AALBORG UNIVERSITY

Implementeringen av NIS2-direktivet og GDPR i norsk og dansk rett: Nasjonal sikkerhet vs. privatliv

Hvordan balanseres hensynene til nasjonal sikkerhet og personvern?

Speciale av Tirill Marie Tønseth Hedel
Kandidat ved Aalborg Universitet

Universitet: Aalborg universitet

Utdannelse: Kandidat Jura

Oppgave: Kandidatspeciale

Fagområde: Cybersikkerhet

Norsk tittel: Implementeringen av NIS2-direktivet og GDPR i norsk og dansk rett: Nasjonal sikkerhet vs. privatliv

Engelsk tittel: The Implementation of the NIS2 Directive and GDPR in Norwegian and Danish Law: National security vs. privacy

Forfatter: Tirill Marie Tønseth Hedel

Veileder: Fenella Billing

Avleveringsdato: 15. mai 2025

Antall anslag:

Abstract:

An ever-increasing digitalization of critical infrastructures has made the member states of the European Union to reinforce their legal foundations for cybersecurity and data protection through the Network and Information Security Directive (NIS2) and the General Data Protection Regulation (GDPR).

This thesis will investigate how Norway, an EEA country and Denmark, an EU member, have implemented these regulatory frameworks into national law and how each jurisdiction seeks to reconcile national security considerations with the right to privacy. By using academic literature, legislation, preparatory materials and relevant case law, the study combines legal-dogmatic method with comparative perspectives to map institutional responsibilities, compliance duties and enforcement practices in both countries.

The thesis shows that Norway relies on an expanded national security act which delegates the day-to-day oversight to sector authorities under the coordination of the National Security Authority. Denmark has enacted a law for the purpose of implementing NIS2. This law puts the Centre for Cybersecurity in charge of strategy while the line ministries conduct inspections. In both countries GDPR requirements are integrated through risk-based assessments and guidance from both cybersecurity and data protection authorities. However, some friction may appear.

Factors such as public trust, administrative capacity and politics may further affect the balance between the considerations of national security and also the right to privacy. Regulatory approaches can range from guidance to systems with clearly defined enforcement steps and sanctions. Across these regulatory approaches, tools like proportionality assessments, technical standards and coordination with relevant agencies are being used as flexible mechanisms instead of a static solution.

The thesis finds that ongoing cooperation, regular joint audits and shared rules on when security logging is legal are vital for ensuring that the cybersecurity is strong while also safeguarding basic rights such as privacy. By carefully comparing the experiences of Norway and Denmark, it offers practical and concrete thoughts on how the balance between resilient digital systems and respect of the individual privacy are today and how it potentially could be improved in future development and implementation of legislations.

Innholdsfortegnelse

1.0 Introduksjon

1.1 Formål

I en stadig mer digitalisert verden blir samfunnskritiske sektorer, som energisektoren, finanssektor og helsesektoren, mer avhengig av digitale systemer for å sikre stabil drift og en effektiv håndtering av samfunnskritiske enheter.[1] Parallelt med økt digitalisering vokser trusselbildet, og cyberangrep mot kritisk infrastruktur forekommer med økende hyppighet.[2] Alvorlige svikt i en slik sektor vil kunne få omfattende samfunnsmessige og nasjonale konsekvenser, noe som fremgår tydelig i årlige sikkerhetsrapporter og i offentlige utredninger.[3]

Tidligere angrep som Stuxnet-angrepet på Irans kjernekraftverk i 2010, angrepene på Ukrainas strømnett i 2015 og 2016, og Colonial Pipeline-angrepet i USA i 2021, illustrerer hvor store skadevirkninger cyberangrep på energisektoren kan få.[4] Disse hendelsene viser hvor viktig robuste regelverk som både sikrer kritisk infrastruktur mot digitale trusler og samtidig ivaretar grunnleggende rettigheter som personvern er.[5]

For å møte disse utfordringene har EU vedtatt Network and Information Security Directive 2 (NIS2-direktivet)[6], som skjerper kravene til cybersikkerhet i kritiske samfunnsfunksjoner. Samtidig stiller General Data Protection Regulation (GDPR)[7] opp omfattende regler for hvordan personopplysninger skal behandles på en lovlig, rettferdig og transparent måte.[8] Balansen mellom kravene til digital sikkerhet og hensynet til individets personvern kan dermed skape spenninger, særlig i sektorer hvor digitalisering og databehandling er omfattende.

1.2 Problemstilling

Denne oppgaven undersøker hvordan Norge og Danmark har implementert kravene fra NIS2-direktivet og GDPR innenfor sine nasjonale reguleringer for kritiske samfunnsfunksjoner. Særlig rettes det fokus mot hvordan de to landene forsøker å balansere hensynet til nasjonal sikkerhet mot beskyttelsen av personvern.

Problemstillingen for oppgaven er følgende: *Hvordan har Norge og Danmark implementert NIS2-direktivet og GDPR i kritiske samfunnsfunksjoner, og hvordan balanserer de nasjonal sikkerhet og personvern?*

---

[1] Maglaras, L.; Kantzavelou, I.; Ferrag, M.A. (2021) *Digital Transformation and Cybersecurity of Critical infrastructures*, s. 1
[2] Küfeoğlu, S., & Akgün, A. T. (2023). *Critical infrastructure and cyber resilience frameworks* s. 1
[3] NOU 2006:6 s. 29., Nasjonal sikkerhetsmyndighet. (2024). *Risiko 2024*., Center for Cybersikkerhed. (2024). *The cyber threat against Denmark 2024*., Justis- og beredskapsdepartementet. (2019). *National cyber security strategy for Norway.*
[4] Symantec Threat Hunter Team. *Attacks Against Critical Infrastructure: A Global Concern.*
[5] Küfeoğlu, S., & Akgün, A. T. (2023). *Critical infrastructure and cyber resilience frameworks* s. 17
[6] Directive (EU) 2022/2555 (NIS2-direktivet)
[7] Regulation (EU) 2016/679 (GDPR)
[8] Datatilsynet. *Personvernprinsippene*

For å nærmere besvare problemstillingen vil oppgaven først kartlegge hvordan NIS2 og GDPR er implementert i norsk og dansk rett. Deretter vil oppgaven analysere hvordan kravene til digital sikkerhet og hensynene til personvern håndteres og balanseres i Norge og Danmark. Avslutningsvis vil det gjennomføres en sammenligning av regulatoriske forskjeller og konsekvensene dette kan ha for samfunnskritiske samfunnsfunksjoner.

1.3 Metode og avgrensning

Oppgaven tar utgangspunkt i en rettsdogmatisk metode ved å analysere gjeldende rett slik det fremgår av lover, forarbeider, forskrifter, veiledere og eventuelle andre relevante rettskilder.[9] Ved å kartlegge rettsregelens innhold og anvendelse sikter oppgaven på å danne en forståelse av hvordan kravene til digital sikkerhet fremmes i NIS2-direktivet, samt hvordan disse balanseres med kravene som stilles av personvernregelverket. Oppgaven fokuserer på hvordan EU-reguleringer samt nasjonal lovgivning i Danmark og Norge regulerer cybersikkerhet innenfor kritiske samfunnsfunksjoner.

Det vil i tillegg benyttes komparativ metode for å sammenligne hvordan implementeringen er gjennomført i norsk og dansk rett. På denne måten kartlegger oppgaven om de to landene har utviklet ulike løsninger på relativt like utfordringer knyttet til å ivareta hensynene til både nasjonal sikkerhet og personvern.

Oppgaven avgrenses til å fokusere på kritiske samfunnsfunksjoner med eksempler fra enkelte sektorer. Blant annet belyses energisektoren fordi den er spesielt utsatt for cyberangrep og spiller en avgjørende rolle for samfunnssikkerheten. Samfunnskritiske enheter behandler på samme tid store mengder personopplysninger[10], noe gjør GDPR relevant.

1.3.1 Relevans av Norge og Danmark som casestudier

Bakgrunnen for at Norge og Danmark er interessante casestudier i denne sammenhengen er at begge landene er blant verdens mest digitaliserte samfunn, med en høy avhengighet av velfungerende digitale systemer.[11] Samtidig opererer landene med ulike rettslige rammeverk. Danmark, som EU-medlem, er direkte forpliktet til å implementere NIS2-direktivet og GDPR i tråd med EU-rettens krav. Norge, som EØS-medlem, er også forpliktet til å innføre store deler av EU-retten, men har noe større fleksibilitet i gjennomføringen.[12]

Danmark har lange tradisjoner for sterk offentlig styring og et nært samarbeid mellom myndigheter og næringsliv.[13] Innenfor energisektoren har eksempelvis Danmark utviklet en egen nasjonal strategi for cybersikkerhet, som ble lansert av Energistyrelsen.[14] En desentralisert modell i Norge legger grunnlag for

[9] Aqbal Amiri. (2013). *Kompendium i Retssystemet og juridisk metode*. s. 29
[10] Maglaras, L.; Kantzavelou, I.; Ferrag, M.A. (2021) *Digital Transformation and Cybersecurity of Critical infrastructures* s. 5
[11] Digitaliserings- og forvaltningsdepartementet, *Fremtidens digitale Norge*, s.10., Danmarks Statistik, *Digitalisering*
[12] Utenriksdepartementet. (2025) *Spørsmål og svar om EØS*
[13] Styrelsen for Forsyningssikkerhed. (2023) *Erhvervsliv og det offentlige skulder ved skulder*
[14] Energistyrelsen. (2025) *Lov om styrket bereskab i energisektoren er vedtaget*

et nært samarbeid mellom myndigheter og private aktører.[15] Dette fremgår også av Norges nasjonale strategi for digital sikkerhet fra 2019.[16]

Både Norge og Danmark har de senere årene erfart alvorlige cybertrusler mot kritisk infrastruktur. Det store cyberangrepet mot energisektoren i Danmark i 2023, som rammet flere selskaper og krevde omfattende frakobling av systemer, illustrerer sårbarheten i sektoren. Danmark ble utsatt for et omfattende cyberangrep som medførte at flere drivere av den danske energisektoren ble kompromittert i et koordinert angrep. Ved oppnådd tilgang til industrielle kontrollsystemer måtte flere av selskapene frakobles hovednettet. Dette angrepet omtales som det største cyberangrepet opplevd i Danmark. Angrepet var grunnlaget for at det ble fremhevet en rekke anbefalinger implementert i driften av kritisk infrastruktur i Danmark.[17] I Norge har Norges vassdrags- og energidirektorat arbeidet aktivt for å styrke sikkerheten i energisektoren, blant annet gjennom anbefalinger om økt sikkerhetsstyring.[18]

1.4 Rettskildebildet

For å kunne analysere hvordan NIS2-direktivet og GDPR er implementert i norsk og dansk rett er det nødvendig å ta utgangspunkt i rettskildebildet som danner grunnlaget for reguleringen av cybersikkerhet og personvern i EU og EØS.

NIS2-direktivet er en videreutvikling av NIS1-direktivet fra 2016 og har som formål å harmonisere og styrke cybersikkerheten i samfunnskritiske enheter.[19] GDPR har som formål å sikre vern av fysiske personers personopplysninger og stiller strenge krav til behandlingen av personopplysninger.[20] Begge regelverkene har et felles mål om å beskytte samfunnet mot digitale trusler, men er likevel i risiko for å komme i konflikt, særlig i sammenhenger hvor cybersikkerhetstiltak innebærer datainnsamling og overvåkning som utfordrer hensynet til personvern. Gjennom EØS-avtalen er Norge forpliktet til å innføre store deler av EU-retten i nasjonal rett.[21] Det foreligger likevel en stor fleksibilitet i hvordan reglene skal gjennomføres nasjonalt. Norge må i tillegg forholde seg til Grunnloven § 102[22] og EMK artikkel 8 som verner om retten til privatliv.[23]

Både norske og danske reguleringer er utformet med utgangspunkt i EU-retten. I norsk lovregulering er NIS2 implementert gjennom sikkerhetsloven, og GDPR gjennom personopplysningsloven. I Danmark implementeres NIS2 gjennom NIS2-loven som trer i kraft i juli 2025[24] og relevante sektorlover som «Lov om styrket beredskab i energisektoren»[25].

---

[15] Hansen, T. (2025, 24. februar). *Desentralisering*. I *Store norske leksikon*
[16] Justis- og beredskapsdepartementet. (2019, 30. januar). *Nasjonal strategi for digital sikkerhet* s. 6
[17] SektorCERT. (2023, november). *Angrebet mod dansk kritisk infrastruktur*
[18] Hagen mfl., *Regulering av IKT-sikkerhet*, s. 28-29
[19] Justis- og beredskapsdepartementet. (2021, 22. februar). *NIS2-direktivet*.
[20] Datatilsynet, *Om personopplysningsloven*
[21] Bekkedal, T, og Andenæs, M. (2024) "*EØS-avtalen og kontinentalsoklene."* s. 14-16
[22] LOV-1814-05-17. Norges Grunnlov § 102
[23] Den europeiske Menneskerettskonvensjon. Artikkel 8
[24] LFF 2025-02-06 nr 141. Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS2-loven)
[25] L 2025-03-06 nr 258. Lov om styrket beredskab i energisektoren

Siden cybersikkerhetstiltak ofte innebærer innsamling, lagring og analyse av data[26], kan det oppstå spenninger mellom kravene i NIS2 og GDPR. Ved å fokusere på disse to regelverkene, fremfor andre internasjonale reguleringer, får oppgaven en tydelig og avgrenset tilnærming til hvordan Norge og Danmark håndterer balansen mellom nasjonal sikkerhet og personvern i kritiske samfunnsfunksjoner.

1.5 Definisjoner

For å sikre en presis fremstilling er det nødvendig å avklare noen sentrale begreper som anvendes i oppgaven. Kritiske samfunnsfunksjoner er i EUs direktiv om kritiske samfunnsfunksjoner definert som "anlegg, systemer eller deler av slike som befinner seg i medlemsstatene og er avgjørende for å opprettholde viktige samfunnsfunksjoner og menneskers helse, sikkerhet og økonomiske eller sosiale velferd, og der driftsforstyrrelse eller ødeleggelse ville få betydelige følger for en medlemsstat ved at disse funksjonene ikke kan opprettholdes".[27]

En cybertrussel eller cyberangrep betegnes som mulige omstendigheter, hendelser eller handlinger som kan skade, forstyrre eller på annen måte negativt påvirke nettverks- og informasjonssystemer.[28] Cybersikkerhet er tiltak og strategier som blir iverksatt for å beskytte digitale systemer mot cyberangrep. I NIS2-direktivets artikkel 2 (1) defineres cybersikkerhet som aktivitet som er nødvendig for å beskytte nettverks- og informasjonssystemer, brukere av slike systemer og andre personer som kan bli påvirket.

1.6 Struktur for oppgaven

Oppgaven vil først presentere de rettslige rammene for digital sikkerhet og personvern slik de fremgår av NIS2-direktivet og GDPR. Deretter vil oppgaven ta for seg implementeringen i norsk og dansk rett, og om det foreligger noen ulikheter. Analysen vil så fokusere på hvordan Norge og Danmark håndterer spenningsforholdet mellom nasjonal sikkerhet og personvern, og hvordan kravene til digital sikkerhet balanseres opp mot kravene til lovlig behandling av personopplysninger. Avslutningsvis vil en sammenlignende vurdering oppsummere forskjellene mellom landene, og om det er oppnådd en balanse mellom hensynene til nasjonal sikkerhet og personvern.

På bakgrunn av denne introduksjonen vil neste kapittel gå nærmere inn på den metodiske tilnærmingen som danner rammen for analysen om hvordan Norge og Danmark balanserer kravene til nasjonal sikkerhet og personvern.

2.0 Metode

2.1 Innledning

Dette kapittelet redegjør for den metodiske tilnærmingen som benyttes i analysen av hvordan nasjonal sikkerhet og personvern balanseres ved implementeringen av NIS2-direktivet og GDPR i norsk og dansk rett. Hovedmetodene som anvendes er rettsdogmatisk metode og komparativ metode. Den rettsdogmatiske

[26] CFCS. *Logging – part of resilient cyber defence*
[27] Directive (EU) 2022/2557. *Direktiv om kritiske samfunnsfunksjoner*. Artikkel 6
[28] Regulation (EU) 2019/881. *Cybersikkerhetsakten*. Artikkel 2 nr. 8

metoden danner grunnlaget for å kartlegge gjeldende rett. Den komparative metoden benyttes for å systematisere og sammenligne likheter og ulikheter ved implementeringen i nasjonal rett.

2.2 Rettsdogmatisk metode

Den rettsdogmatiske metoden har som formål å analysere, systematisere og beskrive gjeldende rett på et område.[29] I denne oppgaven brukes metoden for å kartlegge rettstilstanden knyttet til digital sikkerhet og personvern i europeisk rett, og hvordan dette er implementert i norsk og dansk rett.

Utgangspunktet til rettsdogmatisk metode er å gjennomføre en analyse av rettskilder som lovtekster, forarbeider, rettspraksis og juridisk litteratur. Gjeldende rett vil på den måten defineres av en systematisk, metodisk og transparent virksomhet hvor fokuset foreligger på systematikken av rettsreglene og en beskrivelse av rettstilstanden.[30] Metoden anses som den som "ligger nærmest rettsanvendelsen" fordi den har i oppgave å "ta standpunkt til rettsspørsmål".[31]

Ved beskrivelsen av gjeldende rett i Norge vil analysen ta utgangspunkt i sikkerhetsloven[32] [33] og personopplysningsloven.[34] I Danmark vil fokuset være på NIS2-loven[35], Lov om behandling av personopplysninger (Databeskyttelsesloven)[36] og sektorlover som Lov om styrket beredskab i energisektoren[37]. I tillegg vil rettskilder som viser hvordan EU-retten er gjort gjeldende i norsk og dansk rett bli undersøkt, med særlig vekt på kravene som følger av NIS2-direktivet og GDPR.

Rettsregler kan deles inn i tre kategorier: kompetanseregler, pliktregler og kvalifikasjonsregler. Kompetanseregler er regler som angir betingelser som må være til stede for at det skal foreligge kompetanse. Pliktregler er regler som pålegger eller fritar noen for plikter, og kvalifikasjonsregler er regler som angir hva som skal regnes med i en kategori.[38]

For å sikre en tolkning av lovbestemmelsene som skaper en unison forståelse underbygges forståelsen av lovteksten av forarbeider og rettspraksis. [39] Med forarbeider menes forslag, utredninger, debatter og høringer som fremkommer fra de som har deltatt i lovens forberedelse og vedtakelse.[40] Forarbeidene gjør rede for bakgrunn for utviklingen av bestemmelsen, og for hvordan lovteksten skal tolkes. Å forstå lovteksten ut ifra forarbeidene er omtalt som å være "lojal mot lovgiverviljen"[41] og er en tradisjon i

[29] Munk-Hansen, C. (2022), Retsvidenskabsteori s. 211.
[30] Munk-Hansen, C. (2022), Retsvidenskabsteori s. 211.
[31] Graver, H. P. (2008), *Vanlig juridisk metode? Om rettsdogmatikken som juridisk sjanger* s. 149 og 157
[32] LOV-2018-06-01-24. Lov om nasjonal sikkerhet (Sikkerhetsloven)
[33] Ny digitalsikkerhetslov vil ikke omtales i denne oppgaven da den tar utgangspunkt i NIS1, og har enda ikke tredd i kraft. Det vil likevel bli henvist til forarbeider til denne loven da disse er anvendelig for norsk tolkning av NIS2.
[34] LOV-2018-06-15-38 Lov om behandling av personopplysninger (personopplysningsloven)
[35] LFF 2025-02-06 nr 141 Forslag til lov om om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven)
[36] LBKG 2024-03-08 nr 289 Databeskyttelsesloven
[37] L 2025-03-06 nr 258 Styrket beredskab i energisektoren
[38] Eckhoff, T. (2001), Rettskildelære s. 45
[39] Tvarnø, C. D. og Nielsen, R. (2021), Retskilder og Retsteorier. s. 55
[40] Eckhoff, T. (2001), Rettskildelære s. 65
[41] Juridika. (2022), *Forarbeiderne – de som utreder lovgiverviljen*

nordiske land, herunder Norge og Danmark.[42] Bruken av lovforarbeider kjennetegnes av troen på en kollektiv fornuft.[43]

Lovtolkningen kan også tolkes av rettspraksis. Etter hvert som samfunnsforhold og oppfatninger endres, eldes også lovtekster og forarbeider.[44] Det er derfor viktig å undersøke hvordan bestemmelsene blir praktisert slik at det kan dannes presedenser for hvordan de skal tolkes. Hvor mye man kan forstå ved å lese dommer beror på hvordan dommerne har ordlagt seg, og dette kan variere fra land til land. I Norge er domsgrunnene gjerne lengre og opplysende, og i Danmark er domsgrunnene mer knappe og mindre opplysende. Eksempelvis gis det individuelle begrunnelser i Norge, men i Danmark er begrunnelsene felles.[45]

Et sentralt hensyn med analysen er at lovgivningen skal tolkes i lys av sin kontekst og utvikling. Gjennom rettspraksis, særlig fra EU-domstolen, fremgår det klare prinsipper om EU-rettens forrang og tolkningsforpliktelse. EU-retten har forrang hvor det oppstår konflikt mellom et aspekt i EU-retten og et aspekt i lovgivningen i en medlemsstat. I Costa v ENEL[46] ble prinsippet om EU-rettens forrang videreført av Domstolen. Ved å overføre visse fullmakter til EU begrenses statenes suverenitet, og for at EU sine rettsakter skal gjøres gjeldende, må de ha forrang over nasjonale lover, inkludert grunnlover.[47]

Rettsdogmatisk metode benyttes da den er særlig egnet for å gi en systematisk fremstilling av gjeldende rett og gjør det mulig å gjennomføre en sammenligning av de to forskjellige rettssystemene.

