Styrets ansvar for aksjeselskapets etterlevelse av EUs personvernforordning (GDPR)

Betydningen av GDPR for styrets forvaltningsansvar etter aksjeloven § 6-12 og styremedlemmenes erstatningsansvar etter aksjeloven § 17-1

Kandidatnummer: 165

Antall ord: 14 883

JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

1. juni 2018

Innholdsfortegnelse

1 Innledning

1.1 Om avhandlingens tema og aktualitet

EUs personvernforordning, General Data Protection Regulation[1] (heretter "GDPR", "personvernforordningen" eller "forordningen"), trådte i kraft i EU den 25. mai 2018. Forordningens har satt personvern på agendaen og ført til økt bevisstgjøring rundt personvernets stilling. Alle selskaper som behandler personopplysninger har blitt tvunget til å ta stilling til hvordan de behandler personopplysninger i dag og til hvilke krav GDPR stiller til behandling av personopplysninger i selskapet for tiden fremover.

Personvernregelverk skal beskytte den enkelte mot at personvernet krenkes ved behandlingen av personopplysninger, i tillegg til at enkeltindividets personlige integritet skal ivaretas.[2] Når selskaper behandler personopplysninger forvaltes viktige verdier. Det er i samfunnets interesse at de selskapene som behandler disse verdiene forvaltes og ledes på en betryggende måte.[3] Det er derfor av vesentlig betydning at selskapene er klar over hvilke krav GDPR stiller, og hvilket ansvar som følger av forordningen. I dagens samfunn finnes det knapt noen teknologiske grenser for innsamling og bruk av personopplysninger. De rettslige rammene rundt hvordan disse opplysningene forvaltes blir desto viktigere.[4] Når personopplysninger forvaltes i stadig større grad og på nye måter, samtidig som et nytt og strengere regelverk om personvern gjør seg gjeldende, aktualiseres spørsmålet om selskapenes ansvar for personvernet.

Avhandlingens overordnede tema er betydningen av GDPR for styrets ansvar etter aksjeloven[5] (heretter "asl."). I dette ligger både en vurdering av betydningen for styrets ansvar for forvaltningen av selskapet etter asl. § 6-12, og en vurdering av styremedlemmenes personlige erstatningsansvar etter asl. § 17-1 første ledd. Personvernspørsmål løftes med GDPR fra IT-avdelingene og inn på styrerommene, hvilket aktualiserer spørsmålet om styrets ansvar og rolle ved manglende etterlevelse av personvernforordningens krav.

[1] Regulation (EU) of the European Parliament and 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).
[2] Prop. 1 S (2017-2018) s. 118.
[3] Norsk anbefaling eierstyring og selskapsledelse (2014) s.7.
[4] Prop. 1 S (2017-2018) s. 119.
[5] Lov 13. juni 1997 nr. 44 om aksjeselskaper (aksjeloven).

Det har de senere år vært en økning i antall fellende dommer om styreansvar,[6] og erstatningsansvar for styremedlemmene har gått fra å innebære en teoretisk mulighet for ansvar, til en reell risiko som styremedlemmene må forholde seg til.[7] Når personlig erstatningsansvar for styremedlemmene blir stadig mer aktuelt, er det nyttig og nødvendig å vurdere dette ansvaret i lys av nytt regelverk. De generelle forventingene til styrets profesjonalitet har økt de senere år, og spørsmålet om hvordan styret skal utøve sin funksjon som forvaltningsorgan for selskapene har vært tiltakende aktuelt. De senere års diskusjoner rundt eierstyring og selskapsledelse - corporate governance[8] - i norsk rett, bidrar ytterligere til å reise spørsmål om styret i aksjeselskap har en selvstendig rolle med hensyn til å legge til rette for at selskapet etterlever GDPR. Når den erstatningsrettslige vurderingen sentrerer rundt en ansvarsnorm som bygger på de forventninger som stilles til et alminnelig styremedlem, er det aktuelt å analysere hvorvidt disse forventingene endres med GDPR.[9]

Ny personopplysningslov ble vedtatt av Stortinget 22. mai 2018.[10] Ny personopplysningslov vil inkorporere personvernforordningen i norsk rett gjennom inkorporasjonsbestemmelsen i lovens § 1.[11] For at personvernforordningen kan tre i kraft som gjeldende norsk lov må den innlemmes i EØS-avtalen. Da forordningen pr. dato for innlevering av masteravhandlingen ikke er tatt inn i EØS-avtalen, gjelder den enda ikke direkte i Norge.[12] Dette er likevel av underordnet betydning for avhandlingens drøftelser, da forordningens regler uansett blir gjeldende i Norge så snart forordningen er innlemmet i EØS-avtalen og ny personopplysningslov trer i kraft. Videre i avhandlingen anvendes "personopplysningsloven (2000)" om gjeldende personopplysningslov[13] og "ny personopplysningslov" om personopplysningsloven som får virkning i Norge når personvernforordningen er innlemmet i EØS-avtalen.[14]

---

[6] Se eksempelvis dom fra Borgarting lagmannsrett fra mai 2018, LB-2016-181811, om en styreleder som ble holdt erstatningsansvarlig etter asl. § 17-1. Se også artikkel publisert på Rett24.no, *Advokat pålagt styreansvar etter Visit Moss-kollapsen.* (2018), http://rett24.no/articles/advokat-palagt-styreansvar-etter-visit-moss-kollapsen.
[7] Perland (2013) s. 1.
[8] Se Norsk anbefaling eierstyring og selskapsledelse (2014).
[9] Perland (2013) s. 1-2.
[10] Lovvedtak 54 (2017-2018). Stortingets vedtak bifalt ved andre gangs behandling 28. mai 2018, se https://www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Referater/Stortinget/2017-2018/refs-201718-05-28?all=true. Det er ikke fastsatt tidspunkt for lovens ikrafttredelse.
[11] Se forslag til ny personopplysningslov i Prop. 56 LS (2017-2018).
[12] Innlemmelse i EØS-avtalen forutsetter at alle EØS/EFTA-land har vedtatt EØS-komiteens beslutning og opphevet eventuelle konstitusjonelle forbehold. Se for øvrig Justisdepartementets uttalelse https://www.regjeringen.no/no/aktuelt/nar-far-vi-ny-personopplysningslov/id2599511/.
[13] Lov 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven).
[14] Se forslag til ny personopplysningslov i Prop. 56 LS (2017-2018).

1.2 Problemstilling

Avhandlingens problemstilling er betydningen av GDPR for styrets forvaltningsansvar etter aksjeloven § 6-12 og, i forlengelsen av dette, betydningen av GDPR for styremedlemmenes erstatningsansvar etter aksjeloven § 17-1. Ved vurderingen av GDPRs betydning for styremedlemmenes erstatningsansvar er det sentralt å se på hvilke plikter og ansvar som påhviler styret etter asl. § 6-12, og hvordan disse pliktene og ansvaret eventuelt endres eller skjerpes med personvernforordningen. Ansvaret som pålegges styret etter asl. § 6-12 danner grunnlaget for vurderingen av vilkåret om ansvarsgrunnlag etter erstatningsregelen i asl. § 17-1.

Med GDPR innføres blant annet skjerpede krav til iverksetting av retningslinjer for vern av personopplysninger, nye krav til internkontroll og strengere krav til informasjonssikkerhet, jf. GDPR artikkel 24, 30 og 32. For enkelte virksomheter stilles det krav om at selskapet har personvernombud[15] jf. forordningens artikkel 37 flg. Videre har Datatilsynet etter GDPR artikkel 83 hjemmel for å ilegge høye bøter ved brudd på forordningen, i tillegg til at andre typer sanksjoner kan anvendes ved manglende etterlevelse.[16] De overordnede prinsipper for behandling av personopplysninger følger av GDPR artikkel 5. Etter GDPR er selskapet som juridisk person pliktsubjekt og det er selskapet som er behandlingsansvarlig etter forordningen. Spørsmålet avhandlingen søker å avklare nærmere, er *hvem* i et aksjeselskap som mer konkret har ansvar for at de overordnede prinsippene i forordningen etterleves og gjennomsyrer den behandlingen av personopplysninger som skjer i selskapet, og om dette ansvaret kan tillegges styret og styremedlemmene i medhold av aksjeloven § 6-12. Det privatrettslige styreansvaret etter aksjeloven ligger i utgangspunktet utenfor Datatilsynets tilsynsområde, men overtredelser av GDPRs bestemmelser kan utløse Datatilsynets påleggs- og beleggingskompetanse.

Der selskapet bøtelegges, oppstår spørsmålet om selskapet i enkelte tilfeller kan søke erstatning fra styremedlemmene personlig jf. asl. § 17-1. Erstatningsansvar for styremedlemmene er aktuelt dersom overtredelsen og dermed boten er et resultat av manglende forsvarlig forvaltning av selskapet etter asl. § 6-12.

[15] Den opprinnelige norske oversettelsen av forordningen anvendte begrepet "personvernrådgiver". I Prop. 56 LS (2017-2018) s. 126 fremholdes det at termen "personvernombud" benyttes i loven og den norske oversettelsen av forordningen. Dette innebærer en videreføring av gjeldende terminologi.
[16] Se eksempelvis forslag til ny personopplysningslov, Prop. 56 LS (2017-2018) § 29 om tvangsmulkt.

Avhandlingens tittel omtaler styrets ansvar for etterlevelse av GDPR. I spørsmålet om ansvar for etterlevelse ligger også et spørsmål om ansvar for tilstrekkelig og korrekt implementering av forordningens krav i selskapet. I det videre vil styrets ansvar både for implementering og etterlevelse omtales.

1.3 Rettskilder og metodiske utfordringer

Avhandlingen tar utgangspunkt i de kravene som fremgår direkte av GDPR med fortale, da forordningen vil gjelde direkte som norsk lov, og det er begrenset rom for nasjonale tilpasninger. Forordningens fortale utdyper forordningens bakgrunn og innhold. De tilpasninger og tilføyelser som gjøres i ny personopplysningslov er av underordnet betydning for avhandlingens tema og problemstilling.

Styrets forvaltnings- og erstatningsansvar for etterlevelse av personvernregelverk er en ny og umoden problemstilling i norsk (selskaps)rett, og rettskildebildet er fragmentert. Det finnes mange rettskilder om styrets ansvar for forsvarlig forvaltning av selskapet etter aksjeloven § 6-12 og om styremedlemmenes erstatningsansvar etter aksjeloven § 17-1. Likeså finnes mye litteratur om GDPR, både i form av bøker og artikler og ulike uttalelser og veiledere. Det er likevel begrenset kildetilfang på personvernforordningens område, da det er tale om et nytt regelverk hvor det enda ikke foreligger aktuell rettspraksis.

Pr. dato for avhandlingens innlevering foreligger en uoffisiell norsk oversettelse av forordningen inntatt i forslag til ny personopplysningslov i Prop. 56 LS (2017-2018). Det ventes at denne oversettelsen blir offisiell. I det følgende siteres det, av hensyn til leservennlighet, fra forordningens norske oversettelse når det siteres direkte fra forordningen. Vurderingene og argumentasjonen baseres på overordnede prinsipper og krav etter forordningen, slik at enkeltbestemmelsers konkrete ordlyd ikke er avgjørende.

I avhandlingen anvendes ulike typer av juridisk litteratur. Herunder Norsk anbefaling for eierstyring og selskapsledelse[17], Artikkel 29-gruppens retningslinjer[18], uttalelser fra EU-kommisjonen og Datatilsynets veiledere for implementering av GDPR i norske selskaper. I mangel på andre autoritative rettskilder rundt fortolkningen av GDPR blir slike anbefalinger,

[17] Tilgjengelig på www.nues.no.
[18] EUs rådgivende organ i personvernspørsmål, se under.

retningslinjer og veiledere av vesentlig betydning for å forstå og diskutere forordningens innhold.

Den norske anbefalingen for eierstyring og selskapsledelse ("NUES") retter seg i første rekke mot selskaper med aksjer notert på regulerte markeder i Norge (allmennaksjeselskap).[19] I avhandlingen anses NUES å gi utrykk for enkelte overordnede prinsipper og tanker om hvordan selskaper bør ledes og organiseres. Anbefalingen kaster også lys over styrets ansvar og selskapets samfunnsansvar. Selv om avhandlingen er begrenset til aksjeselskap,[20] og de plikter som følger av aksjeloven, antas at mange av de av tankene og føringene anbefalingen legger til grunn gjør seg gjeldende også for aksjeselskap. NUES ble for første gang utgitt i 2004 og sist revidert i 2014. Anbefalingen er ikke rettslig bindende, men er i praksis viktig som uttrykk for bransjepraksis.[21]

Artikkel 29-gruppen er EUs rådgivende organ i personvernspørsmål, nedsatt med hjemmel i det tidligere personverndirektivet[22] artikkel 29. Gruppens mandat var opprinnelig å tolke og konkretisere innholdet i personverndirektivet fra 1995, men er nå utvidet til også å omfatte personvernforordningen. Artikkel 29-gruppen har vedtatatt ulike uttalelser og anbefalinger om hvordan bestemmelsene i personvernforordningen bør forstås og håndheves.[23] Artikkel 29-gruppens veiledninger er ikke rettslig bindende, men er anbefalinger til datatilsynene og til de selskapene som favnes av forordningen.

1.4 Avgrensninger

Avhandlingen begrenses til kun å behandle erstatningskrav fra selskapet mot styremedlemmene etter asl. § 17-1 første ledd, og det avgrenses således mot erstatningskrav etter det alminnelige ulovfestede culpaansvaret og det ulovfestede organansvaret. Det avgrenses videre mot erstatningskrav reist mot selskapet av enkeltpersoner, der enkeltpersoner har lidd skade/økonomisk tap som følge av personvernbrudd hos selskapet, jf. også GDPR artikkel 82.

[19] Norsk anbefaling eierstyring og selskapsledelse (2014) s.7.
[20] Om avgrensning mot allmennaksjeselskap se kapittel 1.4.
[21] Woxholt (2012) s. 119.
[22] Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data.
[23] Datatilsynet (2017), *Artikkel 29-gruppen om de nye reglene i personvernforordningen*, https://www.datatilsynet.no/regelverk-og-skjema/lover-og-regler/uttalelser-fra-artikkel-29-gruppen/eus-personverngruppe-om-innspill-forordningen/.

Videre begrenses avhandlingen til kun å vurdere styrets plikter og ansvar etter asl. § 6-12, og det avgrenses også mot øvrig selskapslovgivning. Når avhandlingen omtaler "selskap" siktes det til aksjeselskap. Avhandlingen avgrenser mot allmennaksjeselskap som selskapsform. Mye av det som i avhandlingen skrives om styrets forvaltnings- og erstatningsansvar i aksjeselskap vil likevel være sammenfallende med hva som gjelder i allmennaksjeselskap.

Når det reises spørsmål om styremedlemmenes erstatningsansvar overfor selskapet, ses det i det følgende bort fra adgangen til å avtale begrensninger i styremedlemmenes erstatningsansvar, adgangen til å tegne styreansvarsforsikring samt andre former for ansvarsfrihet. Styremedlemmenes erstatningsansvar etter § 17-1 er individuelt for hvert enkelt styremedlem. For enkelhets skyld vil det i hovedsak vises samlet til "styrets erstatningsansvar".

GDPR stiller mange krav til selskapene, men å belyse disse i sin helhet vil sprenge avhandlingens rammer. For å belyse avhandlingens problemstilling, er fire sentrale artikler fra GDPR valgt ut for å eksemplifisere og belyse styrets forvaltnings- og erstatningsansvar. Styrets ansvar vil kunne variere etter andre bestemmelser, både i forordningen selv og i øvrig lovverk.

Enkelte plikter etter forordningen gjelder eksempelvis kun for offentlige organ,[24] mens andre plikter kun kommer til anvendelse der selskapet har mer enn 250 ansatte.[25] For avhandlingens vedkommende ses bort fra disse begrensninger, da dette ikke er av betydning for avhandlingens mer generelle drøftelse av styrets rolle i etterlevelse av ulike bestemmelser i GDPR. Typen av aksjeselskap varierer stort i type og størrelse, slik at enkelte aksjeselskap også vil favnes av bestemmelsene som inneholder slike begrensninger.

