73	0.022	0	1
>50 000	13	0.85	0.018	0	1
Totalt	399	0.52	0.025	0	1

personvernombudet kan synes å ha kunne vært verd grundigere analyser. Datamaterialet er imidlertid for lite til at det er heniksmessig i denne studien. En foreløpig analyse er vedlagt, men resultatene av denne utdypes ikke nærmere.

5.6 Sammenligning mellom 2010 og 2017

5.6.1 Internkontroll i 2010

Deskriptiv statistikk. Resultatene fra kommuneundersøkelsen i 2010 er sammenstilt med antall innbyggere i kommunene og fordelt på seks kommunestørrelser. Datasettet fra 2010 inneholder data om 420 kommuner. Når fylkeskommunene samt enkelte kommuner med manglende informasjon om internkontroll er tatt ut består datasettet av 399 kommuner. Deskriptiv statistikk er oppstilt i tabell 5.11.

52 % av de 399 kommunene oppga å ha internkontroll i 2010. Fordelt på kommunestørrelser hadde 34 % av de minste kommunene internkontrollsystem stigende til 85 % for de største kommunene. Dette er et resultat som avviker fra Datatilsynets årsrapporter om inntrykk fra sine tilsyn (se for eksempel Datatilsynet, 2016, s. 28, 2015, s. 36).

Modellene. Avviket gir grunnlag for å vurdere om det var en statistisk signifikant sammenheng mellom kommunestørrelse og internkontrollsystem

Tabell 5.12: Andel med internkontroll etter innbyggertall 2010. Prosent.

Internkontroll	Kommunestørrelse						Sum
	<2 000	2 000 - 4 999	5 000 - 9 999	10 000 - 19 999	20 000 - 49 999	>50 000	
2010							
Ja	34	48	56	61	73	85	52
Nei	66	52	44	39	27	15	48
Sum	100	100	100	100	100	100	100
n	86	129	80	54	37	13	399

Pearsons χ^2 26.74221 d.f. = 5 p = 6.402852e-05

i 2010. Krysstabellen er satt opp i tabell 5.12. Denne viser en klar tendens til at det var mindre sannsynlig at de mindre kommunene hadde internkontrollsystem enn de større kommunene i 2010. En krysstabellanalyse gjøres innledningsvis, med følgende hypoteser:

H_0 : Det var ingen sammenheng mellom kommunestørrelsen og internkontroll blant norske kommuner i 2010.

H_{kstr} : Det var en sammenheng mellom kommunestørrelsen og internkontroll blant norske kommuner i 2010.

Med fem frihetsgrader og et signifikansnivå på 5% skal nullhypotesen forkastes hvis $\chi^2 > 11.07$ (Ringdal, 2013, s. 523). Med en verdi på 26.7 forkastes H_0 og testen viser at det var statistisk sammenheng mellom kommunestørrelse og internkontroll i 2010.

Regresjonsanalyser med internkontroll som avhengig variabel er deretter gjennomført for å finne om det er noen av kommunegruppene som skiller seg ut ved sterkere eller svakere statistisk sammenheng. Både lineær og logistisk regresjonsanalyse er valgt for å vise at en bedre funksjonell form gir samme resultat både mellom faktorene og modellenes R^2 /pseudo- R^2 . Modellene er satt opp i tabell 5.13 på side 73.

Nullhypotesen H_0 er at det ikke var sammenheng mellom folketallet i kommunen og om kommunen hadde internkontrollsystem. Den alternative hypotesen H_{ftall} er at det var en sammenheng mellom antall innbyggere

i kommunen og om den hadde et internkontrollsystem, under ellers like forhold.

Alle koeffisientene er positive og signifikante med et 95 % konfidensintervall eller bedre. Det var over 50 % større sannsynlighet for at kommuner med flere enn 50 000 innbyggere hadde et internkontrollsystem. Sannsynligheten sank relativt jevnt med synkende folketall. Lavest relativ sannsynlighet hadde den nest minste kommunegruppen, men også blant disse kommunene var det 15 % større sannsynlighet for at de har etablert internkontroll enn blant de minste kommunene. Regresjonsanalysen bekrefter resultatene fra kryss-tabellanalysen, H_0 kan forkastes og vi kan slå fast at i 2010, under ellers like forhold, økte sannsynlighet for at kommunene hadde internkontrollsystem med økende folketall.

Dette resultatet avviker som nevnt fra hva Datatilsynet har formidlet i sine årsrapporter de siste årene. Rapporten fra kommuneundersøkelsen i 2010 drøftet ikke kommunestørrelse. Uten å ha tilgang til de detaljerte tallene fra den undersøkelsen er det ikke mulig å vite om forklaringen kan ligge der. Det er fullt mulig at kontrollspørsmålene i undersøkelsen avdekket at det ikke var en reell forskjell mellom store og små kommuner. En annen og like sannsynlig forklaring på avviket er at Datatilsynets konklusjon er trukket ut fra gjennomførte tilsyn og annen dialog med kommunesektoren som har gitt dem et bredere grunnlag for sine konklusjoner. Det er også et bredere sett av kriterier som er trukket fram som svake områder i årsrapporten.

Allikevel er det interessant at en så klar statistisk sammenheng mellom kommunestørrelse og internkontrollsystem ikke er formidlet i rapporten fra kommuneundersøkelsen i 2010.

5.6.2 Internkontroll – utvikling fra 2010 - 2017

Grunnlaget for sammenligning

Sammenligningene i dette avsnittet er gjort mellom de 102 kommunene og fylkeskommunene som deltok i undersøkelsen høsten 2017. Forskjellene er oppstilt i tabell C.1 på side 119 og et søylediagram viser forskjellene grafisk (figur C.1 på side 120). Større kommuner er overrepresentert og mindre

Tabell 5.13: Internkontroll og kommunestørrelse i 2010

	<i>Dependent variable:</i>	
	ik2010	
	<i>OLS</i>	<i>logistic</i>
	Internkontroll	
	(1)	(2)
2 000 - 4 999	0.143* (0.068)	0.598* (0.288)
5 000 - 9 999	0.225** (0.076)	0.927** (0.321)
10 000 - 19 999	0.274** (0.084)	1.128** (0.360)
20 000 - 49 999	0.393*** (0.096)	1.669*** (0.435)
> 50 000	0.509*** (0.145)	2.381** (0.802)
Constant	1.337*** (0.052)	-0.676** (0.228)
Observations	399	399
R ²	0.067	
Adjusted R ²	0.055	
McFadden R ²		0.050
Log Likelihood		-262.370
Residual Std. Error	0.486 (df = 393)	
F Statistic	5.646*** (df = 5; 393)	

Note: Standardfeil i parenteser.

*p<0.05; **p<0.01; ***p<0.001

Tabell 5.14: Kommuner med internkontroll i 2010 og 2017. N = 92

	Svar 2010	Svar 2017	n	%	Sum %
1	Ja	Ja	43	46.74	46.74
2	Ja	Nei	17	18.48	65.22
3	Nei	Ja	21	22.83	88.04
4	Nei	Nei	11	11.96	100.00

Cramers V: 0.087 p = 0.552

kommuner underrepresentert. De sammenligningene som gjøres er begrenset av hvilke data som er tilgjengelige fra Datatilsynets kommuneundersøkelse og hva som kan utledes av andre kilder.

Økningen i antallet kommuner som har internkontroll fra 2010 til 2017 er marginal, fra 67 til 70 % av kommunene. 92 av de 102 kommunene hadde besvart spørsmålet om internkontroll i begge undersøkelsene. En krysstabellanalyse som sammenligner svarene i 2010 med svarene i 2017 mellom disse 92 kommunene er satt opp i tabell 5.14. Antakelsen var at det ville være sammenheng, at de som hadde internkontroll i 2010 også ville ha det i 2017 og at den sammenhengen ville være statistisk signifikant.

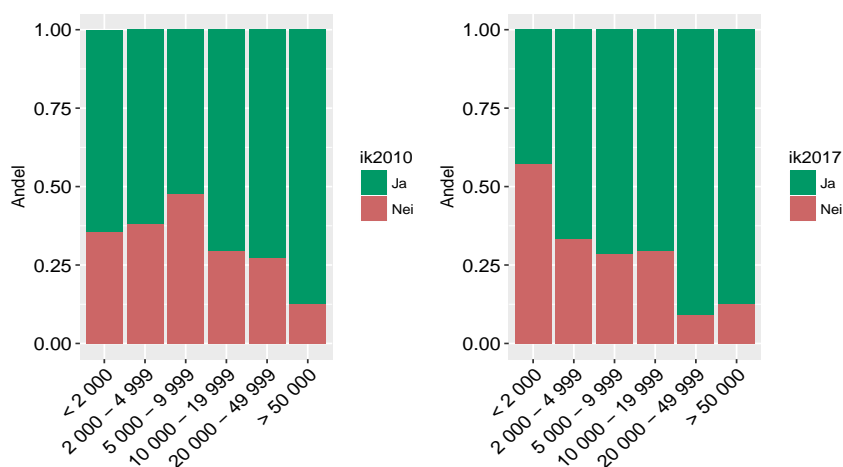
Dette testes ut fra følgende hypoteser:

H_0 : Det er ingen sammenheng mellom hvilke kommuner som har internkontrollsystem i 2017 og de som hadde det i 2010.

H_{ik1017} : Det vil være en signifikant sammenheng mellom de som hadde et internkontrollsystem i 2010 og de som har det i 2017.

Korrelasjon mellom variablene er testet med Cramers V siden begge variablene er målt på nominalnivå. Testen viser at det er en svak og ikke signifikant sammenheng mellom de som hadde internkontroll i 2010 og de som hadde det i 2017. Det betyr at H_0 beholdes og den alternativ hypotesen forkastes. Figur 5.5 viser forskjellene i status mellom kommunegruppene grafisk.

Det er særlig overraskende at 17 av de 92 kommunene, 18 %, av de som oppga å ha et internkontrollsystem i 2010, ikke hadde det høsten 2017. En mulig tolkning av den manglende sammenhengen er at styringssystemene



Figur 5.5: Internkontroll i kommunene 2010 og 2017. N = 92

i mange kommuner ikke har vært «levedyktige». De er blitt utarbeidet, og deretter lagt bort uten at de er blitt implementert i kommunen. Virusteoriens analogier til immunitet og forklaringen om indre forsvarsverker som har virket, underbygger en slik tolking. En annen forståelse som kan legges til grunn er at systemet er i dvale og at det på et tidspunkt vil reaktivieres. Hvorvidt deler av det styringssystemet som en gang var har manifestert seg i endret organisatorisk praksis kan en ikke si noe om.