2.3 Komparativ metode

For å analysere likheter og ulikheter ved implementeringen av NIS2-direktivet og GDPR i Norge og Danmark, vil komparativ metode bli benyttet. Den komparative metoden søker å utvikle en systematisk sammenligning av flere rettssystemer for å identifisere hvordan lignende utfordringer håndteres. [48]

Å sammenligne ulike rettssystemer kan være verdifullt av flere grunner. En grunn er ønsket om kunnskap og forståelse. Komparativ rett har en tilhørende betydning innenfor juridisk forskning og utdanning.[49] Det er av verdifullt å ha kunnskap om andre staters lovverk hvor slike lover er relevant for nasjonale lovverk.[50] Komparativ rett skaper også en forståelse av hvordan regler fungerer i praksis, ved å sammenligne både likheter og ulikheter. En annen grunn til å ville gjøre en komparativ analyse er at inspirasjon fra eller sammenligning med andre land kan tydeliggjøre for lovgiver hvordan gitte lover kan være velfungerende

[42] Tvarnø, C. D. og Nielsen, R. (2021), Retskilder og Retsteorier. s. 261
[43] Bergo, K., (2002), *Høyesteretts forarbeidsbruk*, s. 17
[44] Boe, E. M. (2010) *Innføring i juss* s. 299-319
[45] Eckhoff, T. (2001), Rettskildelære s. 157.
[46] C-6/64 1964 – Costa v ENEL
[47] EUR-Lex, Primacy of EU law
[48] Gisle, J. Komparativ rett i Store norske leksikon
[49] Siems, M. (2022), Comparative Law. s. 3
[50] Siems, M. (2022), Comparative Law. s. 3

på et bestemt område.[51] På internasjonalt nivå kan det dreie seg om å utvikle overnasjonale reguleringer som baserer seg på flere staters nasjonale lover.[52]

En sammenligning av Norge og Danmark gir et spennende utgangspunkt. Begge landene har rettslige bindinger til EU og opererer innenfor en felles europeisk rettsramme selv om de har ulike regulatoriske tradisjoner.[53] Ved en komparativ analyse sikter oppgaven på identifisere hvorvidt ulik implementering har gitt forskjellige praktiske konsekvenser for kritiske samfunnsfunksjoner og hvorvidt balansen med nasjonal sikkerhet og personvern ivaretas. Metoden gir en mulighet for å identifisere hvorvidt Norge og Danmark har valgt ulike løsninger for å balansere nasjonal sikkerhet og personvern, og hvilken virkning dette kan ha for samfunnet.

For å sikre en systematisk komparativ analyse vil følgende spørsmål benyttes som grunnlag for sammenligning:

- Hvor skiller implementeringen seg mellom Norge og Danmark?
- I hvilken grad prioriteres nasjonal sikkerhet i forhold til personvern?
- Hvordan har myndighetene i hvert land valgt å organisere tilsyn og regulering?
- Hvilke praktiske konsekvenser kan komme av ubalanse mellom nasjonal sikkerhet og personvern?

En kombinasjon av rettsdogmatisk metode og komparativ metode sikrer et godt utgangspunkt for å identifisere hvordan NIS2 og GDPR balanseres i norsk og dansk rett. Den rettsdogmatiske analysen etablerer en oversikt over gjeldende rett og den komparative analysen klargjør likheter, ulikheter og mulige utfordringer. Dette gir videre grunnlag for en diskusjon om hvorvidt balansen mellom cybersikkerhet og personvern opprettholdes i praksis, eller om en av hensynene gis en større vekt.

3.0 Rettslig ramme

3.1 Introduksjon til NIS2 og GDPR

NIS2-direktivet og GDPR er to sentrale reguleringer i EU-retten som påvirker hvordan cybersikkerhet og personvern håndteres i offentlig og privat sektor. Reguleringene har ulike hovedformål, men de overlapper likevel hverandre på flere områder når det gjelder krav til sikkerhetstiltak og databeskyttelse. For å forstå hvordan hensynet mellom nasjonal sikkerhet og personvern balanseres, er det viktig å etablere en grunnleggende forståelse av reguleringenes formål, innhold, og forholdet mellom dem.

3.1.1 NIS2

NIS2-direktivet fremhever medlemsstatenes ambisjon om cybersikkerhet på et bredere område med klare regler og gode tilsynsverktøy.[54] Direktivet stiller krav til at medlemsstatene forbedrer deres cybersikkerhet

[51] Siems, M. (2022), Comparative Law. s. 5
[52] Siems, M. (2022), Comparative Law. s 5
[53] AVT-1992-05-02-1 (EØS-avtalen) og Traktaten om Den europeiske unions (TEU)
[54] NIS2-direktivets fortalepunkt 1

ved å introdusere tiltak for risikohåndtering og rapportering, og regler for samarbeid, informasjonsdeling, tilsyn og håndheving av cybersikkerhetstiltak.[55] Det følger av direktivet at hver medlemsstat plikter å utvikle en nasjonal cybersikkerhetsstrategi som inkluderer retningslinjer for cybersikkerhet.[56]

NIS2 har i forhold til NIS1 et større omfang, strengere krav og sterkere håndheving. NIS1-direktivet var den første EU-legislasjonen som siktet på å fremheve cybersikkerhet for nettverks- og informasjonssikkerhet for å beskytte kritiske samfunnsfunksjoner.[57] Hvor NIS1 var gjeldende for "operatører av essensielle tjenester" i kritiske samfunnsfunksjoner som energi, transport, helse og finans, har NIS2 utvidet listen til flere sektorer, blant annet post, avløp og offentlig administrasjon. NIS2 fremlegger en inndeling hvor sektorene er listet opp som "essensielle" eller "viktige" enheter, basert på størrelse og kritikalitet.[58]

3.1.2 GDPR

GDPR beskytter personer i sammenheng med behandling og fri bevegelse av personlig data.[59]. Forordningen erstattet personverndirektivet av 1995, men viderefører direktivets systematikk, terminologi og grunnprinsipper.[60] Den mest sentrale forskjellen mellom GDPR og Personverndirektivet er deres juridiske bindende kraft. En forordning er en bindende rettsakt for alle EUs medlemsland. Et direktiv er derimot en rettsakt som fastsetter mål som medlemslandene skal oppnå, hvor det imidlertid er medlemslandet selv som skal velge form og utforming av innhold i nasjonale rettsakter.[61]

GDPR har blitt inkorporert i EØS-avtalen og gjelder dermed for hele EU og EØS. Forordningen består av to deler; en fortale hvor det følger hjelp til tolkning av artiklene som fremgår i del to. Det er uttrykt i EØS-loven at forordningen skal gå foran norsk lov ved konflikt.[62] Det følger av reguleringens formålsbestemmelse at forordningens mål er å sikre vern av fysiske personer grunnleggende rettigheter og friheter, særlig deres rett til vern av personopplysninger.[63] Alle som behandler personopplysninger må opptre i samsvar med grunnprinsippene som skal sikre forutsigbarhet og forholdsmessighet.[64]

3.2 Sikkerhetstiltak vs. dataminimering

Balansen mellom sikkerhetstiltak og dataminimering er en av de største utfordringene innenfor cybersikkerhet og personvern i kritiske samfunnsfunksjoner. På en side stiller NIS2 krav om at virksomheter skal implementere sikkerhetstiltak som kan innebære logging, overvåkning og lagring av data for å oppdage og håndtere sikkerhetstrusler.[65] På en annen side fremheves prinsippet om

[55] European Commission. *NIS2 Directive: New rules on cybersecurity of network and informationssystems*
[56] NIS2-direktivets fortalepunkt 30
[57] European Commission. *NIS2 Directive: New rules on cybersecurity of network and informationssystems*
[58] NIS2-direktivets fortalepunkt 89
[59] European Commission, *Legal framework of EU data protection*
[60] Prop. 56 LS (2017-2018) s. 9
[61] Lovdata Europalov. *Om EU-rettsaktene*
[62] LOV-1992-11-27-109. EØS-loven § 2
[63] GDPR artikkel 1 (2)
[64] Datatilsynet. Grunnprinsippene., GDPR artikkel 5
[65] NIS2-direktivet artikkel 21

dataminimering i GDPR, som krever at virksomheter kun skal behandle personopplysninger som er strengt nødvendig for å oppnå et formål.[66] En foreliggende konflikt er spørsmålet om hvor mye data virksomheter kan samle inn og lagre for å ivareta sikkerheten uten å stride mot grunnprinsippet om dataminimering.

3.2.1 NIS2 artikkel 21

Kritiske samfunnsfunksjoner er pålagt å innføre "passende" og "proporsjonale" tekniske, operative og organisatoriske tiltak for å håndtere risiko knyttet til sikkerheten i nettverks- og informasjonssystemer som benyttes i essensielle og viktige enheter.[67] Slike tiltak har som hensikt å forebygge og minimere virkningen av hendelser, gjenopprette systemets funksjon etter angrep og ivareta kontinuitet i kritiske tjenester. [68]

Tiltakene omfatte risikoanalyse og sikkerhetspolicyer, håndtering av hendelser, forretningskontinuitet og krisehåndtering, forsyningskjedesikkerhet, tiltak ved anskaffelse, utvikling og vedlikehold av systemer og bruk av krypteringer, tilgangskontroll og opplæring.[69]

Bestemmelsens ordlyd bruker skjønnsmessige uttrykk som "appropriate" og "proportional".[70] En alminnelig forståelse av uttrykkene åpner for en konkret vurdering av tilfellet, sektoren, risiko og virksomhetstype. Det åpnes på den måten for en vurdering av forholdsmessighet og skjønnsavhengig tolkning. Vurderingen må altså gjøres i samsvar med den aktuelle sammenhengen. Et tiltak som er "passende" bør være egnet til å redusere eller håndtere en risiko. Vurderingen om hva som utgjør et "passende" tiltak må bero på en konkret og praktisk vurdering. Denne tolkningsmåten har indirekte støtte i EU-domstolens praksis. EU-domstolen vurderte gyldigheten av overføring av personopplysninger til tredjeland og la til grunn at vurderingen av hva som kan regnes som "appropriate" må bygge på faktiske forhold og rettslige rammer i det aktuelle miljøet.[71]

Videre fremgår det av bestemmelsen at tiltakene skal være "proporsjonale". Uttrykket bygger på en avveining mellom mål og konsekvens. Det kan tolkes av ordlyden at tiltaket må stå i rimelig forhold til både risikoens alvor og virksomhetenes størrelse. Eksempelvis kan det forventes at tiltak som innføres i store nasjonale energiselskaper er mer omfattende enn tiltak som innføres av mindre bedrifter. I henhold til proporsjonalitetsprinsippet skal innhold i tiltak ikke gå lengre enn hva som er nødvendig for å oppnå målene i traktatene i EU.[72] Det betyr at selv om det av sikkerhetsmessige grunner er ønskelig med mest mulig omfattende tiltak, må de tilpasses til formålet og nødvendigheten.

Bestemmelsen lister opp tre typer tiltak; "technical", "operational" og "organisational". Ordlyden uttrykker at tiltakene kan være av ulike arter, og at det kreves en helhetlig tilnærming. Forståelsen av

[66] GDPR artikkel 5 (1) bokstav c
[67] NIS2-direktivet artikkel 21 nr. 1
[68] NIS2-direktivet artikkel 21 (2)
[69] NIS2-direktivet artikkel 21 (2) bokstav a-j
[70] Appropriate oversettes til «passende» på norsk. Proportional oversettes til «proporsjonal på norsk». Norske begrep vil benyttes videre.
[71] C-311/18. Schrems II
[72] TEU artikkel 5 (4)

ordlyden i bestemmelsen er teknologinøytral og peker på hva som skal oppnås, men ikke hvordan dette skal oppnås. Formuleringen gir på den måten rom for at tiltakene skal kunne utvikles over tid, i samsvar med trusselbildet og den bestemte sektorens behov.

NIS2 er et direktiv, og gir dermed medlemsstatene noe handlingsrom.[73] I tillegg fremgår det en fleksibilitet ved bruk av uttrykk som "appropriate" og "proportional" som åpner for tilpasning av tiltakene slik at de passer inn i det aktuelle landet. Det følger av rapport om "Impact Assessment" utarbeidet av EU-kommisjonen at det har eksistert store forskjeller mellom medlemslandenes håndtering av cybersikkerheten.[74] Rapporten påpeker et behov for å redusere denne forskjellen for å sikre en effektiv og mer enhetlig håndtering. Artikkel 21 innfører ikke fullstendig harmonisering, men en minimumsstandard som åpner for reguleringer, så fremt EU-kravene opprettholdes. Eksempelvis kan et tiltak være å adoptere en "nulltillitsstrategi" hvor ingen enheter automatisk får tillit.[75] En slik strategi er basert på konseptet å ikke stole på noen enheter, og å alltid verifisere. På slik måte får ingen enheter tillit selv om de er tilkoblet nettverket.[76] Identiteten til brukeren må alltid bekreftes, og man mottar kun en gitt tilgang for en viss periode.[77]

Oppsummert representerer artikkel 21 en kjernebestemmelse som pålegger en bred plikt til risikostyring. Bestemmelsen er av bindende karakter, men åpner likevel for skjønn og tilpasning. Artikkelen fremstår som en funksjonell norm, hvor tolkning og anvendelse må skje i lys av formål og risikobilde.

3.2.2 GDPR artikkel 5 (1) bokstav c

Artikkel 5 i GDPR fastsetter de grunnleggende prinsippene for behandling av personopplysninger. Prinsippene er føringer som er aktuelle uansett behandlingsgrunnlag og setter normative føringer for hele regelverket. Personopplysninger skal være «adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for".[78] Bestemmelsen legger grunnlag for et dataminimeringsprinsipp, hvor det fremgår en tydelig føring for en formålsbegrensning og proporsjonalitetsvurdering.

Det følger av Den europeiske menneskerettighetsdomstolen at det skal tas hensyn til de konkrete omstendighetene, herunder arten, omfanget og varigheten av behandlingen og bakgrunnen for å iverksette tiltakene. Saken handler om masseovervåkning og om britiske overvåkningsordninger som krenket rettighetene til privatliv, i henhold til EMK artikkel 8.[79] Bestemmelsen inneholder tre kumulative vilkår for behandling av personopplysninger. Kumulative vilkår er vilkår som alle må være oppfylt for at bestemmelsen skal få sin anvendelse.[80]

---

[73] Lovdata Europalov. *Om EU-rettsaktene*
[74] European Commission. (2020) *Impact Assessment*
[75] Berrefjord, V. R. og Lund. M. S. (2024) Cybermakt s. 302
[76] Berrefjord, V. R. og Lund. M. S. (2024) Cybermakt s. 302
[77] Küfeoğlu, S., & Akgün, A. T. (2023). *Critical infrastructure and cyber resilience frameworks* s. 19
[78] GDPR artikkel 5 (1) bokstav C
[79] CASE OF BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM
[80] Boe, E. M. (2010) *Innføring i juss* s. 40

Det første vilkåret er at personopplysningene skal være adekvate. En alminnelig ordlydstolkning av uttrykket "adekvat" er at noe må være egnet for å oppnå et formål. Det følger av fortalen til GDPR at personopplysninger som er "adekvat" kan forstås som at de er relevante og at de er begrenset til det som er nødvendig for formålene de behandles for.[81]

Neste vilkår er at personopplysningene må være relevante. At de skal være relevante må forstås som at de må ha en saklig tilknytning til det formålet behandlingen gjelder. Det må derfor gjøres en vurdering av om opplysningen har en faktisk rolle i gjennomføringen av behandlingsformålet.

Det siste vilkåret er at personopplysningene må begrenses til det som er nødvendig. En forståelse av ordlyden tilsier et krav om at opplysningene ikke bare kan anses som nyttige eller ønskelige, men at de må være nødvendige for formålet. I en slik ordlydsforståelse foreligger en proporsjonalitetsvurdering hvor opplysningene sitt innhold må stå i forhold til formålet av behandlingen.

Dataminimeringsprinsippet i henhold til GDPR artikkel 5 (1) bokstav c må vurderes i rettslig sammenheng med andre bestemmelser som følger av GDPR. Det følger blant annet av artikkel 6 (1) et krav om rettslig grunnlag for at data skal behandles. Det foreligger også en formålsbegrensning i artikkel 5 (1) bokstav b, som uttrykker at innsamling av data skal gjennomføres i tråd med spesifikke, uttrykkelig angitte og berettigede formål.

I forordningens fortale fremgår det at dataminimering er av særlig nødvendighet og at behandling av personopplysninger skal skje på en lovlig, rettferdig og åpen måte. Det presiseres at innsamling kun skal skje i sammenheng med spesifikke og legitime formål og at de skal lagres i minst mulig tid. [82]

3.3 Rapportering av hendelser vs. personvernbeskyttelse

Et sentralt spørsmål i balansespørsmålet mellom cybersikkerhet og personvern er hvordan virksomheter skal etterleve sin plikt til å rapportere sikkerhetshendelser, uten å samtidig la det gå på bekostning av rettighetene som personvernsforordningen skal verne. I denne sammenhengen gjør NIS2 artikkel 23 og GDPR artikkel 33 seg særlig gjeldende. Begge artiklene pålegger virksomheter en plikt til å varsle relevante myndigheter ved sikkerhetshendelser, og selv om formålet i begge regelverkene er sammenlignbare, reises likevel flere praktiske utfordringer.[83]

Ved rapportering og varsling av hendelser må det vurderes hvorvidt opplysningene som inngår i varselet inneholder personopplysninger. I et slikt tilfelle må det vurderes hvorvidt kravene til dataminimering i GDPR artikkel 5 påvirker varselets innhold, og det kan oppstå en mulig interessekonflikt mellom behovet for rask og presis rapportering av cybersikkerhetshendelser, og forpliktelsen til å beskytte rettigheter i henhold til personvernlovgivningen.[84]

---

[81] GDPR fortalepunkt 39
[82] GDPR fortalepunkt 39
[83] Schmitz-Berndt, S. (2023) *Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive*, s. 9
[84] Koops, B.J. (2014). *The trouble with European data protection law*. *International Data Privacy Law*, s. 257

3.3.1 NIS2 artikkel 23

NIS2 artikkel 23 omhandler rapportering av hendelser og risikostyring. Bestemmelsen regulerer plikten for essensielle og viktige enheter til å varsle om hendelser som har en betydelig innvirkning på tjenesten. Det presenteres et materielt krav i bestemmelsen om at virksomheter tar ansvar for å dele informasjon med myndigheter ved sikkerhetshendelser.[85] Informasjonsdeling er et sentralt mål og ledd for å oppnå bedre beredskap i EU og EØS.[86]

En alminnelig forståelse av bestemmelsens ordlyd er at det skal varsles om sikkerhetshendelser til kompetent myndighet uten ugrunnet opphold. Uttrykket "incident having a significant impact" i lys av at "incident" defineres som enhver hendelse som kompromitterer "the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems".[87] Dette kan tolkes slik at det må foreligge et sikkerhetsbrudd som kan skape reduksjon eller fullstendig svikt i funksjonalitet, og som forstyrrer de fire pilarene som er tilgjengelighet, autentisitet, integritet og konfidensialitet.[88]

Det avgjørende for rapporteringen kan tolkes å være at hendelsen har en "significant impact". Uttrykket er ikke eksplisitt definert i direktivet, men kan tolkes analogisk med artikkel 6 nr. 11. Bestemmelsen uttaler at en "significant cyber threat" tolkes som en trussel, basert på sine tekniske kjennetegn, som med rimelighet kan antas å ha potensiale til å ha en alvorlig innvirkning på en enhets nettverks- og informasjonssystemer eller på brukerne av enhetens tjenester ved å forårsake betydelig skade.[89]

Varslingsprosessen skjer i tre trinn. Varsling skal skje innen 24 timer, en hendelsesrapport skal være tilgjengelig innen 72 timer og at endelig rapport som inkluderer en detaljert beskrivelse av hendelsen, dens alvorlighetsgrad og anslag, hvilken type trussel eller grunn for at hendelsen ble utløst og avbøtende tiltak, skal utarbeides senest innen en måned etter hendelsesrapporten er levert.[90]

Det fremgår tydelig av ordlyden at varslingen ikke er betinget av at det har skjedd en hendelse, men heller risikoen for en hendelse som vil ha en betydelig kompromitterende effekt. Rettslig sett er artikkel 23 en materiell regel som stiller krav til det innholdet i plikten, herunder at virksomheten må vurdere hvilke hendelser som potensielt kan ha en "significant impact".[91] Virksomheten må også vurdere alvorlighetsgrad og hvor kritisk deres tjeneste skal vurderes som.[92] Det stilles også prosessuelle krav[93] i bestemmelsen, blant annet om fremgangsmåte og tidsfrister.

---

[85] Boe, E. M. (2010) *Innføring i juss* s. 53
[86] NIS2-direktivets fortalepunkt 3 og 65
[87] NIS2 -direktivet artikkel 6 nr. 6
[88] NIS2-direktivet artikkel 6 nr. 6.
[89] NIS2-direktivet artikkel 6 nr. 11
[90] NIS2-direktivet artikkel 23 nr. 4 bokstav a, b og d
[91] Boe, E. M. (2010) *Innføring i juss* s. 53
[92] NIS2-direktivets fortalepunkt 101
[93] Boe, E. M. (2010) *Innføring i juss* s. 53

3.3.2 GDPR artikkel 33

Det fremgår av GDPR artikkel 33 at behandlingsansvarlig uten ugrunnet opphold og når det er mulig, senest 72 timer etter å ha fått kjennskap til brudd på personopplysningssikkerheten, skal melde bruddet til tilsynsmyndighetene.[94] Bestemmelsen finner sin plass i kapittel IV om behandlingsansvarliges og databehandleres forpliktelser, og utgjør en sentral del av reguleringens retningslinjer for håndtering av brudd på sikkerhet. Artikkel 33 retter seg alene mot kommunikasjon med myndighetene, og har et overordnet formål om å sikre en effektiv myndighetskontroll.

Det følger videre av bestemmelsen at det ved forsinkelse skal oppgis årsak for forsinkelsen.[95] Plikten kan dermed tolkes å være både tidsbundet og ubetinget ved at forsinkelse aktivt må begrunnes og at unnlatelse av varsling i tide anses som et brudd på forordningen. Det følger videre av bestemmelsen at den får anvendelse ved "brudd på personopplysningssikkerheten". "brudd på personopplysningsplikten" defineres som "et brudd som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på en annen måte behandlet".[96]

Videre fremgår det en forutsetning at bruddet skal varsles dersom det *kan* medføre risiko for fysiske personers rettigheter og friheter.[97] Det kan tolkes dithen at ikke alle sikkerhetsbrudd er varslingspliktig, og at det må gjennomføres en konkret risikovurdering. Direktør i Datatilsynet i Danmark har uttalt at den konkrete risikovurderingen medfører en bevisbyrde på den dataansvarlige, og at det må kreves en høy grad av sikkerhet.[98] Vurderingen må bero på om brudd på personvernsikkerheten kan påføre fysisk, materiell eller immateriell skade som eksempelvis tap av kontroll eller begrensning av personopplysninger, forskjellsbehandling, identitetstyveri, finansielle tap eller skade på omdømme. Vurderingen må altså ta stilling til hvorvidt sikkerhetsbruddet kan medføre økonomiske, fysiske, psykiske tap eller tap av kontroll over egne data.[99]

Artikkel 33 nr. 3 oppstiller minstekrav til hva varslingen skal inneholde. Det fremgår av bokstav a at varslingen skal beskrive arten av bruddet på personopplysningssikkerheten, herunder kategoriene av og omtrent antall registrerte og antall registreringer av personopplysninger som er berørt. Bokstav b setter et krav om at varslingen må inneholde navnet på og kontaktopplysningene til personvernombudet eller et annet kontaktpunkt der informasjon kan innhentes. Varslingen skal beskrive de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten, og avslutningsvis beskrive tiltak truffet eller foreslått for å håndtere bruddet og ved relevans tiltak for å redusere skadevirkning.[100]

Oppsummert etablerer bestemmelsen en plikt for behandlingsansvarlige som oppstår ved oppfylte vilkår. Ved å ikke varsle innenfor fristen eller unnlate å gjøre en vurdering av om det foreligger varslingsplikt i det gitte tilfellet kan administrative sanksjoner medføres. Det vil si at det ikke foreligger noe krav om forsett eller uaktsomhet, men heller en konkret vilkårsvurdering og varslingsplikt. Det må foreligge en

[94] GDPR artikkel 33 nr. 1
[95] GDPR artikkel 33 nr 1 siste punktum.
[96] GDPR Artikkel 4 nr. 12
[97] GDPR Artikkel 33 nr. 1 og GDPR fortalepunkt 85
[98] Lovkommentar til artikkel 33. nr 1, Direktør for Datatilsynet Cristina Angela, hentet fra Karnov
[99] GDPR fortalepunkt 85
[100] GDPR artikkel 33 (3) bokstav c og d

sannsynlig risiko for fysiske personers rettigheter og friheter, og det stilles krav til både innhold, dokumentasjon og frist.