Hva gjelder behandling av personopplysninger, kan selskapet i henhold til forordningen opptre som behandlingsansvarlig eller databehandler, avhengig av om selskapet behandler personopplysninger på egne eller andres vegne.[26] Etter GDPR pålegges databehandleren i mange tilfeller de samme plikter som behandlingsansvarlig hva gjelder krav til hvordan personopplysninger behandles, dokumentasjonskrav med videre. Kravene som stilles til styrene i selskapene vil dermed i praksis ofte være de samme. For både behandlingsansvarlig

[24] Eksempelvis en ubetinget plikt til å utnevne personvernombud etter GDPR artikkel 37.
[25] Eksempelvis gjelder GDPR artikkel 30 om protokollføring kun for selskap med over 250 ansatte.
[26] Jf. også GDPR artikkel 4 nr. 7 og nr. 8. Nærmere om hva som menes med "behandlingsansvarlig" i kapittel 2.3.2.

og databehandler gjelder at behandlingen av personopplysninger skal foregå på en måte som sikrer et tilstrekkelig beskyttelsesnivå og også slik at forordningens øvrige regler overholdes.[27] Avhandlingen begrenses til å omhandle styrets plikter i de tilfeller hvor selskapet opptrer som behandlingsansvarlig.

Av forordningens fortale avsnitt 18 fremgår det at forordningen ikke får anvendelse på behandling av personopplysninger som utføres av fysisk person i forbindelse med rent personlige eller familiemessige aktiviteter, og som av den grunn ikke er knyttet til forretningsvirksomhet. For avhandlingens vedkommende forutsettes at alle aksjeselskap driver forretningsvirksomhet slik at selskapet underlegges kravene i GDPR.

Under vurderingen av GDPR sin betydning for styremedlemmenes erstatningsansvar etter asl. § 17-1 belyses denne problemstillingen og de vilkår som oftest er problematiske, fordi spørsmål om erstatningsansvar er en naturlig følge av eventuelle endringer i styrets forvaltningsansvar. Denne delen av avhandlingen går mindre i dybden enn vurderingen av forvaltningsansvaret etter asl. § 6-12, og må anses for å være en inngangsport til en drøftelse av spørsmålet om personlig erstatningsansvar for styremedlemmene i lys av brudd på personvernforordningen.

1.5 Fremstillingen videre

I kapittel 2 vil det kort redegjøres for bakgrunnen for nytt personvernregelverk samt hvilke nye krav selskapene pålegges med GDPR. Herunder vil ansvarsfordelingen etter GDPR presenteres.

I kapittel 3 behandles styrets rolle ved etterlevelse av personvernregelverket. Her vil styrets ansvar for forvaltning av selskapet etter asl. § 6-12 utpensles, og det vil vurderes om det i dette ansvaret også ligger et ansvar for ivaretakelse av personvernregelverket. Deretter vil styrets rolle ved og ansvar for etterlevelse av personvernforordningen analyseres ved hjelp av fire utvalgte artikler fra GDPR. Det vil vurderes hvilket ansvar styret har etter den generelle ansvarsbestemmelsen i GDPR artikkel 24, for protokollføring etter artikkel 30, for informasjonssikkerhet etter artikkel 32, og for personvernombudets stilling etter artikkel 38.

[27] Prop. 56 LS (2017-2018) s. 108.

I kapittel 4 behandles sammenhengen mellom styremedlemmenes erstatningsansvar etter aksjeloven § 17-1 og manglende etterlevelse av GDPR. Vilkårene for erstatning om økonomisk tap, ansvarsgrunnlag, herunder hvilken aktsomhetsnorm som påhviler styremedlemmene, og årsakssammenheng gjennomgås.

I kapittel 5 sammenfattes så GDPR sin betydning for styremedlemmenes forvaltningsansvar etter asl. § 6-12 og styremedlemmenes erstatningsansvar etter asl. § 17-1.

2 General Data Protection Regulation (GDPR)

2.1 Bakgrunnen for ny forordning

Teknologisk utvikling og økt grad av digitalisering de senere år har ført til en drastisk økning i omfanget av personopplysninger som behandles, samt en tilsvarende økning i utveksling av personopplysninger mellom virksomheter og over landegrensene.[28] Når teknologien muliggjør bruk av personopplysninger på nye måter, og fysiske personer i større grad enn tidligere gjør tilgjengelig sine personopplysninger, medfører dette nye muligheter for handel og næringsliv, men også større trusler for personvernet.[29]

Det tidligere personverndirektivet fra 1995 ble implementert gjennom nasjonal lovgivning i hvert enkelt land. Dette førte til fragmentert personvernlovgivning i Europa. Reglene var ulike og ble håndhevet forskjellig. Dette ga et behov for harmonisering av personvernregelverket i Europa, og et ønske om en enhetlig og samsvarende lovgivning.[30] Ved fremleggelse av forslaget til ny personvernforordning i 2012 viste EU-kommisjonen til at det teknologiske landskapet er betydelig endret siden personverndirektivet (som nå oppheves og erstattes) trådte i kraft, og at personopplysninger i dag samles inn, brukes og overføres på andre måter og i helt annen målestokk enn tidligere.[31] Det var derfor behov for en oppdatering av det europeiske personvernregelverket for fortsatt å kunne ivareta den enkeltes personvern.[32]

Ønsket med innføringen av GDPR er å skape et ansvarsbasert, modernisert og forenklet regelverk. Dette fremgår også av forordningens fortale avsnitt 170. Personvernforordningens tekst virker direkte i det enkelte medlemsland, og GDPR gir begrenset rom for nasjonal tilpasning, noe som fører til et mer helhetlig personvernregelverk i Europa. Dette betyr igjen at alle europeiske selskaper må forholde seg til de samme reglene.

[28] Gimmingsrud (2017) s. 3.
[29] Gimmingsrud (2017) s. 3.
[30] Rüker/Kugler (2018) s. 1.
[31] Justis- og beredskapsdepartementet (2017) *Høringsnotat – Ny personopplysningslov* s. 9.
[32] Justis- og beredskapsdepartementet (2017) *Høringsnotat – Ny personopplysningslov* s. 9.

2.2 Overordnet om hva nytt forordningen bringer med seg for selskapene

Personvernforordningen innebærer ingen substansiell endring i de grunnleggende krav til behandling av personopplysninger som fulgte av personverndirektivet fra 1995.[33] Nytt med GDPR er at fokuset skiftes fra forhåndskontroll hos tilsynsmyndighetene til ansvarlighet hos selskapet selv.[34] Forordningen bringer med seg betydelig større grad av ansvar for behandlingsansvarlig enn hva som var tilfelle etter personverndirektivet.[35] Dette fordrer at selskapene må implementere nye strukturer og prosesser for å tilfredsstille nye krav.[36]

Forordningen vil gjøre det enklere for norske nærlingslivsaktører å operere internasjonalt i EU/EØS når regelverket i Europa harmoniseres.[37] Dette gir et naturlig incitament for selskapene til å opptre i tråd med de krav forordningen oppstiller. I GDPR artikkel 83 gis hjemmel for Datatilsynet til å ilegge høye bøter ved brudd på enkelte av forordningens krav.[38] Adgangen til å ilegge administrative bøter er en sentral nyvinning med forordningen og skal, sammen med andre sanksjoner, være et kraftig verktøy i arbeidet med å håndheve forordningen.[39]

Det er viktig at selskaper sørger for at personopplysninger behandles ikke bare på en måte som møter kravene som eksplisitt oppstilles i bestemmelser i GDPR, men også at behandlingen skjer i samsvar med de grunnleggende prinsipper for behandling av personopplysninger som følger av GDPR artikkel 5. Av artikkel 5 følger prinsipper om lovlighet, rettferdighet og åpenhet, formålsbegrensning, dataminimering, riktighet, lagringsbegrensning, integritet og konfidensialitet og ansvar.[40] Disse prinsippene må gjennomsyre all behandling av personopplysninger som skjer i selskapet.

For å sørge for at prinsippene overholdes, stiller GDPR i artikkel 24 krav til at selskapene utarbeider retningslinjer for behandling av personopplysninger. Videre er det et krav etter artikkel 30 at selskapet fører protokoll over de behandlingsaktiviteter som foretas. I henhold til artikkel 32 skal selskapene sørge for tilstrekkelig grad av informasjonssikkerhet.

[33] Communication from the commission to the European Parliament (2018) s. 9 og Innst. 278 L (2017-2018) s. 9
[34] Innst. 278 L (2017-2018) s. 8.
[35] Guidelines on the application and setting of administrative fines (2017) s. 13.
[36] Rüker/Kugler (2018) s. 105.
[37] Justis- og beredskapsdepartementet (2017) *EØS-notat.*
[38] Nærmere om bøtesatsene i kapittel 4.2.1.
[39] Guidelines on the application and setting of administrative fines (2017) s. 4.
[40] Rüker/Kugler (2018) s. 50-74 og Skullerud, Rønnevik, Skorstad m.fl. (2018) s. 75-79.

Ytterligere pålegges enkelte virksomheter etter artikkel 37 å utnevne et personvernombud for å sikre systematisk oppfølging av de pliktene forordningen pålegger selskapet.[41] Disse bestemmelsene presenteres nærmere i kapittel 3.2 flg.

En viktig presisering ligger i at det innenfor rammen av hva som klassifiseres som aksjeselskap, finnes store variasjoner i typen av virksomhet som drives og selskapenes størrelse. I dette ligger at det vil variere fra selskap til selskap hvilken type behandling av personopplysninger som foregår, og i hvilken skala dette gjøres. Et forsikringsselskap med bredt kundetilfang vil for eksempel behandle helt andre typer av opplysninger og i mye større skala enn et aksjeselskap med få ansatte som i mindre grad behandler kundeopplysninger. Alle deler av GDPR vil ikke være like relevant for alle aksjeselskap. Selskapene har derfor en viktig jobb å gjøre i å bestemme hvilke krav etter GDPR som treffer selskapet direkte og hvilke tiltak som må iverksettes for å overholde de aktuelle krav.[42] Videre er mange av kravene etter GDPR risikobasert, slik at hvilke tiltak som skal iverksettes for å etterleve kravene vil variere med hvilke risiki det enkelte aksjeselskapet står overfor.

2.2.1 Data protection compliance program / internkontrollprogram

GDPR stiller strenge krav til at selskapene kan dokumentere at kravene i forordningen etterleves og til at selskapene kan vise at de har "orden i eget hus". At selskapene pålegges internkontroll er ikke i seg selv nytt, men derimot et vanlig verktøy for å sikre at lovverk etterleves. Med internkontroll siktes her til systematiske tiltak som sikrer at selskapet planlegger, organiserer og utfører sin virksomhet i samsvar med gjeldende regelverk.[43] Internkontroll er ledelsens redskap for å styre virksomheten på en forsvarlig og lovlig måte.[44] En rekke ulike regelverk pålegger selskapene krav om internkontroll.[45] Eksempelvis nevnes

[41] Skullerud, Rønnevik, Skorstad m.fl. (2018) s. 226.
[42] Rüker/Kugler (2018) s. 8.
[43] Regelhjelp.no (2017), http://www.regelhjelp.no/Emner-A---A-/Internkontroll/.
[44] Datatilsynet – En veiledning om internkontroll og informasjonssikkerhet s. 7. Veilederen er basert på personopplysningsloven (2000), men Datatilsynet fremholder at grunnprinsippene i veilederen er i tråd med de nye reglene som følger av personvernforordningen, se mer på https://www.datatilsynet.no/regelverk-og-skjema/veiledere/internkontroll_informasjonssikkerhet/.
[45] Veum (2010) s. 204.

personopplysningsloven (2000) § 14, personopplysningsforskriften[46] kapittel 3, forskrift om risikostyring og internkontroll[47] og ulike bestemmelser i arbeidsmiljøloven.[48]

Formålet med interkontroll etter GDPR er å sørge for at behandlingen av personopplysninger i selskapet til enhver tid skjer i samsvar med gjeldende personvernregelverk. Internkontrollen skal typisk inneholde selskapets dokumentasjon på at behandlinger skjer i tråd med regelverket, at det finnes interne rutiner for å sikre dette, samt at revisjons- og kontrollrutiner er på plass.[49] Det kan være hensiktsmessig for selskapet å benytte et felles system for å tilfredsstille internkontrollplikter etter ulike lovverk.[50]

Utarbeidelse av velfungerende systemer for internkontroll virker preventivt i den forstand at ansatte og de ulike organer i selskapet vet at misligheter oppdages. På den måten kan ansvaret kanaliseres dit det hører hjemme.[51] Internkontrollen deles normalt inn i tre deler. En styrende del, en gjennomførende del og en kontrollerende del.[52] De overordnede valg skal dokumenteres i den styrende delen.[53]

Internkontroll er et kvalitetssystem for etterlevelse av regelverk,[54] og et kontinuerlig arbeid i så måte. Arbeidet må årlig revideres, og ledelsen må vurdere om rutinene følges og er funksjonelle og om det har skjedd endringer i regelverket. Dette siste er særlig aktuelt i avhandlingens sammenheng, når det med GDPR innføres strengere krav til internkontroll. Videre må det vurderes om risikobildet er endret, eller om selskapet behandler nye personopplysninger på nye måter. [55]

I GDPR kommer kravet til internkontroll og at denne kontrollen kan dokumenteres til uttrykk i flere bestemmelser.[56] Artikkel 30 stiller krav til at det kartlegges hvordan personopplysninger behandles i selskapet, at avvik kommer frem i lyset og at det utarbeides

[46] Forskrift 15. desember 2000 nr. 1265 om behandling av personopplysninger (personopplysningsforskriften).
[47] Forskrift 22. september 2008 nr. 1080 om risikostyring og internkontroll.
[48] Lov 17. juni 2005 nr. 62 om arbeidsmiljø, arbeidstid og stillingsvern mv. (arbeidsmiljøloven). Også lov 13. mars 1981 om vern mot forurensning og om avfall (forurensningsloven) § 52 b om adgang til å gi forskrift om interkontroll kan nevnes i denne sammenheng.
[49] Veum (2010) s. 205.
[50] Datatilsynet – En veiledning om internkontroll og informasjonssikkerhet s. 6.
[51] Bugge Reiersen (2007) s. 38.
[52] Veum (2010) s. 206.
[53] Veum (2010) s. 206.
[54] Datatilsynet – En veiledning om internkontroll og informasjonssikkerhet s. 7.
[55] Datatilsynet – En veiledning om internkontroll og informasjonssikkerhet s. 9.
[56] Se særlig kapittel 3.2.1 og 3.2.2 om GDPR artikkel 24 og 30 for nærmere redegjørelse rundt styrets ansvar i å sikre selskapets internkontroll etter GDPR.

protokoller over de behandlingsaktiviteter som utføres. Dette er internkontrollen i sin kjerne. Bestemmelsen forutsetter dokumentasjon på at rutiner og prosedyrer etter forordningen er implementert. Likeså følger det av GDPR artikkel 32 et krav om at tekniske og organisatoriske tiltak skal gjennomføres for å oppnå et egnet informasjonssikkerhetsnivå, sett hen til risikoen. Det ligger i bestemmelsens karakter at det må foreligge dokumentasjon på at tekniske og organisatoriske tiltak er iverksatt. Dokumentasjonen som utarbeides kan ved behov forelegges Datatilsynet for å bekrefte at selskapet opptrer i tråd med forordningen, jf. også GDPR artikkel 30 nr. 4.

Videre følger det av GDPR artikkel 24 at behandlingsansvarlig i enkelte tilfeller skal iverksette retningslinjer for vern av personopplysninger. Også slike retningslinjer må være dokumenterbare, og har effekt ikke bare som bekreftelse overfor Datatilsynet, men også for internt virke. Skal selskapet etterleve forordningen, må det føres kontroll med at hver enkelt ansatt arbeider i henhold til de krav GDPR stiller. Videre er også personvernombudet, som skal utnevnes i medhold av GDPR artikkel 37, et ledd i selskapets internkontroll.

Det kan dermed hevdes at GDPR i sin kjerne innfører et data protection compliance-program eller et internkontrollprogram. Interkontroll og dokumentasjonskrav er den store nyvinningen med GDPR. Kravene til internkontroll gjør at det er viktig å klargjøre hvor dette ansvaret ligger, og hvem som har ansvar for å sikre at brudd på forordningen ikke forekommer.

