Styrets ansvar ved aksjeselskapets brudd på EUs personvernforordning (GDPR)

Betydningen av GDPR for styremedlemmets personlige erstatningsansvar etter aksjeloven § 17-1 (1)

Kandidatnummer: 123

Antall ord: 14 997

JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

12. desember 2022

Innholdsfortegnelse

1 Innledning

1.1 Avhandlingens tema og aktualitet

Retten til å bestemme over egne personopplysninger er en grunnleggende rettighet, som kan utledes av Grunnloven § 102[1] og Den Europeiske Menneskerettighetskonvensjonen art. 8[2] om rett til respekt for sitt privatliv. Teknologisk utvikling, digitalisering og en stadig voksende internasjonal økonomi er faktorer som har ført til en stor økning i mengden personopplysninger som behandles og utveksles hver eneste dag.[3] Samtidig har både private selskaper og offentlige myndigheter anledning til å nyttiggjøre seg personopplysninger i sine virksomheter i et annet omfang enn før, for eksempel for å bedre forstå forbrukerens interesser og handlingsmønster.[4] Når fysiske personer i tillegg gjør slike opplysninger offentlig tilgjengelig i større grad enn tidligere, gjennom blant annet mer omfattende bruk av digitale tjenester og handel over landegrensene, har dette ført til nye utfordringer for personvernet.[5]

EUs personvernforordning, General Data Protection Regulation[6] (heretter «GDPR», «personvernforordningen» eller «forordningen»), trådte i kraft i EU den 25. mai 2018,[7] og handler om nettopp beskyttelse av personopplysninger.[8] Forordningen fastsetter ulike regler om vern av fysiske personer i forbindelse med behandling[9] av personopplysninger, hvilket skal sikre deres grunnleggende rettigheter og friheter, jf. GDPR art. 1. Personvernforordningen ble formelt innlemmet som norsk lov den 20. juli 2018 gjennom vedtakelsen av personopplysningsloven.[10]

[1] Lov 17. mai 1814 om Kongeriket Norges Grunnlov [Grunnloven].
[2] Convention for the Protection of Human Rights and Fundamental Freedoms, Roma, 4. november 1950 [Den europeiske menneskerettskonvensjonen, EMK].
[3] Gimmingsrud (2017) s. 221-222.
[4] Datatilsynets veileder (2020). *Digitale tjenester og forbrukeres personopplysninger*, avsnitt: *«Databaserte forretningsmodeller»*.
[5] Gimmingsrud (2017) s. 222.
[6] Europaparlamentets og Rådets forordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning) [PVF, GDPR].
[7] Se GDPR art. 99 nr. 2.
[8] Med personopplysninger menes i det videre «enhver opplysning om en identifisert eller identifiserbar fysisk person», jf. GDPR art. 4 nr. 1.
[9] Med «behandling» menes «enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke», jf. GDPR art. 4 nr. 2.
[10] Lov 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven).

Alle norske selskaper som behandler personopplysninger, må derfor forholde seg til og innrette sin virksomhet etter disse reglene. I praksis er det umulig å drive en virksomhet uten å behandle personopplysninger i noen grad, fordi det utgjør en sentral del av ansettelsesprosesser, markedsføring og kontraktsforhold,[11] hvilket medfører at GDPR får betydning for så å si alle norske selskap. Styret utgjør en obligatorisk del av enhver virksomhet, jf. aksjeloven[12] (heretter «asl».) § 6-1, og har kollektive forpliktelser om forvaltning av selskapet og for tilsynet med dets virksomhet etter henholdsvis asl. §§ 6-12 og 6-13. Når GDPR fastsetter regler som norske selskaper må innrette seg etter, er det derfor av interesse å vurdere hvordan dette påvirker styrets ansvar som et selskapsorgan.

Styremedlemmer kan bli holdt personlig erstatningsansvarlig etter asl. § 17-1 (1) om de bryter en forpliktelse som objektivt gjelder for dem, kan lastes for normbruddet, og gjennom dette har påført selskapet, aksjeeier eller andre et økonomisk tap.[13] Temaet for avhandlingen er betydningen av GDPR for styremedlemmenes personlige erstatningsansvar. I dette ligger overordnet en vurdering av om et brudd på forordningen kan oppfylle vilkårene i bestemmelsen. Når GDPR pålegger selskapene forpliktelser de må etterleve, kan mangelfull etterlevelse av forordningen i et styreansvarsperspektiv tenkes å utgjøre et ansvarsbetingende brudd på forvaltnings- og tilsynspliktene om det resulterer i et økonomisk tap. Et sentralt tema i avhandlingen blir derfor hva som kan forventes av et styremedlem i arbeidet med etterlevelsen av GDPR.

Temaet er på dagordenen fordi det i tiden før avhandlingen har blitt avsagt en tysk dom, der en direktør ble holdt personlig ansvarlig for brudd på GDPR.[14] Saken har fått stor oppmerksomhet i Norge, og det har blitt uttrykt i flere kronikker og artikler at det antakeligvis også vil komme saker om styreansvar her, for eksempel ved alvorlige dataangrep.[15] Det tas der til orde for at dommen kan få betydning for rettsutviklingen i Norge, og skjerpe styremedlemmers individuelle ansvar. Sakens faktum er imidlertid svært spesielt,[16] hvilket gjør det interessant å vurdere om dommen rent faktisk kan få slik betydning

[11] Trzaskowski/Sørensen (2022) s. 34.
[12] Lov 13. juni 1997 nr. 44 om aksjeselskaper (aksjeloven).
[13] Bråthen (2022) s. 257.
[14] *Ankeinstans*: OLG Dresden, 30.11.2021 - 4 U 1158/21. *Første instans*: LG Dresden, 26.05.2021 - 8 O 1286/19.
[15] DN (2022) *Innlegg: Direktør dømt personlig ansvarlig for personvernbrudd*, https://www.dn.no/innlegg/jus/personvern/gdpr/innlegg-direktor-domt-personlig-ansvarlig-for-personvernbrudd/2-1-1181801 og Finansavisen (2022) *Alle styremedlemmer – skjerp dere*, https://www.finansavisen.no/nyheter/debattinnlegg/2022/03/29/7841435/alle-styremedlemmer-skjerp-dere
[16] Dommen behandles under kapittel 2.2.1.

for rettsutviklingen som det hevdes.

Videre har det blitt registrert en økning i antall styreansvarssaker for norske domstoler de siste årene, og flere saker har resultert i erstatningsansvar.[17] Fra å tidligere være en nærmest teoretisk mulighet, har styreansvar de senere år blitt en praktisk realitet for styremedlemmer.[18] Samtidig finnes det ingen eksempler i norsk rettspraksis på at et styremedlem har blitt holdt personlig erstatningsansvarlig for brudd på GDPR. Mangelen på rettslig avklaring gjør det aktuelt å vurdere spørsmålet.

Det norske Datatilsynet har også begynt å skrive i sine vedtak at enkeltpersoner, herunder styremedlemmer, anses å ha opptrådt uaktsomt. Datatilsynet fører tilsyn med at personvernregelverket overholdes i Norge, og kan ilegge overtredelsesgebyr ved brudd.[19] I 2021 ble bomselskapet Ferde AS ilagt et overtredelsesgebyr på kr. 5 millioner på grunn av overføringer av opplysninger knyttet til passering i bomringer til en databehandler i Kina.[20] Ferde AS hadde brutt sentrale regler i GDPR, hvilket Datatilsynet uttalte at «måtte klassifiseres som klart uaktsomt», og «at ansvaret ligger hos styret i Ferde AS, jf. aksjeloven § 6-12 første ledd første punktum».[21] Hvis et selskap bryter GDPR, er det virksomheten og ikke enkeltpersoner som sitter igjen med gebyret.[22] Erstatning er juridisk sett noe annet enn overtredelsesgebyr, og Datatilsynets uttalelser utløser i seg selv ikke et personlig ansvar for et styremedlem. At Datatilsynet formulerer seg på denne måten, og retter ansvarlighet mot styret, kan likevel tenkes å gi grobunn for erstatningssaker også på området for GDPR.

Samtidig ser vi økt oppmerksomhet rundt overholdelse av grunnleggende personvernprinsipper i samfunnet generelt. Personvernkommisjonen leverte den 26. september 2022 sin utredning til regjeringen, der det etterlyses en nasjonal personvernpolitikk som omfatter både offentlig og privat sektors behandling av personopplysninger.[23] Utredningen belyser personvernet som samfunnsverdi, og hvordan det er en forutsetning for et åpnet samfunn og et velfungerende demokrati.[24] Rapporten setter personvern på dagsorden, også i styrerommet.

[17] Dahlum (2021) s. 223.
[18] Perland (2013) s. 22.
[19] Jf. kapittel 2.3.
[20] Datatilsynet (2021). *Vedtak om overtredelsesgebyr – Ferde AS.*
[21] Datatilsynet (2021). *Vedtak om overtredelsesgebyr – Ferde AS.* s. 12.
[22] Kuner (2020) s. 149.
[23] NOU: 2022:11 s. 11.
[24] NOU: 2022:11 s. 9.

1.2 Problemstillingen

Avhandlingens problemstilling er om et styremedlem kan holdes personlig erstatningsansvarlig etter asl. § 17-1 (1) for brudd på GDPR av selskapet, aksjeeier eller andre. I dette ligger både en vurdering av om vilkårene etter bestemmelsen kan tenkes oppfylt, og hvorvidt og i hvilke tilfeller det kan være aktuelt å reise sak mot styremedlemmene for erstatning for tapet forårsaket av bruddet.

Etter GDPR er det selskapet selv, som juridisk person, som er pliktsubjekt og ansvarlig etter forordningen for de behandlingene som foretas av virksomheten.[25] Et spørsmål avhandlingen søker å belyse, er hvem som innad i et aksjeselskap har ansvar for at virksomheten etterlever forordningen, og mer konkret hvilke forpliktelser styremedlemmene har som del av et selskapsorgan. Spørsmålet aktualiserer seg ved vurderingen av vilkåret om ansvarsgrunnlag. Her vil kravene GDPR stiller til selskapet vurderes opp mot asl. §§ 6-12 og 6-13. Avhandlingen vil derfor også ta for seg styrets forvaltnings- og tilsynsansvar, og mer konkret hvilke forpliktelser styret har i selskapet for å sikre etterlevelse av GDPR. Slik sett blir avhandlingen både en vurdering av de materielle vilkårene i asl. § 17-1 (1) opp mot GDPR, og en redegjørelse for hvilke krav forordningen i prinsippet stiller til det enkelte styremedlem gjennom aksjeloven.

1.3 Rettskilder og metodiske utfordringer

Den juridiske analysen tar utgangspunkt i asl. § 17-1 (1), kravene som fremgår av GDPR, samt asl. §§ 6-12 og 6-13. Det foreligger ingen autorative rettskilder som behandler spørsmålet om styreansvar for brudd på GDPR etter asl. § 17-1 (1) samlet. I relasjon til asl. § 17-1 (1) om styreansvar, og asl. §§ 6-12 og 6-13 om forvaltnings-, og tilsynsansvaret isolert sett, foreligger det derimot mange rettskilder. Tilsvarende er det skrevet mye rundt GDPR, og det finnes flere bøker, kommentarutgaver, artikler, veiledere osv. som redegjør for forordningens innhold. Selve spørsmålet om styrets personlige erstatningsansvar for brudd på GDPR er like fullt en umoden problemstilling i norsk rett, med et stort og fragmentert rettskildebilde.

[25] Kuner (2020) s. 149.

GDPR gjelder som norsk lov etter personopplysningsloven § 1, og den vedlagte offisielle norske oversettelsen av personvernforordningen vil benyttes i avhandlingen. Det er adgang til å fastsette supplerende nasjonale bestemmelser innenfor det handlingsrommet forordningen gir, hvilket Stortinget har gjort.[26] Personopplysningslovens supplerende bestemmelser vil trekkes frem der det er relevant. Videre er fortalen til GDPR en del av konteksten til forordningen, og må tas i betraktning.[27] En rettsakts fortale gir anvisning på hva forordningens overordnede formål er, samt i noen utstrekning hvilket spesielt formål de enkelte artiklene nærmere har.[28] Fortalen er ikke rettslig bindende for medlemslandene, og gir kun presiseringer, hvilket er lagt til grunn av EU-domstolen.[29]

I avhandlingen anvendes også forskjellige typer juridisk litteratur, herunder Datatilsynets veiledere og retningslinjer og uttalelser fra Det europeiske personvernrådet (heretter kalt «Personvernrådet»). Til tross for at personvern er svært viktig, finnes det bare en begrenset mengde rettspraksis fra EU-domstolen om emnet og tolkningen av GDPR. [30] På grunn av dette får slike retningslinjer, veiledere og uttalelser stor betydning for forståelsen av forordningens innhold.

Personvernrådet er EUs rådgivende organ i personvernspørsmål, og skal sikre en ensartet anvendelse av forordningen ved å bl.a. gi retningslinjer og uttalelser om tolkningen av den, jf. GDPR art. 70. Det viderefører og videreutvikler den tidligere Artikkel 29-gruppen, og har gitt sin tilslutning til 16 av deres veiledere.[31] Tolkningene er ikke autorativt bindende, men fungerer som verdifulle retningslinjer og har i praksis stor vekt.[32] I avhandlingen vil veiledere fra Personvernrådet, samt tilsluttede veiledere fra Artikkel 29-gruppen, derfor bli henvist til.

Når det gjelder Datatilsynet, så er hver medlemsstat forpliktet til å sikre at minst én uavhengig offentlig myndighet har ansvar for å føre tilsyn med anvendelsen av forordningen, jf. GDPR art. 51 nr. 1. Personopplysningsloven § 20 bestemmer at Datatilsynet er Norges tilsynsmyndighet. Datatilsynet fatter vedtak i enkeltsaker,[33] men utformer også generelle

[26] Prop. 56 LS (2017-2018) s. 15-16.
[27] Fredriksen/Mathisen (2022) s. 338.
[28] Fredriksen/Mathisen (2022) s. 338-339.
[29] *Karen Millen Fashions* [C5] C-345/13, avsnitt 31.
[30] Trzaskowski/Sørensen (2022) s. 47.
[31] Personvernrådets nettsider angir de tilsluttede veilederne:
https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en
[32] Prop. 56 LS (2017–2018) s. 168 og Trzaskowski/Sørensen (2022) s. 47.
[33] Klageorgan er Personvernnemda, jf. personopplysningsloven § 22.

veiledere for implementering og overholdelse av GDPR.[34] Selv om Datatilsynets veiledere og praksis har begrenset rettskildemessig vekt, kan de likevel gi retningslinjer og føringer rundt forståelsen av forordningen.

1.4 Avgrensninger og presiseringer

Avhandlingen begrenses til kun å behandle erstatningskrav mot styremedlemmene etter asl. § 17-1 (1). Det avgrenses følgelig mot erstatningskrav hjemlet i det alminnelige ulovfestede culpaansvaret, og selvstendig i GDPR art. 82 i tilfeller der styremedlemmene selv anses å være «behandlingsansvarlig». Når det er spørsmål om styrets erstatningsansvar, ses det bort fra muligheten til å tegne styreansvarsforsikring, samt andre former for lemping av ansvar eller avtalte begrensninger i erstatningsansvaret. Videre avgrenser avhandlingen i sin helhet mot allmennaksjeselskap som selskapsform.

Ytterligere avgrenser avhandlingen mot et skille mellom styreleder/styremedlem, interne og eksterne styremedlemmer, styremedlemmer som skiller seg ut på grunn av særlig kunnskap eller erfaring om GDPR, er fraværende/passive fra styrevervet, eller opptrer proforma. De særskilte problemstillingene disse forholdene eventuelt reiser, er ikke av interesse for avhandlingens generelle drøftelse av styremedlemmets erstatningsansvar ved brudd på GDPR.