3.4 Informasjonsdeling vs. databeskyttelse

I skjæringspunktet mellom en effektiv informasjonsdeling og beskyttelse av personopplysninger oppstår det et spenningsforhold. For å styrke cybersikkerheten er det ofte nødvendig at virksomheter og myndigheter deler informasjon om trusler, sårbarheter og hendelser.[101] I slike situasjoner vil informasjonsdeling på samme tid være gjenstand for å innebære at personopplysninger er inkludert.[102] Dette reiser spørsmål om både hjemmelsgrunnlag, formålsbegrensning og forholdsmessighet, og skaper et mulig motsetningsforhold mellom forpliktelsene til informasjonsdeling som følger av NIS2 artikkel 29 og kravene til lovlig behandling av personopplysninger i henhold til GDPR artikkel 6.

3.4.1 NIS2 artikkel 29

Artikkel 29 i NIS2-direktivet regulerer hvordan kompetente myndigheter i medlemsstatene på frivillig basis kan dele informasjon med hverandre og med EU-organer i arbeidet med cybersikkerhet. Bestemmelsen finner sted i kapittel VI som omhandler "Cybersecurity information sharing", og utgjør én av to artikler i dette kapittelet. Artikkel 30 i NIS2 omhandler frivillig varsling av relevant informasjon fra essensielle og viktige enheter, med hensyn til hendelser, cybertrusler og nesten-hendelser til Computer Security Incident Response Team (CSIRT) eller til kompetente myndigheter.[103] Kapittelet kan samlet sett anses som en anerkjennelse av at deling av informasjon er et nødvendig virkemiddel i arbeidet for å oppnå et høyt felles sikkerhetsnivå i unionen.

Bestemmelsen lyder at "medlemsstatene skal sikre at enheter som omfattes av direktivet, og der det er relevant, andre enheter som ikke omfattes av dette direktivet, på frivillig basis kan utveksle relevant informasjon om cybersikkerhet seg imellom, inkludert informasjon om cybertrusler, nesten-hendelser, sårbarheter, teknikker og prosedyrer (...) varsler om cybersikkerhet og anbefalinger for konfigurasjon av sikkerhetsverktøy for å oppdage dataangrep". Ordlyden kan tolkes som bred og teknologinøytral, og gir adgang til deling av både tekniske og strategiske data, og innblikk i pågående angrep og gi forebyggende innsikt. Det skilles mellom at informasjonsdeling skal skje for å 1) støtte forebygging, deteksjon, respons eller gjenoppretting fra hendelser[104], og 2) for å øke nivået av cybersikkerhet gjennom felles bevissthet, teknisk kapasitet og samarbeidsdrevet kunnskapsdeling.[105] Artikkelen er altså en kompetanseregel for enhetene, og pliktregel for myndighetene.[106] Enhetene gis rett til å delta i deling av informasjon, og medlemslandene pålegges å sørge for at slik deling er gjennomførbar.

---

[101] Brilingaitė, A., m.fl. (2022) Overcoming information-sharing challenges in cyber defence exercises, *Journal of Cybersecurity*. s. 2
[102] Nweke, L. O., & Wolthusen, S. D. (2020). *Legal issues related to cyber threat information sharing among private entities for critical infrastructure protection*. s. 74
[103] Center for cybersikkerhed. *Om os*
[104] NIS2-direktivet artikkel 29 bokstav a
[105] NIS2-direktivet artikkel 29 bokstav b
[106] Boe, E. M. (2010) *Innføring i juss* s. 53

Formålet bak bestemmelsen er i samsvar med det overordnede formålet for direktivet som er å sikre et høyt felles sikkerhetsnivå i hele EU. Dette tydeliggjøres at essensielle og viktige enheter bør håndtere risikoer som oppstår fra deres interaksjoner og forhold til andre aktører innenfor et bredere økosystem.[107] Informasjonsdeling bidrar til økt bevissthet om cybertrusler, som videre styrker enhetenes evne til å forhindre at slike trusler blir til faktiske hendelser, og gjør det mulig for enhetene å håndtere konsekvensene av hendelser bedre.[108] Medlemsstatene skal oppfordre og bistå enheter til å utnytte egen kunnskap og praktisk erfaring på strategisk, taktisk og operasjonelt nivå, med å sikte på å styrke deres evne til å forebygge, oppdage, håndtere eller gjenopprette etter hendelser, eller til å redusere konsekvensene av dem.[109]

NIS2 artikkel 29 etablerer en frivillig ordning for informasjonsdeling mellom enheter som faller inn under direktivet. Rettslig sett er bestemmelsen en kombinasjon av en pliktregel og kompetanseregel som tillater essensielle og viktige enheter å delta i delingsordninger som medlemsstatene er pålagt å legge til rette for.

3.4.2 GDPR artikkel 6

Artikkel 6 i GDPR fastsetter vilkårene for lovlig behandling av personopplysninger. Bestemmelsen finner sin plass i kapittel 2 som omhandler forordningens prinsipper for behandling av personopplysninger. Det følger av bestemmelsen seks alternative vilkår for lovlig behandling av personopplysninger. At vilkårene er alternative betyr at ett av vilkårene må være oppfylt for at behandlingen skal kunne vurderes som lovlig.[110]

Første vilkåret er at den registrerte har gitt samtykke til behandlingen av sine personopplysninger for ett eller flere spesifikke formål.[111] Det fremgår ingen formelle krav til hvordan samtykke gis i forordningen, men det er en rekke krav for at det skal anses som lovlig. Det fremgår av forordningen at samtykke skal være en "frivillig, spesifikk, informert og utvetydig viljesytring fra den registrerte".[112] Det skal altså foreligge en tydelig erklæring eller bekreftelse på at det foreligger samtykke.[113]

Andre vilkår er at behandlingen er nødvendig for å oppfylle en avtale som den registrerte er part i, eller for å gjennomføre tiltak på den registrertes anmodning før en avtaleinngåelse.[114] Personopplysningene må være en del av avtalen, og nødvendig for gjennomføring av avtalen. I dette vilkåret er nødvendighetskravet en viktig begrensning.[115]

[107] NIS2-direktivets fortalepunkt 88
[108] NIS2-direktivets fortalepunkt 119
[109] NIS2-direktivets fortalepunkt 120
[110] Boe, E. M. (2010) *Innføring i juss* s. 40
[111] GDPR artikkel 6 nr. 1 bokstav a
[112] GDPR artikkel 4 (11)
[113] Jarbekk, E. Og Sommerfeldt, S. (2019) *Personvern og GDPR i praksis*. s. 63
[114] GDPR artikkel 6 nr. 1 bokstav b
[115] Jarbekk, E. Og Sommerfeldt, S. (2019) *Personvern og GDPR i praksis*. s. 71

Tredje vilkår er at behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige.[116] I dette vilkåret foreligger en plikt for å følge lov eller forskrift.[117] Hvilke lovbestemmelser som er aktuelle er avhengig av hvilken situasjon som oppstår og hvilke forpliktelser en virksomhet er underlagt.

Fjerde vilkår er at behandlingen skal være nødvendig for å verne den registrertes eller annen fysisk persons vitale interesser, herunder akutte situasjoner hvor det er noens helse og liv som krever det.[118] Femte vilkår er at behandling skal være nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt.[119] Det kan variere hva som vurderes å være i allmennhetens beste interesse.

Siste vilkåret er at behandlingen er nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger, særlig dersom den registrerte er et barn.[120] Det følger av vilkåret at det skal gjennomføres en interesseavveining, hvor konklusjonen må være at den behandlingsansvarliges interesser overskrider den registrertes.[121] Det presiseres i artikkel 6 (3) at det må foreligge hjemmel i lov, og at ikke artikkel 6 (1) bokstav e er hjemmel nok alene.[122]

En vurdering om det foreligger berettiget interesse består vanligvis av tre deler: hvilke interesser og formål ønskes ivaretatt, er behandlingen nødvendig og vurdering av om det finnes alternative fremgangsmåter og en vurdering av hvilke konsekvenser behandlingen gir og hvordan balansen ivaretas opp mot de individer som berøres.[123]

Felles for vilkårene er bruk av uttrykket "nødvendig", med unntak av bokstav a. Behandlingen må dermed være nødvendig i forhold til det aktuelle formålet, og det er dermed rimelig å fastslå at ordlyden fastsetter at det gjennomføres en proporsjonalitetsvurdering, hvor det må vurderes om formålet kan oppnås på mindre inngripende måte.

Fortalen til forordningen legger gode grunnlag for tolkning av bestemmelsen. Det presiseres at alle behandlinger må være knyttet til et behandlingsgrunnlag.[124] Et moment er å forhindre vilkårlig og formålsløs behandling av personopplysninger. Cybersikkerhet er ansett som en legitim interesse som omfattes av bokstav f.[125] Det uttales at behandling av personopplysninger i den grad det er strengt nødvendig og proporsjonalt for formålene med å sikre nettverks- og informasjonssikkerhet, det vil si evnen til et nettverk eller et informasjonssystem å ha et visst nivå, sikkerhet og å motstå utilsiktede

[116] GDPR artikkel 6 nr. 1 bokstav c
[117] GDPR fortalepunkt 45
[118] GDPR artikkel 6 nr. 1 bokstav d
[119] GDPR artikkel 6 nr. 1 bokstav e
[120] GDPR artikkel 6 nr. 1 bokstav f
[121] Jarbekk, E. Og Sommerfeldt, S. (2019) *Personvern og GDPR i praksis* s. 58
[122] Jarbekk, E. Og Sommerfeldt, S. (2019) *Personvern og GDPR i praksis* s. 58
[123] Jarbekk, E. Og Sommerfeldt, S. (2019) *Personvern og GDPR i praksis* s. 75
[124] GDPR fortalepunkt 40
[125] GDPR fortalepunkt 49

hendelser eller ulovlige eller ondsinnede handlinger som kompromitterer tilgjengeligheten, autentisiteten, integritet og konfidensialiteten av lagrede eller overførte personlige data utgjør en berettiget interesse for den behandlingsansvarlige.[126]

Artikkel 6 har en rettslig karakter av en kvalifikasjonsnorm. En kvalifikasjonsnorm bestemmer hva som skal høre til en bestemt kategori som regelverket opererer med.[127] Bestemmelsen kvalifiserer når en behandling kan anses som "lovlig". Bestemmelsen skaper en betingelse om at et av de nevnte vilkårene skal være oppfylt for at behandlingen skal kunne gjennomføres. Samlet sett utgjør bestemmelsen kjernen i vurderingen av om databehandling er tillatt.

3.5 Kontroll og tilsyn

Et effektivt regelverk for personvern og cybersikkerhet forutsetter ikke bare klare materielle krav, men også regler for tilsynsføring og sanksjonering ved brudd.[128] Både NIS2-direktivet[129] og GDPR[130] bygger på et prinsipp om regulering basert på risiko, men i praksis vil dette ha en liten effekt uten konkret tilsyn og håndheving. Tilsynsmyndighetenes rolle er avgjørende for å sikre likebehandling, rettssikkerhet og effektiv beskyttelse av samfunnsinteresser og individuelle rettigheter, som alle er viktige prinsipper bak utarbeidelsen av begge reguleringene. Både NIS2 artikkel 31 og GDPR artikkel 58 etablerer myndighetskompetanse til å gjennomføre kontrolltiltak, men med ulike fokus- og virkeområder.

3.5.1 NIS2 artikkel 32

Medlemsstatene skal sikre at tilsyns- og håndhevingstiltak som ilegges essensielle enheter med hensyn til forpliktelsene fastsatt i direktivet er effektive, proporsjonale og avskrekkende, og med hensyn til omstendighetene i hvert enkelt tilfelle.[131] Bestemmelsen fastsetter i andre ledd hvilke konkrete virkemidler tilsynsmyndigheter skal gjennomføre for å sikre overholdelse av direktivet, blant annet krav om nødvendig informasjon, dokumentasjon og data, pålegg om etterlevelse, inkludert krav om risikoreduserende tiltak og tidsfrister for gjennomføring av korrigerende tiltak.

Ordlyden kan tolkes som bred og teknologinøytral, og at det er åpnet for at nasjonale myndigheter kan utvikle og tilpasse tiltak slik at de vil passe nasjonal rett. Selv om det foreligger noe tilpasningsfrihet stilles det krav til at tiltakene skal være "appropriate, proportionate and effective", noe som gjenspeiles gjennom hele direktivet og som styrker EU-rettens krav om forholdsmessighet og rettssikkerhet.[132]

---

[126] GDPR fortalepunkt 49
[127] Boe, E. M. (2010) *Innføring i juss* s. 53
[128] Kun, E. (2021) *Strengthening the Supervision and Enforcement in the EU Cybersecurity Law: Are All Organisational Measures Created Equally?* s. 9-10
[129] NIS2-direktivet fortalepunkt 124
[130] GDPR fortalepunkt 83-85
[131] NIS2-direktivet artikkel 32
[132] TEU artikkel 5 nr. 4 og artikkel 2

Formålet er å sikre et faktisk gjennomslag for de kravene som følger av direktivet, og å sørge for at nasjonale myndigheter har tilstrekkelige midler til å kontrollere og gripe inn ved avvik.[133] Selv om listen omfatter detaljerte punkter, fremgår det av ordlyden at myndigheten har adgang til å underlegge virksomhetene andre og eventuelle strengere tiltak.[134]

Bestemmelsen må forstås i sammenheng med at tilsynstiltakene bør ta hensyn til alvorlighetsgrad, varighet og grad av overtredelse og skyld.[135] Dette innebærer at myndighetene har en viss frihet til å prioritere etter hvilket behov som foreligger. Artikkel 32 er både en kompetansenorm og pliktnorm for medlemsstatene.[136] Den gir ikke direkte virkning for virksomhetene i seg selv, men fungerer som et hjemmelsgrunnlag for inngrep. Bestemmelsen pålegger medlemsstatene å gi myndighetene de nødvendige fullmaktene i nasjonal rett, åpner for forholdsmessig håndheving, og etablerer en rettsgrunn for inngrep.

3.5.2 GDPR artikkel 58

GDPR artikkel 58 fastsetter hvilke virkemidler og beføyelser de nasjonale myndighetene skal ha for å kunne føre effektiv kontroll med behandlingsansvarlige og databehandlere. Bestemmelsen finner plass i kapittelet som regulerer tilsynsmyndighetenes uavhengighet, ansvar og virkemidler. Bestemmelsen utgjør en sentral kompetansehjemmel som gir det rettslige grunnlaget for at tilsynsmyndighetene kan iverksette undersøkelser, pålegge tiltak og sanksjonere overtredelser. Bestemmelsen er delt i tre hovedgrupper: undersøkelsesmyndighet[137], korrigerende myndighet[138] og godkjennings- og rådgivningsmyndighet[139].

Undersøkelsesmyndighetene tildeler tilsynsmyndighetene kompetanse til å gjennomføre undersøkelser og revisjoner, innhente informasjon, få tilgang til lokaler og systemer og pålegge fremleggelse av dokumentasjon. I praksis tilegnes myndighetene et bredt grunnlag for å aktivt kontrollere etterlevelse. Ordlyden er detaljert og gir adgang til kontroll både skriftlig og fysisk, på eget initiativ, men også dersom det fremlegges en klage.

Den korrigerende myndigheten følger videre av bestemmelsen. Det fremgår at tilsynsmyndighetene har myndighet til å beslutte korrigerende tiltak nevnt videre i bestemmelsen. Slike korrigerende tiltak kan blant annet være å gi advarsel, pålegge å etterkomme registrertes rettigheter, pålegge sletting, korrigering eller tilgang. Ordlyden tyder på at tilsynsmyndighetene har disiplinære virkemidler, og at det kan treffes individuelle avgjørelser som direkte påvirker den behandlingsansvarlige. Bestemmelsens tredje ledd tildeler tilsynsmyndighetene myndighet til å godkjenne og gi råd, og understreker tilsynsmyndighetenes rolle som veiledende og ikke bare sanksjonerende.

Artikkel 58 må forstås i lys av GDPR artikkel 57 og artikkel 55. Artikkel 57 inneholder en detaljert, men ikke uttømmende liste over obligatoriske oppgaver tillagt tilsynsmyndighetene, herunder blant annet å føre

[133] NIS2-direktivet artikkel 32
[134] Fremgår av uttrykket «at least to» i NIS2-direktivet artikkel 32 nr. 2 siste punktum.
[135] NIS2-direktivet fortalepunkt 124
[136] Boe, E. M. (2010) *Innføring i juss* s. 53
[137] GDPR artikkel 58 nr. 1
[138] GDPR artikkel 58 nr. 2
[139] GDPR artikkel 58 nr. 3

tilsyn med og håndheve anvendelsen av denne forordningen[140] og rådgive om lovgivning og administrative tiltak knyttet til vern av fysiske personers rettigheter og friheter ved behandling[141]. Artikkel 55 er en kompetanseregel som gir tilsynsmyndighetene kompetanse til å utføre de oppgaver og utøve den myndighet som gis i samsvar med forordningen.

Personvernsforordningen bygger på rettssikkerhet, transparens og vern av individet. Tilsynsmyndighetene i hver medlemsstat bør ha de samme oppgavene og effektive fullmaktene for å sikre en enhetlig overvåkning og håndheving av forordningen.[142] Dette understreker at artikkel 58 må tolkes i lys av et overordnet mål om harmonisering, effektiv håndheving og beskyttelse av grunnleggende rettigheter[143].

Artikkel 58 har karakter av en kompetansenorm for tilsynsmyndighetene, og en pliktnorm for medlemsstatene. Artikkelen lister opp hvilke rettslige virkemidler tilsynsmyndighetene har når de skal utøve sin funksjon, og gir myndighetene fullmakter til å treffe vedtak eller iverksette tiltak. For medlemsstatene pålegger bestemmelsen å sikre at de aktuelle myndighetene eksisterer, at de kan bruke virkemidlene og at virkemidlene får rettskraft for å være effektive.

På bakgrunn av denne gjennomgangen vil neste kapittel ta for seg hvordan regelverkene er implementert i norsk rett.

4.0 Innledning til norsk implementering

Som EØS-stat står Norge overfor en unik utfordring når det kommer til implementering av EU-rett. Norge er ikke direkte underlagt EU-retten, men er forpliktet til å implementere store deler av EU-lovgivningen gjennom EØS-avtalen.[144] Norge får i denne posisjonen mulighet til å tilpasse direktiv til nasjonale forhold, men samtidig innebærer en slik frihet et ansvar for å sikre samsvar med overordnede mål og krav i EU-retten.

I lys av økende cybersikkerhetstrusler i kritiske samfunnsfunksjoner er implementeringen av NIS2 spesielt relevant da effektiv beskyttelse mot cyberangrep er avgjørende for å sikre nasjonal sikkerhet. Implementeringen av GDPR i Norge er betydelig viktig for å sikre en enhetlig og rettferdig behandling av personopplysninger.

For å sikre en tilstrekkelig cybersikkerhet i kritiske samfunnsfunksjoner har Norge valgt en tilnærming preget av samarbeid mellom offentlige myndigheter og virksomheter.[145] Implementeringen bygger på et prinsipp om at virksomheter selv skal ta ansvar for sikkerheten i sine systemer, samtidig som det fremgår ved nasjonale strategier og retningslinjer. Sikkerhetsloven implementerer kravene som følger av NIS2 og

[140] GDPR artikkel 57 bokstav a
[141] GDPR artikkel 57 bokstav b
[142] GDPR fortalepunkt 129
[143] EU-charteret om Grunnleggende Rettigheter artikkel 8
[144] Sverdrup, U. (2004). *Compliance and conflict management in the European Union: Nordic exceptionalism*. s. 26
[145] Nasjonal sikkerhetsmyndighet (NSM). *Oppgaver og styring* s. 130

pålegger virksomheter i kritiske samfunnsfunksjoner å selv sørge for at sikkerhetsarbeidet er i tråd med foreliggende sikkerhetsrisiko.[146]

Sikkerhetsloven er et eksempel på hvordan ansvaret for cybersikkerhet er delegert til virksomhetene selv ved at risikovurderingen og tiltak tilpasses etter behov. Personvernet er ivaretatt gjennom Personopplysningsloven som gjennomfører GDPR i norsk rett. Loven pålegger virksomheter som behandler personopplysninger å beskytte og gjøre nødvendige vurderinger av potensiell risiko for individers rettigheter i sammenheng med håndtering av data.[147] Personopplysningsloven § 1 uttaler at GDPR gjelder som lov for norsk rett, og har sitt virkeområde ved både helt og delvis automatisert, samt ikke-automatisert behandling av personopplysninger, jf personopplysningsloven § 2.

Dette kapittelet kartlegger hvordan NIS2-direktivet og GDPR er implementert i norsk rett, med spesielt fokus på hvordan reguleringene balanserer cybersikkerhet og personvern i kritiske samfunnsfunksjoner. Det vil også i denne delen av oppgaven bli undersøkt hvordan norske myndigheter som Nasjonal sikkerhetsmyndighet (NSM) og Datatilsynet håndhever kravene og samarbeider med private aktører for å sikre at både digital sikkerhet og personvern blir tatt hensyn til.

4.1 NIS2 i norsk rettsorden

NIS2-direktivet representerer EUs mest sentrale regulering av cybersikkerhet, og har et formål om et høyt felles sikkerhetsnivå i medlemsstatene. I Norge er landet gjennom EØS-avtalen forpliktet til å gjennomføre store deler av de reglene som gjelder for EUs indre marked. Norsk rett har gjennom etableringen og utviklingen av sikkerhetsloven implementert store deler av NIS2-direktivet.