2.3 Ansvar for etterlevelse av GDPR

2.3.1 Om ansvarsfordeling etter GDPR

Det nye personvernregelverket legger stor vekt på ansvarlighet i virksomhetene.[57] Ansvarlighet er et grunnleggende konsept i GDPR, og det uttrykkes et gjennomgående, overordnet og viktig ansvarsprinsipp i forordningen. Dette kommer klart til uttrykk gjennom eksempelvis GDPR artikkel 5, 24, 30 og 32. Av forordningens fortale avsnitt 79 fremgår at vern av de registrertes rettigheter og friheter samt fordeling av den behandlingsansvarliges ansvar, krever en tydelig fordeling av ansvar i henhold til forordningen. Det som her fremgår av fortalen tas til inntekt for at det er viktig å presisere hvilke krav som stilles til roller og ansvarsfordeling i selskapet for å sikre etterlevelse av forordningen. Til tross for dette er

[57] Datatilsynets veileder – Virksomhetens ansvar etter nytt regelverk s. 1.

forordningen vag og uklar hva gjelder hvor ansvaret for etterlevelse av forordningen plasseres.

Der selskapene tidligere måtte få konsesjon fra Datatilsynet for behandling av personopplysninger, legger GDPR en større del av ansvaret på selskapene selv. Spørsmålet som da oppstår er hvem som egentlig er ansvarlig for at selskapet opptrer ansvarlig etter forordningen. Etter GDPR artikkel 5 nr. 2 er det den behandlingsansvarlige som er ansvarlig for at prinsippene i artikkel 5 overholdes. For å avgjøre GDPRs betydning for styremedlemmenes forvaltnings- og erstatningsansvar er det helt sentralt å klargjøre hvor ansvaret for etterlevelse av GDPR plasseres innad i det enkelte selskap.

2.3.2 Pliktsubjekt og behandlingsansvarlig etter GDPR

Det følger av GDPR artikkel 4 nr. 7 at den behandlingsansvarlige er en "*fysisk eller juridisk person*" som "*alene eller sammen med andre*" bestemmer "*formålet med behandlingen og hvilke midler som skal benyttes*". Den behandlingsansvarlige har hovedansvaret for etterlevelse av personvernforordningen.[58] Det er den behandlingsansvarlige som pålegges plikter etter GDPR.

Med mindre det er klare indikasjoner på at en enkeltansatt i selskapet skal ansvarliggjøres etter forordningen, for eksempel der vedkommende har misbrukt personopplysninger til egen vinning, er det selskapet som subjekt og juridisk person som anses å være ansvarlig for behandlingen av personopplysninger.[59] Behandlingsansvarlig etter GDPR er selskapet selv.

Spørsmålet som så søkes besvart er *hvem* i selskapet som er behandlingsansvarlig.

Etter personopplysningsloven (2000) § 2 nr. 4 er behandlingsansvarlig definert som "*den som bestemmer formålet med behandlingen av personopplysninger*". Innholdet i denne definisjonen er i det vesentlig det samme som etter GDPR artikkel 4 nr. 7, og det er relevant å se hen til forarbeider og kilder etter personopplysningsloven (2000) for aspekter som kan belyse spørsmålet om hvem som er behandlingsansvarlig.

Dag Wiese Schartum skriver i note 10 til personopplysningsloven (2000) § 2 nr. 4 på Rettsdata at behandlingsansvar betegner en formell posisjon i virksomheten, hvilket

[58] Rüker/Kugler (2018) s. 24.
[59] Rüker/Kugler (2018) s. 105.

innebærer krav til etterlevelse av en rekke plikter i loven.[60] Han skriver videre at den instans innen et hierarki med den øverste instruksjonsmyndigheten ofte vil være behandlingsansvarlig. Der behandlingen av personopplysninger skjer i regi av en bedrift, vil vedkommende selskaps øverste ledelse være behandlingsansvarlig. Schartum skriver at "*dette innebærer at behandlingsansvaret i store organisasjoner må plasseres høyt over de nivåer i organisasjonen som har daglig ansvar*."

Samme synspunkt følger av forarbeidene til personopplysningsloven (2000) § 2.[61] Her fremgår at det formelle ansvaret for at de plikter som pålegges den behandlingsansvarlige oppfylles ligger hos selskapets ledelse.

Etter asl. § 6-12 legges ansvaret for forvaltningen av selskapet til selskapets styre, og etter asl. § 6-13 gis daglig leder ansvar for den daglige ledelse av selskapet. Når Wiese Schartum skriver at behandlingsansvaret i selskapet "*må plasseres høyt over de nivåer*" som har daglig ansvar, tas dette til inntekt for at behandlingsansvaret i siste rekke må plasseres hos selskapets styre.

Spørsmålet blir dermed om ansvaret GDPR pålegger den behandlingsansvarlige nærmere kan plasseres hos selskapets styre.

Når GDPR plasserer ansvaret hos selskapet, og det med selskap i denne avhandlingen menes aksjeselskap, må ansvarsplasseringen etter GDPR tolkes i lys av aksjelovgivningen. Styret er selskapets øverste ledelse, og har etter asl. § 6-12 et særskilt ansvar for forsvarlig forvaltning av selskapet. Hvem som er behandlingsansvarlig må følgelig drøftes i lys av aksjeloven og særlig § 6-12.[62]

Styrets kompetanse omfatter i utgangspunktet all ledelse av selskapet som ikke i medhold av lov, vedtekter eller beslutning av generalforsamlingen hører under andre organer.[63] Når ansvaret etter GDPR tillegges selskapet, og det ikke er holdepunkter i forordningen som legger ansvaret til et annet organ eller person, må det med selskapet, i lys av aksjelovgivningen, menes styret. Dette støttes av EU-kommisjonens uttalelse fra januar 2018 hvor det fremgår at det i prosessen med å sikre etterlevelse av GDPR er viktig å involvere

[60] Schartum (2012) note 10.
[61] NOU 1997: 19 s. 132 og Ot.prp. nr. 92 (1998-1999) s. 97.
[62] Nærmere om bestemmelsens innhold i kapittel 3.
[63] Bråthen (2013) s. 152.

selskapet øverste ledelse i utarbeidelsen av selskapet retningslinjer for etterlevelse av forordningen.[64]

Når behandlingsansvaret etter ordlyden i GDPR tillegges selskapet, må det med dette, basert på overstående drøftelse, menes styret hva gjelder for behandlingsansvar i aksjeselskap.[65] Det legges i det videre til grunn at styret er øverste behandlingsansvarlig i aksjeselskap. I praksis vil det naturlig være slik at dette ansvaret delegeres,[66] men det er styret som har det øverste ansvaret for at personvernforordningen etterleves i selskapet og som pålegges plikter etter personvernforordningen.

[64] Communication from the commission to the European Parliament and the council (2018) s. 9.
[65] Reglene om felles behandlingsansvarlige etter GDPR artikkel 26 og behandlingsansvar i konsernforhold presenteres ikke nærmere i denne avhandlingen.
[66] Schartum (2012) note 10.

3 Styrets rolle i selskapets etterlevelse av GDPR

Som det fremgår av drøftelsen i kapittel 2.3.2 pålegges styret i et aksjeselskap, i kraft av sin rolle som behandlingsansvarlig, plikter og ansvar etter GDPR. I det følgende vil det drøftes nærmere hvordan dette påvirker styrets ansvar for forvaltningen av selskapet etter asl. § 6-12. Endringer i styrets ansvar etter asl. § 6-12 vil igjen kunne få betydning for styremedlemmenes erstatningsansvar etter asl. § 17-1.

3.1 Overordnet om styrets ansvar etter aksjeloven § 6-12

Det følger av asl. § 6-12 første ledd første punktum at "*[f]orvaltningen av selskapet hører under styret*". Av bestemmelsens annet punktum følger at styret skal sørge for "*forsvarlig organisering av virksomheten*". Styret er selskapets øverste ledelse. Aksjeloven § 6-12 gir uttrykk for styrets forvaltningskompetanse og styrets forvaltningsplikt.

Ordlyden i asl. § 6-12 tilsier at det overordnede ansvaret for å lede virksomheten ligger hos styret. Styret har også ansvar for at selskapet drives innenfor rammene som følger av lov, vedtekter og generalforsamlingens beslutninger.[67] Som generelt krav gjelder at forvaltningen av selskapet skal være forsvarlig. Dette forutsettes i lovens ansvarsbestemmelser, herunder erstatningsbestemmelsen i asl. § 17-1.[68]

Styrets ansvar for forsvarlig organisering av virksomheten innbefatter blant annet utarbeidelse av rutiner og retningslinjer, og å sikre at den daglige ledelsen har tilstrekkelig midler til å utføre sine oppgaver, herunder midler til å ansette tilstrekkelig og kompetent personell.[69]

Når styret etter § 6-12 gis ansvar for at selskapet drives innenfor rammene som følger av lov, ligger det i dette et ansvar for å følge opp, og å sørge for at selskapet etterlever gjeldende regelverk, og at selskapet implementerer nytt regelverk. Styret har i selskapet to sentrale roller, kontroll og rådgivning.[70] Dette medfører for forvaltningsansvarets del at styret må ha kontroll på at selskapet etterlever det regelverket selskapet underlegges, og at styret må gi råd om og iverksette tiltak for å sørge for at regelverket etterleves. Det følger således et ansvar for å etablere betryggende interne kontrollrutiner i selskapet.

[67] Bråthen (2015) note 1082 og Woxholt (2012) s. 201.
[68] Knudtzon (2004) s. 107.
[69] Woxholt (2012) s. 201.
[70] Bøhren (2011) s. 108.

Styrets plikt til forsvarlig forvaltning av selskapet etter asl. § 6-12 henger sammen med det erstatningsansvaret styremedlemmene kan pålegges etter asl. § 17-1.[71] Det er derfor nødvendig å kartlegge hvilke plikter styret har etter GDPR som faller innunder forvaltningsansvaret etter asl. § 6-12 for å kunne avgjøre om styremedlemmene har utvist erstatningsbetingende handling eller unnlatelse.[72]

3.1.1 Aksjeloven § 6-12 som dynamisk rettslig standard

Styret har et ansvar for og en plikt til forsvarlig forvaltning av selskapet etter asl. § 6-12. Hva som anses å være forsvarlig forvaltning av selskapet, og hvilke krav som stilles til styret for å oppfylle denne plikten, må ses i lys av samfunnsutviklingen, og de eksterne krav som stilles til selskapets virksomhet.

Det er fastslått i kapittel 3.1 at det i forvaltningsansvaret ligger et ansvar for at selskapet opererer i samsvar med gjeldende regelverk. Et nytt regelverk av stor betydning, som GDPR, medfører det at det stilles nye krav til selskapet og selskapets ledelse. Spørsmålet er om de plikter styret pålegges etter GDPR utgjør et ledd i hva som anses for å utgjøre forsvarlig forvaltning av selskapet i medhold av asl. § 6-12.

Normann Aarum skriver i "*Styremedlemmenes erstatningsansvar i aksjeselskaper*" at det i forarbeidene til aksjeloven ikke gis anvisning på i hvilken utstrekning styret pålegges en generell plikt til å påse at selskapet opptrer i samsvar med eksisterende lovgivning.[73] Dette ble imidlertid skrevet før dagens aksjelov trådte i kraft, og er basert på forarbeidene til aksjeloven fra 1976.

Da dagens aksjelov trådte i kraft i 1997 ble styret pålagt flere plikter, eksempelvis asl. § 3-4 om krav til forsvarlig egenkapital og likviditet, som nå utgjør et ledd i plikten til forsvarlig forvaltning av selskapet etter asl. § 6-12. Disse nye pliktene ledet til diskusjoner om hvorvidt den nye lovgivningen innebar skjerpede regler om styrets erstatningsansvar, og spørsmålet var om skjerpet forvaltningsansvar etter asl. § 6-12 innebar skjerpet erstatningsansvar etter asl. § 17-1[74]

[71] Perland (1999) s. 6.
[72] Normann Aarum (1994) s. 60. Nærmere om erstatningsansvaret i avhandlingens kapittel 4.
[73] Normann Aarum (1994) s. 260.
[74] Perland (1999) s. 2.

Diskusjonen rundt styret ansvars i etterkant av innføringen av dagens aksjelov i 1997, eksemplifiserer hvordan endringer i rammelovgivningen medfører i endringen i hvordan asl. § 6-12 anvendes og forstås. Diskusjonen fra 1997 oppstår nå på nytt i ny drakt. Nå er spørsmålet hvilken betydning de pliktene som pålegges styret etter GDPR får for anvendelsen og forståelsen av asl. § 6-12. Dette viser bestemmelsens dynamiske karakter og forvaltningsansvaret etter asl. § 6-12 sin rolle som rettslig standard.

Styret har det øverste ansvaret for å ivareta selskapets samfunnsansvar.[75] Med selskapets samfunnsansvar menes det ansvaret som selskapet har for mennesker, miljø og samfunn som påvirkes av selskapets virksomhet.[76] GDPR har medført sterkere bevisstgjøring rundt personvern i samfunnet, og forordningens inntog har tydeliggjort hvilke verdier selskapene håndterer når de behandler personopplysninger. Når samfunnet setter personvern på dagsorden, medfører dette også en skjerpelse av forventningene til hvordan selskapene ledes. Varslingslovutvalget har i sin utredning anbefalt at brudd på personvernregelverk og informasjonssikkerhet anses som kritikkverdig forhold som arbeidstaker har rett til å varsle om.[77] Utvalgets forslag underbygger at brudd på personvernregelverket av samfunnet er ansett uønsket, og viser viktigheten av at selskapene etterlever gjeldende personvernregelverk på en tilfredsstillende måte.[78] De skjerpede forventningene fra samfunnet kan få betydning for hvor terskelen ligger for hva som anses som forsvarlig forvaltning av selskapet fra styrets side etter asl. § 6-12.

Styret har det overordnede ansvaret for den forretningsmessige driften av selskapet.[79] I forarbeidene til aksjeloven ble behovet for å nærmere konkretisere hvilke forvaltningsoppgaver styret har ansvar for drøftet, og man landet på at en slik konkretisering ikke ville være hensiktsmessig.[80] Hvilke oppgaver og plikter som naturlig faller innunder forvaltningsansvaret vil variere fra selskap til selskap og i tråd med samfunnsutviklingen og de eksterne krav som stilles. Denne vurderingen i forarbeidene viser at innholdet i styrets forvaltningsansvar kan endres over tid. Samfunnsutviklingen og økt bevissthet rundt personvern gjør det nå naturlig å vurdere om og hvordan etterlevelse av personvernforordningen kan tillegges styret som ansvar og plikt i medhold av asl. § 6-12.

[75] Norsk anbefaling eierstyring og selskapsledelse (2014) s. 36.
[76] Norsk anbefaling eierstyring og selskapsledelse (2014) s. 12.
[77] NOU 2018: 6 s. 157.
[78] NOU 2018: 6 s. 132.
[79] NOU 1996: 3 s. 136.
[80] NOU 1996: 3 s. 136.

3.1.2 Nærmere om styrets ansvar for etterlevelse av personvernforordningen

Forvaltningsansvaret etter asl. § 6-12 er dynamisk, og hva dette ansvaret nærmere innbefatter, endres i takt med samfunnsutviklingen. Spørsmålet er i hvilken grad GDPR representerer en lovregulering av en del av styrets forvaltningsansvar.

Alle selskaper behandler personopplysninger, og personvernspørsmål berører hele virksomheten. Dette i kontrast til en tradisjonell tankegang om at personvern sikres i IT-avdelingene.[81] Når det nå kommer nytt personvernregelverk må ansvaret for etterlevelse av personvernregelverk løftes inn på styrerommene. Personvern er en kritisk del av virksomhetens risikostyring og samfunnsansvar.

Personvernforordningen pålegger selskapet en plikt til selvregulering. Med plikt til selvregulering menes typer av lovgivning som overlater til selskapene å regulere seg selv og å etablere interne regelverk med sikte på å etterleve lovgivningens formål.[82] GDPR pålegger gjennom flere bestemmelser, herunder artikkel 24 og artikkel 32, selskapet en plikt til å iverksette hensiktsmessige tekniske og organisatoriske tiltak for å oppnå bestemmelsenes formål. Gjennom slike bestemmelser griper GDPR inn i selskapets organisering og plikten til selvregulering kommer til uttrykk.