Tranvik har i sin forskning lansert begrepet «etterlevelsillusion» (Tranvik 2009c, 2012) om kommunal regeletterlevelse på personvernområdet. Viljen er tilstede og utad gis det inntrykk av at reglene følges i god norsk forvaltningstradisjon. Ulike indre barrierer hindrer imidlertid at endringer som lovverket krever blir gjennomført i praksis. Det at en så stor andel som hadde internkontrollsystemer i 2010 ikke har vedlikeholdt disse gir indirekte støtte til Tranviks funn og er også konsistent med virusteoriens forklaring om ytre forsvar og kontrasten mellom beslutninger og å følge opp implementering.

Et annet forhold som undersøkelsen viser er at sammenhengen mellom kommunestørrelse og internkontroll for de kommunene som deltok i undersøkelsen, er endret. Blant disse 92 var det relativt marginale forskjeller

mellom kommunegruppene i hvor stor andel som hadde internkontroll i 2010, til forskjell fra tallene for alle kommunene slik tabellene 5.12 og 5.13 viser). Ved undersøkelsen i 2017 hadde andelen av de minste kommunene med internkontroll sunket, mens den for alle kommuner med over 2000 innbyggere enten var uforandret eller hadde økt slik figur 5.5 viser.

6 Er personvern smittsomt?

6.1 Europeisering

EU-nasjoner og de organisasjonene som representerer regionalt og lokalt nivå har formidlet klare budskap og prioriteter inn i debatten om hvordan et endelig regelverk for personvern skulle se ut. I grovt kan en si at kommisjonen har lyktes med å få vedtatt et felles regelverk ved at personverndirektivet erstattes av en forordning som gjelder for både offentlige og private virksomheter i hele EU. Regionenes organisasjoner fikk ikke gehør for sine innvendinger mot en forordning eller det omfattende regelverket (innvending nr 2 og 3 i avsnitt 4.4.1 på side 41).

Regionale innvendinger er blitt hørt ved at det er opp til den enkelte nasjon om det skal benyttes overtredelsesgebyr overfor offentlige virksomheter. Sammen med nasjonene har de fått gjennomslag for at kommisjonens fullmakt til å utgi «forskrifter» er betydelig innskrenket i forhold til det opprinnelige forslaget.

Norske myndigheter har i perioden 2012 til 2016 fulgt prosessen mellom rådet, parlamentet og kommisjonen om hvordan et endelig regelverk skulle bli. Datatilsynets årsrapporter fra 2012 og 2013 gir konkret informasjon om arbeidet med forordningen og aktuelle problemstillinger og tema som har vært behandlet. De har også redegjort for samarbeid med FAD/KMD og deltakelsen i JDs referansegruppe for DAPIX. For øvrig er det få åpne spor av *hvordan* arbeidet har foregått. Hvilke mandat og ambisjoner JD har hatt med arbeidet i DAPIX foreligger muligens i interne notater, men er ikke

allment tilgjengelig¹⁸. Det er få spor av norske forsøk på å påvirke innholdet i forordningen.

KS fremstår som passiv i perioden fram til forordningen ble vedtatt i 2016. De benyttet ikke anledningen til å koordinere med kommunene eller gi innspill til høringen i 2012. KS digitaliseringsstrategi for kommuner og fylker i 2013-2016 nevner ikke de forestående endringene i personvernregelverket, selv om et kapittel er viet personvern (KS, 2013). Et søk på domenet ks.no avgrenset til perioden 2012 - 2016 gir ett treff av substans. En artikkel i informasjonsfolderen «På gang i EØS» orienterte om at EU-parlamentet hadde godkjent utkastet til forordning (KS, 2014). Totalt sett har KS hatt en avventende og reaktiv holdning til nytt personvernregelverk i den perioden det kunne påvirkes.

eInnsyn gir ingen informasjon om at kommunene er orientert om forordningen fra noen av de aktuelle departementene (FAD/KMD eller JD) eller andre statlige aktører. Det første sporet av formell informasjon er Datatilsynets brev til alle landets rådmenn våren 2017 (Datatilsynet, 2017).

Generelt vil det være slik at momenter som lanseres eller problemstillinger som reises tidlig i en prosessen har størst sjanse for å bli realitetsbehandlet. Mens forslag fortsatt er utkast er det gode muligheter for å få innpasset enkeltmomenter. Solid argumentasjon og god fagkunnskap kan også bidra til å justere innretningen på hele forslaget. Av norske aktører er det bare Datatilsynet som har vært i nærheten av en slik posisjon gjennom sitt arbeid i Artikkel 29-gruppen. Den rollen de har som fagmyndighet og den faglige uavhengigheten de har gjennom lovverket tilsier at tilsynets påvirkning trolig har vært av rent faglig art.

Også i en tidlig fase etter at forslag er lansert er det muligheter for å påvirke innholdet. For Norge er for eksempel muligheten å gjøre felles sak med Sverige og Danmark, noe som er naturlig fordi vi samarbeider på andre områder og fordi vi har mange felles forvaltningstradisjoner. Slik innsats fra norsk side er ikke sporbar ut fra åpne kilder, ut over et norsk posisjonsnotat til rådet i 2012 som er innhentet etter en innsynsforespørsel. KS hevder å

¹⁸Stikkprøver er gjort som innsynsforespørsler til relevante dokumenter i JDs postliste, men vesentlig informasjon er unntatt offentlighet

ha gitt sine innspill gjennom CEMR, men noen formell dialog med norske myndigheter eller kommunesektoren er ikke å finne.

Samlet er bildet at norske aktører har sittet på gjerdet mens EU utviklet et nytt regelverk for personvern i EU/EØS-området. De sentrale norske myndighetene synes å ha forholdt seg til EUs institusjoner, men i liten eller ingen grad til fylkeskommunene eller kommunene. Dette til tross for at kommunene vil være det offentliges utførende ledd på lokalt nivå for nytt personvernregelverk.

Datatilsynet har ivaretatt sin faglige rolle i de EU-fora de har hatt adgang til. De synes heller ikke å ha vært i dialog med kommunesektoren, eksempelvis for å få innspill til en utforming av regelverket som er hensiktsmessig fra perspektivet til det utførende leddet. Orienteringer om at det kommer nytt regelverk er riktig nok gitt til de kommunene som deltok på tilsynets årlige fag-konferanser for personvernombud de siste årene¹⁹, men det dreier seg om et fåtall av kommunene.

Kontakten med kommunene om nytt regelverk ble først prioritert i 2017, da sentrale myndigheter innså at implementeringen av nytt regelverk i det offentlige vil kreve betydelig innsats, spesielt fra kommunene.

6.2 Hva gjør forordningen med kommunen

Analysen av svarene tegner et brokete bilde av hva som faktisk er status i de 102 kommunene som deltok i undersøkelsen. Både ytre og indre faktorer har en viss betydning for hvor modne kommunene kan sies å være i å behandle personopplysninger.

Hendelser i nærområdet fremstår som den viktigste ytre faktoren og fører til at egen modenhet vurderes til å være lavere. Lokale hendelser er for eksempel at det skjer alvorlige brudd på personopplysningsloven enten i egen organisasjon eller hos nære samarbeidspartnere. Intuitivt skulle man tro at det motsatte ville være tilfelle, at lokale hendelser ville bidra til å øke modenhetsnivået ved å sette temaet på dagsorden. Forklaringen kan ligge i at det skjer en realitetsorientering i virksomheten ved at ledelsen og

¹⁹Egne notater fra konferansene i 2015 - 2018

medarbeidere blir oppmerksom på svakheter i egen organisasjon og systemer og erkjenner at det samme kunne skjedd i egen kommune.

To mekanismer i virusteorien kan forklare hvorfor modenheten påvirkes av lokale hendelser. En lokal hendelse kan gjøre organisasjonen mere mottakelig for «idésmitte». Et redusert ytre og indre forsvar øker sannsynligheten for at elementene i ideen, eller i dette tilfellet loven, blir implementert og fører til at konkrete tiltak blir iverksatt. Adsorpsjon er begrepet som brukes på denne virkningsmekanismen.

Et annet kjennetegn er virusets evne til å reaktiveres etter å ha vært inaktiv i en periode. Etter en periode med aktivitet, for eksempel for å etablere et internkontrollsystem, blir det mindre oppmerksomhet rundt systemet. Lokale hendelser fører til at systemet hentes fram igjen, reaktiveres, og implementeringen fortsetter.

Det at medieoppslag har effekt kan også forklares med at temaet settes på dagsorden. Årsaken til at effekten på egenvurdert modenhet er positiv kan ligge i at nasjonale oppslag om negative hendelser i mindre grad er gjenkjennbare til egen organisasjon og at man derfor ikke får samme realitetsorientering. Medieoppslag med positive fortegn vil også bidra til å sette personopplysninger og informasjonssikkerhet på dagsorden. Sikkerhetsmånedens oktober som arrangeres hvert år er et slikt eksempel.

Uavhengig av fortegnet på korrelasjonskoeffisientene i analysene er oppmerksomhet en driver for bedre personvern i kommunene. Hvordan oppmerksomheten skal holdes ved like når oppmerksomheten rundt nytt regelverk har lagt seg vil være utfordringen for de mange nyutnevnte personvernombudene.

Av interne faktorer er årlige egenkontroller den faktoren som synes å ha størst betydning. Det er ikke uventet fordi det bidrar til å holde vedlike dokumentasjon og prosedyrer. Det samsvarer også godt med at oppmerksomhet er den ytre faktoren som virker sterkest.

Jevnlig oppmerksomhet om temaet kan være med på å bryte ned kommunens immunitet mot endring av praksis ved at ytre og indre forsvar svekkes. Det kan også forklares ved virusteoriens beskrivelse av

inaktivering og reaktivering. Årlige egenkontroller er med på opprettholde oppmerksomhet rundt systemet og hindre at det blir inaktivt.

Det at ROS-analyser muligens kan ha motsatt effekt, kan skyldes at slike analyser er øyeåpnere for svakheter og risiko og påvirker hvordan man anser egen modenhet. En slik tolking er analog til tolkingen av at lokale hendelser fører til en realitetsorientering av egen praksis og egne svakheter.

Sunn fornuft skulle tilsi at hvis medarbeidernes manglende vilje er reell så ville det ført til en lavere vurdert modenhet. Analysene viste det motsatte, de kommunene som anførte vilje hos medarbeiderne som hinder for regeletterlevelse hadde under ellers like forhold en mer optimistisk vurdering av egen kommunes modenhet enn de øvrige. En mulig forklaring kan finnes i at temaet over tid har vært på dagsorden og at oppfatningen av indre motstand henger igjen, men at «idésmitten» i en inkubasjonstid har trettet ut motstanden. I virusteorien er dette kalt «replikasjon og institusjonalisering».