Norge har uttrykt støtte til etableringen av NIS2 direktivet og har klart anerkjent behovet for å styrke cybersikkerheten. Regjeringen har fremhevet at forgjengeren til direktivet, NIS1, har vært en viktig begynnelse i reguleringen av digital sikkerhet, men at det måtte endringer til som kunne være tilstrekkelig for å møte dagens og fremtidens utfordringer innenfor digital sikkerhet. NIS2-direktivet har sammenlignet med NIS1, et utvidet virkeområde som inkluderer flere sektorer som anses som kritiske for samfunnet.[148] Norge har uttalt at denne utvidelsen er viktig i arbeidet for en bedre rustet cybersikkerhet. Norge har måttet foreta flere nødvendige endringer i regelverk for å gjennomføre NIS2-direktivet, blant annet endringer i sikkerhetsloven, og i tilhørende forskrifter. [149]

Lov om nasjonal sikkerhet av 2018, videre omtalt som sikkerhetsloven (sikkl.), har som formål å bidra til: a) å trygge Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser, b) å forebygge, avdekke og motvirke sikkerhetstruende virksomhet og c) at sikkerhetstiltak gjennomføres i samsvar med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn.[150] Angivelsen er ikke en uttømmende liste av de grunnleggende nasjonale interessene loven

[146] Lov om nasjonal sikkerhet (Sikkerhetsloven) § 4-2
[147] GDPR fortalepunkt 4
[148] Regjeringen. (2023) NIS2-direktivet. EØS notat
[149] Regjeringen. (2023) NIS2-direktivet. EØS notat
[150] Sikkerhetsloven § 1-1

sikter på å beskytte, men en fremheving av de interessene det er viktig for norsk rett å ivareta.[151] Sikkerhetsloven erstattet sin forgjenger fra 1998 grunnet et trusselbilde i stadig endring og en rask teknologisk utvikling.[152] Det følger av Forsvarsdepartementet sin proposisjon til ny lov at den nye sikkerhetsloven har som overordnet mål å styrke nasjonal sikkerhet i møte med et økende og mer komplekst trusselbilde, og at den nye loven skal gi et "mer dynamisk og fleksibelt rammeverk" enn forgjengeren.[153]

Det er forventet at ny lov om digital sikkerhet skal tre i kraft i løpet av 2025. Dato for ikrafttredelse har derimot ikke blitt satt. Denne loven skal formalisere krav til digital sikkerhet hos tilbydere av samfunnsviktige tjenester, men det er kun NIS1-direktivet som vil gjennomføres gjennom denne loven, men på sikt er det forventet at også NIS2-direktivet skal bli gjennomført.[154] Denne loven vil på grunnlag av dette ikke bli behandlet i denne oppgaven, men gir en tydelig indikasjon på at Norge prioriterer å utarbeide et lovverk som samsvarer med EU-retten.

4.1.1 Sikkerhetstiltak

Sikkerhetsloven åpner allerede i formålsparagrafen opp for at sikkerhetstiltak skal gjennomføres i samsvar med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn.[155] Et demokratisk samfunn bygges opp av grunnleggende verdier om personvern, nasjonal sikkerhet og rettssikkerhet. Inngripende tiltak må derfor ha hjemmel i formell lov i henhold til de forpliktelser som følger av Grunnloven § 113 og EMK artikkel 8. Det fremgår av proposisjonen at utvalget mener at det økende trusselbildet innenfor cyberdomenet i mange tilfeller er sektorovergripende.[156]

Utvalget uttaler at informasjonsdeling om trusler på tvers av sektorer, og etablering sikkerhetstiltak som skal forebygge truslene, "underbygger behovet for å ivareta et helhetlig og sektorovergripende ansvar".[157] Utvalget nevner et generelt utgangspunkt vil være å vurdere om sikkerhetsmessige tiltak kan få en negativ innvirkning på den enkeltes rettssikkerhet og personvern ved å vurdere tiltakets formålsmessighet og forholdsmessigheten mellom den sikkerhetsmessige effekten og hvor inngripende tiltakene er i forhold til personvern og rettssikkerhet og vurdere om andre tiltak som er mindre inngripende kan oppnå samme effekt.[158]

Sikkerhetsloven kapittel 2 og kapittel 4 stiller opp krav til forebyggende sikkerhetsarbeid. Kapittel 2 tar for seg det offentliges ansvar og myndighet for forebyggende sikkerhetsarbeid og kapittel 4 omhandler virksomheters plikter og ansvar for sikkerhetsarbeid, og funksjonelle krav til virksomhetene.

[151] NOU 2016:19 s. 252
[152] LOV-1998-03-20-10 og NOU 2016:19 s. 18
[153] Prop. 153 L (2016-2017) s. 7
[154] NSM. Risikorapport 2025, s. 35
[155] Sikkerhetsloven § 1-1
[156] Prop. 153 L (2016-2017) s. 15
[157] Prop. 153 L (2016-2017) s. 42-43
[158] NOU 2016:19 s. 95

Sikkerhetsloven § 2-1 skriver at departementene er ansvarlige for forebyggende sikkerhetsarbeid innenfor sine ansvarsområder. Bestemmelsen er en pliktnorm og utgjør en rettslig forpliktelse for departementene. Bestemmelsen pålegger departementene å ha kunnskap og en løpende oversikt over samfunnsfunksjoner som anses som en "grunnleggende nasjonal funksjon".[159] En "grunnleggende nasjonal funksjon" er definert som "tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser"[160], også forstått som en essensiell samfunnsfunksjon eller en kritisk infrastruktur.

At ordlyden i bokstav a er at departementet skal "holde oversikt" antyder at det ikke skal være en engangsoppgave, men en kontinuerlig oppgave i lys av det aktuelle risikobildet. Bokstav b utvider bokstav a ved å koble funksjoner til konkrete virksomheter. Det følger av bestemmelsen at departementene skal "identifisere og holde oversikt over virksomheter som har vesentlig betydning for grunnleggende nasjonale funksjoner eller for nasjonale sikkerhetsinteresser". Det legges til grunn at det skal gjennomføres en kvalifisert vurdering av hvilke virksomheter som er av "vesentlig betydning".[161] Ordlyden i § 2-1 er presis og strukturert, og påpeker at Norge bygger på en desentralisert forvaltning med sektoransvar som skal samordnes med sikkerhetsmyndigheten.

I sikkerhetsloven § 2-2 heter det at "Sikkerhetsmyndigheten har det sektorovergripende ansvaret for at forebyggende sikkerhetsarbeid i virksomhetene utføres i samsvar med loven.". Sikkerhetsmyndigheten (NSM) utgjør en av Norges tre etterretnings-, overvåknings-, og sikkerhetstjenester. Hovedoppgaven til NSM er å bedre Norge til å kunne beskytte seg mot blant annet sabotasje, terror og sammensatte trusler.[162] Det følger av bestemmelsens andre ledd at NSM har et overordnet ansvar for at sikkerhetstilstanden i alle sektorer kontrolleres og bidra til samordning på tvers av sektorene. Dette innebærer ikke nødvendigvis at kontrollen skal gjennomføres av NSM, men at de har et ansvar for at kontrollen faktisk foretas. At NSM skal se til at virksomhetene oppfyller sine "plikter" kan forstås som en klar handlingsplikt, og at NSM ikke bare har en rådgivende, men aktiv rolle.

I henhold til tidligere nevnte bestemmelser i sikkerhetsloven er det klart at mye av ansvaret med å sørge for at sikkerhetsarbeidet er tilstrekkelig, faller på virksomhetene selv. Det følger av § 4-1 første ledd, første punktum at "virksomhetens leder har ansvaret for det forebyggende sikkerhetsarbeidet". Det fremgår en klar ansvarsplassering og pliktnorm på virksomheten og dens leder ved ordlyden. Ved bruk av uttrykket "har ansvaret" foreligger et ansvar for etterlevelse som tildeles den med formelt og reelt lederansvar. På den måten forankres sikkerhet som et ledelsesansvar. Det fremgår av bestemmelsens andre punktum at forebyggende sikkerhetsarbeid "skal" være en del av virksomhetens styringssystem. Bestemmelsen er dermed en pliktregel og angir en ubetinget plikt, hvor det stilles krav om at sikkerhet skal integreres i virksomhetens overordnede styring, herunder for eksempel i rutiner om risikovurdering, internkontroller og planlegging.

Innenfor forebyggende sikkerhetsarbeid, ligger et ansvar for å gjennomføre sikkerhetstiltak i § 4-3. Det følger av bestemmelsen at "virksomheten skal gjennomføre de forebyggende sikkerhetstiltakene som må

[159] Sikkerhetsloven. § 2-1. Bokstav a
[160] Sikkerhetsloven. §1-5 (2)
[161] Sikkerhetsloven. § 2-1 bokstav b.
[162] NSM. Om oss.

til for å gi et forsvarlig sikkerhetsnivå og redusere risikoen knyttet til sikkerhetstruende virksomhet". Det følger av forarbeidene at slike tiltak omfatter alle tiltak som bidrar med å ivareta lovens formål, informasjonssikkerhet og sikkerheten til informasjonssystemer.[163]

NIS2 artikkel 21 stiller krav til at essensielle og viktige enheter, også kalt enheter i kritiske samfunnsfunksjoner skal innføre sikkerhetstiltak som er "passende" og "proporsjonale" for å håndtere risiko knyttet til nettverks- og informasjonssystemer, forebygge og minimere virkningen av uønskede hendelser, sikre tjenestekontinuitet og gjenopprette systemfunksjoner etter angrep. Disse kravene er i stor grad reflektert i norsk rett gjennom sikkerhetsloven av 2018, særlig i kapittel 2 og 4. Sikkerhetsloven er utformet med vekt på forholdsmessighet og rettssikkerhet. I proposisjonen understrekes det at sikkerhetstiltak skal gjennomføres i samsvar med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn, og at tiltakene må vurderes opp mot blant annet personvern og legalitetsprinsippet.[164]

Det er viktig å bemerke at implementeringen av NIS2 artikkel 21 i Norge ikke er gjort gjennom en ordrett kopiering av direktivet. I stedet er direktivets krav gjennomført gjennom en funksjonell tilpasning til norsk rett som innebærer at kravene er integrert i eksisterende reguleringer. Norsk rett bygger på nasjonale begreper som "grunnleggende nasjonale funksjoner" istedenfor EUs "essensielle og viktige enheter". Tilpasningen ivaretar likevel fullt ut innholdet og formålet i direktivet, men tar hensyn til norsk forvaltningsstruktur og begrepsbruk.

4.1.2 Rapportering av hendelser

Et sentralt element i det forebyggende sikkerhetsarbeidet er krav til tidlig varsling i henhold til sikkerhetsloven § 4-5. Virksomheter har en plikt til å varsle NSM og eventuelle relevante tilsynsmyndigheter dersom det foreligger sikkerhetstrusler, brudd på sikkerhetskrav eller mistanke om slike forhold.[165] Plikten for varsling gjelder også ved planlagt eller pågående aktivitet som kan medføre ikke ubetydelig risiko for nasjonale sikkerhetsinteresser, og den gjelder uavhengig av eventuell taushetsplikt. Bestemmelsen har som hensikt å sikre en rask informasjonsflyt og muliggjøre tiltak på tvers av sektorer.[166]

Første ledd av bestemmelsen uttaler at en virksomhet "skal straks" varsle sikkerhetsmyndigheten og andre myndigheter dersom det foreligger potensielle trusler. Uttrykket "skal" henviser til en klar pliktnorm som rettslig forplikter virksomheter, og uttrykket "straks" innebærer at varselet må gis uten unødig opphold, og kan tolkes som at en hurtig handling skal gjennomføres. Bestemmelsen lister så opp ved bokstav a-c hva som utløser varslingsplikten. Bokstav a og b utløser varslingsplikten dersom virksomheten er rammet av sikkerhetstruende virksomhet, eller dersom det foreligger begrunnet mistanke om sikkerhetstruende virksomhet som har eller kan ramme virksomheten.

[163] Prop. 153 L (2016-2017) s. 173
[164] Prop. 153 L (2016-2017) s. 164
[165] Sikkerhetsloven § 4-5
[166] Prop. 153 L (2016-2017) s. 61

Varslingsplikten ble innført for å sikre at myndighetene får rask kjennskap til hendelser som kan true nasjonal sikkerhet, slik at tiltak tidlig kan iverksettes. Det følger av forarbeidene at tidlig varsling er avgjørende for hurtig respons fra myndighetene.[167] Varslingsplikten er en forutsetning for at myndighetene skal kunne ivareta sitt overordnede ansvar for forebyggende sikkerhetsarbeid, og når virksomheten pålegges å varsle, har myndighetene mulighet til å se hendelser i sammenheng på tvers av både sektorer og nasjonalt nivå.[168] Varslingsplikten spiller dermed en sentral rolle i forebyggende sikkerhetsarbeid og tillater myndighetene å koordinere informasjon mellom sektorer, og bidrar til at fattelser og vedtak gjøres på informert grunnlag.[169]

Plikten til å varsle som følger av § 4-5 er tett knyttet til cybersikkerhet. Dagens trusselbilde består av mange digitale sikkerhetstrusler, og loven er derfor bevisst utformet til å være sektorovergripende og omfatter "tilsiktede handlinger som kan skade informasjon, informasjonssystemer, infrastruktur eller objekter".[170] I praksis har NSM etablert kontaktpunkter for å motta slike varsler døgnet rundt, for eksempel et varslingsskjema.[171] En slik umiddelbar informasjon kan brukes til å varsle andre potensielt berørte virksomheter, eksempelvis kan et dataangrep mot én samfunnskritisk virksomhet være en del av et større mønster. Ved tidlig varsel vil NSM tidlig kunne analysere angrepet og advare andre virksomheter i samme eller andre sektorer, og man får dermed hindret en videre spredning.[172] Tidlig varsling er derfor viktig for at cybersikkerheten skal være robust.

Varslingsplikten er også en del av det internasjonale bildet. Gjennom NIS2-direktivet har EU pålagt medlemsland å ha varslingsordninger for alvorlige datahendelser. Direktivet krever at operatører av essensielle enheter og tjenester varsler myndighetene om hendelser som kan ha en betydelig påvirkning på tjenesten, jf. NIS2 artikkel 23. Norge har implementert tilsvarende tiltak for å beskytte kritisk infrastruktur og digital sikkerhet. Både sikkerhetsloven og NIS2 bygger på en grunntanke om at rask varsling er avgjørende for å beskytte samfunnskritiske funksjoner mot cyberangrep.

4.1.3 Informasjonsdeling

Sikkerhetsloven § 2-3 tar for seg utveksling av trusselvurderingen og annen sikkerhetsinformasjon. Bestemmelsen stiller opp en plikt for sikkerhetsmyndigheten til å legge til rette for informasjonsdeling. Bestemmelsen består av tre ledd, hvorav første ledd lyder at sikkerhetsmyndigheten skal "legge til rette for at virksomheter som loven gjelder for, får tilgang til informasjon om trusselvurderinger og andre opplysninger som er av betydning for virksomhetens forebyggende sikkerhetsarbeid".

At sikkerhetsmyndigheten "skal" legge til rette for kan tolkes som en rettslig plikt, hvor uttrykket "legge til rette" må tolkes som en tilretteleggingsplikt fremfor en gjennomføringsplikt.[173] Sikkerhetsmyndigheten må altså legge opp til at informasjon kan deles, selv om myndighetene selv ikke kontrollerer all

[167] Prop. 153 L (2016-2017) s. 81
[168] Prop. 153 L (2016-2017) s. 81
[169] Prop. 153 L (2016-2017) s. 82
[170] Prop. 153 L (2016-2017) s. 82
[171] NSM. (2020) Veileder for virksomheters håndtering av uønskede hendelser.
[172] Prop 153 L (2016-2017) s. 81
[173] Prop 153 L (2016-2017) s. 167

informasjon. Dette kan tolkes i samsvar med at NSM ikke anses å ha "full råderett over all trussel- og sikkerhetsinformasjon".[174] "Virksomheter som loven gjelder for" tolkes ut ifra en virksomhet oppfyller visse kriterier av betydning for nasjonal sikkerhet.[175] Hvilke opplysninger som anses å være av betydning for "forebyggende sikkerhetsarbeid" oppstiller en vurdering av relevans. Det må med andre ord tolkes slik at det kun er opplysninger som faktisk er nyttige for å styrke sikkerheten som skal deles.

I bestemmelsens første ledd pålegges sikkerhetsmyndigheten å sørge for etablering av arenaer for deling. En slik opprettelse skal i henhold til bestemmelsen skje i samråd med "sektormyndigheter og andre relevante myndigheter". NSM skal derfor samarbeide med de ansvarlige fagmyndighetene i ulike sektorer, noe som sikrer at det reelle behovet blir møtt med den mest relevante fagkunnskapen. Det presiseres at en slik arena som opprettes skal benyttes til "informasjons- og erfaringsveksling", noe som understreker at det ikke bare en konkret informasjon som skal deles, men også erfaringer som kan legge til rette for at det tas lærdom fra ulike øvelser eller hendelser.

Tilgang til trusselvurderinger og sikkerhetsopplysninger er viktig for at virksomheter skal kunne utføre egne oppgaver. Informasjonsdelingen kan forstås slik at den er ment å styrke virksomhetenes forebyggende sikkerhetsarbeid ved å gi et bedre grunnlag og innsikt i trusselbildet, trender og teknikker, og dermed skape et grunnlag for å vurdere risiko og hvilke tiltak som bør iverksettes.[176] Det følger av forarbeidene at informasjonsutveksling må skje "innenfor rammene av lovbestemt taushetsplikt" og aktørenes lovlige adgang til å dele informasjon.[177] Dette medfører at selv om det oppfordres til en bred informasjonsdeling i bestemmelsen, kan ikke for eksempel sikkerhetsgradert informasjon deles med virksomheter uten nødvendig hjemmel.

Forarbeidene viser oppsummert at bestemmelsen er ment å være en praktisk samarbeidsbestemmelse som skal bedre flyten av informasjon om potensielle trusler og hendelser, og kan anses som nødvendig for at myndigheter og virksomheter skal ha mulighet til å være i forkant av trusler og utvikle fungerende sikkerhetstiltak.

NIS2-direktivet artikkel 29 tar for seg ordninger for deling av informasjon om cybersikkerhetstrusler mellom relevante aktører. Sikkerhetsloven § 2-3 og forarbeidene oppfyller mye av den samme intensjonen som fremgår av artikkel 29. Både § 2-3 og artikkel 29 tar sikte på å øke situasjonsforståelsen av trusler hos virksomheter ved å legge til rette for deling av informasjon. Det understrekes i artikkelen at medlemsstatene skal sørge for at enheter kan utveksle relevant cybersikkerhetsinformasjon for å heve det generelle sikkerhetsnivået. § 2-3 fokuserer på trusselvurderinger og opplysninger av betydning for forebyggende sikkerhetsarbeid. I praksis betyr dette mye av de samme typene informasjon. Begge regelsettene fremmer deling av informasjon som et middel for å styrke beredskap.

En viktig forskjell er hvilket omfang reguleringene har. NIS2-direktivet har et konkret indre-markeds-orientert formål om å sikre et høyt nivå av nettverks- og informasjonssikkerhet for essensielle og viktige virksomheter i samfunnskritiske sektorer. Sikkerhetsloven har som formål å beskytte nasjonale

[174] Prop 153 L (2016-2017) s. 167
[175] Jf. Sikkerhetsloven § 1-3
[176] Prop. 153 L (2016-2017) s. 167
[177] Prop. 153 L (2016-2017) s. 167

sikkerhetsinteresser, og gjelder statlige, fylkeskommunale og kommunale organer, og utvalgte virksomheter.[178] Sikkerhetsloven vil for eksempel kunne omfatte nasjonale sikkerhetsorganer og forsvarssektoren, men NIS2 inkluderer sektorer som sikkerhetsloven kun dekker dersom de er definert som kritiske funksjoner i samfunnet. Sikkerhetsloven og direktivet deler begge målet om å fremme informasjonssamarbeid for økt sikkerhet, men sikkerhetsloven omfatter nasjonal sikkerhet generelt, mens direktivet fokuserer på cybersikkerhet.

4.1.4 Kontroll og tilsyn

Sikkerhetsloven kapittel 3 tar for seg reglene om tilsyn, og utgjør et viktig hjemmelsgrunnlag for oppfølgning av forebyggende sikkerhetsarbeid. § 3-1 regulerer fordelingen av tilsynsansvar etter loven, og åpner for at tilsyn kan delegeres til sektormyndigheten. Det følger av første ledd at det er NSM som fører tilsyn, men at departementet kan bestemme at myndigheter med sektoransvar skal føre tilsyn med virksomheter som er omfattet av loven jf. andre ledd. Dette er i tråd med det norske sektorprinsippet i forvaltningen, og innebærer at ansvarlig departement har kompetanse til å fastsette hvilken myndighet som skal føre tilsyn innenfor sitt område. Det betyr at NSM har et overordnet sektorovergripende ansvar, men at faktisk tilsyn kan være delegert til for eksempel Finanstilsynet, Norges vassdrags- og energidirektorat eller Helsedirektoratet.

Det følger av andre ledd i § 3-1 at sikkerhetsmyndigheten skal gjennomføre tilsyn når det følger av internasjonale forpliktelser, eller når det er "tvingende nødvendig". Forarbeidene uttaler at "tvingende nødvendig" forutsetter at det foreligger konkrete sikkerhetsinteresser som tilsier at NSM skal føre tilsyn.[179] Bestemmelsen skal sikre at virksomheter etterlever de kravene som følger av loven, og må forstås som en sentral pliktnorm og kompetansehjemmel.

Forarbeidene til loven presiserer at tilsynsmyndighetene skal kunne benytte en risikobasert tilnærming i utvelgelsen og prioriteringen av tilsynsobjekter.[180] Dette speiler NIS2 artikkel 32 nr. 2, som fremhever nødvendigheten av målrettet, risikojustert tilsyn, og muligheten for myndighetene til å gjennomføre inspeksjoner og sikkerhetsrevisjoner ved mistanke om alvorlige hendelser.

Videre fremgår det i forarbeidene at tilsynet også skal bidra til læring og veiledning. I dette ligger det at tilsyn ikke kun skal være sanksjonsorientert, men også støtte virksomhetene i å heve sitt sikkerhetsnivå. Dette er i tråd med artikkel 32 i NIS2 som understreker både veiledning og preventive tiltak som formål med tilsynet. Sikkerhetslovens kapittel 10 gir på samme tid adgang til å ilegge reaksjoner, blant annet i form av overtredelsesgebyr, der det er nødvendig for å sikre etterlevelse. Dette reflekterer NIS2 artikkel 32 nr. 4 og 5, som krever at medlemsstatene kan iverksette effektive, proporsjonale og avskrekkende tiltak, inkludert bøter, pålegg, offentliggjøring av brudd og midlertidige suspensjoner.