Styret og ledelsen i ethvert selskap har ansvar for at det innad i selskapet bygges opp prosesser og strukturer for å sikre verdiskapningen.[83] Disse prosessene må sikre at aktuelt lovverk etterleves og at adekvate regler og rutiner utarbeides i selskapet.[84] En del av styrets forvaltningsansvar etter asl. § 6-12 er å påse at rettsregler overholdes.[85] Av forarbeidene til asl. § 6-12 fremgår det at styret har det overordnede ansvaret for at selskapet organiseres på en formålstjenlig måte.[86] Når styret etter § 6-12 har det overordnede ansvaret for forvaltningen av selskapet, og en alminnelig plikt til å skaffe seg kunnskap om forhold knyttet til selskapets virksomhet, har styret primæransavaret for at selskapet oppfyller de krav selskapet som subjekt pålegges, herunder kravene i GDPR.

[81] Se følgende artikkel for tilsvarende tankegang hva gjelder cybersikkerhet, som har enkelte paralleller til personvern: https://home.kpmg.com/no/nb/home/nyheter-og-innsikt/2018/03/cybersikkerhet-fra-serverrom-til-styrerom.html.
[82] Eriksen (2015) s. 28.
[83] Thorsby (2004) s. 83.
[84] Thorsby (2004) s. 83.
[85] Perland (2013) s. 8.
[86] Ot.prp. nr. 23 (1996-1997) s. 147.

Etter asl. § 6-1 er styret et obligatorisk organ i alle selskap. Styremedlemmene skal forvalte selskapet på vegne av aksjeeierne, og er aksjeeiernes tillitspersoner.[87] Styrevervet er et tillitsverv for hele selskapsinteressen.[88] Hvilke interesser som anses som legitime selskapsinteresser endres i takt med nye forventninger fra ansatte, samfunnet rundt selskapet og nye krav gjennom eksterne lovregler. Det er lett å argumentere for at det er i selskapets samlede interesse at kravene i GDPR etterleves og at personvernet ivaretas. Ved brudd på forordningens krav risikerer selskapet bøtelegging og (økonomisk) tap, hvilket igjen kan få betydning for aksjonærenes økonomiske interesser. Sett hen til at personvern (ofte) berører tilnærmet alle sider av selskapets virksomhet er det nærliggende å anse personvern som en legitim selskapsinteresse styret kan og må ta hensyn til i sitt arbeid og under sitt forvaltningsansvar i medhold av asl. § 6-12.[89]

Ytterligere vil det også kunne være tale om omdømmetap for selskapet dersom det blir kjent at selskapet ikke etterlever kravene for å sikre personvernet etter GDPR. Personvern er et viktig ideal å sikre. Alle tiltak som iverksettes for å sikre etterlevelse av GDPR bør derfor forankres i ledelsen, og etterlevelse av GDPR spiller en sentral rolle i styrets forvaltningsansvar etter asl. § 6-12.

Etter asl. § 6-12 tredje ledd skal styret holde seg orientert om selskapets økonomiske stilling og påse at selskapets formuesforvaltning er "*gjenstand for betryggende kontroll*". Etter bestemmelsens annet ledd skal styret i nødvendig utstrekning fastsette budsjetter for virksomheten. Det følger implisitt av disse bestemmelsene at styret har et ansvar i selskapets ressursbruk. Bøtelegging for brudd på GDPR, med det bøtenivået som foreligger, kan få store konsekvenser for selskapets økonomiske stilling.[90] Når selskapet løper økonomisk risiko dersom forordningen ikke etterleves, kan det argumenteres at styret også etter § 6-12 tredje ledd har en plikt til å holde seg orientert om risikoen for at slik tap inntrer, for å ha kontroll med selskapets økonomiske stilling. Videre vil senere endring av interne rutiner og organisering etter eventuelt pålegg etter tilsyn fra Datatilsynet kunne innebære enorme kostnader. Når styret har et ansvar i selskapets økonomiforvaltning og ressursbruk er det følgelig i styrets, og selskapets, interesse at forordningen etterleves kontinuerlig. Av artikkel

[87] Bugge Reiersen (2007) s. 21.
[88] Selskapsinteressen betegner normalt aksjonærenes interesse i å oppnå profittmaksimering ("shareholder value") og andre legitime interesser med tilknytning til selskapet, slik som hensyn til ansatte, kreditorer og samfunnsinteresser ("stakeholder value"). Definisjon hentet fra Eriksen (2015) s. 42.
[89] Perland (2013) s. 7.
[90] Se kapittel 4.2.1.

29-gruppens retningslinjer fremgår det at brudd på forordningen ikke kan legitimeres ved at selskapet påberoper seg manglende ressurser.[91]

De høye bøtesatser og risiko for omdømmetap er sterke argument for at etterlevelse av GDPR løftes til styret. Når GDPR i tillegg pålegger styret nye plikter innebærer dette at rammene for hva som anses som forsvarlig forvaltning av selskapet etter asl. § 6-12 endres. Etterlevelse av GDPR faller således innunder hva som tillegges styret som ansvar som ledd i forsvarlig forvaltning av selskapet jf. asl. § 6-12. GDPR representerer en lovregulering av en del av styrets forvaltningsansvar.

Dersom styret ikke involveres i implementering og etterlevelse av personvernforordningen, øker risikoen for at etterlevelse av personvernregelverk ikke prioriteres nedover i organisasjonen. Styret anfører "the tone at the top"[92] i selskapet og skaper holdninger for de ansatte i selskapet som står for den daglige behandlingen av personopplysninger.[93] Styret har, i tillegg til sitt lovfestede forvaltningsansvar etter asl. § 6-12, således også et ansvar for å skape kultur for ivaretakelse av personvern i selskapet. Styret må skape legitimitet for de rutiner og tiltak som iverksettes i selskapet for å sikre etterlevelse av personvernforordningen, slik at disse tiltak til slutt gjennomsyrer den behandlingen av personopplysninger som skjer i selskapet.

GDPR bidrar til å klargjøre de ulike delene av styrets ansvar etter asl. § 6-12 ved at forvaltningsansvaret ses i lys av forordningens krav. GDPR representerer et regelverk som setter skjerpede krav til intern selvregulering. Med GDPR skjerpes styrets forvaltningsplikt på den måten at styret må vite om og vise årvåkenhet rundt de krav forordningen stiller, være delaktig i prosessene med implementering og etterlevelse, og stille de riktige spørsmålene, både til seg selv og til de ansatte som i den daglige driften skal sørge for at personvernregelverket etterleves.

I det videre eksemplifiseres koblingen mellom GDPR artikkel 24, 30, 32 og 38 og styrets ansvar for etterlevelse av GDPR i medhold av asl. § 6-12.

[91] Guidelines on the application and setting of administrative fines (2017) s. 12.
[92] Deloitte (2015) s. 3, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-tone-at-the-top-sept-2014.pdf.
[93] Skullerud, Rønnevik, Skorstad m.fl. (2018) s. 170.

3.2 Sentrale bestemmelser etter GDPR hvor styrets ansvar aktualiseres

Artiklene i GDPR som behandles i det følgende er bestemmelser hvor forordningen stiller krav til selskapene og hvor spørsmålet om styrets rolle og ansvar etter asl. § 6-12 aktualiseres. Det vil nedenfor belyses nærmere hva som forventes av styret i relasjon til hvert enkelt krav, og hvorfor det er naturlig at styret tillegges ansvar for etterlevelse i medhold av forvaltningsansvaret i § 6-12.

3.2.1 GDPR artikkel 24 – Den behandlingsansvarliges ansvar

Det følger av GDPR artikkel 24 nr. 1 at den behandlingsansvarlige skal gjennomføre egnede "*tekniske og organisatoriske tiltak*" for å "*sikre og påvise at behandlingen utføres i samsvar med denne forordning*". Av artikkel 24 nr. 2 fremgår det at tiltak nevnt i nr. 1 skal, dersom det står i forhold til behandlingsaktivitetene, omfatte den behandlingsansvarliges iverksetting av "*egnede retningslinjer for vern av personopplysninger*". Artikkel 24 krever at den behandlingsansvarlige utfører all behandling av personopplysninger i samsvar med GDPR, og at slik etterlevelse objektivt sett kan demonstreres. GDPR artikkel 24 oppstiller en generell plikt til internkontroll.[94]

Det er styret som i siste instans er behandlingsansvarlig etter forordningen og som pålegges plikter i medhold av GDPR.[95] Sammenholdt med GDPR artikkel 24 har styret som organ ansvar for tilfredsstillende organisering av virksomheten og iverksetting av tekniske og organisatoriske tiltak for å sikre bestemmelsens krav. Hvilke tekniske og organisatoriske tiltak som skal gjennomføres fremgår ikke nærmere av forordningen, men det må foretas en risikovurdering hvor forholdene ved behandlingen og risikoen ved denne vurderes mot personvernhensynet til den registrerte.[96]

Iverksetting av retningslinjer for behandling av personopplysninger etter artikkel 24 nr. 2 må ses i sammenheng med asl. § 6-12 annet ledd, hvor det fremgår at styret i nødvendig utstrekning "*kan*" fastsette retningslinjer for virksomheten. Det følger av forarbeidene at styret selv må avgjøre om det skal gis retningslinjer, og hvilke spørsmål retningslinjene skal

[94] Skullerud, Rønnevik, Skorstad m.fl. (2018) s. 168. Kravet etter GDPR artikkel 24 samsvarer langt på vei med internkontrollplikten slik denne reguleres i personopplysningsforskriften kapittel 3.
[95] Se kapittel 2.3.2.
[96] Sandtrø (2017), https://www.sandtro.no/2017/12/05/hva-kreves-av-dokumentasjon-etter-gdpr/.

regulere.[97] Styret kan for eksempel i retningslinjer fastsette saksbehandlingsregler, strategiske mål eller gi retningslinjer som uttrykker hvordan ulike virksomhetsområder skal prioriteres.[98]

Det ble i forarbeidene til asl. § 6-12 annet ledd drøftet om fastsettelse av retningslinjer skulle gjøres obligatorisk for styret.[99] Man landet da på en løsning hvor en slik plikt ikke ble lovfestet fordi man først ville vinne erfaringer med bestemmelsen. Når GDPR stiller krav til utarbeidelse av retningslinjer ut over det som følger direkte av aksjeloven, trekker dette i retning av at styret ikke "*kan*",[100] men *må* fastsette retningslinjer for vern av personopplysninger. Videre taler det overordnede ansvarsprinsippet i GDPR for at styret har et ansvar for å fastsette retningslinjer. Ytterligere nevnes at personvernforordningen er lex specialis[101] til aksjeloven, slik at plikten for styret til å fastsette retningslinjer etter GDPR artikkel 24 går foran styrets skjønnsmessige adgang til å iverksette retningslinjer etter asl. § 6-12 annet ledd.

Styrets mulighet til å imøtekomme de krav som pålegges i forordningen, avhenger av daglig leders ansvar. Daglig leder skal sørge for at styret mottar presis, relevant og tidsriktig informasjon som er tilstrekkelig for at styret skal kunne utføre sine oppgaver.[102] Styret må utforme retningslinjer for personvern som sikrer en hensiktsmessig fordeling av roller og arbeidsoppgaver i selskapet. Herunder må daglig leder gis et rapporteringsansvar til styret[103] om viktige spørsmål som angår etterlevelse av GDPR.[104] Styret har en selvstendig aktivitetsplikt, og kan ikke uten videre avvente at informasjon skal tilflyte styret fra administrasjonen.[105] Styret kan sikre seg informasjon ved å implementere gode rapporteringsrutiner gjennom retningslinjer for slik rapportering. Retningslinjer som legger til rette for målrettet og effektiv virksomhet i selskapet vil gjøre det mulig å håndtere risiko for

[97] NOU 1996: 3 s. 137 og Ot.prp. nr. 23 (1996-1997) s. 147.
[98] NOU 1996: 3 s. 137.
[99] Ot.prp. nr. 23 (1996-1997) s. 219.
[100] Jf. asl. § 6-12 annet ledd.
[101] Tolkningsregel som kommer til anvendelse ved motstrid mellom rettsregler av samme rang. Regelen innebærer at mer spesialiserte rettsregler går foran generelle regler. Definisjon hentet fra Jusleksikon, tilgjengelig på https://www.jusleksikon.no/wiki/Lex_specialis.
[102] Norsk anbefaling eierstyring og selskapsledelse (2014) s. 33.
[103] Se kapittel 3.2.4 om personvernombudets rapportering til styret.
[104] Jf. også asl. § 6-14 annet ledd om at saker som etter selskapets forhold er av "*uvanlig art*" eller "*stor betydning*" skal behandles av styret.
[105] NOU 1996: 3 s. 137.

overtredelse av GDPR, og gjøre det enklere å sikre at selskapet opptrer i tråd med gjeldende personvernregelverk.[106]

Plikten etter artikkel 24 til å gjennomføre tiltak for å sikre at behandlingen av personopplysninger skjer etter forordningens krav innebærer en plikt til å utarbeide rutiner for de ansatte som behandler personopplysninger i selskapets daglige virke. Det minsker risikoen for datainnbrudd og øvrige brudd på forordningen dersom både styret, øvrig ledelse og ansatte er innforstått med hvilke interne retningslinjer og lovpålagte krav som gjelder. Styret har en rolle i å fastsette disse retningslinjene samt å bevilge midler til opplæring av kompetent personell. I NUES anbefales at styret skal lede selskapets strategiske planlegging og fatte vedtak som danner grunnlag for selskapets daglige ledelse til å forberede og gjennomføre strukturelle tiltak.[107] Som ledd i dette kan, og bør, selskapets retningslinjer for vern av personopplysninger forankres hos styret.

I vurderingen av om, og eventuell hvor stor, bot som skal ilegges selskapet ved brudd på GDPR, skal det i henhold til Artikkel 29-gruppens retningslinjer ses hen til om bruddet på forordningen er et resultat av manglende rutiner.[108] Dette viser viktigheten av å iverksette retningslinjer for vern av personopplysninger, og at retningslinjene bør forankres i styret. Dette fordi styret er øverste ansvarlige ledelse i selskapet og kan rammes hardt av eventuell bøtelegging, jf. drøftelsen i avhandlingens kapittel 4 om styremedlemmenes personlige erstatningsansvar.

3.2.2 GDPR artikkel 30 – Protokoller over behandlingsaktiviteter

I henhold til GDPR artikkel 30 nr. 1 skal hver behandlingsansvarlig "*føre en protokoll over behandlingsaktiviteter som utføres under deres ansvar.*" Protokollen skal blant annet inneholde informasjon om formålet med behandlingen, en beskrivelse av kategorier av registrerte og kategorier av personopplysninger, tidsfrister for sletting, og en generell beskrivelse av de tekniske og organisatoriske sikkerhetstiltak nevnt i artikkel 32 nr. 1. GDPR artikkel 30 representerer et viktig ledd i selskapets internkontroll, all den tid en oversikt over hvilke personopplysninger som behandles på hvilken måte er sentralt for å fastslå om

[106] Norsk anbefaling eierstyring og selskapsledelse (2014) s. 36.
[107] Norsk anbefaling eierstyring og selskapsledelse (2014) s. 33.
[108] Guidelines on the application and setting of administrative fines (2017) s. 10.

forordningens krav etterleves. Styrets ansvar for selskapets samlede internkontroll behandles derfor i det alt vesentlige under dette kapittelet.

Protokollene som utarbeides i medhold av artikkel 30 skal virke som dokumentasjon på at behandling av personopplysninger skjer i tråd med kravene etter GDPR og har også en kontrollfunksjon i at avvik oppdages.[109] Det følger av fortalen til GDPR, avsnitt 42, at protokollene skal tjene som dokumentasjon på at selskapet overholder og etterlever kravene etter GDPR.

I henhold til forskrift om risikostyring og internkontroll § 3, som gjelder for enkelte typer av aksjeselskap[110], skal "*[s]tyret påse at foretaket har hensiktsmessige systemer for risikostyring og internkontroll.*" Forskriftens formål er å utdype styrets ansvar ut over det som følger av selskapsrettslige regler og regler i særlovgivningen.[111] Det følger av veiledningen til forskriften at styret skal påse at det etableres og gjennomføres tiltak for å korrigere eller redusere svakheter i selskapet.[112]

Manglende etterlevelse av kravene i personvernforordningen vil klart utgjøre en svakhet for selskapet. Dette både grunnet i den økonomiske risikoen for eventuell bøtelegging og risikoen for omdømmetap. Kravene etter forskriften underbygger at styret har et ansvar i å sikre internkontroll etter GDPR artikkel 30,[113] jf. også asl. § 6-12. Protokollføringen GDPR artikkel 30 gir anvisning på sikrer et system for internkontroll. God internkontroll og effektiv risikostyring bidrar på sikt til å sikre aksjonærenes investering og selskapets eiendeler, hvilket igjen er i styrets interesse. Dette trekker i retning av at styret har et klart overordnet ansvar i å legge til rette for og sikre god internkontroll i medhold av GDPR artikkel 30.