Videre nevnes at personvernforordningen opererer med to ansvarssubjekter ved behandling av personopplysninger. Et selskap kan opptre som «behandlingsansvarlig» eller «databehandler» avhengig av om virksomheten handler på egne eller andres vegne, jf. GDPR art. 4 nr. 7 og nr. 8. Avhandlingen begrenses imidlertid til å kun behandle selskaper i rollen som behandlingsansvarlig, fordi det er den behandlingsansvarlige som er forordningens primære pliktsubjekt.[35] Databehandleren pålegges imidlertid i mange tilfeller de samme pliktene som den behandlingsansvarlige, og mye av det som fremkommer i avhandlingen vil også gjelde for et styremedlem i et slikt selskap.

En helhetlig gjennomgang av alle kravene GDPR stiller til selskapene er ikke mulig innenfor rammen av denne avhandlingen, og er heller ikke nødvendig for å besvare avhandlingens problemstilling. Av disse grunner vil særlig kravene GDPR stiller til internkontroll og informasjonssikkerhet etter GDPR art. 24 og 32 analyseres. Dersom selskapet overholder

[34] Wessel-Aas/Ødegaard (2018) s. 303.
[35] Kuner (2020) s. 146.

kravene til internkontroll og informasjonssikkerhet, vil virksomheten stort sett også tilfredsstille forordningens mer spesifikke forpliktelser, jf. kapittel 2.2.3. Bestemmelsene er valgt ut fordi de av den grunn er svært sentrale, men også egnede til å belyse styrets ansvar for etterlevelse av forordningen.

1.5 Den videre fremstillingen

Fordi det er selskapet selv som hovedregel ilegges forpliktelser etter GDPR,[36] skal det i kapittel 2 gjøres rede for personvernforordningen som ramme for norske selskapers behandling av personopplysninger. Her vil sentrale krav forordningen stiller til virksomhetene, og konsekvensene av å bryte dem, presenteres. En fastleggelse av kravene GDPR stiller til selskapet, er nødvendig for å senere kunne vurdere styremedlemmenes ansvar for manglende etterlevelse etter aksjeloven.

I kapittel 3 presenteres vilkårene for styremedlemmenes erstatningsansvar etter asl. § 17-1 (1). Årsaken til at dette gjøres i et eget kapittel, er fordi det anses hensiktsmessig med en generell og helhetlig fremstilling av erstatningsvilkårene. På denne måten er det mulig å gi et overblikk over bestemmelsen, og gå fra det generelle til det spesielle når vilkårene skal belyses i en bestemt ansvarssituasjon. I kapittel 4 stilles det spørsmål om brudd på GDPR kan oppfylle vilkårene som har blitt presentert, og hvilket eventuelt ansvar et styremedlem har for å sikre at selskapet etterlever forordningen. Til slutt vil det konkluderes, og trekkes noen avsluttende betraktninger om den praktiske relevansen for styreansvar ved brudd på GDPR i kapittel 5.

[36] Kuner (2020) s. 149. Se nærmere under kapittel 2.2.1.

2 GDPR som ramme for norske selskaper

2.1 Kort om forordningens bakgrunn og formål

Før GDPR trådte i kraft var det EU-direktivet om behandling av personopplysninger som regulerte virksomhetenes adgang til å behandle personopplysninger.[37] Direktivet ble i hvert enkelt land implementert gjennom nasjonal lovgivning. I Norge ble det gjennomført i den nå opphevede personopplysningsloven fra 2000.[38] Konsekvensen av dette var ulik og fragmentert personvernlovgivning i Europa, hvilket førte til at personvernreglene ble håndhevet forskjellig.

Den raske teknologiske utviklingen, globaliseringen, og økningen i omfanget og måtene personopplysninger ble utvekslet og behandlet på, førte etter hvert til nye personvernutfordringer, jf. kapittel 1.1. Det var altså et behov for harmonisering av regelverket, hvilket resulterte i GDPR. Fordi den er gjennomført som en forordning, ved at rettsakten «som sådan gjøres til del av avtalepartens interne rettsorden»,[39] jf. EØS-avtalen[40] art. 7 bokstav (a) og TEUV[41] art. 288 (2), gjelder den direkte i alle medlemslandene. Innføringen av GDPR har dermed ført til et felles regelsett, som i utgangspunktet skal tolkes og praktiseres likt i samtlige EU/EØS-medlemsland.[42]

Målet med forordningen er et ensartet regelverk som sikrer vern av fysiske personers grunnleggende rettigheter og friheter, og fri flyt av personopplysninger i EU/EØS, jf. GDPR art. 1 nr. 2 og nr. 3, samt fortalepunkt 170. Regelverket er ment å skape den tillit som er nødvendig for at den digitale økonomien kan utvikle seg i det indre marked, jf. GDPR fortalepunkt 7. Hensikten er å bidra til å skape frihet, sikkerhet og rettferdighet, samt en økonomisk union, jf. GDPR fortalepunkt 2. For å nå disse målene stiller regelverket grunnleggende krav til behandling av personopplysninger, noe som skal presenteres i det følgende.

[37] Europaparlaments og Rådsdirektiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger [Personverndirektivet 1995].
[38] [Opphevet] Lov 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven).
[39] Den faktiske innføringen skjedde ved EØS-komiteens beslutning nr. 154/2018 av 6. juli 2018.
[40] Avtale om Det europeiske økonomiske samarbeidsområde [EØS-avtalen].
[41] Traktaten om Den europeiske unions virkeområde – TEUV – Roma-traktaten konsolidert 2016.
[42] Schartum (2020) s. 17. Merk at det er rom for visse nasjonale tilpasninger, se f.eks. GDPR art. 8.

2.2 Kravene GDPR stiller til selskapene

2.2.1 Om ansvarsfordelingen etter forordningen

Etter GDPR art. 4 nr. 7 er «behandlingsansvarlig» en «fysisk eller juridisk person» som «alene eller sammen med andre» bestemmer «formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes». Når det kommer til selskapenes behandling av personopplysninger, er det virksomheten selv som juridisk person som anses å være behandlingsansvarlig, med mindre ansvaret klart kan plasseres hos en enkeltansatt.[43] Dette vil kunne være tilfellet der vedkommende har brukt personopplysningene til sitt eget formål utenfor virkeområdet og kontrollen til selskapet,[44] for eksempel igangsatt en ulovlig overvåkning av ansatte for å kunne true til seg personlige tjenester.[45]

Ansvaret kunne plasseres hos en enkeltansatt i den nevnte tyske avgjørelsen fra OLG Dresden.[46] Her hadde en direktør, i forbindelse med en medlemsforespørsel, ansatt en privatdetektiv for å undersøke om søkeren hadde begått kriminelle handlinger. Opptredenen medførte at direktøren sammen med virksomheten ble ansett å være «behandlingsansvarlig», og ble dømt til å betale en erstatning på 5000 euro. Erstatningsansvaret fulgte direkte av GDPR art. 82,[47] og det var ikke nødvendig å gå via et annet ansvarsgrunnlag. Det er viktig å merke seg at saken er veldig spesiell, fordi direktøren iverksatte privatetterforskning på eget initiativ, og at opplysningene som ble samlet inn er særlig vernet i GDPR art. 10.

Disse omstendighetene begrenser også dommens betydning for avhandlingens tema. Det er vanskelig å se hvordan dommen påvirker rettstilstanden i Norge når et styremedlems erstatningsansvar vurderes etter asl. § 17-1 (1). Om dommen har betydning for forståelsen av innholdet i «behandlingsansvarlig» i relasjon til et styremedlem, faller utenfor avhandlingens tema, jf. kapittel 1.4.

I det videre legges det til grunn at selskapet alene er behandlingsansvarlig ved behandlingen av personopplysninger. Det er dermed virksomheten og ikke styremedlemmene som er

[43] Rüker/Kugler (2018) s. 105.
[44] Kuner (2020) s. 149.
[45] Wessel-Aas/Ødegaard (2018) s. 180.
[46] *Ankeinstans:* OLG Dresden, 30.11.2021 - 4 U 1158/21. *Første instans*: LG Dresden, 26.05.2021 - 8 O 1286/19.
[47] Se kapittel 2.3 for en redegjørelse for erstatningsregelen i GDPR art. 82 når selskapet er «behandlingsansvarlig».

direkte ansvarlig etter GDPR, og som risikerer konsekvensene som kan utledes av forordningen ved brudd.[48]

2.2.2 Selskapets forpliktelser som «behandlingsansvarlig»

GDPR art. 5 nr. 1 oppstiller generelle prinsipper som gjelder for behandling av personopplysninger etter forordningen, som selskapet er ansvarlig for og skal kunne dokumentere overholdelsen av, jf. bestemmelsens nr. 2. De må betraktes som en introduksjon og grunnleggende ramme for de spesifikke kravene som kommer frem av de etterfølgende bestemmelsene i GDPR.[49] Disse personvernprinsippene vil være styrende tolkningsfaktorer ved fastleggelsen av kravene i forordningens øvrige bestemmelser.[50]

I GDPR art. 5 (1) fremgår prinsipper om lovlighet, rettferdighet, åpenhet, ansvarlighet, riktighet, dataminimering, lagringsbegrensning, integritet og konfidensialitet, og formålsbegrensning ved behandlingen. Særlig sentralt er at selskapene, før en behandling av personopplysninger iverksettes, er nødt til å ta stilling til hvilke personopplysninger de kommer til å behandle, og til hvilket formål de ønsker å bruke disse, jf. GDPR art. 5 nr. 1 bokstav b. Dette er fordi typen personopplysninger og behandlingsformålet påvirker kravene forordningen ellers stiller til den aktuelle behandlingen, jf. drøftelsen nedenfor.

Et selskap må også ta stilling til hvilket rettslig grunnlag de kan vise til for å kunne behandle personopplysninger til den registrerte på en lovlig måte, jf. GDPR art. 6.[51] Med «den registrerte» menes den identifiserte eller identifiserbare fysiske personen selskapet behandler personopplysninger om, jf. GDPR art. 4 nr. 1, altså den personen som opplysningene gjelder. Utenom tilfeller der den registrerte samtykker til behandlingen for et spesifikt formål, bygger de aktuelle hjemmelsgrunnlagene på situasjoner der behandlingen er et «nødvendig» tiltak for et gitt formål, jf. GDPR art. 6 nr. 1 bokstav a-f. Et rettslig grunnlag kan eksempelvis være at behandlingen av personopplysninger er nødvendig for å kunne gjennomføre en arbeidsavtale. Videre har den registrerte også en rekke rettigheter og friheter som fremgår av forordningens kapittel 3, som virksomheten har plikt til å oppfylle. Dette omfatter blant annet

[48] Konsekvensene av brudd på forordningen gjøres rede for under kapittel 2.3.
[49] Rüker/Kugler (2018) s. 49-50.
[50] Blekastad/Hirst (2021) s. 49.
[51] Merk at GDPR art. 9 angir behandlingsgrunnlagene for særlige kategorier av personopplysninger, og at GDPR art. 10 angir vilkår for å behandle personopplysninger om straffedommer og loverovertredelser. Videre fremgår det krav til gyldig samtykke av GDPR art. 7 og 8, som må være oppfylt om hjemmelsgrunnlaget til en behandling bygger på samtykke etter GDPR art. 6 nr. 1 bokstav a.

rett til informasjon om behandlingen (art. 12-14), innsyn (art. 15), retting og sletting (art. 16-17), og til å protestere mot behandling av personopplysninger (art. 21).

For å påse at disse prinsippene og rettighetene overholdes, stiller forordningen overordnede krav til etablering og dokumentering av tiltak basert på risikovurderinger for selskapene ved behandlingen av personopplysninger. Dette kommer klarest frem av GDPR art. 24 nr. 1, om den behandlingsansvarliges ansvar, der det uttrykkes at selskapet må gjennomføre «egnede tekniske og organisatoriske tiltak» for å «sikre og påvise at behandlingen utføres i samsvar med denne forordning». Selskapet må ta stilling til og vurdere hvordan det skal gjennomføre behandlingen av personopplysninger slik at det etterlever regelverket, dvs. i overensstemmelse med personvernprinsippene, virksomhetens plikter og den registrertes rettigheter og friheter. Aktuelle tiltak kan eksempelvis være å fordele oppgaver knyttet til ivaretakelsen av forordningen innad i selskapet.[52] Tiltakene som iverksettes må dokumenteres, jf. «påvises», noe som sikrer etterprøvbarhet og gjør dem tilgjengelig for selskapets ansatte.

Hvilke tiltak som kreves av det enkelte selskap er underlagt en forholdsmessighet, hvor man ser på behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoen for at behandlingen kan krenke fysiske personers rettigheter og friheter, jf. GDPR art. 24 nr. 1. Kravene vil altså variere fra selskap til selskap, avhengig av hva som er nødvendig for å sikre en forsvarlig behandling av personopplysninger. Disse tiltakene skal «omfatte den behandlingsansvarliges iverksetting av egnede retningslinjer for vern av personopplysninger» dersom det står i et «rimelig forhold til behandlingsaktivitetene», jf. GDPR art. 24 nr. 2. Her stilles det altså krav om styrende dokumenter for å ivareta personvernet til den registrerte om behandlingsaktivitetene tilsier det.[53] Selv om kravene til tiltak varierer må selskapet i alle tilfelle skaffe nødvendig kunnskap om forordningen, og etablere en oversikt over behandlingene av personopplysninger, så det i det hele tatt er mulig å opptre i tråd med regelverket. Virksomheten er deretter nødt til å identifisere hvilke forpliktelser den har og tilpasse tiltakene til sin organisasjon.

[52] Kuner (2020) s. 564.
[53] Skullerud (2022) *kommentar til Artikkel 24*, avsnitt: *«Nummer 2 Styrende dokumenter»*.

Det kan sies at GDPR art 24 med dette oppstiller en generell plikt til å ha internkontroll,[54] eller med andre ord et styringssystem for etterlevelse av regelverket.[55] Med internkontroll menes her systematiske tiltak som skal sikre at selskapets behandlinger av personopplysninger planlegges, organiseres, utføres og kontrolleres i samsvar med kravene GDPR stiller.[56] Selskapene må sørge for at de internt har innført og iverksatt de nødvendige tiltakene og prosessene for å etterleve kravene forordningen stiller til dem.

2.2.3 Internkontrollsystem / GDPR compliance program

Krav om å ha internkontroll er et vanlig verktøy for å sikre at lover etterleves.[57] Fordi en virksomhet må forholde seg til flere regelverk, vil den være underlagt en rekke krav om internkontroll. Eksempelvis stilles internkontrollkrav i relasjon til helse-, miljø- og sikkerhet (HMS),[58] og innenfor finanssektoren.[59] Det er imidlertid ikke nødvendig å lage en egen internkontroll for hvert regelverk, og systemet kan utvides og tilpasses de ulike kravene virksomheten må overholde.[60] Om selskapet ikke allerede har et styringssystem bør det imidlertid etableres en egen internkontroll for personvernregelverket.