Med en $\pm 10\%$ feilmargin og kontrollert for øvrige variabler vil de som angir ressursser som en begrensende faktor vurdere egen modenhet lavere enn gjennomsnittet. Reell ressursmangel vil gi seg konkrete utslag i at oppgaver skyves i tid eller prioriteres bort. En annen forklaring kan være at immunforsvarets indre forsvarsverk bruker ressursmangel som et vikarierende argument for ikke å gjøre endringer.

Gjennomføring av risikovurderinger har vært et sentralt element i personopplysningsloven. Det er noe overraskende at ROS-analyser ikke gir signifikante og større utslag på modenhetsskalaen enn et kvart poeng. Det mest overraskende resultatet er allikevel den marginale betydningen personvernombudet synes å ha for kommunenes plassering på modenhetsskalaen. Feilmarginen er riktig nok over $\pm 10\%$, men resultatet er allikevel gyldig for de 102 som deltok i undersøkelsen.

Personvernombud blir obligatorisk for alle kommuner og andre offentlige virksomheter når forordningen trer i kraft. En grundigere analyse av årsakene til personvernombudets tilsynelatende begrensede innflytelse på kommunens modenhet ville vært på sin plass, men det er det ikke rom for i dette prosjektet.

6.3 Teori og praksis

Studien innledet presentasjonen av problemstillingene med å hevde at de er to sider av samme sak, selv om de fremstår som uavhengige. Når en omfattende «oppskrift» på behandling av personopplysninger som forordningen representerer skal implementeres i en så mangslungen organisasjon som en kommune er, så vil den måtte oversettes til en form som gjør den håndterbar i en kommunal organisasjon.

«Privacy by design» – innebygd personvern – er ett av prinsippene som markedsføres overfor utviklere av systemer som skal behandle personopplysninger. Ideen er at når personvernet tas med som perspektiv fra starten av utviklingsprosessen så vil det både gi bedre systemer og bedre personvern. Det samme prinsippet kunne vært fulgt av myndighetene ved utviklingen av ny personopplysningslov. Ved å engasjere kommunene tidlig i arbeidet så vil oversettelsene kunne bli bedre og implementering bli enklere. KINS har nå rundt 300 medlemmer og bør kunne ta rollen som en slik dialogpartner for sentrale myndigheter.

Det nettverket som KINS representerer, med rundt 300 kommuner, fylkeskommuner og kommunale driftsselskap som medlemmer er en arena som departementene, KS og Datatilsynet har en unik mulighet til å bruke for å holde oppmerksomheten om personvern vedlike i kommunal sektor. Det vellykkede samarbeidet mellom KS, Datatilsynet og KINS om NYPE-konferansene var et løft for personvernet i sektoren og en unik arena for «smitte» som bør videreutvikles, særlig når Datatilsynet synes å skalere ned sin rolle overfor personvernombudene.

Datatilsynet har ikke det samme regionale nettverket av «smittbærere» som DSB har i kraft av fylkesberedskapslederne. De må følgelig tenke anderledes. Ved å opprettholde tett kontakt med KINS og engasjere foreningen som dialogpartner vil de få tilgang til et lokalt nettverk som de ikke organisatorisk er utstyrt med. Det nettverket vil også kunne bidra til at veiledningsmateriellet blir mest mulig praktisk nyttbart for kommunene. Med andre ord, unngå veiledere som er «skrevet av jurister og for jurister» (sitat fra intervju med Datatilsynet, hentet fra Andersen, 2017, s. 45). KINS

vil også kunne bidra når etterfølgeren til Artikkel 29-gruppen skal utforme tolkingsuttalelser og definere beste praksis for personvernet.

Det kan hevdes at denne oppgaven er et «langskudd» som kobler to så tilsynelatende ulike felt som europeisering av forvaltningen og regletterlevelse i kommunene. Svaret på det er at det ikke burde vært slik ...

7 Oppsummering og konklusjon

Denne studien har belyst europeisering av forvaltningen og kommunenes praktisering av personopplysningsloven fra ulike synsvinkler. Foranledningen er at EUs personvernforordning trer i kraft den 25 mai 2018 og skal innlemmes i norsk rett som ny personopplysningslov. I EU tok behandlingen av forordningen mer enn fire år, blant annet fordi det var vanskelig å bli enige om offentlige organisasjoner skulle behandles på samme måte som næringslivet eller om det var ønskelig med egne ordninger for det offentlige.

Første del av studien handler om prosessen fra personvernforordningen ble sendt på høring av kommisjonen i 2012 og til den ble vedtatt i 2016. Vinklingen er hvilken rolle norske myndigheter og andre aktuelle aktører inntok i de mer enn fire årene forhandlingene pågikk. Hensikten har vært å spore opp om det fantes norske synspunkter på nytt personvernregelverk og om disse eventuelt var koordinert med eller hadde annen forankring i fylkeskommuner og kommuner.

Årsaken til at denne problemstillingen er interessant er at kommunene er det forvaltningsnivået som får de største utfordringene med å etterleve det nye regelverket på grunn av spennet i oppgaver og konglomeratet av systemer som behandler personopplysninger. Alle de store velferdsordningene som barnehage og skole, skatt, trygd og sosialhjelp samt helse og omsorgstjenester forvaltes av enheter på kommunenivået.

Ut fra åpne kilder er det få indikasjoner på at man fra norsk side har brukt mulighetene til å påvirke innholdet i forordningen. Det er heller ingen formelle spor etter konsultasjoner med kommunene eller sektorinnspill til nasjonale posisjoner. Dette funnet er i tråd med tidligere forskning som er

gjort i forholdet mellom EU og Norge og nasjonale og lokale myndigheter. Det er imidlertid sannsynlig at intern dokumentasjon i departementene vil kunne gi et mer nyansert bilde av Norges rolle overfor EU. En aktiv koordinering av norske synspunkter med kommunalt nivå ville etter all sannsynlighet vært sporbar.

Konklusjonen er entydig i at kommunen hverken har vært konsultert eller på annen måte hatt anledning til å påvirke utformingen av ny personvernforordning i de fire årene den var til behandling før den ble endelig vedtatt.

Andre del av studien har kommunenes praktisering av personopplysningsloven som tema. Bakgrunnen er at Datatilsynet gjennom undersøkelser publisert i 2011 og 2014 samt i rapportene over år har rapportert om en regeletterlevelse i kommunal sektor som de, som tilsynsorgan, finner bekymringsfull.

Kommunenes egen vurdering av status for personvernet i 2017 er innhentet gjennom en undersøkelse høsten 2017 som gikk til alle kommuner og fylkeskommuner. Innledningsvis var den ment å repetere Datatilsynets fra 2011, men ble av flere årsaker endret betydelig. Deltakelsen var på 23 % og skjevfordelt både geografisk og i antall innbyggere, mens Datatilsynets undersøkelse hadde en svarprosent 96 og derfor var representativ for kommunesektoren. Undersøkelsene er ikke direkte sammenlignbare og det er ikke gjort forsøk på å korrigere for skjevhetene. Analyser og konklusjoner fra undersøkelsen i 2017 er gyldige for de som deltok men kan ikke generaliseres til hele kommunesektoren.

På grunnlag av undersøkelsen er det konstruert en modenhetsskala som brukes som avhengig variabel i statistiske analyser av de øvrige svarene. Undersøkelsen fra 2011 målte kommunene i hovedsak etter hvilken dokumentasjon som var utarbeidet. Formålet med å utvikle en modenhetsskala har vært å etablere et rikere begrep og flere indikatorer for å beskrive hvordan kommunene behandler personopplysninger.

Analysene er tolket ved hjelp av virusteorien. Dette er en teori om at organisasjonsideer og organisatorisk praksis har egenskaper til felles med

virus i måten de smitter mellom organisasjoner og hvordan de virker i organisasjonen når ideen/praksisen først har fått feste.

Modellene deler påvirkningen i eksterne og interne faktorer av betydning. Funnene er at kommuner som gjennomgår styringssystemet årlig betrakter seg som mer modne i å behandle personopplysninger enn andre kommuner, under ellers like forhold. Også lokale hendelser, medieoppslag, tilgjengelige ressurser og intern (medarbeidernes) vilje til å følge regelverket korrelerer med hvor modne kommunene oppfatter seg. Noe overraskende syntes det å være marginal samvariasjon mellom kommunenes oppfatning av egen modenhet og om de har personvernombud.

En gjennomgang av resultatene fra 2011 viste at det var signifikant samvariasjon mellom folketallet i kommunen og system for å behandle personopplysninger når kommunene ble inndelt i seks grupper etter folketall. Det var 50 % større sannsynlighet for at kommuner med over 50 000 innbyggere hadde et slikt system enn de minste kommunene med under 2000 innbyggere. Sammenhengen var tilnærmet lineær, det var for eksempel 15 % større sannsynlighet for at kommuner med 2-5 000 innbyggere hadde internkontrollsystem enn de minste kommunene og sannsynligheten økte med økende folketall. Signifikansnivåene var på 5 % eller bedre.

Selv om undersøkelsen i 2017 kan generaliseres til alle kommuner, var det mulig å sammenligne resultatene fra 2011 med svarene fra 2017 for de 92 kommunene som deltok i begge undersøkelsene. I 2017 svarte 70 % at de har internkontroll, en økning på 3 % fra 2011. Vi fant imidlertid ikke samme forskjell etter kommunestørrelse som beskrevet i forrige avsnitt, hverken for 2011 eller for 2017 i denne gruppen. Et overraskende funn var også at nesten hver femte kommune som hadde internkontroll i 2011 ikke lenger hadde det høsten 2017.

Samvariasjon mellom kommunestørrelsen i antall innbyggere og om de har et internkontrollsystem i 2011 avviker fra Datatilsynets inntrykk etter sine tilsyn og dialoger med kommunene de siste årene. De har iblant annet i sine årsrapporter hevdet at egenskaper som kommunestørrelse eller geografi ikke har betydning for regeletterlevelse. Årsaken kan dels ligge i at ved tilsyn så får Datatilsynet et bredere og mer nyansert inntrykk av status enn hva

en undersøkelse kan gi. Det kan også hende at det fulle datasettet fra 2011 inneholder informasjon som ville nyansere forskjellene.

Personvernombudets tilsynelatende marginale betydning for hvordan kommunen oppfatter sin egen kommunes modenhet var overraskende og studien har ikke kunnet identifisere årsaker til det. For øvrig sammenfaller konklusjonene med funn i tidligere forskning på området. Effektene av indre og ytre faktorer lar seg forklare gjennom virusteoriens begrepsapparat og gir logiske konklusjoner.