[178] Jf. Sikkerhetsloven § 1-2
[179] Prop. 153 L (2016-2017) s. 170
[180] Prop. 153 L (2016–2017) s. 175–177

Sikkerhetsloven § 3-1 har dermed en sentral rolle i Norges gjennomføring av de kontroll- og tilsynsmekanismene som følger av NIS2 artikkel 32. Ordlyden gir et bredt hjemmelsgrunnlag for tilsyn, samtidig som den tillater fleksibilitet ved mulighet for delegering til sektormyndigheter.

Sikkerhetsloven § 3-5 regulerer tilsynsmyndighetens adgang til å behandle personopplysninger som et ledd i tilsynsvirksomheten. I første ledd åpnes det for at tilsynsmyndigheten "kan behandle personopplysninger dersom det er nødvendig for å utføre sine oppgaver". Kravet om nødvendighet fungerer som et vilkår for lovlig behandling, og angir at personopplysninger bare kan behandles så fremt det foreligger en klar og saklig tilknytning til myndighetens tilsynsfunksjon, for eksempel ved kontroll av sikkerhetsklareringer, tilgangslogger eller andre forhold som involverer enkeltpersoner.

Andre ledd presiserer at slik behandling ikke må "utgjøre et uforholdsmessig inngrep i personvernet". Formuleringen trekker inn en forholdsmessighetsvurdering, og skal sikre at behandlingens omfang og karakter står i rimelig forhold til formålet. Bestemmelsen er en lovfesting av nødvendighets- og proporsjonalitetsprinsippet.[181]

Bestemmelsen vurderer på denne måten hensynet til effektiv kontroll og håndheving mot den enkeltes rett til beskyttelse av personopplysninger, og representerer en balansering som også er sentral i vurderingen av forholdet mellom cybersikkerhet og personvern ved implementering av tiltak etter NIS2 og vurdering av behandlingsgrunnlag etter GDPR artikkel 6.

4.2 GDPR i norsk rett

GDPR representerer den mest sentrale rettsakten på EU-nivå når det gjelder beskyttelse av personopplysninger.[182] Forordningen har som formål sikre vern av fysiske personers grunnleggende rettigheter og friheter, særlig knyttet til deres rett til vern av personopplysninger.[183] Forordningen skal bidra til et område med frihet, sikkerhet og rettferdighet samt oppnå en styrking og tilnærming av økonomiene i det indre marked og til fysiske personers velferd.[184] Forordningen ble gjennom personopplysningsloven gjennomført i norsk rett med virkning fra 20. juli 2018, og i henhold til lovens § 1 gjelder forordningen som norsk lov.

Departementet fremhever at formålet med gjennomføringen er å sikre en styrket og oppdatert rettslig regulering av behandling av personopplysninger i tråd med den teknologiske utviklingen og økte digitaliseringen i samfunnet.[185] Forarbeidene peker på at GDPR innebærer en styrking av registrertes rettigheter, men også av virksomheters ansvar, blant annet ved å stille strenge krav til behandlingsgrunnlag.[186] GDPR representerer derfor et helhetlig og prinsipielt rammeverk for personvern i et moderne informasjonssamfunn, sammenlignet med tidligere direktiv av 1995.[187]

---

[181] NOU 2016:19 s. 257
[182] GDPR fortalepunkt 1-10
[183] Jf. GDPR artikkel 1
[184] GDPR fortalepunkt 2
[185] Prop. 56 LS (2017-2018) s. 204
[186] Prop. 56 LS (2017-2018) s. 9
[187] Personverndirektivet 1995

Det norske personvernet fremgår av både nasjonale og internasjonale forpliktelser, blant annet Grunnloven § 102 og EMK artikkel 8. Det følger av begge bestemmelsene et grunnprinsipp om at alle har "rett til respekt for sitt privatliv". Med gjennomføringen av GDPR er dette prinsippet tydeligere representert, og det vektlegges i større grad gjennomføring av risikovurderinger, vern av personopplysninger og sikring av etterlevelse. I Norge er Datatilsynet utpekt som kompetent tilsynsmyndighet, og har i oppgave å drive med tilsyn, saksbehandling, veiledning og kommunikasjonsarbeid. Datatilsynet skal føre kontroll med og bidra til at regelverket etterleves.[188]

Samlet sett er GDPR ikke bare en inkorporering av EU-rett i norsk rett, men den består av et rammeverk som preger regulering av behandling av personopplysninger i både privat og offentlig sektor. Forordningen i sin helhet gjelder som norsk lov. Forordningens grunnprinsipper er sentrale når balansen mellom hensynet til informasjonssikkerhet og cybersikkerhet opp mot kravene til beskyttelse av personopplysninger skal vurderes.

Det er viktig å presisere at forskjellen mellom direktiv og forordning kommer til syne ved inkorporering i nasjonal lovgivning. Et direktiv fastsetter et mål som bestemte land skal oppnå, og en forordning er en bindende rettsakt.[189] Dette innebærer at en forordnings tekst er selve rettskilden, og at det ikke foreligger et behov for en særskilt norsk lov for å tilpasse innholdet. Det gir i større grad mulighet for harmonisering og begrenser muligheten for en nasjonal skjønnsfrihet. Det følger av forarbeidene til personopplysningsloven at GDPR åpner nasjonale tilpasninger på enkelte områder, men Norge har vært noe reservert til å innføre slike tilpasninger.[190]

4.3 Balanse i norsk rett

Norsk rett står overfor en krevende balansegang mellom hensynet til personvern og digital sikkerhet. På den ene siden står personopplysningsloven ved GDPR som skal verne individets personvern og setter krav til en forsvarlig behandling av personopplysninger. På den andre siden står sikkerhetsregelverket, herunder sikkerhetsloven, som skal beskytte kritiske samfunnsfunksjoner mot cybertrusler. De to regelsettene overlapper på flere punkter, blant annet når det gjelder informasjonssikkerhet, håndtering av sikkerhetsbrudd og tilsyn, men på samme tid har de ulike formål. GDPR handler om å beskytte «den enkelte borgers rett til personvern, mens NIS2 handler om å beskytte kritiske nettverk og informasjonssystemer for å beskytte det europeiske fellesskapet mot cyberangrep.[191]

Sikkerhetsloven gjelder for virksomheter av vesentlig betydning for nasjonal sikkerhet, og retter seg først og fremst mot tilsiktede trusler.[192] Etter vedtakelsen av NIS2-direktivet er det digitale trusselbildet adressert i bredere forstand i ny lov om digital sikkerhet, kalt digitalsikkerhetsloven som ble vedtatt i 2023. Loven gjennomfører NIS1-direktivet og forventes å tre i kraft i løpet av 2025-[193]. Selv om

[188] Datatilsynet. *Datatilsynets oppgaver*., Datatilsynet. *Om Datatilsynet*
[189] Lovdata Europalov. *Om EU-rettsaktene*
[190] Prop. 56 LS (2017-2018) s. 57
[191] Glenstrup, P. (2025) *NIS2 handler om én eneste ting*
[192] Prop. 109 LS (2022-2023) s. 18
[193] Nasjonal sikkerhetsmyndighet. (2025). *Risiko 2025*

sikkerhetsloven og NIS2 overlapper på noen områder, foreligger det noen forskjeller. Sikkerhetsloven har som formål å beskytte nasjonale sikkerhetsinteresser, mens NIS-regelverket skal beskytte det indre markedet og samfunnskritiske enheter ved krav til cybersikkerhet.

Personopplysningsloven gjennomfører GDPR i Norge og har som formål å beskytte enkeltindividers personvern og grunnleggende rettigheter ved behandling av personopplysninger. GDPR gjelder i alle sektorer. Artikkel 32 i forordningen pålegger behandlingsansvarlige å gjennomføre passende tiltak for å oppnå et sikkerhetsnivå som er egnet, basert på risiko, ved behandling av personopplysninger.[194] Dette medfører i praksis at mange av tiltakene er noe like de tiltakene som god digital sikkerhet krever.

4.3.2 Krav til sikkerhetstiltak

Både sikkerhetsregelverket og personvernregelverket stiller krav til at virksomheter skal etablere gode sikkerhetstiltak, men rammene og terminologien er noe ulik. I henhold til sikkerhetsloven skal virksomheter som omfattes av loven gjennomføre en systematisk risikostyring, og gjøre nødvendige sikkerhetstiltak for å beskytte sine informasjonssystemer, og forhindre hendelser.[195] NIS2 krever at det skal iverksettes tiltak som står i rimelig forhold til risikoen virksomheten står overfor, og for å forebygge og minimere virkningen av hendelser i nettverks- og informasjonssystemer slik at tjenestens leveringsevne ikke forstyrres.[196]

Sikkerhetsloven fremmer sikkerhetstiltak på generell basis for virksomheter hvor deres funksjon er av betydning for nasjonale sikkerhetsinteresser. En sektorovergripende lov er derfor av høy relevans, selv om mange sektorer ofte har egne forskrifter med detaljerte krav til sikkerhet fra før.[197] Tilsvarende krever GDPR at virksomheter skal vurdere risiko for brudd på konfidensialitet, integritet og tilgjengelighet for persondata, og eventuelt iverksette nødvendige sikkerhetstiltak hvor det er nødvendig.[198]

Kravene i GDPR er funksjonsbaserte, som vil si at for eksempel hvor det i artikkel 32 stilles krav til sikkerhet ved behandlingen, er logging en grunnleggende forutsetning for å oppfylle kravene til personopplysningssikkerhet selv om dette ikke er nevnt i bestemmelsen.[199]

Datatilsynet har i flere tilsynssaker pekt på at det mangler en sikkerhetslogg, og at dette kan regnes som et brudd på GDPR. For eksempel i Østre Toten-saken fra 2021 konkluderte Datatilsynet med at det forelå "store og grunnleggende" mangler i personopplysningssikkerheten. Saken dreide seg om en kommune i Norge som ble rammet av et alvorlig dataangrep som resulterte i at kommunens data var blitt kryptert, og sikkerhetskopier med slettet.[200] Manglene besto av enkle konfigureringer som gjorde at mye intern trafikk aldri ble logget og at viktige hendelser ikke ble registrert. Kommunen fikk overtredelsesgebyr på 4

[194] Gulbrandsen, H. P., & Moe, O. M. (2024). Lov, logging, lagring og lengde – Logging som sikkerhetstiltak etter GDPR. Lov&Data
[195] Prop. 109 LS (2022–2023) s. 9-10
[196] Prop. 109 LS (2022–2023) s. 9-10
[197] Prop. 109 LS (2022-2023) s. 21-22
[198] GDPR fortalepunkt 84
[199] Gulbrandsen, H. P., & Moe, O. M. (2024). Lov, logging, lagring og lengde – Logging som sikkerhetstiltak etter GDPR. Lov&Data
[200] Datatilsynet. (2022). *Overtredelsesgebyr til Østre Toten kommune*

millioner norske kroner, og et pålegg om å implementere et styringssystem for informasjonssikkerhet. Saken er et klart eksempel på at datasikkerhetstiltak også er en forutsetning for at personvernet skal kunne ivaretas.[201]

Spørsmålet er om det foreligger en balanse mellom hensynene. Generelt sett kan det konkluderes med at det er en harmoni mellom sikkerhetstiltakskravene i norsk rett. Det som kreves for å sikre kritiske enheter overlapper i stor grad med det som kreves for å sikre personopplysninger. Et tiltak som for eksempel sikkerhetskopiering verner om både kontinuitet i tjenestene og personverninteressene.

Derimot foreligger det noen forskjeller som må bemerkes. Sikkerhetsloven har mer vekt på tilgjengelighet av tjenester, mens GDPR på sin side fokuserer på konfidensialitet av opplysninger. I Østre Toten-saken ble både tilgang til tjeneste og konfidensialitet rammet. Når virksomheter etterlever strenge krav i et regime, oppfylles som regel også minimumskrav i andre regimer. For eksempel vil etterlevelse av sikkerhetslovens prinsipper om sikkerhetsovervåkning normalt sikre at også GDPR artikkel 32 om sikkerhetsnivå er oppfylt.[202] Regelverkene kan derfor regnes å heller komplementere hverandre fremfor å være motstridende.

4.3.3 Rapportering av hendelser

Sikkerhetsloven innfører en plikt for virksomheter omfattet av loven til å varsle myndighetene om alvorlige sikkerhetshendelser.[203] Loven krever at varslingen skal skje "straks", noe som samsvarer med NIS2-direktivets krav om varsling "uten ugrunnet opphold". Terskelen for vurdering av hvilke hendelser som kan anses å kunne ha "betydelig innvirkning" eller "ikke ubetydelig risiko" for nasjonale sikkerhetsinteresser anses å vurderes etter antall berørte brukere, geografisk omfang og potensiell skade[204] og varslingsplikten utløses kun ved hendelser som faktisk påvirker tjenestekontinuiteten.

GDPR har en noe annerledes ordning. Ved brudd på personopplysningsloven skal behandlingsansvarlig melde fra til Datatilsynet innen 72 timer dersom bruddet kan medføre risiko for de registrertes rettigheter, jf. art. 33. I alvorlige tilfeller skal også de registrerte varsles i henhold til artikkel 34. Plikten omfatter enhver personvernrelevant hendelse, uansett om virksomheten er samfunnskritisk eller ikke. Det vil si at en hendelse kan utløse varselsplikt til både Datatilsynet og NSM. Et dataangrep på en samfunnskritisk virksomhet som forstyrrer tjenesteleveransen, men også medfører lekkasje av persondata, krever rapportering til både NSM og Datatilsynet. Det er derfor signalisert et behov for samarbeid for myndighetene.[205]

Det er verdt å bemerke at det ikke er helt likt i de to regelverkene når det gjelder hva som utløser varslingsplikten. Varslingsplikt i henhold til sikkerhetsloven fokuserer på tjenesteutfallet og hvilken påvirkning skade vil ha på samfunnsfunksjonen, mens GDPR fokuserer på hvorvidt personopplysninger er

[201] Datatilsynet. (2022). *Overtredelsesgebyr til Østre Toten kommune*
[202] Gulbrandsen, H. P., & Moe, O. M. (2024). Lov, logging, lagring og lengde – Logging som sikkerhetstiltak etter GDPR. Lov&Data
[203] Sikkerhetsloven § 4-5
[204] Prop. 109 LS (2022-2023) s. 9-10
[205] Prop. 109 LS (2022-2023) s. 9-10

kompromittert. Det vil finnes hendelser derimot hvor kun én varslingsplikt utløses, og det er dersom det foreligger en driftsforstyrrelse uten at persondata kommer på avveie. I dette tilfellet skal kun NSM varsles, og tilsvarende med et motsatt tilfelle. I et slikt motsatt tilfelle er det presisert i NIS-regelverket at det ikke skal varsles til NSM dersom hendelsen ikke har betydning for tjenesteleveransen. I sikkerhetsloven kan tilsvarende tolkes av § 4-5.[206] På denne måten unngås dobbeltarbeid, og det forsøkes å sikre et godt samarbeid mellom sektorene for å unngå motstridende råd og dobbeltbyrde for virksomhetene.[207]

4.3.4 Informasjonsdeling

Deling av informasjon om trusler og hendelser er sentralt for digital sikkerhet, men kan også innebære overføring av personopplysninger. Sikkerhetsloven legger til rette for både nasjonal og internasjonal deling av informasjon. NSM som nasjonal sikkerhetsmyndighet har en sentral rolle i en slik informasjonsdeling. GDPR på sin side tillater informasjonsdeling bare når det finnes et gyldig behandlingsgrunnlag og formålet er forenlig med opprinnelig formål. Deling av personopplysninger om enkeltpersoner krever normalt samtykke eller annet grunnlag, men i sikkerhetskontekst er det oftest uaktuelt å dele tekniske data som logging, for formålet informasjons- og systemsikkerhet.

I GDPR sin fortale anerkjennes det at behandling av personopplysninger som er strengt nødvendig og forholdsmessig for å sikre nettverks- og informasjonssikkerhet anses å være i den behandlingsansvarliges berettigedes interesse.[208] Med andre ord er deling av data for å forebygge eller oppdage cyberangrep klassifisert som en "legitim interesse" i henhold til artikkel 6 nr. 1 bokstav f, så fremt nødvendighets- og proporsjonalitetsprinsippet ivaretas. I et tilfelle hvor en lov pålegger deling av personopplysninger, for eksempel dersom NSM pålegger utlevering av visse data, vil hjemmelen være en rettslig forpliktelse i henhold til GDPR artikkel 6 nr. 1 bokstav c, som tillater utlevering uten samtykke. Det er derfor sjeldent et absolutt forbud mot å dele relevant sikkerhetsinformasjon grunnet personvern, men GDPR krever at man deler målrettet og i begrenset omfang. Dette reflekteres i kravene om dataminimering og formålsbegrensning: man bør kun dele de opplysninger som er nødvendig for formålet.

Et praktisk spørsmål kan være om data som samles inn for sikkerhetsformål senere kan brukes til andre formål eller deles med eksempelvis politi. Her setter GDPR klare grenser. Opplysninger som er samlet inn for et bestemt formål bør ikke brukes til uvedkommende formål uten nytt grunnlag, men dersom det avdekkes straffbare forhold vil unntak i personvernregelverket åpne for å dele med politi. Dette fremgår ikke direkte av personopplysningsloven eller sikkerhetsloven, men det er påpekt av Advokatforeningen i høringen at digitalsikkerhetsloven bør tillate behandling av opplysninger om lovovertredelser.[209] Det fremgår klart at regelverkene forsøkes samordnet slik at nødvendig deling og bruk av data for sikkerhetshensyn er lovlig, men uten å gi åpning for ubegrenset overvåkning.

[206] Prop. 109 LS (20233-2023) s. 9
[207] Prop. 109 LS (20233-2023) s. 9
[208] GDPR fortalepunkt 49
[209] Prop. 109 LS (2022–2023) s. 31

4.3.5 Kontroll og tilsyn

På tilsynssiden har Norge to tydelige aktører: Nasjonal sikkerhetsmyndighet (NSM) for sikkerhetsloven og Datatilsynet for personopplysningsloven og GDPR. Både NSM og Datatilsynet fører tilsyn med hvert sitt regelverk, men kan komme til å føre tilsyn med de samme virksomhetene, men med ulike fokusområder. NSM kontrollerer om en virksomhet oppfyller krav til risikostyring, sikkerhetstiltak, osv., og kan kreve at det utleveres informasjon, og gjennomføre sikkerhetsrevisjoner.

NIS2 artikkel 29 pålegger at tilsynsmyndigheten skal ha tilgang til informasjon som behøves for å gjennomføre gjennomgang av sikkerhetstiltak hos virksomheter. Sikkerhetsloven gir tilsynsmyndighetene adgang til å kreve tilgang til informasjon, informasjonssystemer, objekter og infrastruktur, jf. § 3-4. Sentralt for Norges tilsynsføring er at sektormyndighetene kan bli tildelt tilsynsansvar. En slik tildeling skjer dog i samarbeid med NSM og forutsetter at sektormyndigheten har nødvendig kompetanse for gjennomføring av tilsyn.[210]

Under NIS2-direktivet åpnes det for at tilsynsmyndighetene kan ilegge virksomheter administrativt gebyr ved alvorlige overtredelser, som igjen kan ses parallelt med GDPR. I Sikkerhetsloven har tilsynsmyndighetene adgang til å pålegge virksomheter overtredelsesgebyr ved overtredelse av enkelte bestemmelser i loven, herunder blant annet §§ 4-3 til 4-5.

Datatilsynet fører aktivt tilsyn etter GDPR, og har ilagt en rekke overtredelsesgebyrer for manglende informasjonssikkerhet. Som illustrert i Østre Toten-saken har Datatilsynet grepet inn og ilagt overtredelsesgebyr for manglende informasjonssikkerhet. Datatilsynet har kompetanse til å gi pålegg om retting, midlertidig forbud og bøter. Kompetansen følger av kapittel 8 i GDPR, og vilkårene for overtredelsesgebyr følger av artikkel 83.

Ideelt sett skal tilsynsmyndighetene utfylle hverandre. NSM og Datatilsynet har ifølge årsrapporten fra 2023 etablert et samarbeid, og fremhever at en god dialog er viktig når det finnes overlappende ansvarsområder.[211] NIS2-direktivet legger opp til at man skal unngå dobbeltregulering og motstrid, og det fremgår at høringsrunden til den nye digitalsikkerhetsloven, et mål om å unngå "dublerende og motstridende" reguleringer.[212]

Et konkret tiltak er at den nye Digitalsikkerhetsloven inneholder en bestemmelse som adresserer forholdet til andre lover som stiller krav om sikkerhet og varsling. Bestemmelsen uttaler at "kravene om sikkerhet og varsling som følger av lovens §§ 7, 8, 10 og 11 gjelder så langt det ikke er fastsatt tilsvarende eller strengere krav i eller i medhold av annen lov". Strengere sektorlover eller personvernlovgivning vil derfor fortsatt være gjeldende i sine områder.

[210] Nasjonal sikkerhetsmyndighet. (2020). *Sektormyndighet med tilsynsansvar*
[211] Nasjonal sikkerhetsmyndighet. *Årsrapport for 2023 – Nasjonale samarbeidsrelasjoner*
[212] Prop. 109 LS (2022–2023) s. 21-22

4.5 Harmonisk eller konfliktfull tilnærming?

Samlet sett virker norsk rett å forsøke å illustrere et bilde hvor personvern og digital sikkerhet ikke er motpoler, men heller to sider av samme sak. Sikkerhetsloven respekterer GDPR, og GDPR erkjenner viktigheten av tiltak for cybersikkerhet. Regelverkene er i stor grad harmonisert. NSM og Datatilsynet har etablert et samarbeid for overlappende områder og jobber for å bygge et samarbeid mellom hensynene. Likevel foreligger det noen praktiske spenninger som må håndteres nøye i hvert enkelt tilfelle.

Som tidligere diskutert kan det forekomme krysspress for virksomheter hvor det foreligger krav om å både dokumentere mye for sikkerhetsformål, men også å slette mest mulig for personvernformål. Løsningen virker å foreligge i kravet om å gjøre risikobaserte avveininger, nødvendighetsvurderinger og gode interne rutiner som sikrer at sikkerhetstiltak inkluderer et "innebygd" personvern. Det handler om å etablere et helhetlig styringssystem for informasjonssikkerhet og personvern. Dette reflekteres i Østre Toten-saken hvor kommunen ble pålagt å etablere og implementere et styringssystem for informasjonssikkerhet og personopplysningssikkerhet.[213]

Norsk rett har i all hovedsak lyktes i å legge til rette for at hensynene skal gå hånd i hånd. Sikkerhetstiltak som beskytter kritisk infrastruktur bidrar til å beskytte personopplysninger, og strenge krav til personvern styrker cybersikkerheten. Selv om det i visse situasjoner kan oppstå spenninger, som for eksempel med logging og lagring, finnes det noe fleksibilitet og vurderingsskjønn som tillater virksomhetene å ivareta sikkerhetshensyn uten å ofre personvernet.