Sentrale deler av det som kan forventes i et internkontrollsystem, jf. «egnede tekniske og organisatoriske tiltak» i GDPR art. 24 nr. 1, finnes i andre konkrete internkontrollkrav i øvrige deler av forordningen. De fleste selskaper plikter å «føre en protokoll over behandlingsaktiviteter som utføres under deres ansvar», jf. GDPR art. 30 nr. 1.[61] Denne skal inneholde en rekke opplistede grunnleggende opplysninger, jf. GDPR art. 30 nr. 1 bokstav a-g, herunder behandlingsformålet og ulike opplysningskategorier. Bestemmelsen skal sikre at selskapet har et aktivt forhold til sitt ansvar for behandlingsaktivitetene, ved å ha god

[54] Skullerud (2022) *kommentar til Artikkel 24*, avsnitt: *«Generelt»*.
[55] Datatilsynets veileder (2018). *Etablere internkontroll*, kapittel: *«1. Ansvarlighet, internkontroll og informasjonssikkerhet»*, overskrift: *«Hva er internkontroll?»*.
[56] Datatilsynets veileder (2018). *Etablere internkontroll*, kapittel: *«1. Ansvarlighet, internkontroll og informasjonssikkerhet»*, overskrift: *«Hva er internkontroll?»*.
[57] Veum (2010) s. 204.
[58] Forskrift 12. juni 1996 nr. 1127 om systematisk helse-, miljø- og sikkerhetsarbeid i virksomheter (Internkontrollforskriften).
[59] Forskrift 22. september 2008 nr. 1080 om risikostyring og internkontroll.
[60] Datatilsynets veileder (2018). *Etablere internkontroll*, kapittel: *«1. Ansvarlighet, internkontroll og informasjonssikkerhet»*, overskrift: *«Hva er internkontroll etter personvernregelverket»*.
[61] Dette gjelder i utgangspunktet ikke for et foretak eller en organisasjon med færre enn 250 ansatte, jf. GDPR art. 30 nr. 5. Selv om det er vanskelig å lese ut av bestemmelsen, gjelder plikten likevel nesten alle selskaper. Grunnen er at det følger av GDPR art. 30 nr. 5 at plikten gjelder der «behandlingen ikke skjer leilighetsvis». De aller fleste selskaper behandler personopplysninger systematisk, og må dermed etablere behandlingsprotokoll.

oversikt over hva slags behandling som foregår i virksomheten.[62] Samtidig skal protokollene være tilgjengelig for tilsynsmyndighetene, jf. GDPR art. 30 nr. 4, og de har følgelig en viktig funksjon i selskapets dokumentering av at forordningen overholdes.

Videre plikter den behandlingsansvarlige på nærmere vilkår å utpeke et personvernombud, jf. GDPR art. 37.[63] Personvernombudets hovedoppgave er å informere og gi råd til den behandlingsansvarlige og de ansatte som utfører behandlingen av personopplysninger, om virksomhetens forpliktelser etter personvernlovgivningen, jf. GDPR art. 39. Ombudet har imidlertid også en rekke andre oppgaver, jf. bestemmelsens bokstav a-e, og skal både fungere som et kontrolltiltak i selskapet og et kontaktpunkt for tilsynsmyndighetene. Selskapet plikter å legge til rette for at personvernombudet på riktig måte og til rett tid involveres i alle spørsmål som gjelder vern av personopplysninger, jf. GDPR art. 38 nr. 1. Virksomheten må også stille til rådighet de ressurser som er nødvendig for at personvernombudet får gjennomført sine oppgaver, og sørge for ombudets uavhengighet ved at vedkommende ikke instrueres om utførelsen av sine oppgaver, jf. GDPR art. 38 nr. 2 og 3.

Etter GDPR art. 32 nr. 1 følger det et krav om at selskapet skal gjennomføre «tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet» med hensyn til risikoen ved behandlingen. Hvilket sikkerhetsnivå som er egnet er noe den behandlingsansvarlige må vurdere, sett hen til den tekniske utviklingen, gjennomføringskostnadene, og behandlingens art, omfang, formål og sammenhengen den utføres i, samt hvilken risiko behandlingen medfører for den registrerte, jf. GDPR art. 32 nr. 1. Ivaretakelsen av informasjonssikkerheten, som handler om å håndtere risikoen for at personopplysninger ivaretas på en tilstrekkelig måte, vil være en sentral del av selskapets internkontroll.[64] Med internkontrolltiltak menes derfor i det følgende også tiltak knyttet til ivaretakelsen av informasjonssikkerheten.

Selskapet plikter ved risikovurderingen å ta særlig hensyn til konsekvenser av «utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av eller tilgang til personopplysninger», jf. GDPR art. 32 nr. 2. Dette illustrerer den risikobaserte tilnærmingen til forordningen, der tiltakene og sikkerhetsnivået skal stå i et rimelig forhold til risikoen ved

[62] Kuner (2020) s. 618.
[63] Dette gjelder ubetinget for offentlige myndigheter eller et offentlig organ, og for virksomheter med en viss type «kjernevirksomhet», jf. GDPR art. 37 nr. 1 bokstav a-c. Det avgrenses mot en videre redegjørelse for utpekningsvilkårene, ettersom de er av underordnet betydning for avhandlingens overordnede tema.
[64] Datatilsynets veileder (2018. *Etablere internkontroll,* kapittel: *«1. Ansvarlighet, internkontroll og informasjonssikkerhet»,* overskrift: *«Om informasjonssikkerhet»*.

behandlingen. Selskapet må altså evaluere risikoen for brudd på informasjonssikkerheten, og iverksette adekvate tiltak på bakgrunn av dette. Aktuelle tiltak kan eksempelvis være kryptering og pseudonymisering av personopplysninger, jf. GDPR art. 32 nr. 1 bokstav a. Det følger av bestemmelsens karakter at sikkerhetstiltakene som har blitt iverksatt må kunne dokumenteres. Når selskapet har foretatt risikovurderinger og fastsatt adekvate tiltak i tråd med bestemmelsen, må dette være etterprøvbart.

Selskapet må også ha rutiner på plass for håndtering av sikkerhetsbrudd, herunder iverksettelsen av korrigerende tiltak om nødvendig. Avvikshåndteringen medfører videre en plikt til å dokumentere ethvert brudd på personopplysningssikkerheten,[65] og kan på nærmere vilkår innebære en plikt til å både melde fra om dette til Datatilsynet og underrette den registrerte, jf. GDPR art. 33 og 34.

I Datatilsynets veileder for å etablere internkontroll anbefales det å strukturere internkontrollen i styrende, gjennomførende og kontrollerende elementer.[66] Hvordan virksomheten planlegger/styrer, gjennomfører og kontrollerer etterlevelse av regelverket bør formaliseres, og dokumentasjonen bør være tilgjengelig for selskapets ansatte.[67] Ulike behandlinger og opplysninger medfører at selskapene må forholde seg til ulike forpliktelser, og internkontrollen må tilpasses den enkelte virksomhet. Systemet vil likevel typisk inneholde styrende dokumentasjon som setter rammen for virksomhetens arbeid, rutiner og sikkerhetstiltak som springer ut av og skal gjennomføre dette, samt dokumenterte tiltak for revisjon og kontroll av at arbeidet faktisk foregår i tråd med disse.[68] Det vil være et kontinuerlig arbeid, som jevnlig må revideres og vil kreve oppdateringer.[69]

Internkontrollen er ledelsens verktøy for å ivareta sitt ansvar etter forordningen,[70] hvilket gjør styringssystemet særlig interessant i lys av avhandlingens tema. I det omfanget som er relevant vil ytterligere deler av kravet til internkontroll presenteres under kapittel 4, når styremedlemmets ansvar for etterlevelse av forordningen vurderes etter asl. § 17-1 (1).

---

[65] Med «brudd på personopplysningssikkerheten» menes et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet», jf. GDPR art. 4 nr. 12.
[66] Datatilsynets veileder (2018). *Etablere internkontroll*, kapittel: *«1. Ansvarlighet, internkontroll og informasjonssikkerhet.»*, overskrift: *«Hva er internkontroll?»*.
[67] Veum (2010) s. 205-206.
[68] Datatilsynets veileder (2018). *Etablere internkontroll*, kapittel*: «5. Internkontrollens struktur.»*.
[69] Veum (2010) s. 210.
[70] Datatilsynets veileder (2018). *Etablere internkontroll*, kapittel*: «1. Ansvarlighet, internkontroll og informasjonssikkerhet.»*, overskrift: *«Hva er internkontroll etter personvernregelverket»*.

2.3 Konsekvensene av brudd på GPDR for selskapet

I Norge har Datatilsynet ansvar for å føre tilsyn med forordningen, jf. kapittel 1.3. Datatilsynet kan, i henhold til GDPR art. 83 nr. 4 og nr. 5, ilegge overtredelsesgebyr for brudd på bestemmelser i forordningen som stiller krav til behandling av personopplysninger, jf. GDPR art. 58 nr. 2 bokstav i. Det opereres med to nivåer for overtredelsesgebyr. Avhengig av hvilke bestemmelser som er brutt, kan det gis gebyr på inntil 10 eller 20 millioner euro eller, for foretak, 2 eller 4 % av den samlede globale årsomsetningen i forutgående regnskapsår.

Det minst strenge nivået av gebyrer kan etter forordningen gis for overtredelser av GDPR art. 8, 11, 25-39, samt 42 og 43, jf. GDPR art. 83 nr. 4 bokstav a. Dette omfatter altså de fleste bestemmelsene som er vist til under redegjørelsen for internkontrollen etter GDPR ovenfor. I Norge vil i tillegg også brudd på GDPR art. 24 kunne sanksjoneres av Datatilsynet med overtredelsesgebyr innen disse grensene, jf. personopplysningsloven § 26 (1). Når det kommer til de strengeste overtredelsesgebyrene, kan disse blant annet gis ved overtredelse av de grunnleggende prinsippene for behandling, eller brudd på de registrertes rettigheter i henhold til GDPR art. 12-22, jf. GDPR art. 83 nr. 5 bokstav a og b.

Det finnes flere eksempler på tilfeller der Datatilsynet har ilagt overtredelsesgebyr, herunder det nevnte vedtaket der bomselskapet Ferde AS fikk et gebyr på kr. 5 millioner.[71] Nylig fikk Recover AS et overtredelsesgebyr på kr. 200 000 for å ha foretatt en kredittvurdering uten rettslig grunnlag for å behandle personopplysningene.[72] Datatilsynet påpekte i vedtaket at selskapet manglet tekniske og organisatoriske tiltak for å sikre at innhenting av kredittvurderinger ble utført i samsvar med personvernforordningen, jf. GDPR art. 24.[73]

GDPR art. 83 nr. 2 angir momenter for vurderingen av om det skal gis et overtredelsgebyr, og for utmålingen av gebyrets størrelse. Det skal blant annet ses hen til karakteren, alvorlighetsgraden og varigheten av overtredelsen, og etter Personvernrådets retningslinjer bør tilsynsmyndighetene identifisere et korrigerende tiltak som er effektivt, forholdsmessig og avskrekkende.[74] Den offentlige tilsynsmyndigheten i landet, i Norge Datatilsynet, må

[71] Datatilsynet (2021). *Vedtak om overtredelsesgebyr – Ferde AS.*
[72] Datatilsynet (2022). *Vedtak om pålegg og overtredelsesgebyr – Recover AS.*
[73] Datatilsynet (2022). *Vedtak om pålegg og overtredelsesgebyr – Recover AS.* s. 9.
[74] Guidelines on the application and setting of administrative fines (2017) s. 6.

foreta en helhetsvurdering av alle momentene, og plikter å vurdere alle sakens fakta på en konsistent og objektiv måte.[75]

Videre kan et selskap også bli utsatt for erstatningskrav fra enhver person som har lidd materiell eller ikke-materiell skade som følge av en overtredelse av forordningen, jf. GDPR art. 82 nr. 1. Dette kan eksempelvis være tap som har oppstått som følge av at den registrerte blir utsatt for urettmessige økonomiske krav etter et konfidensialitetsbrudd hos virksomheten som førte til et identitetstyveri.[76] Erstatningen skal svare til det økonomiske tapet den skadelidte har blitt påført, men selskapet kan også pålegges et erstatningansvar for ikke-økonomisk skade (oppreisning), jf. personopplysningsloven § 30. Med ikke-økonomisk skade siktes det i all hovedsak til den psykiske belastningen bruddet har ført med seg for den registrerte, for eksempel der sensitive opplysninger har blitt gjort kjent for uvedkommende.[77] Det må kunne legges til grunn at alminnelige erstatningsrettslige prinsipper og vilkår her kommer til anvendelse, forutsatt at dette ikke er i strid med forordningen.[78]

Når kravene GDPR stiller til virksomhetene som behandlingsansvarlige, og konsekvensene av å bryte dem nå er fastlagt, er spørsmålet hvilket ansvar et styremedlem har for å sikre etterlevelse i selskapet. I kapittel 3 skal først vilkårene for personlig erstatningsansvar presenteres, før spørsmålet under kapittel 4 er om et brudd på GDPR kan oppfylle dem.

[75] Guidelines on the application and setting of administrative fines (2017) s. 6.
[76] Skullerud (2022) *kommentar til Artikkel 82*, avsnitt: *«Skade»*.
[77] Skullerud (2022) *kommentar til Artikkel 82*, avsnitt: *«Skade»*.
[78] Skullerud (2022) *kommentar til Artikkel 82*, avsnitt: *«Generelt»*.

3 Aksjeloven § 17-1 (1)

3.1 Innledende om bestemmelsen

Etter asl. § 17-1 (1) kan «selskapet, aksjeeier, eller andre [..] kreve at [..] styremedlem [..] erstatter skade som de i den nevnte egenskap forsettlig eller uaktsomt har voldt vedkommende». Et styremedlem kan etter bestemmelsen bli holdt personlig ansvarlig for den skade vedkommende, under utøvelsen av sitt styreverv, måtte påføre skadelidte. Asl. § 17-1 (1) er en særlig regulering av den alminnelige erstatningsrettslige culpanormen.[79] Bestemmelsen er følgelig ikke uttømmende, og de alminnelige vilkårene for å ilegge erstatningsansvar må være oppfylt for at asl. § 17-1 (1) skal kunne komme til anvendelse.

Styreansvaret etter asl. § 17-1 (1) fordrer dermed en erstatningsmessig skade, et ansvarsgrunnlag, og adekvat årsakssammenheng mellom skaden og styremedlemmets handlemåte.[80] Styreansvaret er personlig, og ansvarsvilkårene må være oppfylt for hvert enkelt styremedlem som saksøkes. Ved bruken av begrepet erstatningsansvar nedenfor menes personlig erstatningsansvar for styremedlemmene.

3.2 Vilkårene for erstatningsansvar

Styremedlemmene må ha påført «selskapet, aksjeeier eller andre» en «skade» for at det skal være grunnlag for et erstatningskrav. I «skade» ligger et krav om en erstatningsmessig skade, nærmere bestemt et erstatningsrettslig vernet økonomisk tap som kan måles i kroner og øre.[81] Culpaansvaret gjelder for person-, ting-, og formueskader, men det er kun formuestap som er praktisk relevant for styreansvar etter asl. § 17-1 (1).[82] Grunnen er kravet om at skaden må være påført i «den nevnte egenskap», jf. nedenfor, da det vanskelig kan tenkes tilfeller der styremedlemmer under utøvelsen av styrevervet har påført den skadelidte en person- eller

[79] HR-2017-2375-A avsnitt 25.
[80] Lødrup (2009) s. 52-54.
[81] Aarum (1994) s. 74.
[82] Woxholth (2021) s. 356.

tingskade.[83] Praktisk relevante eksempler på formuestap er at selskapet har blitt pådratt omkostninger, økt gjeld eller har gått glipp av inntekter.[84]

Skaden må ha blitt voldt forsettlig eller uaktsomt i «den nevnte egenskap», og vilkåret tilsier at styremedlemmet ved den skadevoldende handlingen må ha opptrådt i egenskap av å være et styremedlem.[85] Asl. § 17-1 (1) gir følgelig ikke hjemmel for et erstatningskrav med grunnlag i en skadevoldende handling som et styremedlem har begått utenfor arbeidstiden og uavhengig av selskapsforholdet. Vilkåret setter klare begrensninger for styreansvaret, og understreker både hensikten bak bestemmelsen, og hvilket vurderingstema som skal legges til grunn ved anvendelsen av den. Det er styremedlemmets tilknytning til sin selskapsrettslige egenskap som er den avgjørende forutsetningen for ansvar.