Avslutningsvis noen ord om sammenhengen mellom de to delene av studien. Et av elementene i et oversettingsteoretisk perspektiv er at organisasjonsideer, eller i dette tilfellet lovverk som skal implementere en EU-forordning, må kontekstualiseres – oversettes til den konteksten de skal virke i – av dyktige oversettere. De må ha så god kjennskap til den organisatoriske sammenhengen at de vet når og hvordan den opprinnelige ideen skal justeres for å kunne fungere i en ny kontekst. Ved å holde kommunal sektor utenfor den utviklingen som pågikk fra 2012 til 2016 ga sentrale myndigheter avkall på å få innspill fra det lokale forvaltningsnivået som skal iverksette forordningen. Samtidig frarøvet de kommunal sektor muligheten til å utvikle denne oversetterkompetansen. Løsningen for fremtidens personvern er det nettverket som KINS representerer.

Litteraturliste

- Amdam, J. & Veggeland, N. (2011). *Teorier om samfunnsstyring og planlegging*. Oslo: Universitetsforlaget.
- Andersen, P. L. (2017). *Informasjonssikkerhet i kommunal sektor* (Masteroppgave, Universitetet i Oslo, Oslo).
- Art 29 WP. (2017). *Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679*. Article 29 Working Party.
- Austvik, O. G. & Claes, D. H. (2011). *EØS-avtalen og norsk energipolitikk*. Europautredningen.
- Baldersheim, H. (2014). Lokalmaktdebatten – fra nessekonger til nettverksstyre. I *Det kommunale laboratorium. Teoretiske perspektiver på lokal politikk og organisering*. Bergen: Fagbokforlaget.
- Bing, J. (1991). *Personvern i faresonen*. Oslo: Cappelen.
- Blume, P. (2015 februar). It Is Time for Tomorrow: EU Data Protection Reform and the Internet. *Journal of Internet Law*, 18, 3–13.
- Bryer, J. & Speerschneider, K. (2016). *likert: Analysis and Visualization Likert Items*. R package version 1.3.5. Hentet fra <https://CRAN.R-project.org/package=likert>
- Börzel, T. A. & Panke, D. (2016). Europeanization. I M. Cini & N. P.-S. Borragán (Red.), *European Union Politics* (5. utg., Kap. 8). Oxford: Oxford University Press.
- CEMR. (2012). CEMR position on the Commission's proposal on General Data Protection Regulation - COM (2012) 11 final. Hentet fra http://www.ccre.org/docs/cemr_position_paper_data_protection_en.pdf

-
- CEMR. (2015). Local and regional governments as service providers. Hentet 24. april 2018, fra <http://www.ccre.org/en/actualites/view/3116>
- Christensen, R. H. B. (2015). ordinal—Regression Models for Ordinal Data. R package version 2015.6-28. <http://www.cran.r-project.org/package=ordinal/>.
- Christensen, T., Egeberg, M., Læg Reid, P., Roness, P. G., & Røvik, K. A. (2015). *Organisasjonsteori for offentlig sektor* (3. utg.). Oslo: Universitetsforlaget.
- Claes, D. H. & Førland, T. E. (2015). *EU: Mellomstatlig samarbeid og politisk system* (4. utg.). Oslo: Gyldendal Akademisk.
- CMMI Product Team. (2001). *Capability Maturity Model Integration V1.1 - Staged Representation*. Carnegie Mellon Software Engineering Institute. CMU/SEI-2002-TR-004.
- CoR. (2012). Opinion on the Data Protection Package. Hentet 24. april 2018, fra https://webapi.cor.europa.eu/documentsanonymous/cdr625-2012_00_00_tra_ac_en.doc
- Dahl, D. B. (2016). *xtable: Export Tables to LaTeX or HTML*. R package version 1.8-2. Hentet fra <https://CRAN.R-project.org/package=xtable>
- Daler, T., Gulbrandsen, R., Høie, T. A., & Sjølstad, T. (2010). *Håndbok i datasikkerhet* (3. utg.). Tapir akademisk forlag.
- Datatilsynet. (2011). *Kommuneundersøkelsen 2010-2011* (Analyserapport Nr. Versjon 1.2).
- Datatilsynet. (2014a). *Personvern i skole og barnehage*.
- Datatilsynet. (2014b). *Årsmelding for 2014*.
- Datatilsynet. (2015). Kommunenes internkontroll. Hentet 3. mai 2017, fra <https://www.datatilsynet.no/regelverk-og-skjema/behandle-personopplysninger/kommuneundersokelsen/>
- Datatilsynet. (2016). *Årsmelding for 2016*.
- Datatilsynet. (2017 mars). *Nye personvernregler fra 2018* (Brev til alle landets rådmenn Nr. 17/00268-1/HHU). Datatilsynet.

-
- Datatilsynet. (2018). Datatilsynets internasjonale arbeid. Hentet 30. mars 2018, fra <https://www.datatilsynet.no/om-datatilsynet/internasjonalt-samarbeid/>
- Difi. (2017). Mål din digitale modenhet. Hentet 22. mars 2018, fra <https://www.difi.no/fagomrader-og-tjenester/digitalt-forstevalg/hvordan-komme-i-gang/mal-digital-modenhet>
- Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, (4), 92–100.
- DSB. (2017). Kommuneundersøkelsen. Hentet 3. april 2018, fra <https://www.dsb.no/menyartikler/statistikk/kommuneundersokelsen/>
- eForvaltningsforskriften. (2004). Forskrift om elektronisk kommunikasjon med og i forvaltningen.
- Egeberg, M. & Trondal, J. (2011). *Forvaltningsmessige konsekvenser av eøs/eu* (Rapport Nr. 1). Europautredningen.
- Eide, H. P. & Nagell-Erichsen, H. (2007). Status for risikostyring i staten, sett fra Senter for statlig økonomistyring. *Internrevisoren*, 15(1), 20–22.
- ESA. (2018). Internal Market Scoreboard. Hentet 23. april 2018, fra <http://www.eftasurv.int/da/DocumentDirectAction/outputDocument?docId=4226>
- European Commission. (udatert). Procedure 2012/0011/COD. Hentet 24. april 2018, fra http://eur-lex.europa.eu/procedure/EN/2012_11?qid=1524518854549&rid=1
- European Commission. (2012). *COM(2012) 11 final - Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Brussels.
- European Commission. (2018a). Article 29 working party archives 1997 - 2016. Hentet 30. mars 2018, fra http://ec.europa.eu/justice/article-29/documentation/index_en.htm

-
- European Commission. (2018b). Single market scoreboard. Hentet 23. april 2018, fra http://ec.europa.eu/internal_market/scoreboard/performance_by_governance_tool/transposition/index_en.htm
- European Council. (1995). Direktiv 95/46/EF - Personverndirektivet. Hentet fra <https://www.regjeringen.no/>
- EU. (2016 mai). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union, L119*, 1–88. Hentet fra <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC>
- Grønnestad, S. (2012). *Subsidiaritetsprinsippet og nasjonale parlamenters rolle i EU*. ARENA.
- Hansen, T. (2017). GSM. Hentet 26. april 2018, fra <https://snl.no/GSM>
- Hellevik, O. (2015). Hva betyr respondentbortfallet i intervjuundersøkelser? *Tidsskrift for samfunnsforskning*, 56(2), 211–231.
- Hellsaa, I. (2013). *En litteraturstudie om implementering og langtids effekter* (Masteroppgave, Universitetet i Stavanger).
- Hlavac, M. (2018). *stargazer: Well-Formatted Regression and Summary Statistics Tables*. R package version 5.2.1. Central European Labour Studies Institute (CELSI). Bratislava, Slovakia. Hentet fra <https://CRAN.R-project.org/package=stargazer>
- Hoem, J. M. (2008). The reporting of statistical significance in scientific journals. *Demographic Research*, 18(15), 437–442.
- Indset, M. & Hovik, S. (2008). *Lojal iverksetting eller målrettet medvirkning?* (NIBR-rapport Nr. 2008:12). Norsk institutt for by- og regionforskning.
- ITU. (2017). Key ICT indicators for developed and developing countries and the world (totals and penetration rates). Hentet 26. april 2018, fra https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2017/ITU_Key_2005-2017_ICT_data.xls

-
- JD. (2017). *Ny personopplysningslov - gjennomføring av personvernforordningen i norsk rett*. Justis- og beredskapsdepartementet.
- Justis- og beredskapsdepartementet. (2012). Høring - EU-kommisjonens forslag til nye personvernregler. Hentet fra <https://www.regjeringen.no/no/no/dokumenter/horing---eu-kommisjonens-forslag-til-nye/id679008/>
- Justis- og beredskapsdepartementet. (2017). Uoffisiell norsk oversettelse av personvernforordningen. Hentet fra <https://www.regjeringen.no/no/no/dokumenter/horing-om-utkast-til-ny-personopplysningslov--gjennomforing-av-personvernforordningen-i-norsk-rett/id2564300/>
- Justis- og beredskapsdepartementet. (2018). Prop. 56 LS (2017–2018) Lov om behandling av personopplysninger (personopplysningsloven) og samtykke til deltakelse i en beslutning i EØS-komiteen om innlemmelse av forordning (EU) nr. 2016/679 (generell personvernforordning) i EØS-avtalen. Hentet fra <https://www.regjeringen.no/no/dokumenter/prop.-56-ls-20172018/id2594627/>
- KINS. (2017). Undersøkelse om Personvernforordningen (GDPR) og norske kommuner. Hentet 3. april 2018, fra <https://kins.no/2017/10/undersokelse-personvernforordningen-gdpr-norske-kommuner/>
- KMD. (2018). TILDELINGSBREV 2018 – Direktoratet for forvaltning og IKT.
- KS. (2013). *Digitaliseringsstrategi 2013–2016 for kommuner og fylkeskommuner*. KS. Oslo.
- KS. (2014). På gang i EØS.
- Langørger, A., Løkken, S. A., & Aaberge, R. (2015). *Gruppering av kommuner etter folkemengde og økonomiske rammebetingelser 2013* (Rapport Nr. 2015/19). Statistisk sentralbyrå.
- Meld. St. 11 (2012–2013). (2012). Personvern – utsikter og utfordringer. Nasjonal sikkerhetsmyndighet. (2015). Veileder - Sikkerhetsstyring. Veileder. Hentet 7. august 2017, fra <https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/veileder-i-sikkerhetsstyring--endelig.pdf>
- Netemeyer, R., Bearden, W., & Sharma, S. (2003). *Scaling Procedures: Issues and Applications*. Calif: SAGE Publications.
-