Med implementeringen av NIS2-direktivet i eksisterende sikkerhetslov og etableringen av en ny digitalsikkerhetslov skjerpes kravene til digital sikkerhet ytterligere, og det vil være enda viktigere med gode rutiner i skjæringsfeltet mellom sikkerhet og personvern. Høringsinstansen har i forarbeidene til den nye digitalsikkerhetsloven etterspurt klare retningslinjer for anvendelse av begge regelsettene samtidig, og det er forventet at NSM og Datatilsynet vil fortsette å sikte på et godt samarbeid og etterleve målet om en gjensidig forsterkende effekt.[214]

Norsk rett har som tilnærming å skape en balanse mellom personvern og digital sikkerhet gjennom samarbeid. I praksis kan det konkluderes med at virksomheter bruker personvernreglenes fleksibilitet i artikkel 6 til å rettferdiggjøre sikkerhetstiltak.

5.0 Innledning til dansk implementering

Som medlemsstat i EU er Danmark direkte underlagt EU-retten, og er dermed forpliktet til å gjennomføre både forordninger og direktiver i nasjonal rett.[215] I motsetning til Norge, som er et EØS-land, har Danmark mindre nasjonalt handlingsrom når det gjelder å tilpasse EU-direktivet til egne forhold. I lys av økende digitale trusler mot kritisk infrastruktur og digital sikkerhet er implementeringen av NIS2-direktivet særlig sentralt. Direktivet stiller som nevnt krav om et høyt felles nivå for cybersikkerhet i hele EU, og for

[213] Datatilsynet (2022) *Vedtak om overtredelsesgebyr og pålegg* s. 2
[214] Prop. 109 LS (2022-2023) s. 21
[215] Folketingets EU-Oplysning, EU-ret i Danmark

Danmark betyr dette at det er avgjørende å beskytte nasjonale interesser og sikre kontinuitet i essensielle og viktige tjenester.

Parallelt har GDPR også en sentral rolle i reguleringen av digital infrastruktur i Danmark. Forordningen er bindende i dansk rett, og gjelder direkte. Forordningen er supplert gjennom databeskyttelsesloven av 2024[216]. GDPR, med navn databeskyttelsesforordningen, er sentral i arbeidet med å beskytte enkeltindividers rettigheter i møte med økt digitalisering, og får derfor stor betydning for virksomheter som behandler mange personopplysninger. Slike virksomheter er ofte samfunnskritiske enheter.

Danmark har per i dag ingen lov som implementerer NIS2-direktivet fullt ut. Gjennom en ny hovedlov med navn "Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau", heretter kalt NIS2-loven, etableres en samlet ramme for cybersikkerhet i offentlig og privat sektor, og innfører tydelige krav til sikkerhetsnivå, hendelseshåndtering og tilsyn. Det forventes at loven skal tre i kraft 1. juli 2025.[217] Loven er planlagt å være sektorovergripende og etablerer en felles ramme.

Det er derimot allerede etablert implementeringslover for enkelte sektorer. For eksempel er energisektoren allerede underlagt egne regler gjennom Lov om styrket beredskap i energisektoren. I lovens formålsbestemmelse uttrykkes det et formål om å fastsette en ramme for motstandsdyktighet i forhold til blant annet teknologiske trusler som kan true eller skade energiforsyningen, jf. § 1. Sentralt i implementeringen er Center for Cybersikkerhed, heretter kalt CFCS. CFCS er Danmarks nasjonale cybersikkerhetsmyndighet, og skal kontrollere tiltak og føre tilsyn med etterlevelse av loven i samarbeid med sektormyndighetene.[218]

Dette kapittelet skal kartlegge hvordan NIS2-direktivet og GDPR er implementert i dansk rett, med særlig fokus på hvordan regelverkene balanserer hensynene til cybersikkerhet og personvern i kritiske samfunnsfunksjoner. Det vil også undersøkes hvordan danske myndigheter som CFCS og Datatilsynet håndhever krav og samarbeider med aktører for å oppnå en god digital sikkerhet samtidig som individets rettigheter respekteres.

5.1 NIS2 i dansk rettsorden

NIS2-direktivet er en del av EUs arbeid for å sikre et høyt felles nivå av cybersikkerhet i medlemsstatene. Direktivet bygger som nevnt videre på NIS1, og utvider både virkeområdet og kravene til sikkerhet. Som et medlemsland av EU, er Danmark forpliktet til å implementere NIS2 i nasjonal rett. Danmark vurderer et mer sammensatt og komplekst trusselbilde nå sammenlignet med noen år tilbake, og da særlig innen cybersikkerhet. Dette fremgår av CFCS sin trusselvurdering fra 2024.[219]

[216] LBKG 2024-03-08 nr 289 *Databeskyttelsesloven*
[217] Ministeriet for Samfundssikkerhed og Beredskab, Lovforslag om cybersikkerhed., LFF 2025-02-06 nr 141 Om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven)
[218] Center for Cybersikkerhed, *Om os*
[219] Center for Cybersikkerhed. (2024). *Cybertruslen mod Danmark 2024*s. 5

Arbeidet med å gjennomføre direktivet har pågått i flere år, og skjer delvis gjennom endringer i eksisterende regelverk, men også gjennom etablering av nye reguleringer.[220] Implementeringen skjer i hovedsak gjennom ny hovedlov som skaper en felles grunnleggende ramme for implementeringen av NIS2 på tvers av omfattende sektorer.[221]

Det følger av forarbeidene til den nye foreslåtte hovedloven, et formål å gjennomføre NIS2-direktivet gjennom en felles hovedlov som omfatter de fleste sektorene som har kritiske samfunnsfunksjoner. På denne måten etableres et felles rettslig rammeverk til fordel for både virksomhetene som omfattes av loven, og for myndighetene som håndhever loven.[222]

Det fremgår likevel av forarbeidene at lovforslaget ikke gjelder for telekommunikasjons-, energi-, og finanssektorene.[223] Dette skyldes at direktivet allerede er implementert ved omfattende sektorspesifikk regulering. For telekommunikasjonssektoren er direktivet implementert gjennom forslag til lov om sikkerhet og beredskap i telesektoren, for energisektoren er det gjennom lov om styrket beredskap i energisektoren, og for finanssektoren er direktivet implementert gjennom lov om finansforetak.

Gjeldende rett gjennomfører NIS1-direktivet gjennom en sektorvis regulering. Da implementeringen av NIS2-direktivet medfører en oppheving av den eksisterende nasjonale gjennomføringen av NIS1-direktivet, vil denne delen av oppgaven ta utgangspunkt implementering av NIS2-direktivet, NIS2-loven og noen av sektorreguleringene.

Ved implementeringen av NIS2 anser Departementet for samfunnssikkerhet og beredskap det som viktig at direktivets krav målrettes og tilpasses de enkelte sektorenes særlige forhold, men også at det i størst mulig grad sikres en enhetlig koordinering på tvers av sektorer for å forhindre at sektorer rammes av motstridende krav.[224] Gjennomføringen av direktivet tar dermed hensyn til at sektoransvarlige myndigheter skal basert på sin kunnskap om forholdene i deres sektor vurdere behovet for en konkret utforming av lovens krav, slik at implementeringen skjer på mest hensiktsmessig måte for den enkelte sektoren.[225]

5.1.1 Sikkerhetstiltak

NIS2-loven § 6 gjennomfører artikkel 21 i direktivet. Bestemmelser stiller opp krav til at vesentlige og viktige enheter skal iverksette sikkerhetstiltak som er "passende, forholdsmessige, tekniske, organisatoriske og operasjonelle" for å håndtere risiko knyttet til sikkerheten i nettverks- og informasjonssystemer. Kravene skal ikke bare forhindre sikkerhetshendelser, men også redusere

[220] Center for Cybersikkerhed. *Implementering av NIS2 i dansk rett*
[221] Center for Cybersikkerhed. *Implementering av NIS2 i dansk rett*
[222] Bemerkninger til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS2-loven) kapittel 2
[223] Bemerkninger til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS2-loven) pkt. 3.1.2
[224] Bemerkninger til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven) pkt. 2.2.1
[225] Bemerkninger til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven) pkt. 2.2.1

konsekvensene for tjenestemottakere og for samfunnet ved eventuelle hendelser, jf. § 6 stk. 1. Det sentrale formålet med bestemmelsen er å sikre operasjonell motstandsdyktighet og tjenestekontinuinet for samfunnskritiske tjenester.[226]

Ordlyden "passende og forholdsmæssige" må tolkes i likhet med tolkningen av NIS2-direktivets artikkel 21 sitt uttrykk "appropriate and proportionate". Tiltakene må stå i rimelig forhold til virksomhetens trusler og mulig skadeomfang av hendelser. Det kan tolkes slik at en mindre virksomhet derfor kan møte kravene med enklere tiltak, mens store og samfunnskritiske enheter må ha mer omfattende sikkerhetstiltak. En slik tolkning samsvarer med forarbeidene til NIS2-loven.[227] Bestemmelsen er i stor grad harmonisert med direktivet og stiller, med likhet som direktivet, opp ti konkrete minimumskrav til sikkerhetstiltakene. Tiltakene skal minimum omfatte blant annet retningslinjer for risikoanalyse og informasjonssikkerhet, hendelseshåndtering, driftskontinuitet, forsyningskjedesikkerhet, utvikling og vedlikehold av systemer, personellsikkerhet, cybersikkerhetsutdannelse og bruk av autentifisering, jf. § 6 stk. 1 nr. 1-10.

Selv om NIS2-loven § 6 i stor grad følger artikkel 21 ordrett, er det likevel lagt opp til en fleksibel implementering hvor det åpnes for sektorvis konkretisering. Dette følger av bestemmelsens tredje ledd som gir ministeren for gjeldende sektor hjemmel til fastsette supplerende regler om tiltak i de enkelte sektorene så fremt det skjer i samråd med ministeren for samfundssikkerhed og beredskab. Formålet med å muliggjøre tilpasninger til enkelte sektorer er å sikre reaksjoner som samsvarer med utviklingen i trusselbildet.[228]

Eksempelvis fremgår det av lov om styrket beredskab i energisektoren § 6 at virksomheter som omfattes av loven skal foreta nødvendig beredskapsplanlegging og gjennomføre passende organisatioriske tiltak for å beskytte leveringen av deres tjenester, og sikre en effektiv gjenopprettelse av deres tjenester ved potensielle hendelser. § 8 pålegger virksomheter som omfattes av loven å foreta nødvendig planlegging og fatte passende tiltak av cybersikker art for å sikre beskyttelsen av nettverks- og informasjonssystemer som brukes til å levere virksomhetens tjenester.

Forarbeidene presiserer at bestemmelsen viderefører gjeldende rett for de virksomhetene kravene gjelder for i henhold til elforsyningsloven, gasforsyningsloven, varmeforsyningsloven og undergrundsloven.[229] Bestemmelsen utvider på samme tid anvendelsesområdet for loven, i henhold til lovens § 2. På denne måten implementerer § 8 sammen med § 6 NIS2-direktivets artikkel 21 i energisektorens reguleringer.

En slik implementering finner sted for finanssektoren også ved lov om finansiel virksomhed. § 333 bokstav a stk. 2 pålegger operatører av finansielle digitale infrastrukturer å fatte passende og forholdsmessige tekniske, operasjonelle og organisatoriske tiltak for å styre risikoen for sikkerhet i nettverks- og informasjonssystemer. Bruk av uttrykk som "passende og forholdsmessige" samsvarer med

[226] Bemerkninger til § 6 i forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven)
[227] Bemærkninger til §6 i forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS2-loven)
[228] Bemærkninger til forslag til lov om foranstaltninger til sikring af et højt (NIS 2-loven) pkt. 3.2.3
[229] Bemærkninger til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven) pkt. 2.4

uttrykkene som benyttes i direktivet. I bestemmelsens stk. 3 fremgår en uttømmende liste som samsvarer med direktivet, og som tilpasses sektoren ved henvisninger til utdypende bestemmelser.[230]

5.1.2 Rapportering av hendelser

Det følger av NIS2-loven § 12, stk. 1 en hovedregel om at vesentlige og viktige enheter er pliktet til å rapportere til den kompetente myndigheten, samt til Computer Security Incident Response Team (CSIRT), ved enhver vesentlige hendelse. I Danmark er Center for Cybersikkerhed utnevnt som CSIRT.[231] Det følger av bestemmelsen at varslingen må inneholde informasjon som gjør det mulig å vurdere grenseoverskridende virkninger av hendelsen.

Ordlyden uttrykker en "plikt" til å rapportere, og det åpnes dermed ikke opp for en skjønnsmessig adgang. Av stk. 2 følger det en definisjon av hva som kan betegnes som en "væsentlig hændelse". Hendelse kan defineres som vesentlig etter to alternative vilkår: hendelsen 1) har eller kan forårsake driftsforstyrrelser eller økonomiske tap for enheten, eller 2) påvirket eller kan påvirke andre fysiske eller juridiske personer, ved å forårsake betydelig skade, fysisk eller ikke-fysisk. Det er altså nok at ett av vilkårene er oppfylt for at en hendelse skal anses som vesentlig. Stk. 3 presiserer at ministeren etter diskusjon med beredskapsministeren kan fastsette nærmere regler om en hendelse anses som vesentlig. Dette åpner for at sektorer selv kan komme med presiseringer eller utdypninger.

I § 13 i NIS2-loven spesifiseres hvordan og når varsling i henhold til § 12 skal skje. I henhold til bestemmelsen skal en tidlig varsling om en vesentlig hendelse som mistenkes å være forårsaket av ulovlige eller ondsinnede handlinger eller kunne hatt en grenseoverskridende virkning, uten unødig opphold, og senest innen 24 timer etter at enheten har fått kunnskap om hendelsen, jf. § 13 nr. 1. Videre stilles det krav om en supplerende oppdatering til den tidlige varselen uten unødig opphold, og senest innen 72 timer etter at enheten ble kjent med hendelser, jf. § 13 nr. 2. En foreløpig rapport skal sendes til CSIRT, og en endelig rapport som inneholder en detaljert beskrivelse av hendelsen, hvilken type trussel eller grunnleggende årsak som mest sannsynlig har utløst hendelsen, foreliggende tiltak og eventuelle konsekvenser av hendelsen må rapporteres innen én måned etter hendelsen.

Bestemmelsene etablerer et trinnvis og tidsstyrt rapporteringssystem for vesentlige hendelser. Rapportering fremgår av bestemmelsene som pliktig, og er hensiktsmessig for grundig etterdokumentasjon. Loven gir også tydelig adgang for supplerende sektorregulering. I Lov om styrket beredskab i energisektoren fremgår det av § 12 at Klima-, energi-, og forsyningsministeren kan fastsette regler om underretning og innrapportering av hendelser og vesentlige cybertrusler.[232] Formålet med bestemmelsen er å gi hjemmel til ministeren til å fastsette de nødvendige reglene som varsling og rapportering av hendelser.[233] I samsvar med NIS2-direktivet kan den danske implementeringen tolkes å

[230] LBKG 2024-08-21 nr 1013 Lov om finansiel virksomhed § 333
[231] Center for Cybersikkerhed, *Om os*
[232] L 2025-03-06 nr 258 Styrket beredskab i energisektoren § 12
[233] L 2025-03-06 nr 258 Styrket beredskab i energisektoren, *Lovkommentar nr. 133 til §12*

fremme tidlig varsling. Den danske loven gjenspeiler artikkel 23 i både struktur, ordlyd og innhold, og følger direktivet tett.[234]

5.1.3 Informasjonsdeling

Effektiv cybersikkerhet forutsetter som tidligere belyst en velfungerende infrastruktur for samarbeid og informasjonsdeling på tvers av sektorer og enheter. NIS2-direktivet fremmer informasjonsdeling og samarbeid som et sentralt formål, og noe som belyses i direktivets artikkel 29.

Tilsvarende NIS2-direktivets artikkel 29 som tilrettelegger for frivillig informasjonsdeling mellom samfunnskritiske enheter regulerer NIS2-loven § 19 frivillig informasjonsdeling i dansk rett.[235] § 19 stk. 1 uttaler at CSIRT'en tilrettelegger for at det på frivillig basis kan skje en utveksling av opplysninger mellom enheter i cybersikkerhetsfellesskaper, herunder fellesskaper på europeisk nivå. I henhold til bestemmelsen plasseres ansvaret for å fasilitere informasjonsdeling hos CSIRT. På lik linje som direktivet, presiseres det også i loven at deltakelse i informasjonsdelingen er valgfritt. Det foreligger altså ingen plikt for deling av informasjon, men det foreligger en plikt for CSIRT å legge til rette for at enheter har mulighet til å dele informasjon.

§ 19, stk. 2 pålegger essensielle og viktige enheter å informere myndighetene dersom de inngår i eller trekker seg ut av et slikt frivillig fellesskap. En slik informasjonsplikt gir en oversikt over hvem som er del av en struktur hvor det frivillig deles slik informasjon. Lovens ordlyd viser også at informasjonsdeling ikke er begrenset til samfunnskritiske enheter som omfattes av loven, § 19 stk. 3 åpner for at også offentlige og private enheter som faller utenfor lovens anvendelsesområde kan ta del i slike fellesskap.

I forarbeidene opplyses det om tre ulike samarbeidsforum hvor medlemsstatene er representert. Det første forumet er "Samarbejdsgruppen" som hovedsakelig består av representanter fra medlemsstatene, Europeiske kommisjon og ENISA.[236] Gruppen fokuserer på strategisk samarbeid om et høyt cybersikkerhetsnivå i EU og utveksling av opplysninger mellom medlemsstatene. Det andre forumet CSIRT-nettverket som består av representanter for medlemsstatenes cybersikkerhetssenter/håndteringsteam. Det tredje forumet er et europeisk nettverk av forbindelsesorganisasjoner for cyberkriser.[237]

Det fremgår tydelig av den danske implementeringen at et inkluderende og helhetlig cybersikkerhetsmiljø er et mål som fremmes, noe som samsvarer med prinsippet om delt ansvar og samarbeid. Dansk rett virker å være fullt ut harmonisert med artikkel 29 i direktivet, hvor det også fremgår en oppmuntring til samarbeid i cybersikkerhetsfellesskapet.

---

[234] Bemærkninger til §13 i forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS2-loven)
[235] LFF 2025-02-06 nr 141 *Om foranstaltninger til sikring af et højt cybersikkerhedsniveau* (NIS 2-loven) § 19
[236] Bemerkninger til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven) pkt. 2.2.3
[237] Bemerkninger til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven) pkt. 2.2.3

5.1.4 Kontroll og tilsyn

For at implementeringen av direktivet skal være effektivt forutsetter det et godt system for tilsyn og håndhevelse. I direktivets artikkel 32 stilles det krav om at medlemsstatene skal sikre at tilsynet med essensielle enheter er effektivt, forholdsmessig og virkningsfullt. I NIS2-loven §§ 20 og 21 gjennomføres artikkelen. Samlet fastsetter de to bestemmelsene den institusjonelle rammen og de operative virkemidlene for kontroll og tilsyn med cybersikkerheten i samfunnskritiske enheter.[238]

§ 20 regulerer hvordan myndighetsansvaret for tilsyn fordeles. I henhold til bestemmelsens stk. 1 er det ministeren for samfundssikkerhed og beredskab som etter forhandling med vedkommende sektorminister fastsetter hvilken myndighet som skal være kompetent innenfor en sektor. Bestemmelsen sikrer at sektorspesifikke hensyn ivaretas gjennom desentralisert tilsyn. Bestemmelsen viderefører også prinsippet om operasjonell uavhengighet i tilsynsarbeidet, særlig hvor det er relevant med å føre tilsyn med egen forvaltning.

Etter § 20, stk. 2 kan ministeren fastsette at tilsyn med Ministeriet for Samfundssikkerhed og Beredskap skal overlates til en annen myndighet for å unngå inhabilitet. Stk. 3 i bestemmelsen åpner for at det kan fastsettes regler om koordinering, ansvarsfordeling og informasjonsutveksling mellom kompetente myndigheter og CSIRT-enheten.

§ 21 i NIS2-loven fastsetter hvilke virkemidler de kompetente myndigheter har i tilsynsarbeidet. Bestemmelsen gjelder spesifikt for vesentlige enheter. I stk. 1 gis myndighetene en rekke kontrollverktøy som omfatter kontroll på stedet, sikkerhetsrevisjoner, sikkerhetsskanninger og krav om utlevering av informasjon og dokumentasjon. Myndigheten må spesifisere formålet med informasjonsinnhentingen, og angi hvordan og i hvilken form dataene skal overleveres, jf. § 21 stk. 2. Direktivets artikkel 32 stiller krav om at medlemsstatene må føre tilsyn som inneholder slike handlinger som er nevnt i § 21. Den danske loven speiler dermed direktivets krav, og det fremgår av forarbeidene at bestemmelsene er utformet med hensikt om at tilsynsformen skal tilpasses samfunnskritikaliteten.[239]

Tilsynsbestemmelsene i NIS2-loven gir et godt bilde av hvordan dansk rett balanserer behovet for håndheving av cybersikkerhet med hensynet til virksomhetenes rettssikkerhet og forutsigbarhet. Samtidig sikres det ved § 20 en klar myndighetsstruktur for oppfølgning og håndheving i hver sektor.[240] Den danske implementeringen fremstår derfor som harmonisert med direktivets artikkel 32.

5.2 GDPR i dansk rett

GDPR er som tidligere nevnt den mest sentrale rettsakten på EU-nivå for vern av personopplysninger. I Danmark gjelder forordningen direkte, da den etter ikrafttredelse ble en bindende rettskilde i alle

[238] LFF 2025-02-06 nr 141 Om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven) §§ 20 og 21

[239] Bemerkninger til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven) pkt. 2.2

[240] Center for cybersikkerhed. *Tilsyn og vejledning varetages af de sektoransvarlige myndigheder*

medlemslandene uten behov for transformasjon.[241] I Danmark er det likevel vedtatt en supplerende lov som trådte i kraft samtidig med forordningen. Databeskyttelsesloven opprettholder og fastsetter supplerende nasjonale bestemmelser om behandling av personopplysninger innenfor de nasjonale valgmulighetene som forordningen gir mulighet for. [242] Personvernet i Danmark bygger også på grunnleggende rettigheter etter EMRK artikkel 8 som uttaler at enhver har rett til beskyttelse av personopplysninger som gjelder vedkommende. Det er denne grunnleggende rettigheten som danner det rettslige rammeverket for personvern i EU.