For å kunne holdes erstatningsansvarlig må styremedlemmet «forsettlig» eller «uaktsomt» ha foretatt en handling eller unnlatelse som har ført til en skade. Det er altså et krav om at skadevolder har utvist skyld. Nærmere bestemt må det foreligge et brudd på en aktsomhetsnorm, og vedkommende må kunne lastes for å ha overtrådt denne.[86] Dette omtales i den juridiske teorien som culpanormens objektive og subjektive side.[87] Utgangspunktet for vurderingen er den kunnskapen styremedlemmet hadde eller burde hatt på beslutningstidspunktet.[88] Innholdet i ansvaret må etter forarbeidene til aksjeloven fastsettes ut fra en konkret vurdering av hva som er en adekvat handlemåte for et styremedlem.[89]

I HR-2016-1440-A fremgår at det må tas «utgangspunkt i om aksjeeier/styreleder har overtrådt de plikter som objektivt sett gjelder for vedkommende».[90] Styremedlemmer må overholde de plikter som følger av aksjeloven, selskapets vedtekter, annen lovgivning, og andre ulovfestede aksjerettslige prinsipper.[91] Sentralt står det overordnede forvalteransvaret av virksomheten etter asl. § 6-12 (1), fordi det er hovedbestemmelsen om styrets gjøremål.[92] Forvalteransvarets innhold presiseres videre i asl. § 6-12, og i asl. § 6-13 om styrets

[83] Aarbakke (2022*) kommentar til asl. § 17-1*, punkt 1.6.
[84] Woxholth (2021) s. 356.
[85] Aarbakke (2022) *kommentar til asl. § 17-1*, punkt 1.6.
[86] Bråthen (2022) s. 257.
[87] Aarum (1994) s. 187-188.
[88] Andenæs (2016) s. 649.
[89] Ot.prp. nr. 36 (1993-1994) s. 250-251.
[90] HR-2016-1440-A, avsnitt 41. Selv om Høyesterett viser til styreleder, må utgangspunktet kunne legges til grunn for ethvert styremedlem.
[91] Aarum (1994) s. 189-190.
[92] Andenæs (2016) s. 364.

tilsynsansvar,[93] hvilket gjør dem sentrale i fastleggelsen av hvilke plikter som objektivt sett gjelder for et styremedlem.

Det er ikke alltid enkelt å konstatere om det foreligger pliktbrudd, fordi reglene har et skjønnsmessig innhold og en dynamisk karakter, som preges av samfunnsutviklingen og de generelle forventingene man har til styremedlemmer. Reglene må fortolkes for at man skal komme frem til hvilke konkrete plikter styremedlemmet har.[94] Det er ikke slik at enhver feilvurdering eller uheldig disposisjon fører til pliktbrudd.[95] Dersom handlingen objektivt sett ikke er uforsvarlig, vil den ikke kunne være erstatningsbetingende etter asl. § 17-1 (1).

Styremedlemmene må videre kunne bebreides for den objektivt sett uforsvarlige handlingen eller unnlatelsen. Det må tas utgangspunkt i de forventninger man kan stille til et normalt og samvittighetsfullt styremedlem i en tilsvarende situasjon.[96] Dersom et styremedlem bevisst, eller med innsikt om at skaden med stor sannsynlighet ville inntre, har handlet i strid med sine objektive plikter slik at skadelidte blir påført et økonomisk tap, vil skyldkravet klart være oppfylt. Det er imidlertid tilstrekkelig å konstatere uaktsomhet, og ved brudd på en plikt som objektivt sett gjelder for styremedlemmet er det en presumsjon for at vedkommende har opptrådt uaktsomt, jf. HR-2016-1440-A.[97] Dette innebærer at det subjektive ansvarselementet får en mer tilbaketrukket plass i uaktsomhetsvurderingen.[98] Det egentlige spørsmålet blir om styremedlemmet kan vise til en unnskyldningsgrunn, for eksempel faktisk eller rettslig villfarelse, eller bestemte forhold ved sin egen person.[99]

Det må videre foreligge årsakssammenheng mellom det tapet skadelidte har lidt og styremedlemmets erstatningsbetingende handling eller unnlatelse, jf. «voldt» i asl. § 17-1 (1). Etter Rt. 1992 s. 64 «P-pilledom II» må det vurderes om handlingen eller unnlatelsen var en «nødvendig betingelse» for skaden, og i forlengelsen av dette om den har vært «så vidt vesentlig i årsaksbildet at det er naturlig å knytte ansvar til den».[100] Skaden må også ha vært en påregnelig følge av styremedlemmets opptreden.[101]

[93] Andenæs (2016) s. 365.
[94] Aarum (1994) s. 190.
[95] Andenæs (2016) s. 646.
[96] Bråthen (2022) s. 257.
[97] HR-2016-1440-A avsnitt 41.
[98] Alteren (2021) *kommentar til asl. § 17-1*, note 2664A.
[99] Aarum (1994) s. 220-221.
[100] Rt. 1992 s. 64, på s. 69-70.
[101] Aarum (1994) s. 74.

Bevismessig er det som hovedregel skadelidte som må sannsynliggjøre at vilkårene for erstatning er til stede, og retten skal legge til grunn det faktum som den finner mest sannsynlig.[102] Hvis alle de kumulative vilkårene i asl. § 17-1 (1) er oppfylt, kan det enkelte styremedlemmet ilegges ansvar for hele det økonomiske tapet. Dersom flere styremedlemmer oppfyller ansvarsvilkårene, vil de imidlertid hefte solidarisk, jf. skadeerstatningsloven[103] § 5-3.

[102] Skoghøy (2022) s. 915. Dette følger av det sivilprosessuelle «overvektsprinsippet».
[103] Lov 13. juni 1969 nr. 26 om skadeserstatning (skadeerstatningsloven).

4 Kan brudd på GDPR medføre styreansvar etter asl. § 17-1 (1)?

4.1 Innledning

I dette kapittelet skal det gjøres rede for om brudd på personvernforordningen kan medføre personlig erstatningsansvar for et styremedlem. Etter asl. § 17-1 (1) kan «selskapet, aksjeeier, eller andre» kreve at «styremedlem» erstatter «skade» som de «i den nevnte egenskap forsettlig eller uaktsomt» har «voldt» vedkommende. I fortsettelsen tas det utgangspunkt i disse vilkårene, og vurderes om man kan se for seg en situasjon ved brudd på GDPR der bestemmelsen er oppfylt. Hovedvekten i redegjørelsen vil ligge på ansvarsgrunnlagets objektive side, herunder hvilke forpliktelser GDPR pålegger styremedlemmet gjennom aksjeloven.

4.2 Skadevilkåret

Et styremedlem kan kun holdes personlig erstatningsansvarlig etter asl. § 17-1 (1) for den «skade» vedkommende har påført «selskapet, aksjeeier eller andre». I «skade» ligger et krav om et erstatningsrettslig vernet økonomisk tap som kan måles i kroner og øre.[104] Spørsmålet er på hvilke måter brudd på GDPR kan medføre et erstatningsmessig økonomisk tap, og for hvem av de aktuelle skadelidte.

Et selskap kan både bli ilagt et overtredelsesgebyr ved brudd på bestemte artikler i GDPR, og bli dømt til å utbetale erstatning til enhver som har lidd skade som følge av selskapets overtredelse av forordningen, jf. henholdsvis GDPR art. 83 nr. 4 og 5, og 82 nr. 1. Både overtredelsesgebyr og erstatningsutbetalinger medfører økte utgifter, og følgelig et tap i selskapets alminnelige formuesstilling.[105] For selskapet vil dette være et erstatningsmessig økonomisk tap. Overtredelsesgebyret på kr. 5 millioner som Ferde AS ble ilagt i 2021, som vist til under kapittel 2.3, var dermed et økonomisk tap for selskapet som ville oppfylt skadevilkåret i asl. § 17-1 (1).

[104] Aarum (1994) s. 74 og 116.
[105] Woxholth (2021) s. 356.

Det finnes riktignok flere andre måter et økonomisk tap kan oppstå på for selskapet som vil oppfylle kravene til en erstatningsmessig skade. Manglende etterlevelse av GDPR kan tenkes å føre til omsetningssvikt, eller tap av forretningsforbindelser som en konsekvens av omdømmetap, hvilket er tap som det er mulig å måle i kroner og øre.

I realiteten er nok imidlertid overtredelsesgebyrene de økonomiske tapene som kunne tenkes å føre til en styreansvarssak i praksis. Grunnen er at det kan være krevende å nå frem med erstatningskrav etter asl. § 17-1 (1), og at det derfor er forbundet en stor prosessrisiko med å gå til sak mot et styremedlem. Det er som hovedregel skadelidte som må sannsynliggjøre at vilkårene for erstatning er til stede.[106] Ansvarsgrunnlaget beror på en helhetsvurdering av flere elementer som kan være sammensatte,[107] og det bekreftes i rettspraksis at kravet til årsakssammenheng på området oppfattes strengt.[108] Det er derfor i hovedsak tapet etter et overtredelsesgebyr som på generell basis vil være av en størrelse som forsvarer en rettssak for selskapet. Videre vil man ved et overtredelsesgebyr ha et vedtak fra Datatilsynet som beskriver og konstaterer bruddet på forordningen, som kan forenkle bevisførselen og argumentasjonen rundt vilkårene om årsakssammenheng og ansvarsgrunnlag.

Når det gjelder erstatningskrav fra et selskap, vil avhandlingen i det videre derfor være rettet mot tap oppstått som følge av et overtredelsesgebyr. Dersom de øvrige vilkårene i asl. § 17-1 (1) er oppfylt, kan selskapet gjennom generalforsamlingen rette erstatningskrav mot styremedlemmene for slike økonomiske tap, jf. asl. § 17-3. Kravet kan også reises av selskapets konkursbo hvis selskapet er insolvent. Bostyrer vil i forbindelse med konkurser kunne gjøre gjeldende krav om erstatning fra styremedlemmene basert på at selskapet er påført tap.[109] Konkursboet har ikke et selvstendig krav, men trer da inn i selskapets krav.[110] Ved konkurs er hensynet til skyldnerens fordringshavere det sentrale,[111] og bostyrer kan velge å gå til styreansvarssak for å skaffe dekning. Når selskapets krav på erstatning omtales i det videre, er det dermed med den forutsetningen at dette, ved konkurs, også er et krav som kan gjøres gjeldende av selskapets konkursbo.

Asl. § 17-1 (1) åpner også for muligheten for «andre» til å fremme krav mot styremedlemmet, herunder tredjeparter. Et erstatningsmessig økonomisk tap kan oppstå ved en direkte

[106] Skoghøy (2022) s. 915.
[107] Se kapittel 3.2.
[108] Aarum (1994) s. 72. Se bl.a. Rt. 1973 s. 821 og Rt. 1979 s. 46.
[109] Aarbakke (2022) *kommentar til asl. § 17-1*, punkt 1.13.
[110] Rt. 1993 s. 1399 og Rt. 2008 s. 833.
[111] Andenæs (2009) s. 11.

erstatningsbetingende handling mot dem, der selskapet ikke har noe korresponderende krav.[112] Som beskrevet under kapittel 2.3 er et eksempel at en fysisk person som selskapet behandler personopplysninger om, betaler et urettmessig økonomisk krav rettet mot vedkommende som følge av et identitetstyveri etter et konfidensialitetsbrudd hos virksomheten.[113]

Et slikt erstatningskrav fra aksjeeiere eller andre tapslidende tredjeparter kan i prinsippet rettes direkte mot styremedlemmene i medhold av asl. § 17-1 (1). Disse kravene vil imidlertid også kunne rettes mot selskapet etter GDPR art. 82, eller alminnelige erstatningsrettslige regler.[114] Et solvent selskap vil som oftest være mer betalingsdyktig enn et styremedlem, og dermed et mer attraktivt søksmålsobjekt. Videre vil ikke disse erstatningskravene være betinget av en bevisgjøring av at ansvarsvilkårene i asl. § 17-1 (1) er oppfylt, som kan være krevende, jf. redegjørelsen ovenfor. En tredjeperson vil derfor kunne anse det mer nærliggende å gå til sak mot selskapet dersom det er tvil om styremedlemmene kan klandres, hvilket igjen kan føre til et økonomisk tap for virksomheten som tidligere beskrevet. På grunn av dette står selskapet igjen som den mest aktuelle skadelidte man kan tenke seg at kunne gått til en styreansvarssak i praksis.

Det reiser riktignok også sammensatte spørsmål knyttet til forholdet mellom selskapets tap/krav ved betaling av et overtredelsesgebyr, og aksjonærenes/kreditorenes avledede tap, jf. asl. § 17-1 (1). Utbetalingen vil medføre en reduksjon av selskapets formuesmasse, men samtidig også kunne føre til at aksjeeier får redusert verdi av aksjene/utbyttemulighet, og at kreditor får redusert dekningsmulighet. Adgangen for aksjonærene/kreditorene til å kreve slike avledede tap dekket av styremedlemmet er omdiskutert.[115] Jeg velger imidlertid å ikke gå inn på disse problemstillingene, da de er av underordnet interesse for avhandlingens overordnede tema.

Som fremstillingen over viser, er det flere måter et økonomisk tap kan oppstå på ved styrets brudd på GDPR, både overfor selskapet og andre. Det er imidlertid selskapets krav mot styremedlemmene, som følge av et overtredelsesgebyr, som fremstår som det økonomiske tapet som kunne aktualisert en styreansvarssak i praksis. Forutsetningen for den videre

[112] Dette betegnes som et særkrav, jf. Woxholth (2021) s. 362.
[113] Skullerud (2022) *kommentar til Artikkel 82*, avsnitt: *«Skade»*.
[114] Woxholth (2021) s. 353. Organansvaret, som vil si ansvaret selskapet har for styrets og daglig leders handlinger og unnlatelser, er her et aktuelt ansvarsgrunnlag.
[115] Woxholth (2021) s. 362-364.

behandlingen av de øvrige vilkårene i asl. § 17-1 (1), er derfor at dette er det økonomiske tapet som har oppstått.

4.3 Ansvarsgrunnlaget

For at et styremedlem skal kunne holdes personlig erstatningsansvarlig, må vedkommende «i den nevnte egenskap» «forsettlig» eller «uaktsomt» ha foretatt en handling eller unnlatelse som har ført til et økonomisk tap som beskrevet ovenfor, jf. asl. § 17-1 (1). Vurdert ut ifra den kunnskapen styremedlemmet hadde, eller burde hatt på beslutningstidspunktet,[116] må det foreligge et brudd på en plikt som objektivt sett gjelder for vedkommende, og styremedlemmet må kunne bebreides for å ha overtrådt denne.[117]

Det er viktig å igjen presisere at erstatningsansvaret er individuelt, og ansvarsvilkårene må være oppfylt for hvert enkelt styremedlem som saksøkes. I det videre legges det imidlertid til grunn, når ikke annet poengteres, at styret har fattet enstemmige avgjørelser, eller at styret i sin helhet har unnlatt å oppfylle sine forpliktelser. Dette gjøres av oppgavetekniske hensyn slik at ansvarsspørsmålet aktualiseres for det enkelte styremedlem. Av denne grunn vil det tidvis vises samlet til «styrets ansvar» nedenfor, selv om det også her siktes til personlig erstatningsansvar for et styremedlem.

Det første spørsmålet er om selskapets etterlevelse av GDPR er en plikt som objektivt sett gjelder for et styremedlem. Med etterlevelse av GDPR menes her at selskapet har på plass et egnet internkontrollsystem og dermed opererer innenfor de rammene som ble presentert under kapittel 2.2. ovenfor. Om et styremedlem skal ha en slik plikt, må den kunne utledes av aksjeloven, tilhørende aksjerettslige prinsipper, selskapets vedtekter eller annen lovgivning.[118] Hovedbestemmelsen om styrets gjøremål er asl. § 6-12 (1) første punktum,[119] og den må være et sentralt utgangspunkt for vurderingen.[120] Her fremgår at «forvaltningen av selskapet hører under styret». En naturlig språklig forståelse tilsier at styret har det overordnede ansvaret for å lede virksomheten. Ledelsesansvaret gjelder ikke bare selskapets rent forretningsmessige side, men forvaltningen av virksomhetens anliggender i sin

[116] Andenæs (2016) s. 649.
[117] Bråthen (2022) s. 257.
[118] Aarum (1994) s. 187-188.
[119] Andenæs (2016) s. 364.
[120] Aarbakke (2022) *kommentar til asl. § 17-1*, punkt 1.6.

alminnelighet.[121] At forvaltningen «hører under» styret, innebærer at dette både er en rett og en plikt for dem. Uttrykket «forvaltningen» favner vidt, og den generelle utforming gjør asl. § 6-12 egnet til å vurdere om mer spesifikke plikter faller inn under styrets ansvar.