-
- Nordal, O., Liseter, I. M., & Rossen, E. (2016). Internetts historie. Hentet 26. april 2018, fra https://snl.no/Internetts_historie
- NorSIS. (2015). *Kommune Cert — utredning av behov og muligheter*. Norsk senter for informasjonssikring. Gjøvik.
- NOU 2011:11. (2011). Innovasjon i omsorg. Hentet 26. april 2018, fra <https://www.regjeringen.no/no/dokumenter/nou-2011-11/id646812/>
- NOU 2012:2. (2012). Utenfor og innenfor. Hentet 27. september 2017, fra <https://www.regjeringen.no/no/dokumenter/nou-2012-2/id669368/>
- Olsen, J. P. (2002). The Many Faces of Europeanization. *Journal of Common Market Studies*, 40(5), 921–952.
- Olsen, J. P. (2006). Europeanization. I M. Cini (Red.), *European Union Politics* (2. utg.). Oxford: Oxford University Press.
- Standard for klassifisering av kommuner etter innbyggertall. (1998). Hentet 18. november 2017, fra <https://www.ssb.no/klass/klassifikasjoner/115>
- Personopplysningsforskriften. (2000). Forskrift av 15. desember 2000 nr. 1265 om behandling av personopplysninger.
- Personopplysningsloven. (2000). Lov 14 april 2000 nr 31 om behandling av personopplysninger.
- Personregisterloven. (1978). Lov 9. juni 1978 nr. 48 om personregistre m.m.
- PwC. (2015). *IKT-samarbeid i kommunal sektor. Modeller for organisering, styring og finansiering* (Rapport Nr. 144016). KS FoU. Oslo.
- R Core Team. (2017). *R: A Language and Environment for Statistical Computing*. R Foundation for Statistical Computing. Vienna, Austria. Hentet fra <https://www.R-project.org/>
- Rambøll. (2018a). Kartlegging av digital modenhet i kommunesektoren. Hentet 22. mars 2018, fra <http://www.ks.no/fagomrader/utvikling/fou/fou-rapporter/hvor-digital-er-kommunesektoren/>
- Rambøll. (2018b). *Oppdatert kunnskapsgrunnlag på digitaliseringsområdet*. KS FoU. Hentet 22. mars 2018, fra <http://www.ks.no/fagomrader/utvikling/fou/fou-rapporter/hvor-digital-er-kommunesektoren/>
- Riksdagen. (2012). Riksdagens uttalelse om personvernforordningen. Hentet 24. april 2018, fra http://ec.europa.eu/dgs/secretariat_general/
-

-
- relations/reasons_other/npo/docs/sweden/2012/com20120011/com20120011_riksdag_opinion_en.pdf
- Riksrevisjonen. (2016). *Riksrevisjonens undersøkelse av digitalisering av kommunale tjenester*. Riksrevisjonen.
- Ringdal, K. (2013). *Enhet og mangfold* (3. utg.). Bergen: Fagbokforlaget.
- Røvik, K. A. (2007). *Trender og translasjoner*. Oslo: Universitetsforlaget.
- Røvik, K. A. (2011). From Fashion to Virus: An Alternative Theory of Organizations' Handling of Management Ideas. *Organization Studies*, 32(5), 631–653. doi:10.1177/0170840611405426. eprint: <https://doi.org/10.1177/0170840611405426>
- Schartum, D. W. & Bygrave, L. A. (2016). *Personvern i informasjonssamfunnet*. Bergen: Fagbokforlaget.
- Schartum, D. W., Jansen, A., & Tranvik, T. (2017). *Digital forvaltning – en innføring*. Bergen: Fagbokforlaget.
- Smismans, S. (2016). Democracy and Legitimacy in the European Union. I M. Cini & N. P.-S. Borragán (Red.), *European Union Politics* (5. utg., Kap. 24). Oxford: Oxford University Press.
- SNL. (2018). Algoritme. Hentet 26. april 2018, fra <https://snl.no/algoritme>
- SSB. (udatert). Statistikkbanken. Hentet fra <https://www.ssb.no/statistikkbanken>
- SSB. (2017a). Standard for fylkesinndeling. Hentet 27. september 2017, fra <https://www.ssb.no/klass/klassifikasjoner/104/versjon/400>
- SSB. (2017b). Standard for kommuneinndeling. Hentet 27. september 2017, fra <https://www.ssb.no/klass/klassifikasjoner/131>
- SSB. (2018). Kommune-Stat-Rapportering. Hentet 3. april 2018, fra <https://www.ssb.no/offentlig-sektor/kostra>
- Storstad, O. (2010). *Kommunal kultursektor i endring*. Bergen: Norsk kulturråd.
- Thrane, C. (2017). *Regresjonsanalyse*. Oslo: Cappelen Damm Akademisk.
- Tranvik, T. (2009a). Datatilsynets virkemiddelbruk. I D. W. Schartum & A. G. B. Bekken (Red.), *Yulex 2009*. Senter for rettsinformatikk.
-

-
- Tranvik, T. (2009b). Kommuner og informasjonssikkerhet. Etterlevelse av kravene i personopplysningsloven og forskriften. I D. W. Schartum & A. G. B. Bekken (Red.), *Yulex 2009*. Senter for rettsinformatikk.
- Tranvik, T. (2009c). *Personvern og informasjonssikkerhet. En studie av rettsreglers etterlevelse i kommunal sektor*. Complex nr. 4. Oslo: Senter for rettsinformatikk.
- Tranvik, T. (2011). Hvordan manipulere risikovurderinger? Erfaringer og observasjoner fra skolesektoren. I D. W. Schartum & A. G. B. Bekken (Red.), *Yulex 2011*. Senter for rettsinformatikk.
- Tranvik, T. (2012). Kommunal regeletterlevelse. Illusjoner og realiteter på personvernområdet. *Tidsskrift for samfunnsforskning*, 53(2), 131–156.
- Utenriksdepartementet. (2009). *Håndbok i EU/EØS-arbeid*.
- Veggeland, N. (2000). *Den nye regionalismen. Europeisk integrasjon og flernivåstyring*. Bergen: Fagbokforlaget.
- Veggeland, N. (2003). *Det nye demokratiet – et politisk laboratorium for partnerskap*. Kristiansand: Høyskoleforlaget.
- Veggeland, N. (2005a). *Det nye lokaldemokratiet – Internasjonale avtaler og europeisering av Norge*. Lokaldemokratikommisjonen.
- Veggeland, N. (2005b). *Europapolitikk, innenrikspolitik og kommunene*. Oslo: Kommuneforlaget.
- Veggeland, N. (2010). *Den nye reguleringsstaten*. Gyldendal Akademisk.
- Veggeland, N. (2012). *Styring og reguleringsparadokser*. Trondheim: Tapir akademisk forlag.
- Wickham, H. (2017). *tidyverse: Easily Install and Load the 'Tidyverse'*. R package version 1.2.1. Hentet fra <https://CRAN.R-project.org/package=tidyverse>
- Østby, H. (2016). *Balansert målstyring i Forsvaret: – En vaksine, en mote og et virus* (Masteroppgave, Norges miljø- og biovitenskapelige universitet, Ås).
- Aaberge, R. & Laake, P. (1984). Om statistiske teorier for tolking av data. *Tidsskrift for samfunnsforskning*, 25(2), 165–185.

A Spørsmål til kommunene



Personopplysninger i kommunesektoren

Formålet med denne undersøkelsen er å be om kommunenes og fylkeskommunenes egen vurdering av om de etterlever personopplysningsloven og -forskriften og hvilke forberedelser som gjøres for ny personopplysningslov. Bakgrunnen er at EUs personvernforordning (også kalt GDPR - General Data Protection Regulation) vil gjelde fra 25. mai 2018 for alle som behandler personopplysninger, blant annet norske kommuner og fylkeskommuner.

Jeg håper at din kommune/fylkeskommune vil delta i undersøkelsen, som er en del av min masteroppgave i offentlig administrasjon (MPA) ved Høgskolen i Innlandet. Oppgaven vil ikke identifisere svarene fra hver enkelt kommune, men søke å gi et samlet bilde av status for kommunesektoren.

De kommuner og fylkeskommuner som deltar i undersøkelsen vil få tilsendt en kopi av oppgaven når den er ferdig i mai/juni 2018.

Det tar rundt 10 minutter å svare på undersøkelsen.

Hilsen

Sverre Holm

1) * Hvilken funksjon har du i din kommune/fylkeskommune?

- Rådmann/Administrasjonssjef
- Kommunalsjef eller tilsvarende
- Sikkerhetsansvarlig
- IKT-ansvarlig
- Jurist
- Personvernombud
- Annet, spesifiser tittel og fagområde



EUs personvernforordning, også kalt GDPR (General Data Protection Regulation), skal fra 25. mai 2018 gjøres gjeldende som ny personopplysningslov i Norge.

2) Når fikk du først høre om EUs personvernforordning?

- I løpet av de siste tre månedene
- I løpet av første halvår 2017
- I 2015 eller 2016
- Før 2015
- Nå, i denne undersøkelsen

3) Hvordan fikk du vite at EUs personvernforordning får virkning for kommunene? Flere svar er mulig.

- Artikler i media
- Foredrag på konferanse/kurs/fagdager
- Informasjon fra KS
- Samtale med kolleger fra andre kommuner
- Datatilsynets brev om reformen våren 2017
- Justisdepartementets høring om ny personopplysningslov i 2017
- Justisdepartementets høring om EUs personvernforordning i 2012
- Gjennom denne undersøkelsen
- Annet, spesifiser

4) Har du noen synspunkter på EUs ambisjon om å etablere et felles europeisk regelverk for behandling av personopplysninger?



Personopplysningsloven §2 sier at behandling av personopplysninger er "enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter"

5) I hvor stor grad er du enig i påstandene under om hvordan din kommune/fylkeskommune behandler personopplysninger?

	I svært stor grad	I stor grad	I noen grad	I liten grad	Ikke i det hele tatt	Vet ikke
Kommunens/fylkeskommunens ledelse har godkjent alle rutiner	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Det er godt kjent hvem som har ansvar for behandlingen av personopplysninger	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Kommunen har dokumentert det som personopplysningsloven krever	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Kommunen reagerer raskt hvis personopplysninger behandles feil	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
De ansatte vet godt hvordan personopplysninger skal behandles	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Kontroll av hvordan kommunen behandler personopplysninger gjennomføres hvert år	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Personopplysningslovens § 13 pålegger alle som behandler personopplysninger å ha et styringssystem for informasjonssikkerhet som baserer seg på anerkjente standarder, og § 14 stiller krav om internkontroll.