Det følger av forarbeidene[114] til verdipapirhandelloven[115] at styret i verdipapirforetak skal fastsette retningslinjer for internkontroll og forvisse seg om at denne kontrollen skjer på en forsvarlig måte.[116] Når styret pålegges et slikt ansvar etter verdipapirhandelloven, som

[109] Skullerud, Rønnevik, Skorstad m.fl. (2018) s. 197.
[110] Forskriften gjelder etter § 1 blant annet for regulerte markeder, verdipapirforetak, eiendomsmeglingsforetak og regnskapsførerselskaper. Slike virksomheter kan organiseres som aksjeselskap.
[111] Finanstilsynet (2009) Innledning.
[112] Finanstilsynet (2009) Kapittel 2.
[113] Forskriften er også relevant for de øvrige deler av selskapets internkontroll, herunder kravene etter GDPR artikkel 24, 32 og 38.
[114] Ot.prp. nr. 34 (2006-2007) s. 201 flg.
[115] Lov 29. juni 2007 nr. 75 om verdipapirhandel (verdipapirhandelloven).
[116] Tilsvarende er forutsatt gjennom ulike bestemmelser i forskrift 19. juni 2007 nr. 876 til verdipapirhandelloven (verdipapirforskriften), jf. §§ 9-7 og 9-10.

tilsvarende som personvernregelverket pålegger selskapet omfattende selvregulering for å ivareta formål med stor samfunnsmessig betydning, taler dette for at styret har et tilsvarende ansvar for internkontroll i medhold av personvernforordningen. Her kan det videre trekkes en parallell til styrets ansvar for iverksetting av retningslinjer etter GDPR artikkel 24.

I henhold til NUES, skal styret påse at selskapet har god internkontroll og hensiktsmessige systemer for risikostyring sett hen til omfanget og arten av selskapets virksomhet.[117] Internkontrollen og systemene bør også omfatte selskapets verdigrunnlag og retningslinjer for etikk og samfunnsansvar. Styret bør årlig foreta en gjennomgang av selskapets viktigste risikoområder og den interne kontroll.[118] Denne gjennomgangen bør også innbefatte internkontrollen og protokollføringen i medhold av artikkel 30. Personvern er en del av selskapets samfunnsansvar, og internkontroll som sikrer etterlevelse av GDPR bør forankres i selskapets styre.[119]

3.2.3 GDPR artikkel 32 – Sikkerhet ved behandlingen

GDPR artikkel 32 klargjør selskapenes ansvar for sikkerhet ved behandlingen av personopplysninger. Kravene til kontinuerlig arbeid med informasjonssikkerhet skjerpes med GDPR. Av artikkel 32 nr. 1 følger det at den behandlingsansvarlige skal gjennomføre "*egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet*" sett hen til risikoen. Det skal ved vurderingen av hvilke tiltak som skal iverksettes blant annet tas hensyn til den "*tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, [og] formål*". Av artikkel 32 nr. 1 bokstav a til d fremgår det at slike tiltak eksempelvis kan være pseudonymisering og kryptering av personopplysninger.

Kravet til sikkerhet ved behandlingen etter artikkel 32 henger tett sammen med internkontrollkravet etter artikkel 30. Styret må kjenne sin virksomhet og de verdier som forvaltes for å kunne vite hvilke risiki selskapet må sikre seg mot, og hvordan. En reell risikovurdering kan ikke gjøres uten en internkontroll og en oversikt over hvilke personopplysninger som behandles hvordan, jf. kravet til protokollføring etter GDPR artikkel 30. Etter forordningens regler vil det måtte gjennomføres en risikovurdering som grunnlag for

[117] Norsk anbefaling eierstyring og selskapsledelse (2014) s. 36.
[118] Norsk anbefaling eierstyring og selskapsledelse (2014) s. 36.
[119] Veum (2010) s. 206.

gjennomføringen av informasjonssikkerhetstiltak.[120] Når styret har et tydelig ansvar for internkontroll etter artikkel 30, smitter dette ansvaret over på de krav som oppstilles etter GDPR artikkel 32. Det har liten betydning om selskapet etterlever regelverket i dag, dersom det ikke også etableres gode rutiner og kontroller for å sikre etterlevelse også i fremtiden. Kravet til internkontroll innebærer et krav til løpende risikovurdering.

Etter GDPR artikkel 32 skal selskapet gjennomføre tekniske og organisatoriske tiltak for å oppnå et egnet sikkerhetsnivå. I dette ligger at selskapet må evaluere risikoen for brudd på informasjonssikkerheten og iverksette tiltak for å minske denne, med sikte på å forhindre datainnbrudd og brudd på GDPR.[121] Dette kravet kan ses i lys av styrets plikt til forsvarlig forvaltning og forsvarlig organisering av selskapet i asl. § 6-12 første ledd. Informasjonssikkerhet er et kontinuerlig arbeid som krever årlig gjennomgang av strategier og organisering av systemer.[122]

Etter GDPR artikkel 32 nr. 2 må selskapet evaluere risiki som oppstår som følge av tap av personopplysninger, uautorisert tilgang til opplysninger med videre. For å unngå at denne risikoen i utgangspunktet oppstår, og for å håndtere den dersom det er tilfelle, er det viktig at selskapet har på plass retningslinjer, rutiner og kontroller. Det vises til de avklaringer som er gjort rundt styrets ansvar for iverksetting av retningslinjer etter forordningens artikkel 24 og ansvaret for internkontroll etter artikkel 30.

Styret har det overordnede ansvaret for selskapets økonomi, en rolle i selskapets ressursbruk, og et ansvar for å bevilge midler.[123] Artikkel 32 stiller krav til at det skal oppnås et tilfredsstillende sikkerhetsnivå for personopplysningene. Styret har da et ansvar i å bevilge midler og allokere ressurser nettopp til disse formål i medhold av forvaltningsansvaret etter asl. § 6-12. Det følger også av forskrift om bruk av informasjons- og kommunikasjonsteknologi[124] § 2 at avtaler om utkontraktering av IKT-virksomhet og endringer i slike avtaler skal behandles av styret.

Forvaltningsfunksjonen pålegger styret aktiv handling på overordnet nivå i saker som er av uvanlig art eller av vesentlig betydning, og som går ut over den daglige drift av virksomheten,

[120] Kommunal- og moderniseringsdepartementet (2017) s. 30.
[121] Rücker/Kugler (2018) s. 114.
[122] Datatilsynet – En veiledning om internkontroll og informasjonssikkerhet s. 23.
[123] Se nærmere under kapittel 3.1.2.
[124] Forskrift 21. mai 2003 nr. 630 om bruk av informasjons- og kommunikasjonsteknologi (IKT).

jf. asl. § 6-14 annet ledd.[125] Dersom det foreligger brudd på informasjonssikkerheten etter GDPR artikkel 32 vil dette kunne ha store konsekvenser for selskapet, både for de registrertes rettigheter og for selskapets interne anliggender. Eksempelvis vil datainnbrudd i mange tilfeller være av stor betydning for selskapet, slik at dette må forelegges styret for behandling. Styret har et ansvar i etterlevelse av GDPR artikkel 32 også ut over det som allerede følger av forvaltningsansvaret etter asl. § 6-12.

3.2.4 GDPR artikkel 38 – Personvernombudets stilling

Det følger av GDPR artikkel 37 at enkelte virksomheter med GDPR pålegges å utnevne et personvernombud.

Før personvernforordningen har det ikke vært noen plikt i norsk rett til at selskapet skal ha personvernombud. Den tidligere ordningen med personvernombud baserte seg på frivillighet for den behandlingsansvarlige, både i privat og offentlig sektor.[126] Forordningens regler som gjør personvernombud obligatorisk for enkelte selskaper, innebærer en betydelig utvidelse av ordningen sammenlignet med gjeldende rett.[127] I henhold til uttalelser fra Artikkel 29-gruppen, er innføring av kravet til personvernombud i hjertet av hva nytt forordningen bringer med seg.[128]

Hvilke virksomheter som pålegges å utnevne personvernombud følger av GDPR artikkel 37.[129] Anvendelsesområdet belyses ikke nærmere, da temaet her er personvernombudets stilling i de aksjeselskap som pålegges å utnevne et ombud. Datatilsynet anbefaler alle virksomheter å utnevne personvernombud, uavhengig av om selskapet pålegges dette etter forordningen.[130] Når styret har et klart ansvar i etterlevelse av GDPR gjennom sitt forvaltningsansvar, innebærer dette også et ansvar i å sikre at selskapet utnevner et personvernombud der dette er påbudt.

Personvernombudet skal informere og gi råd til den behandlingsansvarlige og de ansatte som behandler personopplysninger om de forpliktelser som pålegges selskapet etter

[125] Se også Norsk anbefaling eierstyring og selskapsledelse (2014) s. 8.
[126] Prop. 56 LS (2017-2018) s. 121.
[127] Prop. 56 LS (2017-2018) s. 121.
[128] Rücker/Kugler (2018) s. 175.
[129] I forslag til ny personopplysningslov, Prop. 56 LS (2017-2018) § 19, foreslås en forskriftshjemmel hvor Kongen kan gi forskrift med nærmere bestemmelser om plikt til å utnevne personvernombud.
[130] Datatilsynets veileder – Personvernombud etter nytt regelverk s. 3.

personvernlovgivningen, jf. GDPR artikkel 39 første ledd bokstav a.[131] Videre skal ombudet kontrollere etterlevelse og selskapets retningslinjer for etterlevelse. Personvernombudet er for selskapet et internkontrolltiltak, som skal øke virksomhetens etterlevelse av forordningens plikter.[132] Personvernombudets rolle må derfor ses i sammenheng med de internkontrolltiltak GDPR artikkel 24 og 30 gir anvisning på. Personvernombudet skal sikre at retningslinjer for personvern som gis i medhold av artikkel 24 følges opp og at protokoller over behandlingsaktiviteter utarbeides i henhold til artikkel 30.

Etter GDPR artikkel 38 nr. 2 skal den behandlingsansvarlige stille til rådighet og tilrettelegge for de ressurser som er nødvendig for at personvernombudet skal kunne utføre de oppgaver som følger av artikkel 39. I henhold til Artikkel 29-gruppens retningslinjer skal personvernombudet gis de finansielle ressursene, organisatoriske tiltak, medarbeidere, tid og støtte vedkommende trenger for å gjennomføre sin rolle.[133] Styret har det overordnede ansvar for selskapets økonomi og et ansvar i ressursallokering. Dette ansvaret gjør seg også gjeldende i å sikre at personvernombudet gis de nødvendige ressurser for å utføre sine oppgaver.

Etter artikkel 38 nr. 3 skal den behandlingsansvarlige sikre at personvernombudet ikke mottar instrukser om utførelsen av sine oppgaver. Personvernombudet skal være helt uavhengig i sin stilling.[134] Denne uavhengigheten er det styret som har det øverste ansvar for å sikre. Styret kan ikke instruere personvernombudet.

Personvernombudet er mellommann mellom de ulike interessentene i selskapet, og er ikke personlig ansvarlig ved manglende etterlevelse og brudd på forordningen.[135] For å kunne utøve sin rolle på best mulig måte må personvernombudet gis tilstrekkelig uavhengighet i sin stilling, samt tilstrekkelige ressurser for å kunne ivareta de oppgaver som hviler på stillingen.[136] Styret har det øverste ansvar for å legge disse forhold til rette. Også når et

[131] Rücker/Kugler (2018) s. 175.
[132] Skullerud, Rønnevik, Skorstad m.fl. (2018) s. 226.
[133] Guidelines on Data Protection Officers (2016) s. 23.
[134] Datatilsynet veileder – hva betyr de nye personvernreglene for din virksomhet s. 10.
[135] Rücker/Kugler (2018) s. 182.
[136] Rücker/Kugler (2018) s. 182.

selskap har personvernombud, hviler det overordnede juridiske ansvaret for at personvernlovgivningen følges på den behandlingsansvarlige, styret.[137]

Etter artikkel 38 nr. 3 siste setning skal personvernombudet rapportere "*direkte til det høyeste ledelsesnivået hos den behandlingsansvarlige*". Dette for å sikre at ledelsen holdes informert om relevante forhold som kan ha betydning for om selskapet etterlever sine plikter etter forordningen.[138] På denne måten overlates ansvaret for å følge opp mulige brudd på forordningen til selskapets ledelse og styre.[139] Når personvernombudet rapporterer til styret om forhold av betydning for etterlevelse av GDPR må styret ta personvernombudets rapport til etterretning. I medhold av sin plikt til forsvarlig forvaltning av selskapet plikter styret å handle på rapport dersom det i selskapet foreligger brudd, eller forhold som kan lede til brudd, på forordningen.

I tillegg til personvernombudets rapporteringsplikt til styret, anbefaler Datatilsynet at personvernombudet regelmessig inviteres til møter med toppledelsen, og at ombudets vurderinger høres og tas i betraktning.[140] Det anbefales også at personvernombudet gis aktiv støtte fra øverste ledelse. Datatilsynets anbefaling gir anvisning på et tydelig ansvar for selskapet styre, ut over hva som følger av forordningen selv og asl. § 6-12.

[137] Datatilsynets veileder – Personvernombud etter nytt regelverk s. 13 og Skullerud, Rønnevik, Skorstad m.fl. (2018) s. 232.
[138] Rücker/Kugler (2018) s. 184.
[139] Rücker/Kugler (2018) s. 184 og Skullerud, Rønnevik, Skorstad m.fl. (2018) s. 233.
[140] Datatilsynets veileder – Personvernombud etter nytt regelverk s. 11.

4 Styremedlemmenes erstatningsansvar ved brudd på GDPR

Fremstillingen så langt (se særlig kapittel 3) har vist at styret som organ, i medhold av sin plikt til forsvarlig forvaltning av selskapet i asl. § 6-12, er ansvarlig for selskapets etterlevelse av GDPR. Spørsmålet er hvorvidt dette ansvaret kan utkrystallisere seg i personlig erstatningsansvar for styremedlemmene. Styremedlemmenes personlige erstatningsansvar aktualiseres der selskapet lider tap som følge av brudd på forordningen og selskapet reiser erstatningskrav mot styremedlemmene.[141]

Perland konkluderer i artikkelen "*Styreansvar i de nye aksjelovene*" med at styrets erstatningsansvar ble skjerpet ved ikrafttredelsen av dagens aksjelov, blant annet fordi loven innførte skjerpede plikter rundt styrets forvaltningsansvar.[142] Forarbeidene til aksjeloven slår fast at presiseringen av styrets plikter vil medføre at ansvarsregelen i asl. § 17-1 får større betydning.[143] I de samme forarbeidene forutsettes det at styrets erstatningsansvar kan bli ytterligere skjerpet, som følge av at styrets ansvar og plikter senere utvides og presiseres.[144]

I den videre fremstillingen i dette kapittelet vurderes om innføringen av GDPR, og tilhørende skjerpelse av styrets forvaltningsansvar etter asl. § 6-12, innebærer en tilsvarende skjerpelse av det personlige erstatningsansvaret etter asl. § 17-1 første ledd.

4.1 Erstatningsregelen i asl. § 17-1 første ledd

Det følger av asl. § 17-1 første ledd at selskapet kan "*kreve at (...) styremedlem (...) erstatter skade*" som det i "*den nevnte egenskap forsettlig eller uaktsomt*" har "*voldt*" selskapet. Et styremedlem kan etter bestemmelsen holdes personlig ansvarlig for den skade styremedlemmet måtte påføre selskapet som ledd i utøvelsen av styrevervet. Erstatningsansvaret er betinget av at vedkommende skadevolder var innehaver av styrevervet på tidspunktet for den skadevoldende handling.[145] Avhandlingen avgrenser mot å behandle medvirkningsansvar etter asl. § 17-1 annet ledd.