Som et generelt krav gjelder at styrets forvaltning av selskapet må være forsvarlig.[122] Styret har et ansvar for at selskapet opererer innenfor rammene som følger av lov.[123] Personvernforordningen gjelder som norsk lov, jf. personopplysningsloven § 1, hvilket tilsier at styret under forvaltningsansvaret har det øverste ansvaret for å påse at selskapet etterlever GDPR. Mangelfull etterlevelse av forordningen kan derfor utgjøre et brudd på en objektiv plikt som kan føre til styreansvar etter asl. § 17-1 (1). Hva som ligger i det øverste ansvaret, og hvilke plikter styret mer konkret har, må imidlertid vurderes nærmere ut fra en bredere vurdering av asl. § 6-12 opp mot kravene GDPR stiller.

For det første innebærer ikke det at styret har det overordnede ansvaret at de må utføre all forvaltning selv.[124] Det er en plikt til å lede forvaltningen, og styret kan delegere konkrete oppgaver i forbindelse med gjennomføringen av internkontrollsystemet til kompetente ansatte eller den daglige ledelsen, og på den måten oppfylle sitt ansvar.[125] En slik ansvarsbefriende virkning forutsetter imidlertid at delegasjonen både var lovlig og forsvarlig,[126] og styret vil etter delegering måtte overholde sitt tilsyns- og kontrollansvar. Styret må påse at selskapets virksomhet, regnskap og formuesforvaltning er gjenstand for betryggende kontroll, og føre tilsyn med selskapets virksomhet for øvrig, jf. asl. §§ 6-12 (3) og 6-13 (1) og nærmere under kapittel 4.3.2.3.

Videre vil omfanget av styrets forvaltningsansvar, og hva som er en naturlig oppgave for dem variere fra selskap til selskap.[127] Det vil preges av arten og omfanget av selskapets virksomhet,[128] og blir et spørsmål om hva som er forsvarlig i det enkelte selskap til enhver tid. Hva som anses å være forsvarlig forvaltning vil være en kontinuerlig og dynamisk vurdering, som preges av samfunnsutviklingen og de eksterne kravene som stilles til selskapene. I relasjon til overholdelsen av GDPR vil dette være knyttet til kravene som stilles

[121] NOU 1996:3 s. 136.
[122] Bråthen (2022) s. 209.
[123] Woxholth (2021) s. 226. Dette følger også forutsetningsvis av asl. § 6-28 (2).
[124] Andenæs (2016) s. 365-366.
[125] Aarum (1994) s. 218.
[126] En delegasjon er lovlig dersom den ligger innenfor de grenser loven setter, jf. Andenæs (2016) s. 649. Styret kan følgelig ikke delegere bort oppgaver som spesifikt er tillagt dem i loven.
[127] NOU 1996:3 s. 136.
[128] NOU 1996:3 s. 55.

til internkontrollen i selskapet. Hva som her kreves er underlagt en forholdsmessig tilnærming, der hvilke tiltak som må iverksettes i stor grad avhenger av risikovurderinger og det som er nødvendig for å ivareta personvernprinsippene, virksomhetens plikter, og den registrertes rettigheter og friheter, jf. GDPR art. 24 og 32.

Det finnes mange ulike typer selskap, og det er ikke mulig å ta hensyn til ethvert virksomhetsspesifikt moment som påvirker risikovurderingen i denne avhandlingen. Noen selskap utpeker seg imidlertid mer enn andre hva gjelder behov for en omfattende internkontroll, grunnet risikoforhold ved behandlingene virksomheten foretar. I fortsettelsen vil det av den grunn først knyttes noen betraktninger til bestemte forhold som er egnet til å øke risikopreget til en virksomhet (kapittel 4.3.1). I lys av betraktningene vil deretter det nærmere innholdet av styrets ansvar for etterlevelsen av GDPR vurderes og konkretiseres, ved å ytterligere analysere styrets overordnede ansvar for selskapets virksomhet i asl. §§ 6-12 og 6-13, opp mot GDPRs krav til internkontrollsystem (kapittel 4.3.2). Til slutt vil det gjøres rede for ansvarsgrunnlagets subjektive side (kapittel 4.3.3).

4.3.1 Særlige risikoforhold ved et selskaps virksomhet

Typen og størrelsen av selskap, samt hvilke personopplysninger som behandles der, varierer i stor grad. Dette medfører at ikke alle deler av GDPR vil være relevant for et gitt selskap. For det første vil omfanget av selskapets virksomhet være av betydning for hvilke krav som settes til internkontrollsystemet, og i forlengelsen av dette for hvilke forventinger man kan stille til et styremedlem. Målestokken må da være omfanget av selskapets behandlinger av personopplysninger, jf. GDPR art. 24, eller mer presist antall registrerte, antall opplysningstyper og behandlingenes varighet.[129] Et stort forsikringsselskap med mange kunder som behandler personopplysninger i omfattende skala, vil rimeligvis ha et større behov for rutiner og retningslinjer enn små virksomheter der dette gjøres i liten grad.

Det er ikke bare omfanget av selskapets virksomhet som dikterer kravene til internkontrollsystemet. Mindre virksomheter kan være utsatt for stor risiko, og ha behov for flere tiltak enn omfanget av selskapets behandlinger i seg selv skulle tilsi. Noen opplysningstyper vil ha et større behov for beskyttelse enn andre, og nødvendiggjør dermed

[129] GDPR fortalepunkt 75 og Skullerud (2022) *kommentar til Artikkel 32*, avsnitt: «Behandlingens art, omfang, formål og sammenheng».

et mer omfattende internkontrollsystem, jf. GDPR art. 24 om behandlingens «art». Dette gjelder typisk «særlige kategorier» av personopplysninger som beskrevet i GDPR art. 9, og opplysninger om straffedommer og lovovertredelser, jf. GDPR art. 10. Det ligger i disse opplysningstypenes natur at de er sensitive, og behandlingen av dem medfører en høy grad av risiko. En særlig kategori av personopplysninger er eksempelvis genetiske opplysninger, jf. GDPR art. 9 nr. 1, og en behandling av en slik opplysningstype vil kreve sterkere sikkerhetstiltak enn om det gjaldt alminnelige kontaktopplysninger som navn eller et telefonnummer.

Av videre betydning for graden av risiko ved en behandling er formålet med den, jf. GDPR art. 24, altså hva personopplysningene skal brukes til. Dersom behandlingen vil få stor betydning for den registrertes situasjon, er det noe som kan tale for at risikoen er høy.[130] Dette kan være tilfellet der opplysningen skal ligge til grunn for en avgjørelse eller beslutning som påvirker den registrerte, eller har et kontrollformål.[131] Slik kan situasjonen være der behandlingen tar sikte på å avgjøre om den registrerte skal få tilgang til en tjeneste eller kunne inngå en avtale. Eksempler på dette er der et selskap skal foreta en kredittvurdering for å avgjøre om den registrerte skal få lån, eller der et forsikringsselskap behandler personopplysninger for å vurdere om den registrerte skal få tilgang til deres forsikringsordninger. I disse situasjonene kan manglende ivaretakelse av den registrertes rettigheter og friheter ved behandlingen føre til forskjellsbehandling eller økonomiske og sosiale ulemper for vedkommende, jf. GDPR fortalepunkt 75. Det er dermed større risiko ved behandlingen, hvilket nødvendiggjør flere internkontrolltiltak.

Risikoen ved en behandling påvirkes ytterligere av «sammenhengen» den utføres i, jf. GDPR art. 24. Av stor betydning er om det er tale om en systematisk behandling av personopplysninger. Her siktes det særlig til opplysninger som kontinuerlig samles inn og kobles sammen for å kartlegge og analysere individers preferanser, handlinger og behov, jf. GDPR fortalepunkt 75. Ved slike behandlinger vil den registrerte ofte ha mindre kontroll over sine personopplysninger, fordi vedkommende ikke er klar over at opplysningene registreres. Det er derfor vanskeligere for den registrerte å håndheve sine rettigheter etter forordningen. Systematiske behandlinger er dermed ofte særlig inngripende og risikofylte, og fordrer mer omfattende internkontrolltiltak for å kunne ivareta den registrerte.

[130] Skullerud (2022) *kommentar til Artikkel 24*, avsnitt: *«Forholdsmessighet»*.
[131] Skullerud (2022) *kommentar til Artikkel 24*, avsnitt: *«Forholdsmessighet»*.

I relasjon til brudd på informasjonssikkerheten, utgjør dataangrep en stor risiko for virksomhetene. Nasjonal sikkerhetsmyndighet (NSM) la den 3. oktober 2022 frem sin årlige rapport om nasjonalt digitalt risikobilde, som søker å øke bevisstheten om digital sikkerhet i offentlige og private virksomheter.[132] Rapporten viser for det første en økning i antallet registrerte angrepsforsøk mot norske virksomheter i første halvdel av 2022.[133] Videre påpekes det at det særlig er teknologibedrifter, virksomheter innen forskning og utvikling og offentlige forvaltingsorganer som har vært utsatt for cyberangrep det siste året.[134] Viktigheten av at disse sektorene er særlig årvåkne understrekes her av NSM, og det vises til at statistikken samsvarer med PST og Etterretningstjenestens åpne trusselvurderinger.[135]

Dataangrep er særlig egnet til å føre til brudd på GDPR, fordi angrepene kan medføre omfattende brudd på informasjonssikkerheten og de registrertes rettigheter ved at personopplysninger kommer på avveie. En videre konsekvens kan være et overtredelsesgebyr for virksomheten om Datatilsynet finner grunnlag for det. Østre Toten kommune ble eksempelvis ilagt et overtredelsesgebyr på 4 millioner kroner etter å ha blitt utsatt for et dataangrep i januar 2021.[136] Angrepet omfattet blant annet 30 000 dokumenter som til dels inneholdt svært sensitive opplysninger om kommunens innbyggere og ansatte.[137] Styremedlemmer i teknologibedrifter, eller virksomheter innen forskning og utvikling har dermed, på bakgrunn av rapporten fra NSM, en særlig oppfordring til å ha et godt internkontrollsystem for å ivareta informasjonssikkerheten.

Hvor brudd på personvernforordningen finner sted i selskapet, vil følgelig virksomhetens risikopreg kunne påvirke hvorvidt styremedlemmene kan sies å ha oppfylt kravet til forsvarlig forvaltning eller ikke. Jo høyere risikoen for brudd på GDPR er i selskapet, desto større behov er det for at virksomhetens styremedlemmer tar ansvar for behandlingene av personopplysninger.

[132] Regjeringen (2022) *Nasjonal Sikkerhetsmåned er i gang*, https://www.regjeringen.no/no/aktuelt/nasjonal-sikkerhetsmaned-er-i-gang/id2930570/.
[133] Nasjonalt digitalt risikobilde (2022) s. 15.
[134] Nasjonalt digitalt risikobilde (2022) s. 15.
[135] Nasjonalt digitalt risikobilde (2022) s. 15.
[136] Datatilsynet (2022). *Vedtak om overtredelsesgebyr og pålegg.* s. 1.
[137] Datatilsynet (2022). *Vedtak om overtredelsesgebyr og pålegg.* s. 2.

4.3.2 Det nærmere innholdet av styrets ansvar for etterlevelsen av GDPR

Sentrale deler av styringssystemet for internkontroll har blitt presentert under kapittel 2. Som vist, bør selskapene for å sikre og påvise etterlevelse av GDPR ha en internkontrollstruktur tilpasset deres virksomhet, jf. GDPR art. 24 og 32. Systemet bør inneholde en styrende, gjennomførende og kontrollerende del, med henholdsvis styrende dokumenter, rutiner/retningslinjer og sikkerhetstiltak, og aktiviteter for avvikshåndtering. I det videre skal det nærmere innholdet av styrets ansvar for selskapets etterlevelse av GDPR vurderes med utgangspunkt i deres forpliktelser knyttet til hver av disse delene av styringssystemet. Grunnen er at dette gjør det mulig å illustrere ulike sider av styrets forvaltnings-, og tilsynsansvar, og enklere vurdere hvilken opptreden som mer konkret vil innebære et brudd.

4.3.2.1 Styrets ansvar for internkontrollens styrende dokumentasjon

En god internkontrollstruktur vil ofte innebære opprettelse av styrende dokumentasjon, der selskapets overordnede valg og rammer for behandlingen av personopplysninger i det daglige dokumenteres.[138] Styringsdokumentene bør normalt inneholde informasjon om hvilke plikter og regler selskapet må forholde seg til, hvordan systemet skal gjøres virksomt i organisasjonen for å kunne overholde disse, organisering og fordeling av ansvar internt, og en plan for vedlikehold av systemet.[139] En beskrivelse av hvordan virksomheten ivaretar sikkerheten ved behandlingene er også noe som bør være til stede, jf. GDPR art. 32 om «egnede tekniske og organisatoriske tiltak», og den kan forankres i den styrende dokumentasjonen.[140] Beskrivelsen bør eksempelvis inneholde selskapets sikkerhetsmål og en plan for gjennomføringen og organiseringen av sikkerhetsarbeidet i virksomheten.

Spørsmålet er hvilket ansvar styret har for at det utarbeides styrende dokumentasjon i selskapet. Styret er særlig pålagt å sørge for en «forsvarlig organisering av virksomheten», jf. asl. § 6-12 (1) annet punktum. I dette ligger at styret har ansvaret for at selskapet

[138] Veum (2010) s. 206.
[139] Veum (2010) s. 207.
[140] Datatilsynets veileder (2018). *Etablere internkontroll*, kapittel: *«5 Internkontrollens struktur.»*, overskrift*: «Styrende dokumentasjon»*.

organiseres på en formålstjenlig måte, har tilstrekkelig og kvalifisert personale, og at det er klare ansvarslinjer.[141] Det er et overordet ansvar, og ikke en plikt til detaljstyring.[142]

Når hovedprinsippene i organiseringen av selskapet er en styresak etter kravet til forsvarlig organisering, er det naturlig at dette innbefatter det overordnede ansvaret for opprettelsen av internkontrollsystemets styrende dokumenter i det omfang som er påkrevd. Grunnen er for det første at en virksomhet som behandler personopplysninger vil kunne ha behov for styrende dokumentasjon for å være formålstjenlig organisert. Videre har styret etter asl. § 6-12 ansvaret for å påse at det er klare ansvarslinjer og at det er tilstrekkelige og kompetente ansatte, hvilket i relasjon til GDPR er forhold som fastlegges og beskrives i styringsdokumentene.

At styret har det øverste ansvaret for selskapets styrende dokumentasjon, underbygges ytterligere av at asl. § 6-12 (2) presiserer at de skal i «nødvendig utstrekning fastsette planer og budsjetter for selskapets virksomhet». En plikt til å fastsette «planer» innebærer å legge en virksomhetsplan og trekke opp rammene for fremtidig drift.[143] Internkontrollsystemets styrende dokumentasjon er nettopp selskapets plan for å kunne etterleve kravene GDPR stiller til behandling av personopplysninger, noe som tilsier at det øverste ansvaret for utarbeidelsen av den bør høre til styret.

Totalt sett er det altså klart at styret har ansvar for å fastlegge styrende dokumentasjon. Hva som mer spesifikt ligger i kravet vil variere med virksomheten og behandlingene som foretas, i tråd med det som er diskutert i kapittel 4.3.1.