Det vil også i ny personopplysningslov stilles krav om å «gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet i forhold til risikoen», selv om det ikke stilles konkrete krav til internkontroll.

6) Har kommunen/fylkeskommunen et system for hvordan dere behandler personopplysninger?

Ja Nei Vet ikke



7) Vennligst svar på følgende spørsmål om kommunen/fylkeskommunens system for behandling av personopplysninger.

	Ja	Nei	Vet ikke
Foreligger det en samlet skriftlig dokumentasjon over hvilke personopplysninger som behandles i kommunen/fylkeskommunen?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Er det rettslige grunnlaget (behandlingsgrunnlaget) for behandlingen av personopplysningene dokumentert?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Er det fastsatt dokumenterte sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Er det i løpet av de 18 siste månedene gjennomført en risikovurdering av virksomhetens informasjonssikkerhet?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Er det etablert rutiner for håndtering av avvik fra personopplysningslovens bestemmelser?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Er det etablert rutiner for sletting av personopplysninger når kommunen/fylkeskommunen ikke har hjemmel for å oppbevare dem lenger?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

8) Når ble det sist gjennomført egenkontroll av kommunen/fylkeskommunens system for behandling av personopplysninger?

- Mindre enn 6 måneder siden
- 6 - 12 måneder
- 13 - 24 måneder
- Mer enn 24 måneder siden



9) Har dere planlagt oppstart for arbeidet med et system for behandling av personopplysninger?

- Ja, vi er allerede i gang med arbeidet
- Ja, arbeidet starter i høst
- Ja, vi har planlagt oppstart våren 2018
- Ja, men vi venter til forordningen er trådt i kraft
- Nei

10) Har kommunen/fylkeskommunen inngått databehandleravtale med alle eksterne leverandører av systemer og tjenester som behandler personopplysninger?

- Ja
- Ja, med de fleste
- Bare med noen
- Nei
- Vet ikke

En av de nye bestemmelsene i EUs personvernforordning er at alle offentlige etater må utnevne personvernombud*.

*Justisdepartementet foreslår å bruke begrepet personvernrådsgiver i sitt høringsbrev. I denne undersøkelsen brukes personvernombud som en fellesbetegnelse.

11) Er du kjent med at det blir obligatorisk for alle kommuner/fylkeskommuner å ha eget personvernombud fra 2018?

- Ja, kommunen/fylkeskommunen har personvernombud
- Ja, men vi har ikke utnevnt personvernombud ennå.
- Nei



12) Når ble personvernombudet utnevnt?

- I 2017
- I 2015 eller 2016
- Før 2015

13) Hvilken organisatorisk plassering har personvernombudet?

- I rådmannens stab
- Ved juridisk avdeling eller tilsvarende
- I personalavdelingen eller tilsvarende
- I IKT-avdelingen eller tilsvarende
- I et interkommunalt samarbeid
- Ekstern konsulent
- Annet, vennligst spesifiser

14) Har dere startet prosessen med å utnevne personvernombud for kommunen/fylkeskommunen?

- Ja
- Nei

15) Har dere tatt stilling til hvilken organisatorisk plassering personvernombudet skal få?

- I rådmannens stab
- Ved juridisk avdeling eller tilsvarende
- I personalavdelingen eller tilsvarende
- I IKT-avdelingen eller tilsvarende
- I et interkommunalt samarbeid
- Ekstern konsulent
- Nei
- Annet, vennligst spesifiser



16) Hvilke ytre forhold tror du bidrar mest til at kommunen/fylkeskommunen behandler personopplysningene i tråd med lovverket? Flere svar er mulig.

- Tilsyn
- Forvaltningsrevisjoner
- Veiledere fra Datatilsynet
- Medieoppslag nasjonalt
- Uheldige episoder lokalt eller i nabokommunene
- Annet, vennligst spesifiser

17) Hva mener du er de største hindrene i din kommune for å behandle personopplysninger etter kravene i personopplysningsloven? Flere svar er mulig

- Vi kjenner ikke kravene
- Det er for arbeidskrevende
- Vi kan ikke nok om internkontroll
- Det koster for mye
- Medarbeideres vilje til å følge regler og rutiner
- Annet, vennligst spesifiser

18) Tror du at EUs personvernforordning vil føre til endringer i organisasjon, prosedyrer og/eller prosesser i din kommune/fylkeskommune? Begrunn gjerne svaret.



Datatilsynet sier på sine nettsider at overgangen til ny personopplysningslov blir lettest for de virksomhetene som etterlever kravene i dagens personopplysningslov.

19) Ut fra en totalvurdering, hvor godt forberedt mener du at din kommune/fylkeskommune er på å behandle personopplysninger slik personvernforordningen krever?

- Det mangler mye på at vi følger kravene i gjeldende personopplysningslov
- Vi følger i store trekk dagens lovverk.
- Vi har startet oppdatering av rutinene etter nytt regelverk.
- Alle kjente endringer er planlagt og vil være implementert innen 25. mai 2018
- Vet ikke

20) Er det forhold som angår kommunens/fylkeskommunens behandling av personopplysninger som du ønsker å kommentere eller utdype?

© Copyright www.questback.com. All Rights Reserved.

B Svar avgitt på spørsmålene 4, 18 og 20

B.1 Spørsmål 4 – Synspunkter på felles europeisk regelverk

Spørsmålet lød: «Har du noen synspunkter på EUs ambisjon om å etablere et felles europeisk regelverk for behandling av personopplysninger?» Svarene fra de som besvarte dette spørsmålet er listet opp i tabell B.1.

Tabell B.1: Synspunkter på EUs ambisjon om felles personvernregler N = 28

Synspunkt

På høy tid!

Dette er positivt og er en styrke for personvernet.

Et felles europeisk regelverk vil lette samarbeidet på tvers av landegrenser, men kommer med store utfordringer i forhold til nasjonale lover og regelverk mtp tilpassing.

Det er påkrevd med felles regelverk knyttet til digitalisering og elektroniske lagringer som kan søkes opp globalt. Utveksling av og tilgang på personopplysninger må trygges.

fortsetter ...

... fortsetter fra forrige side

Synspunkt

Når det er mulig med nasjonale tilpasninger i ca 50% av artiklene, kan det stilles spørsmål om i hvilken grad målsetning om likt lovverk vil nås. EU vil som samlet kraft kunne ha stor påvirkning på globale aktørers behandling av personopplysninger. Vi ser allerede (tilsynelatende) tegn til mer åpenhet fra aktører som Google og Facebook.

positiv

Greitt å ha same haldning til slike viktige tema. Spesielt etter alle avsløringane av overvaking av andre land mot Noreg.

En god ambisjon så gjenstår det å se hvordan det vil fungere i praksis.

ok

Positivt med felles regelverk på tvers av landegrenser.

Bra med samordning av regelverk, men det er en krevende øvelse å skaffe seg den fulle oevrsikten over hva som er forventa

Svært positivt med ensartet regelverk og forhåpentligvis lik håndteringa av regelverket

Synes det er kjempeflott, men bøtenivået er noe unorsk. Minner mer om amerikanske tilstander enn slik vi har det.

Blir dette for stort og omfattende - vanskelig å dra ned til vår organisasjon? Det er et spørsmål jeg stiller meg.

Nødvendig og fornuftig i og med at bruk av data og datalagring er økende, og er uavhengig av landegrenser.

Det er en kompliserende faktor at det skal vere et felles regelverk for EU. Det innebærer veldig mye arbeid for kommunene.

fortsetter ...

... fortsetter fra forrige side

Synspunkt

Foreløpig ikke

Synes det er svært positivt og høyst nødvendig.

Det er bra!

Ift rettsvern etc så er dette veldig bra, men ut fra muligheten til å etterleve et så detaljert regelverk så vil dette bli veldig arbeidskrevende for kommunene og sannsynligvis en ikke oppfylt ambisjon for mange

Utgangspunkt er det bra. Dataflyten vil flyte i større grad over landegrenser og få et likt vern i EU er med det et godt utgangspunkt. Likevel vil det by på store utfordringer, spesielt innenfor alle lands særlovgivninger og behandlingsgrunnlag. Ulike land har og ulik praksis med tanke på hyppigheten av bøtelegging og nivå.

Meget positivt. Ikke minst overfor store multinasjonale selskaper som Google, Applre, Facebook, Microsoft, etc som til nå har kunnet diktere betingelser overfor sine kunder.

Positiv, men tror det kan bli en utfordring for flere av kommunene å komme helt i mål med overholdelse av kravene innen fristen.

Positiv

Flott med et felles regelverk

Fornuftig

Fint med felles rammer - men det burde kanskje vært enda mer felles styring av hvordan implementere det nye regelverket i den praktiske arbeidshverdagen - både på leder og på saksbehandlernivå.

Det er absolutt nødvendig.

B.2 Spørsmål 18 – Lokale endringer (kvalitativt)

Spørsmålet lød: Tror du at EUs personvernforordning vil føre til endringer i organisasjon, prosedyrer og/eller prosesser i din kommune/fylkeskommune? Begrunn gjerne svaret.

Svarene fra de 54 som valgte å besvare dette spørsmålet er listet opp i tabell B.2.

Tabell B.2: Spm 18 – Lokale endringer som følge av forordningen N = 54

Synspunkt

Ja, men samtidig må det avklares hva som skal gjelde - forordningen eller norsk særlov. Foreløpig er ting uavklart - f.eks. snakkes det i forordningen om retten til å få slettet opplysninger, mens arkivloven stiller klare begrensninger i forhold til sletting.

Nei

Akkurat når det er nytt - oppfølging over tid, derimot -

Ja, ordningen med personvernombud blir implementert.

Ja, det tror jeg. i dag er det mye mer fokus på fag område. Fra KS, Datatilsynet, intern kontrollorgan

Det vil i høye grad føre til endringer mtp kravene som ligger i den nye personvernforordningen, til tross for at vi allerede har et regelverk som tilsier at dette i stor grad skal være på plass allerede.

Ja innskjerping i ny forordning med bl.a. krav om sikre systemer og dokumentasjon bl.a. på rutiner og kontroller vil føre til endring

Ja, det vil medføre endringer. Størrelse på overtredelsesgebyr gir økt økonomisk risiko. Det medfører større oppmerksomhet fra toppliden og gir kraft bak evne til gjennomføring.

fortsetter ...

... fortsetter fra forrige side

Synspunkt

Ja, det vil definitivt føre til endringer, men etterlevelsen av det vil i så fall tiden vise.

I liten grad endringer i organisasjonen, men vi må endre noen av prosedyrene våre.