[141] Gimmingsrud (2017) s. 23.
[142] Perland (1999) s. 19.
[143] NOU 1992: 29 s. 211, NOU 1996: 3. 89 og Ot.prp. nr. 36 (1993-1994) s. 83.
[144] NOU 1992: 29 s. 211, NOU 1996: 3. 89 og Ot.prp. nr. 36 (1993-1994) s. 83.
[145] Bugge Reiersen (2007) s. 22.

Aksjeloven § 17-1 første ledd gjelder tap som er påført selskapet ved (styremedlemmers) uaktsomme eller forsettlige handlinger eller unnlatelser. Styret handler på vegne av et selskap med begrenset ansvar, og det er først når styremedlemmene forsømmer sine plikter at erstatningsansvar etter asl. § 17-1 kan bli aktuelt.

Bestemmelsen i § 17-1 første ledd er en spesialanvendelse av den alminnelige erstatningsrettslige skyldregel[146], og en kodifisering av det ulovfestede culpaansvar i selskapsretten.[147] Erstatningsansvar for styremedlemmer etter § 17-1 forutsetter i samsvar med dette at de alminnelige vilkårene for erstatningsansvar er oppfylt, slik at det må foreligge en skade, et ansvarsgrunnlag og det må være årsakssammenheng mellom skaden og den handling eller unnlatelse ansvarsgrunnlaget knyttes til.

Erstatningsansvaret etter asl. § 17-1 er individuelt for hvert enkelt styremedlem, og ansvarsvilkårene må derfor være oppfylt for det enkelte medlem. I det følgende forutsettes at styrets beslutninger har vært enstemmige, slik at ansvarsspørsmålet oppstår for hvert enkelt styremedlem.[148] Med erstatningsansvar nedenfor menes personlig erstatningsansvar for styremedlemmene.

4.2 Sammenhengen mellom vilkårene for styremedlemmenes erstatningsansvar etter aksjeloven og manglende etterlevelse av GDPR

4.2.1 Skade

Det følger av asl. § 17-1 at styremedlemmene må ha påført selskapet "*skade*" for å bli erstatningsansvarlig. Det må som utgangspunkt foreligge et økonomisk tap, et tap som kan verdsettes i kroner og øre, for at det skal være tale om en erstatningsrettslig vernet skade.[149]

[146] Aarbakke m.fl. (2017) Kommentar til asl. § 17-1.
[147] Normann Aarum (1994) s. 71 og NOU 1997: 19 s. 197.
[148] Se Aarbakke (1990) s. 4 om diskusjon rundt begrensninger for individualiseringen av ansvaret.
[149] Normann Aarum (1994) s. 116.

I henhold til GDPR artikkel 83 nr. 4 kan Datatilsynet gi bøter på inntil 10 000 000 euro eller, for foretak, på inntil 2 % av samlet global årsomsetning ved overtredelser av GDPR.[150] Bøter med disse høye satsene kan ilegges for overtredelse av artikkel 30 om internkontroll, artikkel 32 om informasjonssikkerhet og artikkel 37-39 som omhandler personvernombud. Det er ingen direkte hjemmel i GDPR for å ilegge bøter av disse størrelsene for overtredelse av bestemmelsen om den behandlingsansvarliges ansvar i GDPR artikkel 24. I forslag til ny personopplysningslov er det foreslått lovhjemmel for å ilegge overtredelsesgebyr også ved overtredelse av artikkel 24.[151]

Det fremgår av Artikkel 29-gruppens retningslinjer at botens størrelse skal svare til typen overtredelse og konsekvensene av overtredelsen. Datatilsynet må før bot ilegges objektivt vurdere alle fakta i saken.[152] Det følger av GDPR artikkel 83 nr. 2 bokstav a at det i vurderingen av om det skal ilegges bot og hvor høy denne skal være skal ses hen til karakteren, alvorlighetsgraden og varigheten av overtredelsen.

Ved bøtelegging av et aksjeselskap ved overtredelse av GDPRs bestemmelser vil det økonomiske tapet som oppstår være et rent formuestap. Et rent formuestap - en formueskade - er en skade som ikke har sammenheng med en person- eller tingsskade.[153] I juridisk teori har det vært problematisert om rene formueskader er erstatningsrettslig vernet som skade,[154] da det tradisjonelt i norsk erstatningsrett siktes til integritetskrenkelsene når skadebegrepet omtales.[155]

I asl. § 17-1 foreligger imidlertid en særskilt erstatningshjemmel. Den praktiske tapsformen for asl. § 17-1 er formuesskade[156] og for styremedlemmenes erstatningsansvar vil det da i de

[150] Pr. i dag er det usikkert om Datatilsynet i Norge vil komme til å ilegge bøter av denne størrelsesorden. For avhandlingens drøftelse er det likevel relevant at det i personvernforordningen finnes hjemmel for å ilegge høye bøter. Videre vil trolig de ulike datatilsynene i Europa på sikt forsøke å legge seg på noenlunde lik linje hva gjelder bøtenes størrelse, all den tid GDPR søker å harmonisere personvernregelverket i Europa.
[151] Forslag til lov om behandling av personopplysninger i Prop. 56 LS (2017-2018) § 26. Datatilsynet har flere ganger ilagt gebyr for overtredelse av personopplysningsloven (2000) § 14 om internkontroll, som er parallellen til GDPR artikkel 24 etter gjeldende rett.
[152] Guidelines on the application and setting of administrative fines (2017) s. 6.
[153] Lødrup (1999) s.53.
[154] Se blant annet Thorson (2010).
[155] Thorson (2010) s. 17.
[156] Aarbakke m.fl. (2017) Kommentar til asl. § 17-1.

fleste praktiske tilfeller være tale om rene formuestap.[157] Slike tap er typisk økte utgifter, økt gjeld eller annet lidt tap i selskapets alminnelige formuesstilling.[158]

Når selskapet bøtelegges for brudd på GDPR vil dette medføre økte utgifter og tap i selskapets alminnelige formuesstilling, og det vil således foreligge et økonomisk tap som kan verdsettes i kroner og øre. Det formuestapet som oppstår for selskapet ved bøtelegging for manglende etterlevelse av GDPR oppfyller følgelig skadevilkåret etter asl. § 17-1, og er å anse som erstatningsrettslig vernet skade.

4.2.2 Ansvarsgrunnlag

Styremedlemmene må, for å bli holdt erstatningsansvarlig etter asl. § 17-1 "*forsettlig*" eller "*uaktsomt*" ha foretatt en handling eller unnlatelse som har ledet til skade. Simpel uaktsomhet er tilstrekkelig for ansvar.[159]

Dersom styremedlemmene bevisst - forsettlig - påfører selskapet skade og økonomisk tap er vilkåret om ansvarsgrunnlag klart oppfylt. Dette vil være tilfellet der styrets medlemmer bevisst har unnlatt å sørge for selskapets etterlevelse av GDPR. Styremedlemmene kan også bli erstatningsansvarlig dersom de har utvist uaktsomhet, såfremt det økonomiske tapet (skaden) var en påregnelig følge av den utviste uaktsomhet.[160] Det følger også av Artikkel 29-gruppens retningslinjer at det ved vurderingen av om bot skal ilegges skal ses hen til om bruddet på GDPR grunner i forsett eller uaktsomhet hos den behandlingsansvarlige, styret.[161]

Styrets erstatningsansvar er et speilbilde av de pliktene som følger av blant annet lov, og styrets ansvar aktualiseres der rettsregler om styrets plikter er overtrådt.[162] Etter asl. § 17-1 og alminnelige erstatningsrettslige regler kreves at styremedlemmet har utvist tilstrekkelig grad av skyld for å kunne ilegges erstatningsansvar. Det må foreligge et normbrudd, og styremedlemmene må kunne lastes for normbruddet.[163] For personlig erstatningsansvar må det foreligge en objektiv overtredelse av en plikt så vel som subjektiv skyld fra styremedlemmet side. Dersom styremedlemmene har opptrådt uaktsomt kan man risikere at

[157] Normann Aarum (1994) s. 71.
[158] Sæbø (2002) s. 200 og Woxholt (2012) s. 304.
[159] Normann Aarum (1994) s. 126.
[160] Se kapittel 4.2.3.
[161] Guidelines on the application and setting of administrative fines (2017) s. 11.
[162] Bugge Reiersen (2007) s. 23.
[163] Perland (2013) s. 2.

styremedlemmene holdes personlig erstatningsansvarlig for hele eller deler av boten som ilegges i medhold av GDPR artikkel 83.[164]

4.2.2.1 Ansvarsgrunnlagets objektive side

Det følger av Høyesteretts dom HR-2016-1440-A at det ved vurderingen av om vilkårene etter asl. § 17-1 første ledd er oppfylt, må tas utgangspunkt i om "*aksjeeier/styreleder har overtrådt de plikter som objektivt sett gjelder for vedkommende*".[165] Sitatet gjelder for styreleder, men det er klart at tilsvarende utgangspunkt må legges til grunn for styremedlemmer i sin alminnelighet.

Utgangspunktet for vurderingen av om det foreligger en erstatningsbetingende handling eller unnlatelse, forsettlig eller uaktsomt, må tas i de plikter som pålegges styret.[166] Styrets plikter kan følge direkte av aksjelovgivningen eller av annen lovgivning. Det er ingen forutsetning for erstatningsansvar at det er bestemmelser i aksjeloven som er overtrådt, styret kan også pålegges ansvar ved overtredelse av plikter som følger av annen lovgivning.[167] Det er imidlertid lavere terskel for å ilegge erstatningsansvar ved brudd på plikter som følger direkte av aksjeloven.[168] Ansvarsgrunnlagets objektive side fastlegges ved en presisering av de selskapsrettslige regler. For avhandlingens vedkommende er plikten til forsvarlig forvaltning av selskapet etter asl. § 6-12 sentral.[169] For brudd på plikter som påhviler styret etter aksjeloven foreligger en presumsjon for utvist uaktsomhet og for at den objektive siden av ansvarsgrunnlaget er oppfylt.[170]

I det videre skisseres enkelte eksempler på hvordan styremedlemmene objektivt sett kan ha overtrådt sine plikter etter GDPR artikkel 24, 30, 32 og 38 og dermed brutt sin plikt til forsvarlig forvaltning av selskapet etter asl. § 6-12. Ansvarsgrunnlagets subjektive side behandles under kapittel 4.2.2.2.

---

[164] Nordli (2018), https://www.eksterngransking.no/single-post/2018/02/03/Fra-25mai-2018-kan-styremedlemmer-i-aksjeselskaper-risikere-erstatningsanvar-p%25C3%25A5-20-millioner-Euro-ved-brudd-p%25C3%25A5-GDPR---forordningen.
[165] HR-2016-1440-A, avsnitt 41.
[166] Dette fremkommer også gjennom at det økonomiske tapet som er voldt selskapet må være pådratt av styremedlemmene "*i den nevnte egenskap*" jf. § asl. 17-1. Vurderingen av om handlingen/unnlatelsen er ansvarsbetingende må da tas i de plikter som pålegges styremedlemmene.
[167] Bugge Reiersen (2007) s. 29 og Aarbakke m.fl. (2017) Kommentar til asl. § 17-1.
[168] Den norske Revisorforening (2004) s. 36.
[169] Jf. kapittel 3.
[170] Ot.prp. nr. 36 (1993-1994) s. 83 og Andenæs, Berge, Christoffersen m.fl. (2016) s. 648.

For styremedlemmers erstatningsansvar er unnlatelsesansvar særlig aktuelt.[171] Eksempelvis er dette aktuelt der styret unnlater å reagere på rapport fra personvernombud om mulige overtredelser av GDPRs bestemmelser. I en dom fra Oslo tingrett følger at styret må ha "*en særlig oppfordring til å foreta undersøkelser*" for at det kan være tale om ansvar etter asl. § 17-1.[172] Dersom selskapets personvernombud for eksempel rapporterer til styret at det foreligger manglende sikkerhetstiltak etter GDPR artikkel 32 og mulig brudd på informasjonssikkerheten gir dette styret en særlig oppfordring til å undersøke nærmere. Særlig gjelder dette sett i lys av det særskilte ansvaret og kompetansen som skal ligge hos personvernombudet. Også der daglig leder eksempelvis informerer eller fremlegger sak for styret om at selskapets retningslinjer for vern av personopplysninger jf. GDPR artikkel 24 ikke er tilstrekkelige eller operative, og styret unnlater å ta dette til etterretning, har styret hatt en særlig oppfordring til å reagere på risikoinformasjon. Dersom styret unnlater å reagere på risikoinformasjon fra personvernombud eller daglig leder, eller handler i strid med råd fra personvernombud, og selskapet bøtelegges for brudd på forordningen har styret klart overtrådt sine plikter etter asl. § 6-12.[173] Dette vil kunne være ansvarsbetingende etter asl. § 17-1.[174] Forsvarlighetskravet i asl. § 6-12 første ledd annet punktum innebærer et generelt krav til løpende vurdering og håndtering av selskapets risikoforhold.[175]

Plikten til å reagere på risikoinformasjon illustreres ved Høyesteretts dom i Rt. 2007 s. 1684.[176] Dommen omhandler et tilfelle hvor en ansatt i et firma som drev installasjon og service av kjøleanlegg forårsaket omfattende fiskedød ved at vedkommende tømte ut et fat med ammoniakkholdig vann i en elv. Den ansatte hadde varslet om at han ville tømme ut det skadelige vannet i elven, men dette foranlediget ingen konkrete tiltak fra ledelsens side.[177] Høyesterett fant at det i selskapet forelå manglende retningslinjer, opplæring og internkontroll, slik at hendelsen kunne vært forhindret.[178] Høyesteretts uttalelser er uttrykk for at selskapets ledelse, herunder styret, har et ansvar for å reagere på risikoinformasjon.

[171] Normann Aarum (1994) s. 71.
[172] TOSLO-2011-26201.
[173] Guidelines on the application and setting of administrative fines (2017) s. 11.
[174] Eriksen (2015) s. 385.
[175] Eriksen (2015) s. 344.
[176] Dommen omhandlet spørsmål om ileggelse av foretaksstraff. De generelle betraktninger om ledelsens og styrets ansvar er likevel av interesse for avhandlingen.
[177] Rt. 2007 s. 1684, avsnitt 33.
[178] Rt. 2007 s. 1684, avsnitt 35.

Styret har et overordnet ansvar for å iverksette retningslinjer for vern av personopplysninger.[179] Unnlatelse av å etablere retningslinjer for behandling av personopplysninger, slik selskapet er forpliktet til etter GDPR artikkel 24, er en overtredelse av styrets plikt etter asl. § 6-12. Ytterligere et eksempel på objektiv overtredelse av styrets plikter er der selskapet ikke har utnevnt personvernombud, i selskap der dette er påkrevd etter forordningen.[180]

Når det overordnede ansvaret for etterlevelse av GDPR ligger hos styret jf. asl. § 6-12, har styret blant annet ansvar for iverksetting av rutiner og retningslinjer, for hensiktsmessig organisering og for selskapets ressursbruk. Hvorvidt styret har overtrådt sine plikter i den konkrete sak vil variere med hvorvidt styret har delegert ansvar og oppfølgning av dette til daglig leder med videre. Styret anses i utgangspunktet ikke for å ha overtrådt sine plikter dersom det er daglig leder som ikke har ivaretatt sitt ansvar.[181]

Til sist bemerkes at etter GDPR artikkel 83 nr. 2 bokstav e skal det ved vurderingen av om selskapet skal bøtelegges ses hen til tidligere overtredelser. Det er følgelig et moment i retning av ansvar for styremedlemmene dersom mangler eller brudd på forordningen tidligere har vært konstatert og styret i etterkant ikke har foretatt noe for å hindre at overtredelser forekommer på nytt.

Selv om styret objektivt sett har brutt sine plikter etter aksjeloven § 6-12 sammenholdt med personvernforordningen, er det en forutsetning for å konstatere erstatningsansvar at styremedlemmene også kan bebreides for å ha opptrådt i strid med plikten.[182]

4.2.2.2 Ansvarsgrunnlagets subjektive side. Aktsomhetsnormen

Styremedlemmene må kunne bebreides for ved handling eller unnlatelse å ha opptrådt uaktsomt.[183] Av aksjeloven § 6-12 følger et alminnelig krav til forsvarlig utøvelse av vervet som styremedlem i aksjeselskap. Den erstatningsrettslige aktsomhetsnorm fastsettes ut fra de forventninger som med rimelighet kan stilles til et normalt og samvittighetsfullt styremedlem.