I forordningen fremgår det at formålet er å sikre et høyt nivå av beskyttelse av grunnleggende rettigheter for fysiske personer.[243] Den danske databeskyttelsesloven skal bidra til å gjennomføre og utfylle forordningen med danske tilpasninger.[244] I Danmark heter også tilsynsmyndigheten Datatilsynet. Datatilsynet fører kontroll med at forordningen og loven etterleves i offentlig og privat sektor, jf. databeskyttelsesloven § 26 og GDPR artikkel 51. Tilsynet har myndighet til å føre kontroll, gi pålegg og ilegge sanksjoner.

I motsetning til et direktiv som krever nasjonal gjennomføring, er GDPR direkte anvendelig, som tidligere illustrert i denne oppgaven. Den danske lovgiver har likevel benyttet seg av flere av de åpne bestemmelsene i forordningen til å konkretisere noen tilpasninger, særlig på området som omfatter behandling av personopplysninger i arbeidsforhold og barns samtykke.[245]

5.3 Balanse i dansk rett

Danmark har vedtatt en ny lovgivning for å implementere NIS2-direktivet, som skal styrke cybersikkerheten i kritiske samfunnsfunksjoner. NIS2-loven trer i kraft i juli i 2025, og fastsetter krav til beredskap og sikkerhetstiltak. NIS2-loven omfatter flertallet av sektorer som direktivet dekker, blant annet transport og helse. De sektorene som ikke omfattes av loven har allerede omfattende sektorspesifikke reguleringer av cybersikkerheten som tilfredsstiller kravene som følger av direktivet, jf. § 1, stk. 2.

Blant annet følger det av lov om styrket beredskab i energisektoren et formål om motstandsdyktighet og beredskap i forhold til teknologiske trusler, jf. § 1. Telesektoren implementerer kravene som følger av direktivet ved lov om sikkerhed og beredskab i telesektoren, og tilsvarende gjør finanssektoren gjennom lov om finansiel virksomhed.[246] NIS2-loven sammen med sektorlovene utgjør grunnlaget for Danmarks rammeverk for cybersikkerhet. En sentral utfordring i denne sammenhengen er hvorvidt balansen mellom digital sikkerhet og personvern ivaretas. I denne delen av oppgaven vil det belyses hvordan lovgivningen søker å styrke cybersikkerheten samtidig som den balanserer respekt for personvernprinsippene.

---

[241] Traktaten om Den europeiske unions virkemåte, Artikkel 288
[242] LBKG 2024-03-08 nr 289 Databeskyttelsesloven. *Lovkommentar*. Cristina Angela Gulisano, direktør, Datatilsynet.*
[243] GDPR artikkel 1
[244] LBKG 2024-03-08 nr 289 Databeskyttelsesloven. *Lovkommentar*. Cristina Angela Gulisano, direktør, Datatilsynet.*
[245] LBKG 2024-03-08 nr 289 Databeskyttelsesloven
[246] Bemerkninger til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven) Kapittel 1 Indledning

5.3.1 Krav til sikkerhetstiltak

NIS2-loven pålegger samfunnskritiske virksomheter å gjennomføre en rekke sikkerhetstiltak for å håndtere cyberrisiko. Dette inkluderer blant annet utarbeidelse av risikoanalyser og innføring av retningslinjer for sikkerhet, tiltak for hendelses forebygging og deteksjon og beredskapsplaner. Formålet er å øke motstandsdyktigheten mot cyberangrep og sikkerhetshendelser. Disse tiltakene er i posisjon til å på samme tid behandle personopplysninger, for eksempel ved logging av hendelser og aktiviteter.

For å sikre en god balanse mellom hensynet om digital sikkerhet og personvern må derfor tiltakene gjennomføres i tråd med GDPR og den danske databeskyttelsesloven. I NIS2-lovens forarbeider uttrykkes behovet for balanse uttrykkelig.[247] Med andre ord gir ikke NIS2-tiltak virksomheten fritak fra å følge personvernprinsippene, men heller stiller krav til at tiltakene utarbeides på en måte som ivaretar konfidensialitet, lovlighet og dataminimering.

I januar 2024 ble et dansk selskap, som utviklet den digitale postløsningen mit.dk, anmeldt grunnet utilstrekkelig sikkerhetsnivå på deres systemer. Mangelen på et godt sikkerhetsnivå medførte at flere brukere fikk uberettiget tilgang til andre brukeres digitale post, noe som inkluderte sensitive personopplysninger og fortrolig informasjon. Det ble påpekt av Datatilsynet at det forelå mangel på risikovurderingen og utilstrekkelig testing som kunne avdekket feilen. Mit.dk som håndterer nasjonal digital post regnes som en kritisk digital samfunnsfunksjon, og saken er derfor relevant i lys av kravene som følger av NIS2.[248]

Samtidig kan NIS2-kravene vurderes å forsterke de pliktene som allerede følger av personvernreglene. GDPR artikkel 32 pålegger behandlingsansvarlige å treffe tekniske og organisatoriske sikkerhetstiltak for å beskytte personopplysninger. NIS2 konkretiserer slike krav for kritiske sektorer ved å stille krav til strengere tilsyn uten at dette naturligvis skaper motstrid. I praksis vil etterlevelse av NIS2 ofte bidra til bedre personvernsikkerhet, og motsatt.[249]

Det kan likevel oppstå spenninger. For eksempel krever sikkerhetsstyring omfattende logging av systembruk og hendelser for å kunne avdekke angrep og hendelser. Slike logger kan inneholde personopplysninger som for eksempel IP-adresser. Dette utløser automatisk kravet om dataminimering i henhold til GDPR artikkel 5 stk. 1 bokstav c. I lys av denne bestemmelsen understreker Datatilsynet at logger skal begrenses og slettes når de ikke lenger er nødvendige.[250]

NIS2-loven åpner for å pålegge sikkerhetslogging, men da påkreves virksomhetene å sikre at opplysningene kun brukes til legitime sikkerhetsformål og oppbevares i en tidsbegrenset periode. Datatilsynet anbefaler i den sammenheng at det fastsettes lagringstider ut fra formålet, og at sletting skjer

[247] Bemerkninger til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven) Kapittel 4 Forholdet til databeskyttelsesreglerne
[248] Datatilsynet. (2024) Politianmeldelse. *Netcompany indstilles til bøde*
[249] Forsvarsministeriet. Høring over udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau. Datatilsynet sine bemerkninger s. 2-5
[250] Datatilsynet. (2023) *Foranstaltning: Logning af brugernes anvendelser af personoplysninger*

automatisk etter et visst antall måneder for å forhindre at personopplysninger oppbevares lenger enn nødvendig.[251] Regelverket kan på denne måten vurderes å forsøke å etablere en balanse ved å både sikre gode sikkerhetstiltak, men også gjennomføre strenge prosedyrer for dataminimering og sletting.

5.3.2 Rapportering av hendelser

Rapportering av hendelser er en viktig del av NIS2. Virksomheter som er underlagt loven plikter å varsle myndighetene om vesentlige cybersikkerhetshendelser innen gitte frister. Det stilles opp en prosess som består av to trinn: tidlig varsling og en utfyllende rapport. Formålet er å sikre at myndighetene har en god oversikt over situasjonen og at det raskt kan gis informasjon til andre potensielt berørte enheter. NIS2-loven viderefører disse kravene til rapportering av vesentlige hendelser, men åpner også for at enheter som ikke omfattes av lovens anvendelsesområde kan rapportere til CSIRT om hendelser og cybertrusler.

Kravene som stilles til innholdet i hendelsesrapporteringen er at virksomhetene må dele relevante detaljer om hendelsen, dens årsak, påvirkede systemer og hvilke tiltak som er gjort. Slike rapporter kan inkludere personopplysninger. I en slik situasjon er behandlingen av personopplysninger lovlig fordi den anses som nødvendig for å oppfylle en rettslig forpliktelse etter NIS2-loven, jf. GDPR artikkel 6 nr. 1 bokstav c. I lovforarbeidene uttaler Datatilsynet et behov for en delt plattform for rapportering. Rapportering av sikkerhetshendelser skjer i dag på en digital plattform som kalles Virk.dk. Via denne plattformen kan både sikkerhetshendelser, men også brudd på persondatasikkerhet rapporteres inn.[252] Dersom rapportering av brudd på både NIS2 og GDPR kan rapporteres ved en innsending, vil en virksomhet kunne oppfylle plikten sin på en effektiv måte. På denne måten reduseres dobbeltarbeid, og samarbeid mellom myndighetene fremmes.

5.3.3 Informasjonsdeling og samarbeid

På lik linje som direktivet, oppfordrer NIS2-loven informasjonsdeling på tvers av enheter. Dette kan innebære informasjonsdeling internt i sektorer, men også mellom ulike sektorer, på både nasjonalt nivå og EU-nivå. I Danmark legger NIS2-loven til rette for at myndighetene kan motta, analysere og dele informasjon om trusler og hendelser videre, jf. § 19. På samme tid utløser dette et ansvar for å sikre at informasjonsdelingen ikke inneholder ulovlig deling av personopplysninger.

NIS2-lovens forarbeider presiserer at ordninger for informasjon deles må etableres i overensstemmelse med personvernretten. Bestemmelsen som er innført i dansk rett er uten innholdsmessige endringer av direktivet, og det presiseres i forarbeidene at bestemmelsen skal anvendes i overensstemmelse med direktivets forutsetninger. GDPRs prinsipper må i lys av slik informasjon likevel vektlegges. Ved deling av informasjon kan anonymisering eller pseudonymisering være et mulig alternativ for å beskytte personopplysninger. I all hovedsak foreligger det et fokus på at opplysninger av relevans for cybersikkerhet skal deles, men personopplysninger skal parallelt beskyttes så lenge det er mulig.[253]

---

[251] Datatilsynet. (2023) *Foranstaltning: Logning af brugernes anvendelser af personoplysninger*
[252] Datatilsynet.dk. *Anmeld brud på persondatasikkerheden* og Center for cybersikkerhed. *Underretning til CFCS*
[253] Bemerkninger til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven) pkt. 4 om Forholdet til databeskyttelsesreglerne

Oppsummert legger NIS2-loven opp til en omfattende informasjonsdeling for å styrke cybersikkerheten, men all deling skal skje konfidensielt og i samsvar med personvernregelverket. Gjennom et samarbeid mellom CFCS og Datatilsynet sikres det at nødvendig informasjon kan deles raskt uten at personopplysninger behøves å kompromitteres. Det understrekes i høringsrunden til NIS2-loven at Datatilsynet og CFCS har et mål om et nært samarbeid for å håndtere tilfeller som faller på grensen mellom cybersikkerhet og personvern.[254]

5.3.4 Kontroll og tilsyn

For å sikre etterlevelse av de nye kravene som følger av direktivet, etablerer NIS2-loven en ordning for tilsyn, kontroll og håndhevelse. Myndighetene gis myndighet til å føre tilsyn med de "vesentlige" og "viktige" enhetene som omfattes av loven. I Danmark er det Ministeriet for Samfundssikkerhed og Beredskab som har det overordnede ansvaret for NIS 2-implementeringen.

Styrelsen for Samfundssikkerhed og Center for Cybersikkerhed hjelper danske myndigheter og virksomheter med å forebygge, imøtegå og beskytte seg mot cyberangrep.[255] CFCS har en nøkkelrolle i dansk rett ved å drive som tilsynsmyndighet på tvers av sektorer. Det fremgår likevel klart av loven at sektormyndighetene skal føre tilsynet i den gjeldende sektor. Enkelte sektorer har egne kompetente myndigheter. Energisektoren på sin side er underlagt tilsyn fra Energistyrelsen, jf. lov om styrket beredskab i energisektoren § 19.[256]

Hvordan tilsynet gjennomføres varierer fra blant annet dokumenttilsyn til inspeksjoner. NIS2-loven gir myndighetene rett til å kreve nødvendig informasjon og dokumenter, samt tilgang til systemer for å verifisere sikkerhetstiltak. Virksomheter kan pålegges å utbedre mangler, og det kan gis pålegg om spesifikke tiltak.

Sentralt er forholdet mellom Datatilsynet og CFCS. Virksomheter kan som allerede nevnt bli underlagt to tilsyn på samme tid. CFCS og sektormyndighetene gjennomfører tilsyn for kravene som følger av NIS2, og Datatilsynet for kravene som følger av GDPR. Begge tilsynsmyndighetene kan gi sanksjoner ved sikkerhetsmangler, noe som kan medføre en potensiell dobbel straffeforfølgning. Dette adresseres i direktivets fortalepunkt 131, hvor det understrekes at pålegg av sanksjoner etter NIS2 ikke skal føre til brudd på prinsippet om å forhindre dobbel straff på samme sak. Dette kan for eksempel skje dersom en virksomhet grunnet mangel på optimal sikkerhet også lider av spredning av personopplysninger. Da vil en hendelse potensielt utløse sanksjoner fra to ulike tilsynsmyndigheter. I forarbeidene presiseres det at dobbel straffeforfølgning er forbudt, og at det derfor er desto viktigere at tilsynsmyndighetene har et godt samarbeid.[257]

---

[254] Forsvarsministeriet. Høring over udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau. Datatilsynet sine bemerkninger s. 2
[255] Ministeriet for Samfundssikkerhed og Beredskab. *Styrelsen for Samfundssikkerhed*
[256] Klima-, Energi- og Forsyningsministeriet. (2025) *Ny lovgivning styrker sikkerheden i energisektoren*
[257] Bemerkninger til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven) pkt. 3.5.2.4 Særligt om brud på persondatasikkerheden

5.4 Harmonisk eller konfliktfull tilnærming?

NIS2-loven endrer ikke virksomheters ansvar for godt personvern. Alle samfunnskritiske enheter må overholde personvernreglene fullt ut, i tillegg til de kravene som følger av NIS2-direktivet. Slik som sett ovenfor virker reguleringene å ofte komplementere hverandre. Ved at begge regelsettene fokuserer på et generelt godt sikkerhetsnivå, vil både hensynet om digital sikkerhet og personvern styrkes. Det er verdt å bemerke at NIS2-loven ikke minsker rettighetene som følger av GDPR. For eksempel gjelder kravet til dataminimering fullt ut selv om NIS2-loven krever logging som et konkret sikkerhetstiltak.

Til tross for intensjon om balanse mellom regelverkene, finnes det enkelte konflikter mellom kravene til digital sikkerhet og personvern som må håndteres. Et godt eksempel er konflikten mellom logging som sikkerhetsformål og prinsippet om dataminimering. Som ledd i NIS2-kravene vil sannsynligvis mange virksomheter måtte øke sin logging av hendelser og nettverkstrafikk for å detektere angrep og analysere sikkerhetshendelser. Dette kan innebære lagring av store datamengder som potensielt kan inneholde personopplysninger. Fra et sikkerhetsperspektiv er det tenkelig at en virksomhet gjerne skulle lagret alt så lenge som mulig. Dette perspektivet krasjer derimot med prinsippet om dataminimering som begrenser lagring og logging til formålets nødvendighet.

Datatilsynet i Danmark har påpekt at loggføring må gjøres målrettet og tidsbegrenset. I sin veiledning fremhever de at automatisk sletting av logging er viktig av hensyn til dataminimering.[258] Hvor lenge logger skal lagres skal vurderes konkret ut fra formålet.[259] Samtidig, for å avdekke langsiktige cyberangrep, anerkjennes behovet for at lagring kan være noe lenger.[260] For eksempel kan trussel-aktører operere i lang tid uten å bli oppdaget, og da kan det være berettiget å beholde logger for å analysere hendelsesforløpet. I et slikt tilfelle må en virksomhet finne en middelvei i sin logging som både tilfredsstiller sikkerhetskravene og personvernkravene.

En annen potensiell konflikt kan være overvåkning av ansatte. NIS2-direktivet kan gjøre at det er nødvendig å implementere overvåkningsverktøy som analyserer ansattes mistenkelige atferd. Slike tiltak må forenes med personvernregler. Datatilsynet har gitt veiledning om at arbeidsgiver må ha saklig grunnlag for overvåkning, og informere de ansatte. [261] NIS2-kravene kan indirekte utgjøre saklig grunn, ved at overvåkingen er gjort av sikkerhetsmessige hensyn. Logging av ansattes handlinger for eksempel er tillatt når formålet er sikkerhet, men det krever at de ansatte får informasjon.

Oppsummert forsøker implementeringen av NIS2 i dansk rett å ivareta balansen mellom digital sikkerhet og personvern gjennom lovkravene, sektorloven og samordning med eksisterende personvernlovgivning. Lovgiver har uttrykt at tiltak etter NIS2-loven skal fattes innenfor rammene som følger av GDPR. Når NIS2-loven trer i kraft vil utarbeidelsen av sektorspesifikke regler og samfunnskritiske enheters standarder følges tett av CFCS og Datatilsynet, slik at motstridende krav kan identifiseres og håndteres.

---

[258] Datatilsynet. (2023) *Foranstaltning: Logning af brugernes anvendelser af personoplysninger*
[259] Datatilsynet. (2023) *Foranstaltning: Logning af brugernes anvendelser af personoplysninger*
[260] Datatilsynet. (2023) *Foranstaltning: Logning af brugernes anvendelser af personoplysninger*
[261] Datatilsynet, (2023) *Kontrol af medarbejdere*, s. 4

6.0 Komparativ analyse

6.1 Innledning

Som tidligere illustrert har både Norge og Danmark iverksatt omfattende tiltak for å gjennomføre EUs NIS2-direktiv og sikre et høyt nivå av cybersikkerhet i samfunnskritiske sektorer. Selv om direktivet er felles for EU- og EØS-land, er det rom for nasjonale tilpasninger og ulik praktisering. Forskjellene mellom norsk og dansk rett gir grunnlag for å gjennomføre en komparativ analyse med mål om å kartlegge juridiske, strukturelle og organisatoriske ulikheter og variasjoner i gjennomføringen og balansen mellom digital sikkerhet og personvern.

Denne delen av oppgaven vil analysere hvordan Norge og Danmark har implementert direktivet i sine rettssystemer, med særlig vekt på forholdet til og balansen med GDPR. Nasjonale tilpasninger vil også bli en sentral del i analysen. Som belyst i metodekapittelet vil følgende spørsmål være sentrale for den komparative analysen:

1. Hvordan skiller implementeringen seg mellom Norge og Danmark?
2. I hvilken grad prioriteres nasjonal sikkerhet i forhold til personvern?
3. Hvordan har myndighetene i hvert land valgt å organisere tilsyn og regulering?
4. Hvilke praktiske konsekvenser kan ubalanse mellom nasjonal sikkerhet og personvern for samfunnskritiske samfunnsfunksjoner medføre?

Som vist i kapittel 4 gir EØS-avtalen Norge et annet utgangspunkt enn land med EU-medlemskap. Norge har et større nasjonalt handlingsrom, men også en plikt til å sikre samsvar med EU-rettens formål. Kapittel 5 har gitt en redegjørelse av Danmarks nasjonale implementering, inkludert NIS2-loven som trer i kraft 1. juli 2025 og relevante sektorlover.
Ved å bygge analysen på de tidligere kapitlenes gjennomgang av regelverk og myndighetsstruktur, og kartlegge hva som følger av forarbeider, sektorlover og veiledere, dannes grunnlaget for en faglig sammenligning. Gjennom en sammenstilling av likheter og ulikheter, samt vurdere rettslige og operative konsekvenser, forsøker analysen å skape en forståelse av hvordan rettssystemene i Norge og Danmark forholder seg til NIS2-direktivet og GDPR og deres samvirkende, med også til tider motstridende bestemmelser.

6.2 Hvordan skiller implementeringen seg mellom Norge og Danmark?

For å sikre en god oversikt over hvordan implementeringen av NIS2-direktivet skiller seg mellom Norge og Danmark er det hensiktsmessig å begynne på regelverksnivå. Norge på sin side har implementert store deler av NIS2-direktivet gjennom allerede eksisterende regelverk. Primært utgjør sikkerhetsloven av 2018 det sentrale regelverket for nasjonal sikkerhet i kritisk infrastruktur, og i den forstand faller digital sikkerhet naturligvis innenfor. Loven ble vedtatt før direktivet, men ble senere endret og tilpasset for å oppfylle de kravene som følger av direktivet. Loven er sektorovergripende, men bygger på et prinsipp om at hvert departement har ansvar for sine sektorer.

Danmark på sin side har implementert NIS2-direktivet gjennom en ny hovedlov med navn NIS2-loven som trer i kraft 1. juli 2025. I motsetning til Norge har Danmark valgt en samlet lovstruktur, men med unntak for enkelte sektorer. Enkelte sektorer er regulert via sektorlover, og direktivet blir implementert fullt ut i disse lovene. Ved å ha én hovedlov synes Danmark å gi uttrykk for et ønske om en samlet og enhetlig lovstruktur for cybersikkerhet på tvers av sektorer. Danmark kombinerer dermed en felles overordnet ramme med sektorspesifikke tilpasninger. Norge har valgt en tilpasningsbasert implementering hvor eksisterende regelverk er videreutviklet for å sikre at kravene i direktivet blir innfridd. Loven er altså sektorovergripende og bygger på at hver sektor har ansvar.

Selv om begge land har høye krav til både digital sikkerhet og personvern, fremgår Danmark som noe "strengere" ettersom kravene som følger av NIS2-direktivet direkte er implementert i en egen lov. Dette kan virke noe mer "samlet" da Norge sin sikkerhetslov ikke begrenser seg til tekniske trusler, men også fysiske.

En annen sentral forskjell i de to rettssystemenes implementering av direktivet er begrepsbruk og terminologi. I sikkerhetsloven benyttes uttrykket "grunnleggende nasjonale funksjoner" og "nasjonale sikkerhetsinteresser" som et begrep for å definere hvilke enheter og virksomheter som omfattes av loven, jf. sikkl. § 1-2. Begrepet "grunnleggende nasjonale funksjoner" har ikke direkte opphav fra direktivet, men knyttes til kritiske samfunnsfunksjoner. Danmark på sin side benytter seg av direktivets begreper direkte oversatt. "Væsentlige og vigtige enheder" viderefører direktivets "essential and important entities", og viser at det ikke har blitt gjort noen tilpasning i begrepsbruken, men heller en videreføring av direktivets ordvalg, jf. NIS2-loven §§ 4 og 5 og NIS2-direktivet artikkel 3. Norge kan vurderes å bruke et språk som er funksjonsbasert ved å henvise til at virksomheten skal ha funksjoner som er grunnleggende for nasjonen. På denne måten tillates virksomhetene selv å vurdere om de faller inn under lovens virkeområde. På Danmark sin side, i likhet med direktivet, listes det opp omfattende enheter og sektorer i lovens bilag 1. En vesentlig forskjell er at NIS2-loven unntar eksplisitt enkelte sektorer i § 1 stk. 2, hvor nevnte sektorer har egne sektorlover som implementerer kravene som følger av direktivet. Oppsummert viser den komparative gjennomgangen at Norge og Danmark har valgt noe ulike tilnærminger til implementeringen av NIS2-direktivet, både når det gjelder regelverksnivå, begrepsbruk og organisering. Norge har videreutviklet et regelverk med funksjonsbasert begrepsbruk, hvor Danmark på sin side har utviklet en ny hovedlov med enhetlig begrepsbruk. Norge har altså en sektorovergripende lov, hvorav Danmark har en felles overordnet ramme, men som ikke gjelder alle sektorer. CFCS på sin side har flere direkte oppgaver, men fører normalt ikke tilsyn direkte. Dette ansvaret ligger hos sektormyndighetene. NSM har et sektorovergripende ansvar, men hver sektormyndighet har mye ansvar og selvstendighet på eget område.