Noen justeringer vil det bli. Det positive er at personvern vil få mer oppmerksomhet og dermed blir temaet mer på agendaen.

ja, blir nok ombud for flere kommuner, og strukturen rundt ledelsens ansvar må bli klarere

Organisasjonen har hatt stort fokus på dette området dei siste to åra, så det vil ikkje få større fokus enn det har no. No vert det berre tilpassa GDPR.

Det er igangsatt prosesser allerede for å sikre at dette blir kjent i egen organisasjon. Vi holder på med informasjon ut i enhetene og i tillegg skal det etableres en arbeidsgruppe for å sikre forankring når det gjelder enhetene, endringer i internkontroll, opplæring av ansatte m.m

Ja, fordi forordningen vil kreve større, kontinuerlig fokus på personvernarbeid. I dag er dette en mindre andel av personvernombudets totale stilling.

ja, vår sikkerhetshåndbok og rutiner må endres iht nye personvernregler.

Ja, felles regler for behandling av personopplysninger

Til en viss grad. Internkontrollsystemet er etablert i regionalt samarbeid, og iverksatt for egen kommune. Det skal gjennom en hovedrevisjon. Personvernforordningen og felles regionalt personvernombud vi bidra til å løfte fram informasjonssikkerhet som tema på nytt.

fortsetter ...

... fortsetter fra forrige side

Synspunkt

Ja, det vil skape større fokus og mer fart og retning på arbeidet med revisjon av rutiner og prosedyrer.

Ja

Vil forhåpentlig føre til større bevissthet og bedre rutiner

Ja på de områdene der det innføres nye regler.

Ja

Det har fått det, ved at det er utnevnt et personvernombud. I tillegg skal mange av kommunen i distriktene vurdere om det er hensiktsmessig med et felles personvernombud, eksternt personvernombud m.m.

Vi er snart i mål med å innføre et internkontrollsystem for informasjonssikkerhet, så det eneste nye hos oss er personvernombud

NEI

Ja det tror vi, vi er nødt til å prioritere og befeste informasjonssikkerhetsarbeidet i organisasjonen. Vi må også ha systemer som gjør det enklere for organisasjonen å jobbe med temaet, og internkontroll.

Vi har mye på plass, men dette vil skjerpe oss ytterligere.

På helseområdet ser det ut til å være gode rutiner allerede, selv om ikke alle rutiner og prosedyrer er nedtegnet på papiret". På andre fagområder kan det være behov for å strukturere prosedyrer bedre. Forordningen vil neppe føre til organisatoriske endringer for øvrig, men det er et behov for å få dokumentert rutinene. Arbeid med dette er under igangsetting.

Sterkere formalisering av internkontroll

Ja, fordi vi må.

fortsetter ...

... fortsetter fra forrige side

Synspunkt

Jeg tror det vil bli store endringer i prosedyrer og prosesser, og hele tankesettet til de ansatte må endres. Vi ligger svært langt bak på dette området, og det er lite bevissthet rundt behandling av personopplysninger.

Ja, i henhold til lovkrav vil vi få en større kunnskap om personvern og internkontroll. Det er tatt i bruk verktøy for å følge opp lovkrav og dette forankres i ledelsen.

Økt fokus nasjonalt vil ha ringvirkninger.

Ja. Må kurse oss, kartlegge system, innhente avtaler, skrive prosedyrar.

Ja, vi er i gang med dette arbeidet. Det er sterkt fokus nasjonalt, og vi mener det en svært viktig oppgave. Digitalisering av stadig flere oppgaver stiller nye krav til oss.

ja både økt kompetanse og bevissthet fører til dette

Nye føringer vil bli implementert i internkontrollrutinene og behandlingsprosedyrene. Tilsetting av personvernombud vil styrke fokuset på internkontroll i forhold til informasjonssikkerhet

Ja, for det blir forpliktende for kommunen å ha et godt system, prosesser og rutiner som dokumenterer/sikrer at personopplysninger behandles forskriftsmessig.

Ja, det vil få større fokus

ja

Det blir i større grad lagt mer ansvar på hver enkelt byrådsledelse. Disse må gjøre noen endringer i sine prosesser.

fortsetter ...

... fortsetter fra forrige side

Synspunkt

Det vil føre til tydeligere krav til sikkerhet ifm anskaffelser, særlig for skyløsninger. Privacy by design/default blir viktig. Personvernombudet har fått oppgradert sin stilling fra 20% til 100%. Forøvrig vil DPIA bli viktig, Vi må også få bedre rutiner for å håndtere innsyns-ønsker, og ønsker om sletting/endring av data.

Ja, gjennom kartlegging og evt. forbedring av dagens rutiner.

Ja. Det er allerede initiert flere prosjekter med mål å være i samsvar med det nye lovverket. Dette har allerede medført endringer i organisasjon og prosedyrer.

Ja enda mer fokus på alle nivå.

I organisasjonen blir det i alle fall endringer siden vi må ha et personvernombud. Det vil også bli store endringer i avtaleverket kommunen har med systemleverandører, siden kravene databehandleravtaler blir endret. Bl. annet med tanke på at det nå må gjøres avtaler om overføring av personopplysninger hvis leverandøren har underleverandører utenfor EØS (mange/de fleste har ofte support i India f.eks). Det må utarbeides løsninger for utlevering av personopplysninger, samt løsninger for sletting av opplysninger. Dette er utfordrende fordi det i de fleste arkivsystemer ikke går an å slette dokumenter. Arkivloven med forskrifter og annen særlovgivning går foran, men det blir kanskje en del nye områder hvor det blir konflikt mellom forskjellig lovverk.

ja, et viktig grep i å få fokus på arbeidet

Ja - fordi denne gangen er det redsel for bøter.

Ja - mer fokus på personvern og behandlingen av disse.

Ja, det vil systematisere arbeidet på området mer enn før.

fortsetter ...

... fortsetter fra forrige side

Synspunkt

Ja - I forbindelse med kommunesammenslåing vil alle rutiner og prosesser gjennomgå. Man vil også da ta hensyn til GDPR ved endring/nye rutiner

Ja, vi må revidere det vi har og sikkert supplere med mer

Ja. Bevisstheten om regelverket har økt allerede, som følge av oppmerksomheten i media og ulike interesseorganisasjoner. Vi er allerede i gang med å revidere og oppdatere rammeverket.

B.3 Spørsmål 20 – Andre kommentarer

Spørsmålet lød: Er det forhold som angår kommunens/fylkeskommunens behandling av personopplysninger som du ønsker å kommentere eller utdype?

Spørsmålet ble stilt som en ventil for å fange opp synspunkter som respondentene anså som vesentlige, men som ikke var dekket i de tidligere spørsmålene i undersøkelsen. 15 av deltakerne valgte å benytte denne muligheten og deres kommentarer finnes i tabell B.3.

Tabell B.3: Spm 20 – andre kommentarer N = 15

Synspunkt

Tror og mener at vi gjør så godt vi kan med de ressursene vi har til rådighet.

Vi er godt i gang med å få på plass nødvendig dokumentasjon, utfordringen hos oss er å få på plass en avvikskultur i hele organisasjonen.

fortsetter ...

... fortsetter fra forrige side

Synspunkt

Saksbehandling foregår fortsatt periodisk pr epost - med sensitive data uten kryptering.

Politiattester flyter fritt"/ lagres i personalmapper som et klart brudd på gjeldende lover. For å nevne noe.

Kommuner/fylkeskommuner konkurrerer om å være mest mulig åpne, transparente og tilgjengelige, eks. på web (åpen postliste). I iveren etter å være best i klassenbrytes personvernet.

Ja det som er spennende er hvordan en skal forholde seg til særlovgivningene. I tillegg er det mange artikler som en også må ta hensyn til i den nye forordningen. En annen utfordring slik jeg ser på er kommunens kunnskap / kjennskap til verdikjeden til alle våre underleverandører, hvilke sårbarheter har de, avhengigheter etc.

Vi deltar i informasjonssikkerhetsprosjekt sammen med <... kommune>. Ved kommunesammenslåing i 2020 vil det foreligge system for internkontroll og felles personvernråd giver tilsettes mai 2018.

Vi opplever dessverre av og til at personopplysninger eller personsensitive opplysninger som blir mottatt eksternt på e-poster, kan bli videresendt internt i organisasjonen, opptil flere ganger. Her har vi absolutt et stort forbedringspotensiale.

Behandling av personopplysninger og informasjonssikkerhet er en del av internkontrollen vår. Vi ser at vi har byttet en del ledere og derfor igangsetter vi prosesser for å sikre kompetanse på området.

fortsetter ...

... fortsetter fra forrige side

Synspunkt

For mange kommuner er det å etablere (og vedlikeholde) en god oversikt over alle behandlinger en av de største utfordringene. Alle som har etablert internkontroll og rutiner for å følge Norm for informasjonssikkerhet har mye på plass, men det er en stor utfordring å få gehør for denne type arbeid ute hos de enkelte ledere.

Jeg savner kursing av kommunale personvernombud. Datatilsynets kurser er alt for "vide", og kurstilbudet burde spisses mot vår virksomhet.

I et tidlig spørsmål i undersøkelsen, framgår begrepet "system". Dette er et noe uklart begrep, også generelt utenfor denne undersøkelsen. Begrepsinnholdet bør defineres bedre for at man skal kunne svare nøyaktig på om man har - og i hvilken utstrekning - etablert et "system", og om dette etterleves. Både nedfelte rutiner, egen dataapplikasjon for systematisering, og uskrevne rutiner og prosedyrer som følges, kan oppfattes som "system". Derfor er dette litt vanskelig å gi svar på.

Små kommuner, som oss, har veldig lite ressurser til å gjøre denne jobben.

I tillegg til mangelfull kunnskap om personvern er det også sviktende kunnskap om risikostyring, virksomhetsstyring og internkontroll. I sum; toppledelsen i kommunen har ofte ikke den kunnskap som lover og regler forutsetter. Forankring og ledelsesinvolvering er utfordrende. Men, det brevet som ble sendt av Datatilsynets direktør til alle rådmenn for noen måneder siden har truffet godt. Selv om ikke kunnskapsnivået er overveldende, så er det fortsatt slik at et godt begrunnet brev fra tilsynsmyndighet sørger for at utfordringene blir identifisert, og arbeidet blir prioritert. Det brevet fra Bjørn Erik Thon må være det mest kosteffektive personverntiltaket i Norge så langt i 2017.

fortsetter ...

... fortsetter fra forrige side

Synspunkt

Spørsmål om alt etterleves er ikke et ja/nei/vet ikke- spørsmål når jeg svarer ja på Risikovurdering så vet jeg at det ikke er gjort over alt men delvis, men vi har system for det som er tilgjengelig for alle. dette gjelder flere av spm. i samme bolk.