4.3.2.2 Styrets ansvar for personvernrutiner og sikkerhetstiltak

Rammene og valgene fastlagt i den styrende dokumentasjonen skal kommuniseres i den gjennomførende delen av internkontrollen.[144] Her dokumenteres virksomhetens rutiner/retningslinjer og sikkerhetstiltak for arbeidet, og gjøres tilgjengelig for de ansatte. De fleste virksomheter bør ha rutiner for innhenting av samtykke, retting, sletting, innsyn, tildeling og avslutning av tilganger, samt informasjon til de registrerte.[145] Rutiner for

[141] NOU 1996:3 s. 136.
[142] Andenæs (2016) s. 366.
[143] Aarbakke (2022) *kommentar til asl. § 6-12*, punkt 2.1.
[144] Veum (2010) s. 208.
[145] Skullerud (2022) *kommentar til Artikkel 24*, avsnitt: *«Behandlingsregler»*.

protokollføring av behandlingene i samsvar med GDPR art. 30, er på sin side et eksempel på noe som må finnes om selskapet har mer enn 250 ansatte.[146] Nødvendige tiltak og rutiner for å ivareta informasjonssikkerheten bør også være til stede i et selskap, jf. GDPR art. 32. Aktuelle tiltak kan eksempelvis være pseudonymisering og kryptering av personopplysninger, jf. GDPR art. 32 nr. 1 bokstav a, eller rutiner for informasjonshåndtering.[147]

Spørsmålet er hvilket ansvar styret har for implementeringen av rutiner/retningslinjer og sikkerhetstiltak i selskapet. En formålstjenlig organisering av et selskap som behandler personopplysninger, fordrer rutiner og retningslinjer for å regulere arbeidet i virksomheten, jf. asl. § 6-12 (1). Forståelsen underbygges av Bråthen, som uttrykker at styret må «sørge for at selskapet har internkontroll og rutiner som tilfredsstiller GDPR».[148]

Det fremgår riktignok av asl. § 6-12 (2) andre punktum at styret «kan» fastsette «retningslinjer for virksomheten». En naturlig forståelse av «kan» tilsier i seg selv at dette er en rett og ikke en plikt. I forarbeidene fremgår det at det er opp til styret å vurdere og avgjøre hvorvidt retningslinjer skal gis og hvilke spørsmål de skal regulere.[149] Dersom retningslinjer er nødvendig for forsvarlig drift, vil det likevel måtte være påkrevd av styret. En slik forståelse underbygges av at den fakultative adgangen til å fastsette retningslinjer synes inntatt av hensyn til særlig små virksomheter,[150] der dette kan være uforholdsmessig byrdefullt. Forståelsen er også i tråd med kravene ellers etter asl. § 6-12, som for styret varierer fra selskap til selskap.[151] I relasjon til iverksettelsen av retningslinjer som er nødvendig for etterlevelsen av GDPR, må dette dermed anses påkrevd av styret etter asl. § 6-12 (2).

Spørsmålet om styrets ansvar for forsvarlig organisering etter asl. § 6-12, og mer spesifikt rutiner, har sjeldent kommet opp i rettspraksis. Forsvarlighetskravet ble imidlertid vurdert av Høyesterett i HR-2013-574-A, som omhandlet en straffesak der en person ble sterkt skadet av en isklump som falt ned fra taket på en bygård. Gårdselskapet hadde en person A som både enestyre og daglig leder. Vedkommende var tiltalt for uaktsom skade etter

[146] Unntaket for selskap med færre ansatte følger av GDPR art. 30 nr. 5.
[147] Datatilsynets veileder (2018). *Etablere internkontroll*, kapittel*: «3. Iverksette styringssystem for informasjonssikkerhet.»*, overskrift: *«Rutiner for informasjonssikkerhet»*.
[148] Bråthen (2022) s. 210.
[149] NOU 1996:3 s. 137.
[150] Ot.prp. nr. 23 (1996-1997) s. 147.
[151] NOU 1996:3 s. 136.

straffeloven 1902 § 238 for å ikke ha sørget for sikkerhetsrutiner som var tilstrekkelige til at risikoen ble oppdaget. Høyesterett uttalte i dommen at A pliktet å sørge for at gårdselskapet hadde «forsvarlige rutiner for avdekking og fjerning av fare for sne- og isras, herunder å påse at arbeidet utføres av kompetente folk, og å føre kontroll med at rutinene følges».[152]

Selv om dommen omhandlet ansvar for rutiner i relasjon til fare for personskade i en straffesak, har Høyesteretts generelle uttalelser i relasjon til asl. § 6-12 overføringsverdi. Høyesterett understreker at bestemmelsen innebærer et ansvar for at det skal være nødvendige rutiner for virksomheten. Avgjørelsen illustrerer også at forsvarlighetskravet er strengere når virksomhetens art innebærer en høy risiko. Her medførte virksomheten fare for sne- og isras, og det måtte ut fra dette sørges for forsvarlige rutiner.

Når det gjelder ansvaret for sikkerhetstiltak, gjør mange av de samme betraktningene seg gjeldende. En forsvarlig ledelse og organisering av en virksomhet som behandler personopplysninger, kan nødvendiggjøre tiltak for å ivareta informasjonssikkerheten, jf. § asl. 6-12 (1). At styret har et ansvar for å ivareta informasjonssikkerheten kan utledes av vedtaket om overtredelsesgebyr mot Ferde AS. Datatilsynet vektla i sin avgjørelse at den aktuelle behandlingen av personopplysninger ble gjennomført uten at det forelå skriftlige risikovurderinger.[153] Det uttales at det «måtte klassifiseres som klart uaktsomt å ikke ha på plass disse sentrale instrumentene etter personvernregelverket», og «at ansvaret ligger hos styret i Ferde AS, jf. aksjeloven § 6-12 første ledd første punktum og aksjeloven § 6-30». Videre ble «styrets tilsynsansvar med selskapets virksomhet, jf. aksjeloven § 6-13» understreket i denne forbindelse. Her hadde styret unnlatt å sørge for at selskapet hadde instrumentene på plass for å fasilitere for risikovurderinger ved den aktuelle behandlingen, noe som ble ansett som uaktsomt av dem.

Hvilke konkrete rutiner og tiltak selskapet trenger, avhenger av hva som er nødvendig for at behandlingen av personopplysninger kan gjennomføres på en forsvarlig måte i tråd med forordningen. Styret i et selskap som driver med utadrettet salgsaktivitet, vil ha større behov for å etablere rutiner for innsamling av personopplysninger enn styret i et helseforetak der hvilke opplysninger om pasienten som skal samles inn fremgår av spesiallovgivningen.[154]

[152] HR-2013-574-A avsnitt 27.
[153] Datatilsynet (2021). *Vedtak om overtredelsesgebyr – Ferde AS.* s. 12. Ved siden av mangelen på risikovurderinger, viste Datatilsynet til manglende databehandleravtale og overføringsgrunnlag. Dette er krav ved behandling av personopplysninger som har falt utenfor avhandlingens tema.
[154] Skullerud (2022) *kommentar til Artikkel 24*, avsnitt: *«Behandlingsregler».*

Tilsvarende vil styret i et helseforetak som behandler sensitive helsepersonopplysninger, måtte fastlegge mer omfattende sikkerhetstiltak enn i et rørleggerfirma som kun behandler kontaktopplysninger.

Når det kommer til fastleggelsen av de nødvendige tiltakene og rutinene for å ivareta informasjonssikkerheten, handler det om å gjennomføre risikovurderinger. For å gjøre det enklere å identifisere og vurdere risikonivået ved behandlingen opp mot det akseptable, anbefaler Datatilsynet at man følger anerkjente internasjonale standarder som gjør rede for kravene til styringssystem for informasjonssikkerhet, som ISO/IEC 27001.[155] Standarden beskriver en strukturert og systematisk tilnærming til selskapets arbeid med å administrere informasjonssikkerhet.[156] Det vil imidlertid ikke være nødvendig å følge en så omfattende standard for en liten virksomhet som behandler få personopplysninger, og her vil det nok være tilstrekkelig med en kortere prosatekst som beskriver tenkelige risikoer.[157] Styret i større virksomheter i motsatte ende av skalaen, bør imidlertid sørge for at selskapet legger seg tettere opp mot en risikovurderingsmetodikk som følger en etablert standard som ISO/IEC 27001. Ansvaret innebærer å iverksette og sette av penger til prosessen med å få dette på plass.

4.3.2.3 Styrets ansvar for kontroll med rutinene og sikkerhetstiltakene

Verdien av arbeidet med rutiner og sikkerhetstiltak er liten om de ikke fungerer eller faktisk følges. Den kontrollerende delen av internkontroll er derfor rettet mot aktiviteter som skal bidra i avdekkingen av om selskapet rent faktisk overholder forpliktelsene etter GDPR.[158] Dette vil i stor grad handle om å måle hvordan internkontrollen fungerer. Sentralt er kontrollerende elementer som sjekklister og avviksrapportering som kan bidra til å avdekke avvik fra rutinene og sikkerhetstiltakene som er satt, slik at det eventuelt kan iverksettes korrigerende tiltak.[159]

Etter asl. § 6-12 (3) og (4) skal styret påse at selskapets «virksomhet» er «gjenstand for betryggende kontroll», samt iverksette «de undersøkelser det finner nødvendig for å utføre sine

[155] Datatilsynets veileder (2018). *Etablere internkontroll,* kapittel: *«3. Iverksette styringssystem for informasjonssikkerhet»,* overskrift*: «Dokumentasjon og oppbygging av styringssystem for informasjonssikkerhet».*
[156] Jøsang (2021) s. 216-217.
[157] Skullerud (2022) *kommentar til Artikkel 32,* avsnitt: *«Nummer 2, Risikovurdering».*
[158] Veum (2010) s. 208.
[159] Datatilsynets veileder (2018). *Etablere internkontroll,* kapittel: *«5. Internkontrollens struktur»,* overskrift: *«Kontrollerende dokumentasjon».*

oppgaver. Her presiseres styrets overordnede ansvar for selskapets interne kontroll.[160] En «betryggende kontroll» av en virksomhet som behandler personopplysninger vil være avhengig av tiltak for å oppdage og håndtere avvik, jf. asl. § 6-12 (3). Styret må følgelig føre kontroll med at virksomhetens rutiner og sikkerhetstiltak fungerer, og dermed påse at selskapet har kontrollerende elementer på plass.

At styret har en slik forpliktelse underbygges av den videre konkretiseringen av kontrollansvaret i asl. § 6-13 (1). Her fremgår det at styret skal «føre tilsyn med den daglige ledelse og selskapets virksomhet for øvrig». Formålet er å presisere styrets ansvar for andres handlinger og unnlatelser i forbindelse med forvaltningen av selskapet.[161] Plikten understrekes også eksplisitt i nevnte HR-2013-574-A, der Høyesterett presiserer at styret har ansvar for å «føre kontroll med at rutinene følges».[162]

Dersom det avdekkes avvik fra rutinene og sikkerhetstiltakene som er satt, må styret reagere på risikoinformasjonen, ettersom noe annet ikke vil innebære en reell og effektiv «betryggende kontroll», jf. asl. § 6-12 (3). Avvikshåndteringen fordrer rutiner og retningslinjer for dokumentering og rapportering av brudd på personopplysningssikkerheten, jf. GDPR art. 33 og 34, samt for iverksettelsen av korrigerende tiltak. Dette kan være strakstiltak for å avgrense følgeskader for berørte, som å umiddelbart informere vedkommende om bruddet og mulige konsekvenser av det. Korrigerende tiltak kan også innebære en større prosess som en revisjon av internkontrollsystemet, ved eksempelvis en endring i virksomhetens generelle organisering eller risikovurderingsmetodikk.

Det er viktig at avvik faktisk blir meldt, og at styret ellers får den informasjonen de trenger for å kunne iverksette korrigerende tiltak. For at styret skal ha forutsetninger for å fange opp eventuelle problemer med internkontrollen, trenger de gode kommunikasjonskanaler med selskapets øvrige ansatte. De er særlig avhengig av oppdateringer fra den daglige lederen, som gjerne vil være involvert i arbeidet med internkontrollsystemet. Den daglige lederen har et ansvar for å gi styret underretning om selskapets virksomhet, jf. asl. § 6-15 (1), herunder selskapets etterlevelse av GDPR. Styret har imidlertid en aktivitetsplikt, og tilsynsansvaret etter asl. § 6-13 (1) omfatter å føre kontroll med at daglig leder oppfyller kravene som følger

[160] Andenæs (2016) s. 366.
[161] Woxholth (2021) s. 226.
[162] HR-2013-574-A avsnitt 27.

med stillingen, og kan innebære en plikt til å gripe inn overfor vedkommende om dette ikke er tilfellet.[163]

En annen viktig kilde til informasjon og råd om personvernkonsekvenser er personvernombudet, jf. GDPR art. 39 nr. 1. Fordi ombudet er et særlig viktig organisatorisk tiltak,[164] hører det naturlig inn under kravet til forsvarlig organisering å tilrettelegge for at personvernombudet skal kunne fungere i sin rolle der dette er påkrevd, jf. GDPR art. 37.[165] Når det kommer til personvernombudet og rådene det skal gi, rapporterer vedkommende «direkte til det høyeste ledelsesnivået hos den behandlingsansvarlige», jf. GDPR art. 38 nr. 3 siste setning. «Høyeste ledelsesnivå» er ikke entydig, men må forstås som at ombudet skal rapportere til det høyeste nivået for den daglige ledelse.[166] Det er imidlertid en viss fleksibilitet i de nøyaktige rapporteringslinjer, og ombudet kan gis en adgang til å rapportere direkte til styret ved behov.[167]

Rådene skal sikre at ledelsen alltid er godt informert om relevante forhold i relasjon til selskapets etterlevelse av forordningen.[168] En viktig presisering er at ombudene er mellomledd mellom interessentene i selskapet, og de vil ikke være personlig ansvarlig etter GDPR i tilfelle av manglende overholdelse av forordningen.[169] Etter at rådene er gitt overlates ansvaret for å iverksette eventuelle korrigerende tiltak til virksomhetens ledelse.[170] Styret må imidlertid før og etter rådene gis ivareta sin tilsynsplikt overfor den daglige ledelse og virksomheten for øvrig, jf. asl. § 6-13. Dersom styret i tillegg eksplisitt mottar rapport vil de ha en særlig oppfordring til å påse at nødvendige tiltak blir gjennomført. Om styret unnlater å ta aksjon ved rapport om risikoforhold fra daglig leder, eller ved direkte råd fra personvernombudet, vil det være en omstendighet som kan tyde på at styret klart har brutt sitt forvalteransvar etter asl. § 6-12.[171]

[163] Andenæs (2016) s. 366.
[164] Guidelines on Data Protection Officers (2017) s. 4.
[165] Se kapittel 2.2.3 for en gjennomgang av personvernombudets oppgaver.
[166] Jarbekk (2019) s. 337.
[167] Jarbekk (2019) s. 337.
[168] Rüker/Kugler (2018) s. 184.
[169] Kuner (2020) s. 707. Om et personvernombud kan holdes personlig ansvarlig etter alminnelige erstatningsrettslige regler, faller utenfor avhandlingens tema.
[170] Rüker/Kugler (2018) s. 184.
[171] Dette er også en omstendighet som kan tyde på et forsettlig brudd på GDPR, jf. Guidelines on the application and setting of administrative fines (2017) s. 11-12.

4.3.2.4 Oppsummerende om styrets ansvar for etterlevelsen av GDPR

Redegjørelsen ovenfor viser at styret har et ansvar i tilknytning til fastsettelsen av den styrende dokumentasjonen, rutinene og sikkerhetstiltakene som springer ut av dette, samt med kontroll av dem, jf. asl. §§ 6-12 og 6-13. Omfanget av ansvaret varierer imidlertid etter det som er nødvendig, avhengig av virksomhetens samlede risikopreg. Enkelte risikoforhold ved virksomheten fordrer særlige rutiner og sikkerhetstiltak, hvilket skjerper forventningene til styremedlemmene.

Brudd på forvalteransvaret kan foreligge både ved handlinger og unnlatelser, men det er unnlatelsesansvar som særlig kan være aktuelt i relasjon til etterlevelsen av GDPR. Om styret unnlater å forholde seg til regelverket eller konkret risikoinformasjon fra personvernombudet eller daglig leder, og det fører til overtredelsesgebyr, må det anses å være et brudd på kravet til forsvarlig forvaltning, jf. asl. § 6-12 (1). Også der styret eksplisitt vedtar en autorisering av en ulovlig behandling av personopplysninger etter motstridende råd, må det betraktes som en ansvarsbetingende unnlatelse av å reagere på risikoinformasjon. Det er imidlertid viktig å merke at dersom et styremedlem aktivt har stemt mot den aktuelle beslutningen i styremøte,[172] vil det ikke være aktuelt med erstatningansvar for vedkommende.[173]

At unnlatelsesansvar i relasjon til etterlevelsen av GDPR er sentralt, viser seg i Datatilsynets vedtak mot Ferde AS. Her hadde styret unnlatt å sørge for at selskapet hadde instrumentene på plass for å fasilitere for risikovurderinger ved en behandling, noe som ble ansett som uaktsomt av dem.[174] Som grunnlag pekte Datatilsynet her både på asl. §§ 6-12 og 6-13.