[179] Jf. konklusjon i kapittel 3.2.1.
[180] Se GDPR artikkel 37.
[181] Normann Aarum (1994) s. 360. Merk imidlertid styrets tilsynsansvar med den daglige ledelse jf. asl. § 6-13 første ledd.
[182] Ved forsettlige overtredelser er det ikke aktuelt å vurdere om styremedlemmene kan bebreides for overtredelsen, dette er kun aktuelt ved spørsmål om uaktsomhet.
[183] Normann Aarum (1994) s. 188.

I utgangspunktet er forventningene de samme for alle styremedlemmer, men ansvaret kan skjerpes ved særskilte kvalifikasjoner.[184] Ved objektive overtredelser av plikten til forsvarlig forvaltning etter asl. § 6-12, må det vurderes om styremedlemmene har handlet slikt som med rimelighet kan ventes, sett i lys av de krav og forventninger som stilles til styremedlemmene. Forventningene til styret har endret seg de senere år, og vil trolig endres i lys av nytt personvernregelverk, jf. det som er skrevet om endringer i styrets forvaltningsansvar etter asl. § 6-12.

Aktsomhetsnormen innebærer at det er avviket fra forsvarlig opptreden som sanksjoneres i form av erstatningsansvar. Handlingsnormen for forsvarlig opptreden følger av plikten til forsvarlig forvaltning av selskapet etter asl. § 6-12. Utgangspunktet når styremedlemmer har opptrådt i strid med pålagte plikter er at de kunne handlet annerledes, og også at de burde gjort det.[185] Kravet til ansvarsgrunnlag er derfor ofte oppfylt allerede når det konstateres brudd på styrets plikter.[186] Styremedlemmene har opptrådt forsvarlig når de har opptrådt i samsvar med deres plikter på det aktuelle ansvarsområdet. Her vises til de plikter som er behandlet i kapittel 3.2 flg. Det foreligger derfor en presumsjon for at styremedlemmene kan bebreides for å ha opptrådt uaktsomt i tilfeller av manglende etterlevelse av GDPR som skyldes forsømmelse av plikten til forsvarlig forvaltning etter asl. § 6-12.

I Høyesteretts dom i Rt. 2013 s. 1143 omtaler Høyesterett aktsomhetsnormen som hviler på styrelederen i et aksjeselskap.[187] Styrelederen i et tankselskap tok del i beslutning om og gjennomføring av mottak av sluttbehandlingsavfall og en påfølgende renseprosess hvor det for selskapet ikke forelå tilstrekkelig og riktig tillatelse fra Statens forurensningstilsyn. Som konsekvens av renseprosessen oppsto en eksplosjon som voldte både personskader og materielle skader.[188] Styrelederen ble i lagmannsretten dømt for overtredelser av forurensningsloven, arbeidsmiljøloven og brann- og eksplosjonsvernloven. Anken ble ikke tillatt fremmet for Høyesterett, som sluttet seg til lagmannsrettens dom.[189]

[184] Eriksen (2015) s. 383.
[185] Bugge Reiersen, upublisert manus, s. 10.
[186] Rt. 1930 s. 481, Perland (2013) s. 3 og Aarbakke m.fl. (2017) Kommentar til asl. § 17-1.
[187] Dommen omhandlet spørsmål om straff for styrelederen, men de generelle uttalelser i dommen om styreleders ansvar og den aktsomhetsnormen som hviler på styreleder er interessante også for spørsmålet om styremedlemmenes erstatningsansvar.
[188] Rt. 2013 s. 1143, avsnitt 7.
[189] LG-2012-23847.

I lagmannsrettens dom vises det til styrets ansvar for virksomheten samt plikten til å holde seg orientert om denne.[190] Lagmannsretten fant at styrelederen, med den kunnskap han hadde om hvilke tillatelser som forelå, skulle ha sørget for at det ble foretatt lovmessige risikovurderinger. Styrelederen hadde ikke sørget for tilstrekkelig risikoanalyse hva angikk eksplosjonsfaren og heller ikke sørget for at det var utarbeidet eksplosjonsverndokument. Det forelå en uaktsom unnlatelse fra styreleders side.[191]

Det kan fra dommen trekkes paralleller til det som ovenfor er skrevet om styremedlemmenes unnlatelsesansvar og styremedlemmenes plikt til å reagere på risikoinformasjon. Uttalelsene i dommen underbygger at styremedlemmene må ta en aktiv rolle i selskapets risikovurdering og utarbeidelse av retningslinjer for å unngå å kunne pådra seg personlig erstatningsansvar der det foreligger brudd på personvernforordningen.

Under en vurdering av om styremedlemmene subjektivt kan lastes for normbruddet, er det viktig å poengtere at det må gå en grense for hva som anses å være avvik fra forsvarlig opptreden. Personvernforordningen er for mange av kravene risikobasert,[192] slik at hvilke tiltak som må iverksettes for å sikre etterlevelse vil variere med typen selskap, typen og mengden av personopplysninger som behandles, hvilke risiki selskapet står ovenfor med videre. Det kan for styret i mange tilfeller være vanskelig å vite hva som er "godt nok". Det kan derfor ikke automatisk bli tale om personlig erstatningsansvar dersom det eksempelvis senere viser seg at informasjonssikkerhetstiltakene etter forordningen artikkel 32 ikke var tilstrekkelig for å forhindre datainnbrudd. Poenget i denne sammenheng er at styret har et overordnet ansvar og må holdes informert, være delaktig og stille de rette spørsmål. Avvik fra forsvarlig opptreden foreligger først der styret inntar en posisjon hvor de ikke vil engasjere seg, ikke legger til rette for eller ikke gir selskapet mulighet til å etterleve forordningens krav.

Videre har styremedlemmene en generell plikt til å fremme selskapets interesse og til å forvalte selskapet etter asl. § 6-12. Det er likevel ikke slik at enhver feilvurdering eller kritikkverdig opptreden innebærer brudd på forsvarlighetsnormen og påfører styremedlemmene personlig erstatningsansvar.[193] Styret handler på selskapets vegne, skal fremme hva som er best for selskapet og ivareta selskapets interesser.[194] Å drive et

[190] LG-2012-23847.
[191] Rt. 2013 s. 1143, avsnitt 11 og 12.
[192] Se kapittel 2.2.
[193] Andenæs, Berge, Christoffersen m.fl.(2016) s. 647 og dom fra Agder lagmannsrett LA-2017-76255.
[194] Normann Aarum (1994) s. 349.

aksjeselskap innebærer økonomisk risiko, og styret har handlingsrom for å ta forretningsrisiko i beslutninger som gjelder driften av selskapet.[195] Aksjonærene har ved å investere midler i selskapet akseptert at den forretningsmessige risiko kan medføre tap, så vel som gevinst.[196] For at ansvarsgrunnlag skal foreligge og selskapet skal kunne kreve erstatning for tap må styremedlemmene ha gjort en feil som går ut over den akseptable forretningsmessige risiko.[197]

For avhandlingens vedkommende er det imidlertid tale om etterlevelse av et lovverk. Den forretningsrisiko som styret kan ta kan ikke gå på akkord med lovpålagte plikter. Manglende implementering og etterlevelse av GDPR er ikke innenfor rammene av tillatt risiko.

4.2.3 Årsakssammenheng

Ved siden av at styret har overtrådt sine plikter og kan bebreides for dette, er erstatningsansvar betinget av at det foreligger årsakssammenheng jf. asl. § 17-1 om at styret har "*voldt*" selskapet skade.[198] Styrets medlemmer kan i samsvar med dette bare ilegges ansvar overfor selskapet for manglende etterlevelse av GDPR der det kan påvises at styremedlemmene, gjennom sin forsettlig eller uaktsomme handling eller unnlatelse, har påført selskapet et erstatningsmessig tap.[199]

Kravet til årsakssammenheng fordrer en konkret vurdering av den aktuelle skaden/tapet i hvert enkelt tilfelle. Det følger av P-pilledom II at det må vurderes om handlingen eller unnlatelsen var en "*nødvendig betingelse*" for tapet som oppsto.[200] I tillegg må tapet ha vært en påregnelig følge av handlingen eller unnlatelsen. Dersom styrets forsettlige eller uaktsomme handling eller unnlatelse var en nødvendig betingelse for at selskapet ikke har etterlevd kravene i GDPR, og selskapet for dette bruddet er bøtelagt, foreligger tilstrekkelig årsakssammenheng.

I at skaden er "*voldt*" av styret, jf. § 17-1, ligger at skaden kan ha oppstått både gjennom aktiv deltakelse i beslutningsprosessen og unnlatelse av å følge opp denne prosessen eller unnlatelse av å følge opp informasjon som fremkommer i prosessen.[201] Dette illustrerer det

[195] Normann Aarum (1994) s. 120.
[196] Normann Aarum (1994) s. 120.
[197] Aarbakke m.fl. (2017) Kommentar til asl. § 17-1.
[198] Knudtzon (2004) s. 110.
[199] Norman Aarum (1994) s. 72 og Lødrup (1999) s. 60.
[200] Rt. 1992 s. 64, s. 50.
[201] Matre (2014) note 2665.

som ovenfor er skrevet om ansvarsgrunnlag og aktsomhetsnorm, og styrets rolle i de prosesser som sørger for etterlevelse av GDPR.

Rettspraksis viser at det i praksis kan være vanskelig å påvise årsakssammenheng mellom styremedlemmenes handling eller unnlatelse og det tapet som selskapet lider.[202] Trolig vil det i mange tilfeller være krevende å peke på hvor det gikk galt, og vanskelig å avgjøre om årsaken til manglende etterlevelse av GDPR ligger hos styret eller hos en eller flere enkeltansatte ved den praktiske gjennomføringen av behandlingen av personopplysninger i selskapet. Terskelen vil trolig være høy for at vilkåret om årsakssammenheng er innfridd, jf. også det som er skrevet om at GDPR er risikobasert og at det er vanskelig for styremedlemmene å avgjøre hva som er "godt nok". Der styret har vært delaktig i prosessene, bevilget midler og iverksatt retningslinjer, og selskapet likevel bøtelegges fordi det på et punkt har sviktet, foreligger det sannsynligvis ikke tilstrekkelig årsakssammenheng til å ilegge styremedlemmene personlig erstatningsansvar.

[202] Se blant annet Rt. 1979 s. 46, Rt. 1923 s. 774 og Rt. 1937 s. 501 som alle gir støtte til oppfatningen om at kravet til årsakssammenheng oppfattes strengt hva gjelder erstatningsregelen i asl. § 17-1.

5 Konklusjon og avsluttende betraktninger

Avhandlingens fremstilling har vist at GDPR innebærer en utvidelse og skjerpelse av styrets plikt til forsvarlig forvaltning av selskapet etter asl. § 6-12, ved at styret må innta en aktiv og temmelig konkret rolle i arbeidet med å sikre etterlevelse av GDPR. Denne rettsutviklingen får igjen betydning for ansvarsgrunnlaget og aktsomhetsnormen under erstatningsregelen i asl. § 17-1, slik at erstatningsansvaret på området i en viss utstrekning skjerpes.[203]

Styret er behandlingsansvarlig etter GDPR og pålegges en rekke nye plikter. Mange av pliktene etter forordningen er likevel en videre utvikling av de plikter som allerede ligger til styret i dag, eksempelvis nevnes kravene til internkontroll og informasjonssikkerhet. GDPR utvider og presiserer enkelte av disse pliktene, blant annet ved at det stilles strengere krav til dokumentert etterlevelse, hvilket innebærer en skjerpelse og utvidelse i hva som faller innunder forvaltningsansvaret etter asl. 6-12. GDPR sin innvirkning på forståelsen av forvaltningsansvaret viser fleksibiliteten i bestemmelsen i aksjeloven § 6-12. Det er en kontinuerlig prosess å vurdere hva som ligger i forventningen om og plikten til forsvarlig forvaltning av selskapet fra styrets side.

Det kan, som følge av rettsutviklingen, få store konsekvenser dersom styret ikke involverer seg tilstrekkelig i virksomhetens håndtering av personopplysninger. Det gjelder både risikoen for omdømmetap og for økonomiske sanksjoner som bøter, personlig erstatningsansvar eller erstatningsansvar for tredjemannstap,[204] samt store kostnader dersom selskapet på et senere tidspunkt får pålegg fra Datatilsynet og må iverksette tiltak for å sikre etterlevelse av forordningen.[205]

En mer overordnet konsekvens av rettsutviklingen er at personvernforordningen trolig vil få betydning for kravene til styrets sammensetning og kompetanse. Når det stilles nye krav til at styret skal arbeide aktivt med og være delaktig i å sikre etterlevelse av personvernregelverket selskapet er underlagt, vil det gi seg utslag i hvilket kompetansebehov som oppstår i styret. Kravet er forankret i GDPR som eksternt lovkrav, men også fra samfunnet rundt når personvern er satt på agendaen. Det stilles ytterligere krav til styret fra selskapets øvrige

[203] Jf. også tilsvarende skjerpelse av erstatningsansvaret ved vedtakelsen av dagens aksjelov, se NOU 1996: 3 s. 275 og kapittel 3.1.1 i avhandlingen.
[204] Se GDPR artikkel 82 om rett til erstatning.
[205] De midler og ressurser selskapet kunne spart ved å ikke iverksette tiltak for å etterleve GDPR i dag, kan senere vise seg å bli en enda større kostnad dersom selskapet på et senere tidspunkt av Datatilsynet pålegges å iverksette tiltak for å sikre etterlevelse.

ansatte, og også aksjonærene, når styret har et ansvar i å sette "the tone at the top" og for å vise at personvern er en prioritet i selskapet. Det blir stadig viktigere å dyrke personvern som en del av selskapskulturen, og arbeidet må starte på toppen, hos styret. Disse forventningene til styret vil samlet påvirke aktsomhetsnormen ved vurderingen av ansvarsgrunnlaget etter asl. § 17-1.

Styremedlemmene kan *unngå* å pådra seg personlig erstatningsansvar ved å være delaktig, stille de rette spørsmålene og ved å aktivt involvere seg i prosessene med etterlevelse av forordningen i selskapet.[206] Styret må sette klare og gode retningslinjer for hvordan personopplysninger skal behandles i virksomheten og bevilge de ressursene som er nødvendig for å overholde personvernforordningens krav. Da vil det vanskelige foreligge årsakssammenheng og heller ikke ansvarsgrunnlag, jf. vilkårene i asl. § 17-1. Jo tidligere personvernhensyn identifiseres og veies mot andre hensyn, dess enklere vil det være å finne gode løsninger for selskapet. Styremedlemmene må være seg bevisst sitt ansvar og verdiene hele veien, fra implementering av forordningen og gjennomgående for etterlevelse. På sikt vil dette tjene selskapet på flere måter, særlig viktig er at solid etterlevelse av personvernregelverket vil styrke selskapets omdømme. I enkelte tilfeller, dersom styret inntar en passiv holdning til etterlevelse, unnlater å reagere på risikoinformasjon eller liknende, kan personlig erstatningsansvar tenkes.

Som eksempel på et tilfelle hvor personlig erstatningsansvar for styremedlemmene for manglende etterlevelse av personvernregelverk kunne vært aktuelt vises til Helse Sør-Øst saken,[207] hvor IT-infrastruktur ble outsourcet og utenlandske IT-arbeidere fikk tilgang på sensitive personopplysninger.[208] Styrelederen i Helse Sør-Øst fikk kritikk av Datatilsynet for manglende styring og ledelse, og ledelsen fikk kritikk for manglende etterlevelse av regelverket.[209] Datatilsynet mente det ikke ble gjennomført nødvendige risiko- og sårbarhetsvurderinger før det ble besluttet å outsource IT-infrastruktur.[210] En gjennomgang av

[206] Videre vil det heller ikke være aktuelt med personlig erstatningsansvar der et styremedlem aktivt har stemt mot et forslag som har ledet til selskapets bøtelegging. Det er derfor viktig at slike protester protokolleres i styrets vedtak.
[207] Saken gjelder forhold som hendte før GDPRs ikrafttreden, og personlig erstatningsansvar for manglende etterlevelse av GDPR er således ikke et aktuelt spørsmål. Saken illustrerer likevel på en god måte styrets ansvar og rolle i spørsmål om etterlevelse av personvernregelverk.
[208] Se om sakens nærmere forløp og innhold: https://www.nrk.no/nyheter/it-svikt-i-helse-sor-ost-1.13502238
[209] NRK (2018) *Datatilsynet fant lovbrudd: Millionbøter etter outsourcing av sykehus-IT,* https://www.nrk.no/norge/millionboter-etter-outsourcing-av-sykehus-it-1.13751516.
[210] NRK (2018) *Datatilsynet fant lovbrudd: Millionbøter etter outsourcing av sykehus-IT,* https://www.nrk.no/norge/millionboter-etter-outsourcing-av-sykehus-it-1.13751516.

alle styredokumenter for Helse Sør-Øst og Sykehuspartner over en toårsperiode viste at informasjonssikkerhet og personvern ikke var drøftet på styremøter.[211] Styrene hadde ikke hatt tilstrekkelig informasjon om selskapenes håndtering av personopplysninger, og viktige beslutninger var ikke forankret i ledelsen.