På spørsmålet om vi har sletterutiner svarte jeg "vet ikkefordi det ikke er på plass overalt ennå.

C Utvalgt deskriptiv statistikk

C.1 Respondentene

C.1.1 Kommunestørrelse

Fordelingen av kommunene som deltok i undersøkelsen avviker ganske betydelig fra størrelsesfordelingen av kommuner på landsbasis. De største kommunene er overrepresentert i forhold til de mindre kommunene, slik det er illustrert i figur C.1 på neste side.

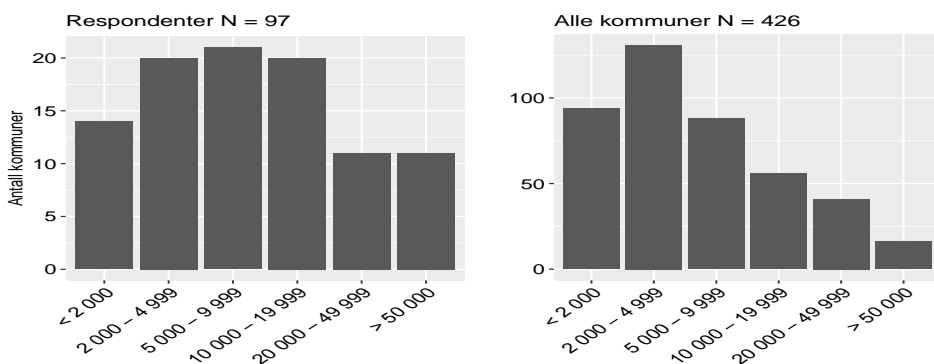
Tabell C.1: Antall svar (n) i forhold til kommuner (N) etter folketall

Folketall	N	N %	n	n %	Andel svar
< 2 000	94	21	14	14	15
2 000 - 4 999	131	30	20	21	15
5 000 - 9 999	88	20	21	22	24
10 000 - 19 999	56	13	20	21	36
20 000 - 49 999	41	9	11	11	27
> 50 000	16	4	11	11	69

Note: Andel – Prosentvis andel av kommunegruppen som har svart

C.1.2 Geografisk fordeling

Tabell C.2 på side 121 viser den geografiske fordelingen av deltakende kommuner. Antall kommuner som deltok i undersøkelsen spenner fra 12 av 23



Figur C.1: Svarfordeling i undersøkelsen (venstre bilde) sammenlignet med alle kommuner (høyre bilde)

kommuner (52 %) i Akershus til 1 av 24 kommuner (4 % i Nord-Trøndelag). Oslo og Svalbard svarte ikke og er ikke med i oversikten.

C.1.3 Rolle i kommunen/fylkeskommunen

Svaralternativene var fem kategorier. Nesten en tredjedel av de som svarte, fant ikke et egnet svaralternativ. Dels er disse tilpasset de eksisterende svaralternativene og dels er de lagt inn som nye grupper. De gruppene som er lagt til er arkivledere eller arkivmedarbeidere og personalsjefer/HR-medarbeidere. Ved denne omkodningen reduseres gruppen «Andre» til tre kategorier som ikke kunne innpasses i de eksisterende gruppene. Tabell C.3 på side 122 viser fordelingen.

C.1.4 Kommunestørrelse som indre faktor

Datatilsynets observasjoner er at kommunestørrelsen ikke skiller mellom hvilke kommuner som følger personopplysningsloven og hvilke som ikke gjør det (Datatilsynet, 2016). Kommunestørrelse er en indre faktor og ble testet i en bivariat regresjon med modenhet som avhengig og kommunestørrelse som uavhengig variabel. Nullhypotesen H_{0str} at modenhet er uavhengig av kommunestørrelse. Den alternative hypotesen H_{str} er at det vil være forskjell i egenvurdert modenhet mellom ulike kommunestørrelser.

Tabell C.2: Fylkesvis oversikt over svarandel

	Fylke	Antall kommuner	Antall svar	Andel (%)
1	Akershus	23	12	52.17
2	Østfold	19	9	47.37
3	Oppland	27	9	33.33
4	Buskerud	22	7	31.82
5	Vestfold	13	4	30.77
6	Rogaland	27	8	29.63
7	Vest-Agder	16	4	25.00
8	Møre og Romsdal	37	9	24.32
9	Nordland	45	10	22.22
10	Sør-Trøndelag	26	5	19.23
11	Aust-Agder	16	3	18.75
12	Sogn og Fjordane	27	5	18.52
13	Hedmark	23	4	17.39
14	Finnmark	20	3	15.00
15	Hordaland	34	5	14.71
16	Telemark	19	2	10.53
17	Troms	25	2	8.00
18	Nord-Trøndelag	24	1	4.17

Tabell C.3: Fordeling av respondentenes roller. N = 102

Rolle	Antall	Andel
Personvernombud	21	21.9%
Sikkerhetsansvarlig	18	18.8%
Kommunalsjef/tilsvarende	13	13.5%
Arkivleder/-medarbeider	12	12.5%
IKT-/infosikkerhetsansvarlig/ -medarbeider	11	11.5%
Kommunalsjef/tilsvarende	11	11.5%
Personalsjef/HR-medarbeider	10	9.7%
Rådmann/Administrasjonssjef	4	4.2%
Jurist	3	3.1%
Andre (kommunikasjonsleder, prosjektleder, Spes.ped leder)	3	3.1%

Kommunene ble delt i seks grupper etter innbyggertall som beskrevet i avsnitt 3.4.2 på side 33. Effekten av kommunestørrelse var ikke signifikant for noen kommunegruppe og med lave regresjonskoeffisienter og marginal forklaringskraft ($R^2 = 0.036$, se tabell C.4 på neste side) ble faktoren forkastet som ikke vesentlig.

C.2 Modenhet

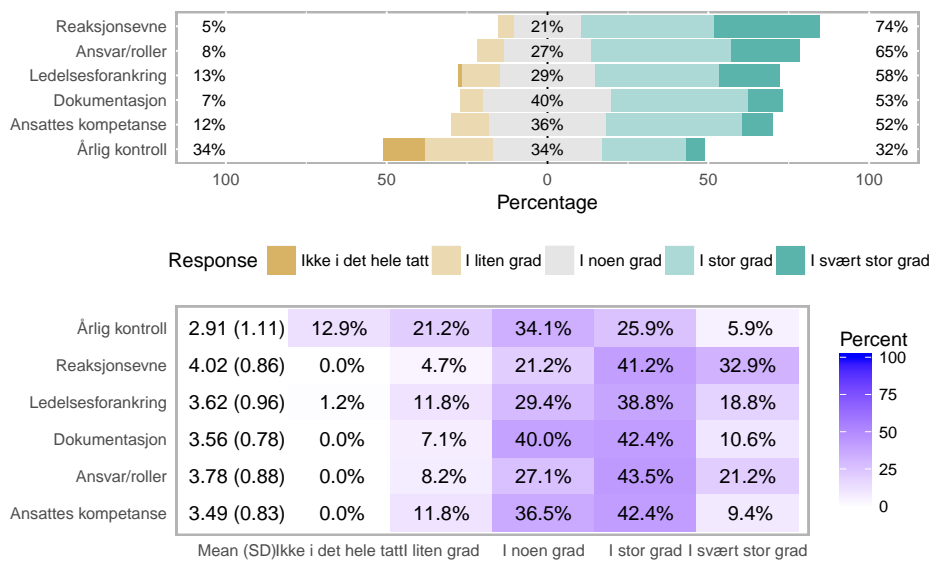
Diagrammene i figur C.2 og C.3 på side 125 viser svarfordelingen til respondentene med ulike perspektiv. Stolpediagramet angir andelen svar for hvert alternativ på likert-skalaen målt i prosent mens varmediagrammet angir prosentvis avgitte svar for hvert svaralternativ i prosent. Fordelingsdiagrammene viser fordelingen av svar på hvert spørsmål. Tendensen er at det laveste nivået (Ikke i det hele tatt) er i liten grad brukt annet enn for årlig kontroll av hvordan personopplysninger behandles. I dette spørsmålet er fordelingen tilnærmet normalfordelt med sentrum midt på skalaen. De øvrige er også normalfordelt, men med fordelingskurvens toppunkt til høyre for midten.

Tabell C.4: Modenhet vs kommunestørrelse. Lineær regresjon

	<i>Dependent variable:</i>
	modenhet2
k_str62 000 - 4 999	-0.174 (0.247)
k_str65 000 - 9 999	-0.165 (0.269)
k_str610 000 - 19 999	0.144 (0.251)
k_str620 000 - 49 999	-0.201 (0.276)
k_str6>50 000	-0.045 (0.284)
Constant	3.595*** (0.183)
Observations	80
R ²	0.036
Adjusted R ²	-0.029
Residual Std. Error	0.685 (df = 74)
F Statistic	0.550 (df = 5; 74)

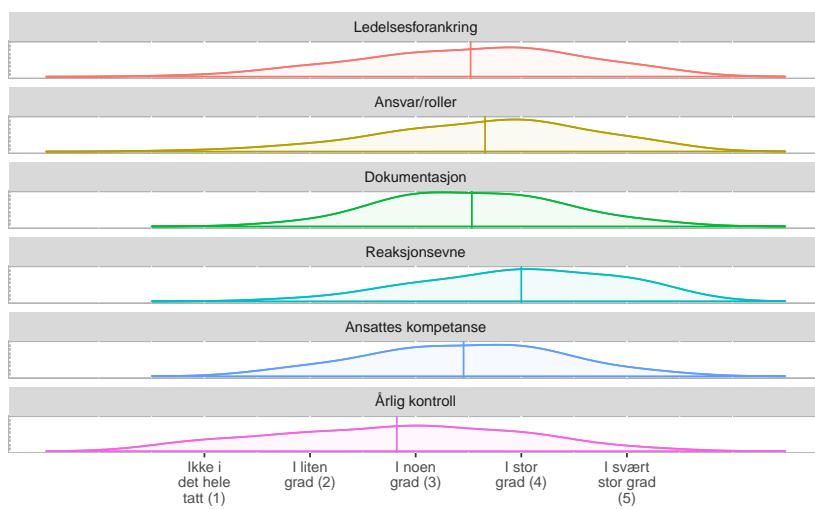
Note:

*p<0.1; **p<0.05; ***p<0.01



Figur C.2: Egenvurdering av modenhet – svarfordeling

Spørsmålet om kommunens reaksjonsevne er det som ligger lengst vekk fra midtpunktet.



Figur C.3: Egenvurdering av modenhet – spredning