Grunnen til at unnlatelsesansvar er særlig aktuelt, er at formålet med risikostyring og intern kontroll er å håndtere, og minimere risikoen som er knyttet til virksomhetsutøvelsen.[175] Selv om styret har iverksatt internkontrolltiltak, kan selskapet likevel ende opp med å bryte GDPR og ilegges et overtredelsesgebyr. Kravene til internkontroll er risikobaserte, og det vil ofte være vanskelig å vite hva som er godt nok. Styremedlemmene må ut fra den kunnskapen de hadde, eller burde hatt på beslutningstidspunktet, kunne treffe sine beslutninger uten at enhver feilvurdering senere skal kunne føre til et personlig erstatningsansvar, jf. asl. §§ 6-12

[172] Om en beslutning ikke er enstemmig, skal det angis i protokollen hvem som har stemt for og imot, jf. asl. § 6-29.
[173] Andenæs (2016) s. 649 og Aarum (1994) s. 238. Om styremedlemmet likevel kan holdes ansvarlig om han er med på å iverksette beslutningen han har stemt mot reiser vanskelige spørsmål, hvilket det avgrenses mot.
[174] Datatilsynet (2021). *Vedtak om overtredelsesgebyr – Ferde AS.* s. 12.
[175] Schartum (2020) s. 240.

(3) og § 6-13.[176] Det er klart nok ingen automatikk i at et styremedlem holdes personlig ansvarlig der selskapet pålegges et overtredelsesgebyr. Selskapet kan betale gebyret, uten at det senere reises erstatningssak mot et styremedlem. Hvis styremedlemmene involverer seg, sikrer at selskapet har på plass nødvendige overordnede rammer og rutiner/sikkerhetstiltak, tilstrekkelig og kompetent personell til å følge og gjennomføre disse, og ivaretar sitt kontroll- og tilsynsansvar, vil kravet til forsvarlig forvaltning vanskelig være brutt.

Dersom dette ikke gjøres vil imidlertid styret, som vist, kunne anses å ha brutt kravet til forsvarlig forvaltning. Selv om et styremedlem ved mangelfull etterlevelse av GDPR dermed har brutt en plikt som objektivt sett gjelder for vedkommende etter asl. § 17-1 (1), er det en videre forutsetning for personlig erstatningsansvar at vedkommende også kan bebreides for å ha overtrådt aktsomhetsnormen.[177]

4.3.3 Ansvarsgrunnlagets subjektive side

Spørsmålet er hva som skal til for at et styremedlem kan bebreides for å ha brutt kravet til forsvarlig forvaltning ved manglende etterlevelse av GDPR, jf. asl. § 6-12. Dersom styremedlemmet bevisst, «forsettlig», har unnlatt å sørge for selskapets etterlevelse av forordningen, vil ansvarsgrunnlaget utvilsomt være oppfylt, jf. asl. § 17-1 (1). Dette kan være tilfellet der vedkommende bevisst autoriserer en ulovlig behandling av personopplysninger.

Det er imidlertid tilstrekkelig å konstatere uaktsomhet, jf. asl. § 17-1 (1). Utgangspunktet for uaktsomhetsvurderingen er de forventninger man kan stille til et normalt og samvittighetsfullt styremedlem i en tilsvarende situasjon.[178] Der et styremedlem har brutt kravet til forsvarlig forvaltning ved manglende etterlevelse av GDPR, vil det være en presumsjon for at vedkommende har opptrådt uaktsomt, jf. HR-2016-1440-A.[179] Betydningen av dette er at ansvarsgrunnlaget i utgangspunktet er oppfylt allerede der det konstateres et slikt brudd på en plikt som objektivt sett gjelder for vedkommende.

Det egentlige spørsmålet blir dermed om styremedlemmet kan påberope seg en unnskyldningsgrunn.[180] Om dette ikke kan gjøres, vil vedkommende lastes for normbruddet.

[176] Andenæs (2016) s. 649.
[177] Bråthen (2022) s. 257.
[178] Bråthen (2022) s. 257.
[179] HR-2016-1440-A avsnitt 41.
[180] Aarum (1994) s. 220.

Bestemte forhold ved det aktuelle styremedlemmets person, sykdom, personlig ferdigheter, manglende erfaring o.l., er som hovedregel ikke relevant, [181] men har i enkelte helt spesielle tilfeller likevel fått gjennomslag.[182] Fordi culpavurderingen tar utgangspunkt i situasjonen på beslutningstidspunktet,[183] vil derimot styremedlemmets eventuelle manglende kunnskap – villfarelse - kunne tenkes å være en legitim subjektiv unnskyldningsgrunn.

Rettslig villfarelse, som vil si en uvitenhet eller uriktig forståelse av en norm som gjør en handling eller unnlatelse rettsstridig, er som hovedregel ikke en relevant subjektiv unnskyldningsgrunn.[184] Styret plikter etter kravet til forsvarlig forvaltning å drive selskapet i henhold til loven. Selv om GDPR er et omfattende regelverk, kan det derfor ikke anses ansvarsbefriende som styremedlem å hevde at man ikke hadde kjennskap til at handlingen eller unnlatelsen var i strid med regelverket. Noe annet er den usikkerheten som vil være forbundet med hvilke tiltak som må iverksettes, og at det kan være vanskelig å vite hva som er godt nok. Dette er knyttet til en konkret forsvarlighetsvurdering, og at ikke enhver feilvurdering eller uheldig disposisjon fører til pliktbrudd, og er følgelig noe annet enn rettslig villfarelse.

Uvitenhet om de faktiske forholdene som danner grunnlaget for lovovertredelsen vil oftere kunne være ansvarsbefriende for et styremedlem.[185] Et faktisk forhold kan være en spesiell risiko ved virksomheten som senere realiserte seg, som at selskapet var særlig utsatt for dataangrep. Dersom internkontrollen ved behandlingen av personopplysninger var mangelfull fordi styremedlemmet var ukjent med risikoforholdet, kan det i prinsippet føre til fritak for ansvar. Styremedlemmets faktiske kunnskap må imidlertid suppleres hvis vedkommende burde skaffet seg slik kunnskap, jf. asl. §§ 6-12 (3) og § 6-13.[186] Om styremedlemmets manglende kunnskap ikke var aktsom, vil vedkommende derfor ikke kunne vise til den manglende kunnskapen som en subjektiv unnskyldningsgrunn. Det avgjørende blir om styremedlemmet forvaltet selskapet på en forsvarlig måte, ut ifra den kunnskapen vedkommende hadde eller burde hatt på tidspunktet den skadevoldende handlingen eller unnlatelsen fant sted. Dette innebærer at der styremedlemmet ville oppdaget

[181] Aarum (1994) s. 221.
[182] RG 1994 s. 145 (Eidsivating). Lagmannsretten kom til at vedkommende var så psykisk og fysisk svekket at ansvar ikke kunne gjøres gjeldende.
[183] Andenæs (2016) s. 647.
[184] Aarum (1994) s. 230.
[185] Aarum (1994) s. 230.
[186] Andenæs. (2016) s. 649.

risikoen ved virksomhet hvis de hadde oppfylt kravet til forsvarlig forvaltning, så vil ikke den faktiske villfarelsen være unnskyldelig.

Det er altså lite rom for subjektive unnskyldningsgrunner om styremedlemmet først anses å ha brutt kravet til forsvarlig forvaltning ved manglende etterlevelse av GDPR. Når asl. §§ 6-12 og 6-13 gir uttrykk for et alminnelig og allment krav til forsvarlig utøvelse av styrevervet i et aksjeselskap, er dette naturlig. Etter bestemmelsene foretas en omfattende vurdering av om styremedlemmets handling eller unnlatelse var aktsom på beslutningstidspunktet, hvilket medfører at store deler av bebreidelsesvurderingen alt er foretatt.

4.4 Årsakssammenheng

Et siste vilkår for at et styremedlem skal kunne holdes personlig erstatningsansvarlig for manglende etterlevelse av GDPR, er at vedkommende har «voldt» skadelidte det tapet som er lidt, jf. asl. § 17-1 (1). Det må påvises adekvat årsakssammenheng, hvilket innebærer at styremedlemmets erstatningsbetingende handling eller unnlatelse må ha vært en «nødvendig betingelse» for det tapet som har oppstått, og i forlengelsen «så vidt vesentlig i årsaksbildet at det er naturlig å knytte ansvar til den».[187] Årsakskravet er vanligvis oppfylt «dersom skaden ikke ville ha skjedd om handlingen eller unnlatelsen tenkes borte».[188] Videre må skaden også være en påregnelig følge av styremedlemmets handling eller unnlatelse.[189]

Spørsmålet blir om et styremedlems brudd på plikten til forsvarlig forvaltning ved manglende etterlevelse av GDPR, kan oppfylle kravet til adekvat årsakssammenheng der selskapet ilegges et overtredelsesgebyr. Vilkåret kan være innfridd der for eksempel personvernrutiner som kunne forhindret et dataangrep ikke er vedtatt, og bruddet på kravet til forsvarlig forvaltning fører til et overtredelsesgebyr fordi personopplysninger kommer på avveie. Her hadde ikke selskapet blitt ilagt gebyret dersom de nødvendige rutinene var på plass. Unnlatelsen er følgelig en nødvendig betingelse for at selskapet ble påført et økonomisk tap. Når grunnen til at selskapet ilegges et overtredelsesgebyr er styremedlemmenes unnlatelse av å vedta personvernrutiner for virksomheten, er unnlatelsen også så vidt vesentlig i årsaksbildet at det er naturlig å knytte ansvar til den. Selskapet ville ikke fått et gebyr om unnlatelsen av å iverksette personvernrutiner tenkes borte. Videre må et slikt gebyr anses å være en påregnelig

[187] Rt. 1992 s. 64, på s. 69-70.
[188] Rt. 1992 s. 64, på s. 69-70.
[189] Aarum (1994) s. 74.

følge av de manglende rutinene i selskapet. GDPR har eksplisitte regler om ilegging av overtredelsesgebyr, jf. GDPR art. 83, og et styremedlem kan ikke vinne frem med å hevde at et overtredelsesgebyr er en fjern eller uventet følge av manglende personvernrutiner.

I praksis vil imidlertid et sentralt spørsmål være om personvernrutinene rent faktisk kunne forhindret dataangrepet. Dersom de ikke kunne det, og personopplysningene uansett ville kommet på avveie, vil ikke unnlatelsen være en nødvendig betingelse for overtredelsesgebyret. Svaret vil i realiteten bero på en bevisførsel av årsaken bak bruddet, og hva som kunne forhindret at det oppsto. Det ovenfor skisserte eksempelet viser uansett at det ikke er vanskelig å tenke seg tilfeller der kravet til adekvat årsakssammenheng vil være oppfylt.

Det kan riktignok også tenkes tilfeller der vilkåret om adekvat årsakssammenheng reiser større utfordringer, for eksempel der selskapet har fått et overtredelsesgebyr for å ha behandlet personopplysninger uten rettslig grunnlag. Selv om styret har unnlatt å iverksette nødvendige personvernrutiner, kan det aktuelle bruddet på GDPR her skyldes en feil hos en enkeltansatt som kanskje ville realisert seg uansett.

I det nevnte vedtaket mot Recover AS, hadde for eksempel en kredittvurdering blitt foretatt ved en feil av en enkeltansatt fordi klageren hadde omtrent samme navn som selskapets egentlige kunde.[190] Selskapet fikk et gebyr for å ha innhentet kredittvurdering uten rettslig grunnlag etter GDPR art. 6, men virksomheten manglet også rutiner for kredittvurderinger som var egnet til å sikre at de ble utført i samsvar med forordningen, jf. GDPR art. 24.[191] Vedtaket belyser ikke styrets opptreden, men i et styreansvarsperspektiv er et interessant spørsmål likevel om kredittvurderingen skyldes mangel på personvernrutiner eller en feil hos den enkeltansatte. I en tenkt styreansvarssak kunne det blitt reist tvil om det var adekvat årsakssammenheng mellom bruddet på forsvarlig forvaltning ved unnlatelsen av å iverksette personvernrutiner, og et overtredelsesgebyr for brudd på GDPR art. 6.

Det sentrale spørsmålet er om unnlatelsen rent faktisk var en nødvendig betingelse for overtredelsesgebyret. Dersom personvernrutiner kunne forhindret at kredittvurderingen ble foretatt uten rettslig grunnlag, så er unnlatelsen det. Argumentet vil være at den enkeltansatte ikke ville foretatt kredittvurderingen om selskapet hadde egnede personvernrutiner på plass. På den andre siden kan det hevdes at den enkeltansatte uansett ville foretatt kredittvurderingen

[190] Datatilsynet (2022). *Vedtak om pålegg og overtredelsesgebyr - Recover AS.* s. 1-2.
[191] Datatilsynet (2022). *Vedtak om pålegg og overtredelsesgebyr - Recover AS.* s. 5.

på grunn av navnelikheten. Et ytterligere argument er at fraværet av rutiner uansett ikke var så vidt vesentlig i årsaksbilde at det er naturlig å knytte ansvar til det. Om kravet til årsakssammenheng her er oppfylt avhenger derfor av en bevisførsel rundt årsaken til bruddet og hva som eventuelt kunne forhindret at kredittvurderingen ble foretatt. Dersom det kan påvises at den enkeltansatte ville gjennomført kredittvurderingen uansett, så vil det ikke være årssakssammenheng mellom styremedlemmets unnlatelse og overtredelsesgebyret. Situasjonen viser i alle tilfelle at det kan tenkes situasjoner der kravet til årsakssammenheng er mer problematisk.

Når man først har kommet til at et styremedlem har brutt kravet til forsvarlig forvaltning, vil det likevel ofte være adekvat årsakssammenheng mellom bruddet og selskapets overtredelsesgebyr. Det er unnlatelsesansvar som særlig kan være aktuelt i relasjon til etterlevelsen av GDPR, og da er situasjonen gjerne at styremedlemmene har unnlatt å forholde seg til regelverket eller konkret risikoinformasjon fra personvernombudet eller daglig leder, jf. kapittel 4.3.2.4. Dersom selskapet først får et overtredelsesgebyr på grunn av mangler på personvernrutiner/sikkerhetstiltak, vil det dermed i mange tilfeller være en klar sammenheng mellom unnlatelsen og overtredelsesgebyret, jf. drøftelsen ovenfor. Unnlatelsen av å iverksette personvernrutiner/sikkerhetstiltak er også noe som ofte kan føre til brudd på andre artikler i forordningen, som nettopp behandling av personopplysninger uten rettslig grunnlag.

Selv om vilkåret om adekvat årsakssammenheng kan reise vanskelige spørsmål, har redegjørelsen dermed vist at et styremedlems brudd på plikten til forsvarlig forvaltning kan oppfylle kravet til adekvat årsakssammenheng der selskapet ilegges et overtredelsesgebyr. Med adekvat årsakssammenheng er også alle vilkårene for å ilegge et styremedlem personlig erstatningsansvar etter asl. § 17-1 (1) innfridd.

5 Konklusjon og avsluttende betraktninger

Avhandlingen har vist at brudd på GDPR kan medføre personlig erstatningsansvar for et styremedlem etter asl. § 17-1 (1), ved å redegjøre for hvordan de materielle vilkårene etter bestemmelsen kan tenkes innfridd. Videre har avhandlingen belyst hva som mer konkret kreves av et styremedlem for å ivareta selskapets forpliktelser etter forordningen, jf. asl. §§ 6-12 og 6-13.