Saken fra Helse Sør-Øst viser både viktigheten av at styret er involvert i saker som omhandler etterlevelse av personvernregelverk, og at styret har tilstrekkelig informasjon og aktivt tar del i beslutningsprosessene. Styrets rolle og involvering har som vist blitt enda viktigere som følge av GDPR.

Personlig erstatningsansvar for styremedlemmene for brudd på GDPR vil være en ytterste konsekvens. Det er ingen automatikk i at selskapet bøtelegges for brudd på kravene i GDPR og at styremedlemmene holdes personlig erstatningsansvarlig for tapet. Der styremedlemmene ikke kan klandres for årsaken til bruddet, betaler selskapet boten uten at det reises erstatningskrav mot styremedlemmene. Ved uklarheter knyttet til hvilket handlingsalternativ som i det enkelte tilfellet best sikrer etterlevelse av personvernforordningen, bør styret i mange tilfeller kunne treffe sin beslutning uten å bli personlig erstatningsansvarlig i ettertid,[212] jf. det som er skrevet om at kravene etter forordningen er risikobasert. Aktsomhetsnormen for styremedlemmene kan ikke bli så streng at det skapes frykt som fører til at man avstår fra å påta seg styreverv. Desto viktigere er det å presisere hvilket ansvar som hviler på styremedlemmene når GDPR får virkning, noe denne avhandlingen har søkt å gjøre.

[211] NRK (2018) *Datatilsynet fant lovbrudd: Millionbøter etter outsourcing av sykehus-IT,* https://www.nrk.no/norge/millionboter-etter-outsourcing-av-sykehus-it-1.13751516.
[212] Normann Aarum (1994) s. 336.

Litteraturliste

Lover og forskrifter

1981 Lov 13. mars 1981 nr. 6 om vern mot forurensning og om avfall (forurensningsloven)

1997 Lov 13. juni 1997 nr. 44 om aksjeselskaper (aksjeloven)

2000 Lov 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven)

2000 Forskrift 15. desember 2000 nr. 1265 om behandling av personopplysninger (personopplysningsforskriften)

2003 Forskrift 21. mai 2003 nr. 630 om bruk av informasjons- og kommunikasjonsteknologi (IKT)

2005 Lov 17. juni 2005 nr. 62 om arbeidsmiljø, arbeidstid og stillingsvern mv. (arbeidsmiljøloven)

2007 Forskrift 19. juni 2007 nr. 876 til verdipapirhandelloven (verdipapirforskriften)

2007 Lov 29. juni 2007 nr. 75 om verdipapirhandel (verdipapirhandelloven)

2008 Forskrift 22. september 2008 nr. 1080 om risikostyring og internkontroll

Lovforarbeider

NOU 1992: 29 Lov om aksjeselskaper

NOU 1996: 3 Ny aksjelovgivning

NOU 1997: 19 Et bedre personvern – forslag til lov om behandling av personopplysninger

NOU 2018: 6	Varsling – verdier og vern. Varslingslovutvalgets utredning om varsling i arbeidslivet
Ot.prp. nr. 36 (1993-1994)	Om lov om aksjeselskaper (aksjeloven)
Ot.prp. nr. 23 (1996-1997)	Om lov om aksjeselskaper (aksjeloven) og lov om allmennaksjeselskaper (allmennaksjeloven)
Ot.prp. nr. 92 (1998-1999)	Om lov om behandling av personopplysninger (personopplysningsloven)
Ot.prp. nr. 34 (2006-2007)	Om lov om verdipapirhandel (verdipapirhandelloven) og lov om regulerte markeder (børsloven)
Prop. 1 S (2017-2018)	Kommunal- og moderniseringsdepartementet. For budsjettåret 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
Innst. 278 L (2017-2018)	Om Lov om behandling av personopplysninger (personopplysningsloven)
Lovvedtak 54 (2017-2018)	Vedtak til lov om behandling av personopplysninger (personopplysningsloven)

Rettspraksis

Rt. 1923 s. 774

Rt. 1930 s. 481

Rt. 1937 s. 501

Rt. 1979 s. 46

Rt. 1992 s. 64 P-pilledom II

Rt. 2007 s. 1684

Rt. 2013 s. 1143

HR-2016-1440-A

LG-2012-23847 (Gulating)

LA-2017-76255 (Agder)

LB-2016-181811 (Borgarting)

TOSLO-2011-26201 (Oslo)

Offentlige dokumenter

Justis- og beredskapsdepartementet. (2017) *Høringsnotat - Ny personopplysningslov – gjennomføring av personvernforordningen i norsk rett,* 6.7.2017 [https://www.regjeringen.no/contentassets/c907cd2776264a6486b8dd3ee00a4e3d/horingsnotat--ny-personopplysningslov--gjennomforing-av-personvernforordningen-i-norsk-rett.pdf] [Sitert 24.3.2018]

Justis- og beredskapsdepartementet (2017). EØS-notat. *Personvernforordningen,* 9.8.2017 [https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2014/aug/forslag-til-personvernforordning/id2433856/] [Sitert 3.3.2018]

Kommunal- og moderniseringsdepartementet. (2017). *Høringsnotat - behandling av opplysninger i kredittopplysningsvirksomhet,* 19.12.2017 [https://www.regjeringen.no/contentassets/8ca0466b2ffb467cbaecf5a1446717eb/kredittopplysningslov_hoeringsnotat.pdf] [Sitert 24.3.2018]

Justis- og beredskapsdepartementet. (2018). *Når får vi ny personopplysningslov?* 23.5.2018 [https://www.regjeringen.no/no/aktuelt/nar-far-vi-ny-personopplysningslov/id2599511/] [Sitert 10.5.2018]

Stortinget – Møte mandag den 28. mai 2018. [https://www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Referater/Stortinget/2017-2018/refs-201718-05-28?all=true.] [Sitert 31.5.2018]

Finanstilsynet. *Veiledning til forskrift om risikostyring og internkontroll,* (2009), [Tilgjengelig på: https://www.finanstilsynet.no/nyhetsarkiv/rundskriv/2009/veiledning-til-forskrift-om-risikostyring-og-internkontroll/] [Sitert 11.4.2018]

Datatilsynets veileder. *Hva betyr de nye personvernreglene for din virksomhet?* (2016). [Tilgjengelig på: https://www.datatilsynet.no/regelverk-og-skjema/veiledere/hva-betyr/] [Sitert 3.3.2018]

Datatilsynets veileder. *Virksomhetens ansvar etter nytt regelverk,* (2017). [Tilgjengelig på: https://www.datatilsynet.no/regelverk-og-skjema/veiledere/virksomhetens-ansvar-etter-nytt-regelverk/] [Sitert 3.3.2018]

Datatilsynets veileder. *Personvernombud etter nytt regelverk,* (2017). [Tilgjengelig på: https://www.datatilsynet.no/regelverk-og-skjema/veiledere/personvernombudsordningen-etter-nytt-regelverk/?print=true] [Sitert 25.3.2018]

Datatilsynet. *En veiledning om internkontroll og informasjonssikkerhet,* (2009). [Tilgjengelig på: https://www.datatilsynet.no/globalassets/global/regelverk-skjema/veiledere/internkontroll_veil.pdf] [Sitert 16.5.2018]

Internasjonale kilder

Regulation (EU) 2016/679	Regulation (EU) of the European Parliament and 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)
Directive 95/56/EC	Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of

individuals with regard to the processing of personal data and the free movement of such data

Communication 52018DC0043 — Communication from the Commission to the European Parliament and the council - Stronger protection, new opportunities – Commision guidance on the direct application of the General Data Protection Regulation as of 25 May 2018, 24. januar 2018

Article 29 Data Protection Working Party, *Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679*, (2017). [Tilgjengelig på: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237] [Sitert 24.3.2018]

Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers ("DPOs"),* (2017). [Tilgjengelig på: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048] [Sitert 24.3.2018]

Juridisk litteratur

Bøker

Normann Aarum (1994) — Aarum, Kristin Normann. *Styremedlemmers erstatningsansvar i aksjeselskaper*, Oslo: Gyldendal, 1994.

Andenæs, Berge, Christoffersen m.fl. (2016) — Andenæs, Mads Henry, Ole Andenæs, Stig Berge og Margrethe Buskerud Christoffersen. *Aksjeselskaper & Allmennaksjeselskaper*, Oslo: M.H. Andenæs, 2016.

Bråthen (2013) — Bråthen, Tore. *Selskapsrett*, 4. utg., Oslo: Focus Forlag, 2013.

Bøhren (2011)	Bøhren, Øyvind. *Eierne, styret og ledelsen – Corporate governance i Norge,* Bergen: Fagnokforlaget, 2011.
Den norske Revisorforening (2004)	Den norske Revisorforening. *Styrets arbeid og ansvar,* Facta, 2004.
Eriksen (2015)	Eriksen, Birthe. *Arbeidstakers rett til å varsle om "kritikkverdige forhold" etter arbeidsmiljøloven § 2-4(1),* (Doktorgradsavhandling) Bergen, 2015.
Knudtzon (2004)	Knudtzon, Sigurd. "Corporate governance i et rettslig perspektiv", i *Corporate governance i et norsk perspektiv,* Øyvind Thorsby (red.), Oslo, 2004, s. 88-113.
Lødrup (1999)	Lødrup, Peter. *Lærebok i erstatningsrett,* 4. utg., Oslo, 1999
Bugge Reiersen (2007)	Reiersen, Hedvig Bugge. *Ansvarsbegrensning og ansvarsfrihet i aksjeselskaper,* Bergen: Fagbokforlaget, 2007.
Rüker/Kugler (2018)	Rüker, Daniel og Tobias Kugler. *New European General Data Protection Regulation – A Practitioner's guide,* 1. utg., Tyskland: C.H.Beck – Hart - Nomos, 2018.
Skullerud, Rønnevik Skorstad m.fl. (2018)	Skullerud, Åste Marie Bergseng, Cecilie Rønnevik, Jørgen Skorstad og Marius Eng Pellerud. *Personvernforordningen (GDPR) Kommentarutgave,* Oslo: Universitetsforlaget, 2018
Thorsby (2004)	Thorsby, Øyvind. "Corporate governance i et rettslig perspektiv", i *Corporate governance i et norsk perspektiv,* Øyvind Thorsby (red.), Oslo, 2004, s.83-84.
Thorson (2010)	Thorson, Bjarte. *Erstatningsrettslig vern for rene formuestap,* Oslo: Det juridiske fakultet, Universitetet i Oslo, 2010.
Veum (2010)	Veum, Helge. "Internkontroll og informasjonssikkerhet", i *Personvern i finanssektoren,* Katrine Berg Blixrud og Christine Ask Ottesen, 1. utg., Oslo: Gyldendal, 2010, s. 204-224.

Woxholt (2012) Woxholt, Geir. *Selskapsrett*, 4. utg., Oslo: Gyldendal, 2012.

Artikler

Aarbakke (1990) Aarbakke, Magnus. "Styremedlemmers og administrerende direktørs erstatningsansvar", *Tidsskrift for rettsvitenskap* (1990) s. 456-468.

Gimmingsrud (2017) Gimmingsrud, Kari. "En ny tidsalder for personvern i Europa", *Arbeidsrett* nr. 2 (2017) s. 220-240.

Perland (1999) Perland, Olav Fr. "Styreansvar i de nye aksjelovene", *Tidsskrift for forretningsjus* (1999) s. 135-159.

Perland (2013) Perland, Olav Fr. "Styremedlemmers erstatningsansvar", *Praktisk økonomi og finans* (2013) s. 21-32.

Bugge Reiersen Reiersen, Hedvig Bugge. "Kravet om forsvarlig egenkapital og likviditet i aksjeselskaper – plikter og ansvar for styremedlemmene", *upublisert manus*.

Sæbø (2002) Sæbø, Rune. "Om erstatningskrav i aksjeselskapsforhold", *Festskrift til Nils Nygaard* (2002) s. 199-212.

Annen juridisk litteratur

Bråthen, Tore. (2015) "Kommentar til Aksjeloven" i *Norsk Lovkommentar, Gyldendal Rettsdata* [Sitert 21.3.2018]

Matre, Hugo P. (2015) "Kommentar til Aksjeloven" i *Norsk Lovkommentar, Gyldendal Rettsdata* [Sitert 24.3.2018]

Schartum, Dag Wiese. (2012) "Kommentar til Personopplysningsloven" i *Norsk Lovkommentar, Gyldendal Rettsdata* [Sitert 20.3.2018]

Aarbakke, Magnus, Asle Aarbakke, Gudmund Knudsen m.fl. (2017) "Aksjeloven: kommentarutgave" i *Kommentarutgaver.no.*

Norsk anbefaling for eierstyring og selskapsledelse, 30. oktober 2014, tilgjengelig på www.nues.no

Nettsider

Alle nettsider sist kontrollert 31.5.2018.

Datatilsynet. *Artikkel 29-gruppen om de nye reglene i personvernforordningen.* (2017), https://www.datatilsynet.no/regelverk-og-skjema/lover-og-regler/uttalelser-fra-artikkel-29-gruppen/eus-personverngruppe-om-innspill-forordningen/ [Sitert 7.4.2018]

Datatilsynet. *Internkontroll og informasjonssikkerhet.* (2011, sist oppdatert 2018), https://www.datatilsynet.no/regelverk-og-skjema/veiledere/internkontroll_informasjonssikkerhet/ [10.5.2018]

Deloitte. *Tone at the top: The first ingredient in a world-class ethics and compliance program.* (2015), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-tone-at-the-top-sept-2014.pdf [Sitert 11.4.2018]

Jan Sandtrø. *Hva kreves av dokumentasjon etter GDPR?* (2017), https://www.sandtro.no/2017/12/05/hva-kreves-av-dokumentasjon-etter-gdpr/ [Sitert 12.3.2018]

Jusleksikon.no. *Lex specialis.* (2017), https://jusleksikon.no/wiki/Lex_specialis [Sitert 10.5.2018]

KPMG. *Cybersikkerhet – fra serverrom til styrerom.* (2018), https://home.kpmg.com/no/nb/home/nyheter-og-innsikt/2018/03/cybersikkerhet-fra-serverrom-til-styrerom.html [Sitert 12.3.2018]

NRK. *Datatilsynet fant lovbrudd: Millionbøter etter outsourcing av sykehus-IT.* (2017), https://www.nrk.no/norge/millionboter-etter-outsourcing-av-sykehus-it-1.13751516 [Sitert 9.5.2019]

NRK. *IT-svikt i Helse Sør-Øst.* (Udatert), https://www.nrk.no/nyheter/it-svikt-i-helse-sor-ost-1.13502238 [Sitert 9.5.2018]

Regelhjelp.no – Veiviser til HMS-regelverket. *Internkontroll.* (2017), http://www.regelhjelp.no/Emner-A---A-/Internkontroll/ [Sitert 11.4.2018]

Rett24.no *Advokat pålagt styreansvar etter Visit Moss-kollapsen.* (2018), http://rett24.no/articles/advokat-palagt-styreansvar-etter-visit-moss-kollapsen [Sitert 18.5.2018]

Roy Nordli. *Erstatningsansvar for styret ved brudd på GDPR.* (2018), https://www.eksterngransking.no/single-post/2018/02/03/Fra-25mai-2018-kan-styremedlemmer-i-aksjeselskaper-risikere-erstatningsanvar-p%25C3%25A5-20-millioner-Euro-ved-brudd-p%25C3%25A5-GDPR---forordningen [Sitert 20.3.2018]