Et overtredelsesgebyr er et økonomisk tap for selskapet som oppfyller kravet om «skade». Styret har etter kravet til forsvarlig forvaltning en overordnet plikt til hindre at virksomheten operer i strid med loven. Ansvaret vil kunne innebære etablering og organisering, gjennomføring og kontrollering av rutiner og sikkerhetstiltak knyttet til internkontrollen. Om plikten ikke overholdes, eksempelvis ved unnlatelse av å vedta nødvendige personvernrutiner, vil det være en presumsjon for utvist uaktsomhet. Det er på grunn av presumsjonen lite rom for subjektive unnskyldningsgrunner, og kravet om ansvarsgrunnlag vil dermed som hovedregel være oppfylt. Dersom personvernrutiner i det skisserte eksempelet ovenfor kunne forhindret et dataangrep, og angrepet fører til et overtredelsesgebyr fordi personopplysninger komme på avveie, vil det også være adekvat årsakssammenheng mellom unnlatelsen og skaden.

Grunnen til at jeg fant temaet av interesse, var for å undersøke hvor realistisk det er at styreansvar for brudd på GDPR faktisk kommer til å aktualisere seg i praksis. Temaet var på dagordenen, særlig på grunn av den nevnte tyske dommen som fikk stor oppmerksomhet i Norge. Som avhandlingen har vist,[192] var sakens faktum imidlertid svært spesielt, og det er av den grunn vanskelig å se hvordan dommen påvirker rettstilstanden i Norge når styrets ansvar vurderes etter asl. § 17-1 (1). Når man ser bort fra den tyske dommen, som har lite overføringsverdi, står jeg derfor i igjen med spørsmålet: Er et erstatningskrav fra selskapet etter asl. § 17-1 (1) mot et styremedlem for brudd på GDPR noe vi *virkelig* kan forvente?

Det er flere omstendigheter som indikerer at det skal en del til for at et slikt erstatningskrav vil aktualisere seg. For det første kan det være krevende å få medhold i styreansvarssaker. Det er skadelidte som hovedregel har bevisbyrden,[193] og særlig vilkåret om ansvarsgrunnlag

[192] Se kapittel 2.2.1.
[193] Skoghøy (2022) s. 915.

beror på en helhetsvurdering av flere elementer som kan være sammensatte. Dette kan gjelde enda sterkere i relasjon til GDPR, som er et relativt nytt og komplisert regelverk, jf. kapittel 4. Prosessrisikoen er derfor stor, og saksomkostningene blir ofte høye. Det er med andre ord ressurskrevende å føre en styreansvarssak for retten.

På grunn av de nevnte omstendigheter, er det mer forsvarlig å akseptere prosessrisikoen der «skaden» er et overtredelsesgebyr av en viss størrelse. Grunnen er at tapet her kan være stort for selskapet, og vedtaket fra Datatilsynet vil konstatere brudd på GDPR som kan forenkle bevisførselen og argumentasjonen om ansvarsgrunnlaget, jf. redegjørelsen i kapittel 4.2.

Slik var situasjonen i vedtaket mot Ferde AS, der Datatilsynet eksplisitt uttalte at unnlatelsen av å gjennomføre risikovurderinger før en behandling «måtte klassifiseres som klart uaktsomt», og «at ansvaret ligger hos styret i Ferde AS, jf. aksjeloven § 6-12 første ledd første punktum».[194] Riktignok var det *kun* et overtredelsesgebyr på kroner 5. millioner, men om man virkelig skal forvente en styreansvarssak for brudd på GDPR, kan man tenke seg at det ville vært i en sak som det.

En viktig påpekning er imidlertid at generalforsamlingen faktisk må velge å rette erstatningskrav mot styremedlemmene, jf. asl. § 17-3. Rettspraksis viser at det er svært sjeldent at selskapet fremmer krav mot sitt eget styre.[195] Sakene det faktisk har skjedd virker å være forbeholdt de tilfellene hvor styremedlemmet har opptrådt illojalt ved å sette egne interesser foran selskapets.[196] Dette vil normalt ikke være tilfellet ved brudd på GDPR, og det skal nok derfor mye til for at generalforsamlingen velger å gå til sak mot sitt eget styret.

Et annet tenkelig alternativ er at krav mot et styremedlem reises av selskapets konkursbo, jf. kapittel 4.2. Ved konkurs er hensynet til skyldnerens fordringshavere det sentrale, og boets hovedoppgave er å skaffe dekning for kreditorene.[197] En bostyrer kan derfor ha et insentiv til å velge å fremme et erstatningskrav mot et styremedlem, for å tilføre boet midler. En forutsetning er nok imidlertid også her at det er tale om et overtredelsesgebyr av en størrelse som forsvarer prosessrisikoen, og at ansvarsgrunnlaget fremstår som rimelig klart, for eksempel gjennom vedtaket som fastsetter overtredelsesgebyret.

[194] Datatilsynet (2021). *Vedtak om overtredelsesgebyr – Ferde AS.* s. 12.
[195] Dahlum (2021) s. 21. Se grafen som viser at kun 7 % av underrettssaker om asl. § 17-1 er reist av selskapet.
[196] Dahlum (2021) s. 32.
[197] Andenæs (2009) s. 11.

Om styreansvar for brudd på GDPR er noe vi virkelig skal forvente, er det etter min mening mye som tyder på at det vil være forbeholdt et erstatningskrav fra et konkursbo etter et større overtredelsesgebyr, som følge av et grovt brudd på forordningen konstatert gjennom et vedtak.

6 Litteraturliste

Lover og forskrifter

1814	Lov 17. mai 1814 om Kongeriket Norges Grunnlov [Grunnloven]
1969	Lov 13. juni 1969 nr. 26 om skadeserstatning (skadeerstatningsloven)
1996	Forskrift 12. juni 1996 nr. 1127 om systematisk helse-, miljø- og sikkerhetsarbeid i virksomheter (Internkontrollforskriften)
1997	Lov 13. juni 1997 nr. 44 om aksjeselskaper (aksjeloven)
2000	[Opphevet] Lov 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven)
2008	Forskrift 22. september 2008 nr. 1080 om risikostyring og internkontroll
2018	Lov 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven)

Lovforarbeider

NOU 1996:3	Ny aksjelovgivning
NOU: 2022:11	Ditt personvern – vårt felles ansvar. Tid for en personvernpolitikk
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. 55 (2005-2006)	Om lov om endringer i aksjelovgivningen mv.

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

Rettspraksis

Rt. 1973 s. 821

Rt. 1979 s. 46

Rt. 1992 s. 64

Rt. 1993 s. 1399

Rt. 2008 s. 833

HR-2013-574-A

HR-2016-1440-A

HR-2017-2375-A

RG 1994 s. 145 (Eidsivating)

Offentlige dokumenter

Datatilsynets veiledere:

Datatilsynets veileder (2020) - *Digitale tjenester og forbrukeres personopplysninger* Datatilsynet. *Digitale tjenester og forbrukeres personopplysninger*, (2020). [Tilgjengelig på: https://www.datatilsynet.no/personvern-pa-ulike-

omrader/kundehandtering-handel-og-medlemskap/digitale-tjenester-og-forbrukeres-personopplysninger/?print=true] [Hentet 12.09.2022]

Datatilsynets veileder (2018) - *Etablere internkontroll*

Datatilsynet. *Etablere internkontroll*, (2018), [Tilgjengelig på: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/] [Hentet 12.09.2022]

Datatilsynets vedtak:

Datatilsynet (2021) - *Vedtak – Ferde AS.*

Datatilsynet. *Vedtak om overtredelsesgebyr – Ferde AS.* (2021), [Tilgjengelig på: https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/avgjorelser-fra-datatilsynet/2021/gebyr-til-ferde-as/] [Hentet 17.08.2022]

Datatilsynet (2022) - *Vedtak – Østre Toten kommune*

Datatilsynet. *Vedtak om overtredelsesgebyr og pålegg.* (2022), [Tilgjengelig på: https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2022/overtredelsesgebyr-til-ostre-toten-kommune/] [Hentet 26.08.2022]

Datatilsynet (2022) - *Vedtak – Recover AS.*

Datatilsynet. *Vedtak om pålegg og overtredelsesgebyr – Kredittvurdering uten rettslig grunnlag – Recover AS.* (2022), [Tilgjengelig på: https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/avgjorelser-fra-datatilsynet/2022/recover-as-far-overtredelsesgebyr/] [Hentet 15.11.2022]

Rapporter og pressemeldinger:

Regjeringen (2022)	Regjeringen. (2022). *Nasjonal Sikkerhetsmåned er i gang*, 03.10.2022, [https://www.regjeringen.no/no/aktuelt/nasjonal-sikkerhetsmaned-er-i-gang/id2930570/] [Hentet 07.11.2022]
Nasjonalt digitalt risikobilde (2022)	NSM. (2022). *Nasjonalt digitalt risikobilde 2022*, [Tilgjengelig på: https://nsm.no/aktuelt/digitalt-risikobilde-2022-cyberangrep-har-blitt-hverdagskost] [Hentet 07.11.2022]

Internasjonale kilder

Retningslinjer:

Guidelines on the application And setting of administrative fines (2017)	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: https://ec.europa.eu/newsroom/article29/items/611237/en] [Hentet 12.09.2022]
Guidelines on Data Protection Officers (2017)	Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers ("DPOs")*, (2017). [Tilgjengelig på: https://ec.europa.eu/newsroom/article29/items/612048] [Hentet 24.10.2022]

Personvernrådet (2018) EDPB, *Endorsement of GDPR WP29 guidelines by the EDPD*, 25.05.2018, [Tilgjengelig på: https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en] [Hentet 24.10.2022]

Traktater og konvensjoner:

EMK Convention for the Protection of Human Rights and Fundamental Freedoms, Roma, 4. november 1950 [Den europeiske menneskerettskonvensjonen, EMK]

EØS-avtalen Avtale om Det Europeiske Økonomiske samarbeidsområde [EØS-avtalen], Porto 2. mai 1992. I kraft 1. januar 1994.

TEUV Traktaten om Den europeiske unions virkemåte – TEUV – Roma–traktaten konsolidert 2016, OJ C 202 7.6.2016, s. 47.

Forordninger og direktiver:

Direktiv 95/46/EF Europaparlaments og Rådsdirektiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger [Personverndirektivet 1995].

GDPR Europaparlamentets og Rådets forordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning) [PVF, GDPR].

Internasjonal Rettspraksis:

Tyskland

OLG Dresden (2021) — OLG Dresden, 30.11.2021 - 4 U 1158/21. [Kun tilgjengelig på tysk: https://openjur.de/u/2381765.html] [Hentet 29.08.2022]

LG Dresden (2021) — LG Dresden, 26.05.2021 - 8 O 1286/19. [Kun tilgjengelig på tysk: https://openjur.de/u/2381632.html] [Hentet 29.08.2022]

EU-domstolen

Sak C-345/13 — Dom av 19. juni 2014, [C5] *Karen Millen Fashions Ltd v Dunnes Stores and Dunnes Stores (Limerick) Ltd*, Case C-345, EU:C:2014:2013.

Beslutninger:

EØS-komiteen (2018) — EØS-komiteens, beslutning nr. 154/2018 av 6. juli 2018, [Tilgjengelig på: https://www.efta.int/media/documents/legal-texts/eea/other-legal-documents/adopted-joint-committee-decisions/2018%20-%20Norwegian/154-2018n.pdf] [Hentet 08.12.2022].

Litteratur

Aarbakke (2022) — Aarbakke, Magnus, Asle Aarbakke, Gudmund Knudsen, Tone Ofstad og Jan Skåre. *Ajourført versjon av Aksjeloven, Kommentarutgave, 2022*. Oslo: Universitetsforlaget, Juridika.no (Hentet 05. september 2022).

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

Alteren (2021)	Alteren, Kristine. «Kommentar til aksjeloven» i *Norsk Lovkommentar, Gyldendal Rettsdata* 2021 [Hentet 22. oktober 2022].
Andenæs (2009)	Andenæs, Mads Henry, *Konkurs*, 3. utg., Oslo: M.H. Andenæs, 2009.
Andenæs (2016)	Andenæs, Mads Henry. *Aksjeselskaper og allmennaksjeselskaper*. 3. utg., ved Ole Andenæs, Stig Berge og Margrethe Buskerud Christoffersen, Oslo: M. H. Andenæs, 2016.
Blekastad/Hirst	Blekastad, Signhild og Marion Holthe Hirst, *Personvern og kontroll i arbeidslivet*, 1. utg., Oslo: Gyldendal, 2021.
Bråthen (2022)	Bråthen, Tore. *Selskapsrett*, 7. utg., Oslo: Fagbokforlaget, 2022.
Dahlum (2021)	Dahlum, Andrea. *Styreansvar i praksis*, 1. utg., Bergen: Fagbokforlaget, 2021.
Fredriksen/Mathisen (2022)	Fredriksen, Halvard Haukeland, og Gjermund Mathisen, *EØS-rett*, 4. utg., Bergen: Fagbokforlaget, 2022.
Gimmingsrud (2017)	Gimmingsrud, Kari. "En ny tidsalder for personvern i Europa", *Arbeidsrett* nr. 2 (2017) s. 220-240.
Jarbekk (2019)	Jarbekk, Eva, Kaare M. Risung, Jeppe Songe-Møller, Inge Kristian Brodersen, Anne-Marit Wang Sandvik, Anette Øvrehus, Øivind K. Foss, Hedda Emilie Bratt, Christopher Thue Jerving og Johanne Førd, *Personopplysningsloven og personvernforordningen (GDPR) med kommentarer*, Gyldendal 2019.
Jøsang (2021)	Jøsang, Audun, *Informasjons-sikkerhet – Teori og praksis*,

Oslo, Universitetsforlaget, 2021.

Kuner (2020) Kuner, Christopher, Lee A. Bygrave, Christopher Docksey og Laura Drechsler. *The EU General Data Protection Regulation (GDPR) – A Commentary*, 1. utg., 2020.

Lødrup (2009) Lødrup, Peter. *Lærebok i erstatningsrett*, 6. utg., Oslo, Gyldendal, 2009.

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

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.

Schartum (2020) Schartum, Dag Wiese. *Personvern-forordningen - En lærebok*, 1. utg., Fagbokforlaget, 2020.

Skoghøy (2022) Skoghøy, Jens Edvin A. *Tvisteløsning*. 4. utg., Oslo: Universitetsforlaget, 2022.

Skullerud (2022) Skullerud, Åste Marie Bergseng, Cecilie Rønnevik, Jørgen Skorstad og Marius Engh Pellerud, *Ajourført versjon av Personvernforordningen, Kommentarutgave*, 2022. Oslo: Universitetsforlaget, Juridika.no [Hentet 01. september 2022]

Trzaskowski/Sørensen (2022) Trzaskowski, Jan og Max Gersvang Sørensen, *GDPR Compliance: Understanding the General Data Protection Regulation*, 2. utg., København: Ex Tuto Publishing A/S, 2022.

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.

Wessel-Aas/Ødegaard (2018) — Wessel-Aas, Jon, og Magnus Ødegaard. *Personvern - Publisering og behandling av personopplysninger*, 1. utg., Oslo: Gyldendal, 2018.

Woxholth (2021) — Woxholth, Geir. *Selskapsrett*, 7. utg., Oslo: Gyldendal, 2021.

Nettsider

DN (2022) — Eva Jarbekk og Jeppe Songe-Møller, «Innlegg: Direktør dømt personlig ansvarlig for personvernbrudd», Dagens Næringsliv, 11. mars 2022 [debattinnlegg], https://www.dn.no/innlegg/jus/personvern/gdpr/innlegg-direktor-domt-personlig-ansvarlig-for-personvernbrudd/2-1-1181801 [Hentet 25. august. 2022].

Finansavisen (2022) — Kristin Haram Førde, «Alle styremedlemmer – skjerp dere.», Finansavisen, 29. mars 2022, https://www.finansavisen.no/nyheter/debattinnlegg/2022/03/29/7841435/alle-styremedlemmer-skjerp-dere [Hentet 25. august 2022].