6.3 I hvilken grad prioriteres nasjonal sikkerhet i forhold til personvern?

Et sentralt spørsmål ved implementeringen av NIS2-direktivet er balansen mellom nasjonal sikkerhet og personvern. Både Norge og Danmark har gjennom sin implementering av NIS2-direktivet lagt vekt på at tiltak som gjennomføres for digital sikkerhet må skje innenfor rammene av personvernregelverket. Det betyr at tiltak etter NIS2, som logging, rapportering og informasjonsdeling, må skje på en måte som respekterer kravene til dataminimering, konfidensialitet og formålsbegrensning, jf. GDPR artikkel 5.

Begge landene virker å ha en grunntanke om at nasjonal sikkerhet og personvern ikke nødvendigvis anses som motstridende hensyn, men snarere som områder som må balanseres.

I Norge fremheves det tydelig i forarbeidene til sikkerhetsloven og gjennom veiledning fra Datatilsynet og NSM. Det understreker at tiltak som iverksettes for å styrke digital sikkerhet som logging og overvåkning må begrenses til det nødvendige og også sikre sletting når formålet er oppnådd. Dette viser at personvern ikke blir tilsidesatt, selv om nasjonal sikkerhet er det primære formålet ved lovgivningen. Et viktig moment er at sikkerhetsloven i Norge benytter en funksjonsbasert tilnærming, hvor virksomheter som er vurdert til å ivareta grunnleggende nasjonale funksjoner, underlegges krav og samtidig får ansvar for etterlevelse. På den måten gis det rom for mer skjønn, men samtidig en klar forventning til at virksomhetene selv skal evne å balansere hensynet mellom sikkerhet og personvern i praksis.

I Danmark fremgår det av forarbeidene til NIS2-loven at tiltakene som gjennomføres i medhold av loven skal skje i samsvar med GDPR.[262] CFCS og Datatilsynet har et tett samarbeid for å sikre at cybersikkerhetshensyn og personvernhensyn skal forenes, og dette gjenspeiles klart i Datatilsynets anbefalinger til vedtakelse av NIS2-loven. Selv om CFCS er plassert under Forsvarsministeriet, og dermed organisatorisk er nærmere den nasjonale sikkerhetssektoren, innebærer ikke dette at hensynet til personvern nedprioriteres. Personvernet vurderes også i Danmark som en rettslig forpliktelse som må opprettholdes i gjennomføringen av sikkerhetstiltak. Sammenlignet viser begge rettssystemene en lojalitet til personvernprinsippene, og at nasjonal sikkerhet ikke prioriteres høyere.

Det er viktig å presisere reguleringenes mål. GDPR fokuserer på individets rett til informasjon og varsling ved databrudd, og NIS2 fokuserer på driftssikkerhet av systemer. I forskningsartikler er det satt lys på at dette kan føre til konkurrerende varslingsplikter, og at det kan medføre at virksomheter kan havne i en situasjon hvor en av reguleringene kan bli prioritert fremfor det andre.[263]

Oppsummert kan balansen mellom hensynene til nasjonal sikkerhet og personvern anses å være i høy grad balansert. Både norske og danske myndigheter har lagt vekt på at et nært samarbeid mellom sikkerhetsmyndighetene og Datatilsynet er viktig for å sikre en god balanse, og forhindre situasjoner for et hensyn blir prioritert bunnløst fremfor det andre.

6.4 Hvordan har myndighetene i hvert land valgt å organisere tilsyn og regulering?

Både Norge og Danmark har valgt en modell hvor ansvarlige sektormyndigheter har hovedansvaret for tilsyn innenfor sine sektorer. I begge land er det altså myndigheten som kjenner sektoren best, som også har ansvar for å føre kontroll, tilsyn og sikre at kravene som følger av direktivet overholdes. En slik organisering av tilsyn følger av sikkerhetsloven § 3-1 i Norge, hvor det fremgår at tilsyn normalt utøves av

[262] Bemerkninger til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven) pkt. 4 om Forholdet til databeskyttelsesreglerne

[263] Vostoupal, J., m.fl. (2024). *The legal aspects of cybersecurity vulnerability disclosure*: *To the NIS 2 and beyond* s. 6-9

sektormyndighetene, men at NSM har en sektorovergripende rolle, og kan føre tilsyn dersom det er tvingende nødvendig. Det er altså sektormyndigheter som har ansvaret for å selv føre tilsyn, men NSM skal bidra som en koordinerende myndighet som skal utarbeide og utvikle grunnleggende kriterier for tilsyn etter loven, og legge til rette for en felles opplæring, jf § 3-2 annet ledd.

Danmark har tilsvarende fordelt tilsynsoppgavene til sektormyndigheter. I § 20 i NIS2-loven presiseres at hver sektor får en kompetent myndighet som skal ha tilsynsansvar for dem. CFCS fungerer dermed på lik måte som NSM, altså som en koordinerende myndighet på tvers av sektorene, som bidrar med veiledning, koordinering og vurderinger av trusselbildet. CFCS har altså en tydelig rolle i å sørge for at retningslinjer blir fulgt og at beredskapsnivået på tvers av sektorene er lik. I Norge foreligger dette ansvaret hos hver sektor, men NSM har et sentralt ansvar for å koordinere håndteringen av alvorlige cybertrusler.

Både Norge og Danmark har valgt en modell hvor sektoransvarlige myndigheter skal gjennomføre tilsyn i egne sektorer. NSM og CFCS fungerer begge som koordinerende og veiledende instanser, men NSM kan ved nødvendighet føre tilsyn, mens CFCS fører normalt ikke tilsyn med mindre de er sektormyndighetene i en sektor. Når det gjelder samarbeidet mellom myndighetene for cybersikkerhet og myndighetene for personvern er dette sentralt for å sikre en god balanse mellom nasjonal sikkerhet og personvern. Både Norge og Danmark har etablert former for og uttrykt viktigheten rundt et godt samarbeid mellom myndighetene for cybersikkerhet og datatilsynene.

I Norge har samarbeidet mellom NSM og Datatilsynet vært tett i flere år, og det har tydelig blitt uttrykt at et samarbeid er viktig, særlig når det gjelder tiltak som innebærer datainnsamling, logging eller overvåkning.[264] I Danmark samarbeider CFCS og Datatilsynet på tilsvarende vis om å sikre at tiltakene som implementeres skjer i tråd med GDPR. I arbeidet med forberedelsene til NIS2-loven var det klart en tett dialog mellom CFCS og Datatilsynet for å sikre at kravene til logging, overvåkning og rapportering ikke bryter med personvernprinsippene. At Datatilsynet deltar og uttaler seg i høringsprosesser knyttet til cybersikkerhetslovgivningen gir en klar indikasjon på en direkte involvering for å sikre en god balanse.

Begge land kan med trygghet anerkjennes å vektlegge betydningen av et godt samarbeid mellom sikkerhetsmyndighetene og datatilsynene. I Danmark kan Datatilsynet anses å ha en aktiv deltakelse ved vedtakelsen av den nye NIS2-loven, mens i Norge følger samarbeidet i stor grad av veiledning og oppfølgning. Det er også klart at begge land følger et prinsipp om at man ikke skal straffes dobbelt for en handling. Dette indikerer at begge landene ønsker et godt samarbeid mellom myndighetene for å sikre en effektiv håndheving av kravene til både digital sikkerhet og til personvern. Dette fremgår klart som et mål og en praksis i på EU-nivå også. Ved implementering av plattformer hvor cybertrussel-informasjon kan deles er det også lagt vekt på at det må foreligge en balanse mellom samarbeid om cybersikkerhet og også beskyttelse av persondata.[265]

[264] Datatilsynet. (2024). *Nasjonale samarbeidsrelasjoner – Årsrapport for 2023*., Datatilsynet. (2021). *Nasjonale samarbeidsrelasjoner – Årsrapport for 2020.*
[265] Rajamäki, J., m.fl. (2024). *Implications of GDPR and NIS2 for Cyber Threat Intelligence Exchange in Hospitals* s. 7

Både i Norge og Danmark bærer samarbeidet mellom datatilsynsmyndighetene og cybersikkerhetsmyndighetene preg av et tydelig mål om å forene hensynet til personvern og nasjonal sikkerhet gjennom tett koordinering.

6.5 Hvilke praktiske konsekvenser kan komme av ubalanse mellom nasjonal sikkerhet og personvern?

En ubalanse mellom hensynet til nasjonal sikkerhet og hensynet til personvern kan få betydelige praktiske konsekvenser for samfunnskritiske samfunnsfunksjoner i både Norge og Danmark. Dersom nasjonal sikkerhet gis en prioritet som går på bekostning av personvern, kan dette potensielt svekke tilliten mellom virksomheter, myndigheter og befolkningen. Samfunnskritiske enheter, som energiselskaper, helsesektoren og finansinstitusjoner, er alle avhengig av god tillit til det offentlige for å kunne fungere effektivt. Dersom overvåkning, datainnsamling eller logging gjøres overdrevet eller med mangel på respekt for personvernprinsippene kan dette føre til et svekket omdømme og brudd på grunnleggende menneskerettigheter. I et digitalisert samfunn kan tap av tillit raskt føre til redusert støtte fra samfunnet og et svekket samarbeid mellom det offentlige og næringslivet. Dette igjen kan medføre en mindre effektiv håndtering av sikkerhetstrusler.

På den andre siden kan en ubalanse som prioriterer personvernet på bekostning av nasjonal sikkerhet, føre til at samfunnskritiske enheter blir mer sårbare for cyberangrep. Dersom virksomhetene i frykt for å krenke personvernrettighetene, begrenser sikkerhetsaktiviteter som å samle inn, analysere eller dele nødvendig sikkerhetsinformasjon, kan slike trusler forhindres i å bli oppdaget. Et sikkerhetsbilde som ikke er helt tilstrekkelig kan svekke beredskapen og øke sannsynligheten for at sikkerhetstruende hendelser som kan ha alvorlige konsekvenser for samfunnet som helhet. Særlig ved varsling og deling av informasjon kan balansen utfordres, og organisasjoner kan prioritere å oppfylle sine forpliktelser overfor tilsynsmyndigheten, og potensielt overse sine plikte overfor tjenestemottakere.[266]

Både Norge og Danmark legger stor vekt på å oppnå en balansert regulering som søker å verne både sikkerhet og personvern. Samtidig viser sammenligningen at det stadig må gjennomføres vurderinger ettersom trusselbildet utvikler seg raskt.

Samlet viser analysen at Norge og Danmark, til tross for et felles utgangspunkt i NIS2-direktivet og GDPR, har valgt ulike regulatoriske og organisatoriske løsninger. Begge landene søker aktivt å balansere nasjonal sikkerhet og personvern, men gjennom forskjellige tilnærminger som reflekterer deres rettsbilde.

[266] Koiava, A., (2023) *Legal Aspects of Vulnerability Disclosure: Navigating GDPR and NIS Directive Obligations for Data Protection and Cybersecurity* S. 7-8

7.0 Konklusjon

7.1 Oppsummering av funn

Ved en analyse av hvordan Norge og Danmark har implementert NIS2-direktivet og GDPR i kritiske samfunnsfunksjoner, viser det seg at begge landene er godt på vei i arbeidet for å sikre at hensynene til nasjonal sikkerhet og personvern balanseres. NIS2-direktivet er felles for begge land, men ved nasjonal implementering er tilnærmingene noe ulik.

Norge har i stor grad valgt å implementere NIS2-direktivets krav ved å utvide eksisterende lovgivning. Sikkerhetsloven fra 2008 var i utgangspunktet tilpasset nasjonale behov, men er i senere tid justert for å oppfylle kravene som følger av EU-retten og direktivet. Norge har Nasjonal sikkerhetsmyndighet som en sentral koordinerende rolle, men selve hovedansvaret for implementering og tilsyn ligger hos hver enkelt sektor og deres ansvarlige myndighet. Dette innebærer en frihet og fleksibilitet som tillater hver sektor å implementere kravene som stilles i direktivet, men med rom for skjønn og tilpasning.

Danmark på sin side har implementert kravene som følger av direktivet ved å vedta en ny hovedlov med samme navn som direktivet. Danmark kombinerer en struktur hvor Center for Cybersikkerhed har et overordnet ansvar for å sikre en koordinering og utvikling av klare retningslinjer, med desentraliserte tilsyn gjennomført av sektormyndighetene. Dette sikrer tydelige felles rammer på tvers av sektorene, men tillater sektorvise tilpasninger innenfor en overordnet struktur.

Den komparative analysen viser at begge land tydelig prioriterer å opprettholde en god balanse mellom hensynet til nasjonal sikkerhet og personvern. Begge rettssystemene presiserer at det er viktig å unngå en ubalanse som kan føre til enten invaderende sikkerhetstiltak, eller redusert evne til å håndtere cybertrusler. Et godt samarbeid mellom cybersikkerhetsmyndighetene og datatilsynene fremstår som særlig viktig i begge land for å sikre en god balanse i praksis.

7.2 Betydning for fremtidig regulering

Det fremkommer av analysen flere viktige tanker som lovgiver bør ha i bakhodet før fremtidig regulering. For det første er det klart av analysen at en effektiv implementering av internasjonale reguleringer ikke utelukkende avhenger av bare lovgivningen, men også strukturen av samarbeid og koordinering mellom relevante myndigheter.

En annen sentral lærdom er at et visst nasjonalt handlingsrom er nødvendig for å sikre at implementering av direktiv skal gjennomføres på en effektiv måte som hensiktsmessig passer til det nasjonale rettsbildet. Dersom EU setter krav om en uniform regulering kan dette svekke medlemslandenes evne til å svare på sine utfordringer på en måte som er i tråd med landenes unike behov. Det kan og svekke effektiviteten av tiltak i ulike sektorer, hvor én regulering ikke nødvendigvis passer alle. Analysen viser også at ved å stille minimumskrav til medlemslandene kan det styrke harmoniseringen i unionen, men at det er nødvendig å åpne for sektorvis eller nasjonsvis tilpasning for å sikre at reguleringen er effektiv der den benyttes.

Fremover vil det være avgjørende å fortsette å styrke informasjonsutveksling og felles koordinering mellom myndigheter på tvers av landegrenser. Medlemslandene med ulike tilnærminger kan med god fordel lære av hverandre gjennom et styrket samarbeid. Ved å utveksle erfaringer og dele informasjon kan medlemsland bidra til en felles forståelse av hva som funker i praksis og hvordan ulike styringsmodeller kan håndtere utfordringer innenfor cybersikkerhet og personvern.

Avslutningsvis viser analysen at evnen til å balansere hensynene til nasjonal sikkerhet og personvern i reguleringen av kritiske samfunnsfunksjoner er avgjørende for et motstandsdyktig samfunn i en digitalisert verden. Dersom hendelser gjør skade på digital sikkerhet, kan dette medføre at personopplysninger kommer på avveie, og motsatt.

8.0 Litteraturliste

Rettsakter:

Internasjonale:

Direktiver:

Den europeiske union. (1995). *Direktiv 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*. Den europeiske unions tidende L 281, 23.11.1995, s. 31–50. Hentet 2. mars 2025, fra https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

Europaparlamentet og Rådet. (2022). *Direktiv (EU) 2022/2555 av 14. desember 2022 om tiltak for et høyt felles nivå av cybersikkerhet i Unionen, som endrer forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972, og opphever direktiv (EU) 2016/1148 (NIS 2-direktivet)*. Den europeiske unions tidende, L 333, 27.12.2022, s. 80–152. Hentet 2. mars 2025 https://eur-lex.europa.eu/eli/dir/2022/2555/oj

Europaparlamentet og Rådet. (2022). *Direktiv (EU) 2022/2557 fra Europaparlamentet og Rådet av 14. desember 2022 om motstandsdyktighet i kritiske enheter og om oppheving av direktiv 2008/114/EF fra Rådet*. Den europeiske unions tidende. Hentet 13. mars 2025, fra https://eur-lex.europa.eu/eli/dir/2022/2557/oj

Forordninger:

Europaparlamentet og Rådet. (2019). *Forordning (EU) 2019/881 av 17. april 2019 om ENISA (Den europeiske unions byrå for cybersikkerhet) og om sertifisering av cybersikkerhet for informasjons- og kommunikasjonsteknologi, og om oppheving av forordning (EU) nr. 526/2013 (Cybersikkerhetsakten)*. Den europeiske unions tidende, L 151, 7.6.2019, s. 15–69. Hentet 12. mars 2015, fra https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng

Den europeiske union. (2016). *Forordning (EU) 2016/679 av 27. april 2016 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger, og om oppheving av direktiv 95/46/EF (generell personvernforordning)*. Den europeiske unions tidende L 119, 4.5.2016, s. 1–88. Hentet 2. mars 2025, fra https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

Konvensjoner

Europarådet. (1950). *Konvensjon om beskyttelse av menneskerettighetene og de grunnleggende friheter (Den europeiske menneskerettighetskonvensjon).* Hentet 13. mars, fra https://www.echr.coe.int/documents/d/echr/Convention_NOR

Traktater

Den europeiske union. (2012). *Artikkel 288: Juridiske virkemidler*. I *Konsolidert versjon av Traktaten om Den europeiske unions virkemåte*. Den europeiske unions tidende, C 326, 26.10.2012, s. 171–172. https://eur-lex.europa.eu/eli/treaty/tfeu_2012/art_288/oj/eng

Den europeiske union. (2016). *Traktaten om Den europeiske union* (Konsolidert utgave). Den europeiske unions tidende C 202, 7.6.2016. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.C_.2016.202.01.0001.01.ENG&toc=OJ%3AC%3A2016%3A202%3ATOC#C_2016202EN.01001301

Norske

EFTA-sekretariatet, Europakommisjonen, & EFTA-statene. (1992, 2. mai). *Avtale om Det europeiske økonomiske samarbeidsområde (EØS-avtalen)* (AVT-1992-05-02-1). https://lovdata.no/dokument/NLX2/avtale/avt-1992-05-02-1

Justis- og beredskapsdepartementet. (2018, 1. juni). *Lov om nasjonal sikkerhet (sikkerhetsloven)* (LOV-2018-06-01-24). https://lovdata.no/dokument/NL/lov/2018-06-01-24

Justis- og beredskapsdepartementet. (2018, 15. juni). *Lov om behandling av personopplysninger (personopplysningsloven)* (LOV-2018-06-15-38). https://lovdata.no/dokument/NL/lov/2018-06-15-38

Justis- og beredskapsdepartementet. (2023, 20. desember). *Lov om digital sikkerhet (digitalsikkerhetsloven)* (LOV-2023-12-20-108). https://lovdata.no/dokument/NL/lov/2023-12-20-108

Danske:

Justitsministeriet. (2024, 7. februar). *Forslag til Lov om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i Danmark* (202412L00141). https://www.retsinformation.dk/eli/ft/202412L00141

Justitsministeriet. (2024, 8. mars). *Bekendtgørelse af lov om behandling af personoplysninger (databeskyttelsesloven)*(LBK nr 289 af 08/03/2024). https://www.retsinformation.dk/eli/lta/2024/289

Klima-, Energi- og Forsyningsministeriet. (2025). *Lov om styrket beredskab i energisektoren* (Lov nr. 258 af 6. marts 2025). Hentet 2. mai 2025 fra https://www.retsinformation.dk/eli/lta/2025/258

Forarbeid

Norske:

Forsvarsdepartementet. (2016). *NOU 2016: 19 Samhandling for sikkerhet: Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid*. Hentet 12. april 2025, fra https://www.regjeringen.no/contentassets/03960058f3f94fbe9d290593bee22c1a/no/pdfs/nou201620160019000dddpdfs.pdf

Justis- og beredskapsdepartementet. (2017). *Prop. 153 L (2016–2017) Lov om nasjonal sikkerhet (sikkerhetsloven)*. Hentet 12. april 2025, fra https://www.regjeringen.no/contentassets/0fcee45affd24280896b88b5413a00aa/no/pdfs/prp201620170153000dddpdfs.pdf

Justis- og beredskapsdepartementet. (2018). *Prop. 56 LS (2017–2018) Endringer i personopplysningsloven (gjennomføring av personvernforordningen)*. Hentet 1. mars 2025, fra https://www.regjeringen.no/contentassets/1a36e88f124d4a1ea92a9c790be2d69a/no/pdfs/prp201720180056000dddpdfs.pdf

Justis- og beredskapsdepartementet. (2023). *Prop. 109 LS (2022–2023) Lov om digital sikkerhet (digitalsikkerhetsloven) og samtykke til godkjenning av EØS-komiteens beslutninger nr. 21/2023 og 22/2023 om innlemmelse i EØS-avtalen av direktiv (EU) 2016/1148 og forordningene (EU) 2018/151 og (EU) 2019/881*. Hentet 4. mars 2025, fra https://www.regjeringen.no/contentassets/97c383444469486887e47e6892dd729b/no/pdfs/prp202220230109000dddpdfs.pdf

Justis- og politidepartementet. (2006). *NOU 2006:6 – Når sikkerheten er viktigst: Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner*. Oslo: Departementenes servicesenter. Hentet 4 mars 2025, fra https://www.regjeringen.no/no/dokumenter/nou-2006-6/id157408/

Danske:

Folketinget. (2018). *Betænkning over forslag til lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven)*. Hentet 25. april 2025 fra https://www.ft.dk/ripdf/samling/20171/lovforslag/l68/20171_l68_betaenkning.pdf

Folketinget. (2024). *Bilag 1 til lovforslag L 79 A: Udkast til bekendtgørelse om behandling af personoplysninger i forbindelse med kontrolforanstaltninger på arbejdspladsen*. Hentet 25. april 2025 fra https://www.ft.dk/samling/20231/lovforslag/L79A/bilag/1/2780324.pdf

Folketinget. (2024). *L 141 Bilag 1 – Forsvars-, Samfundssikkerheds- og Beredskabsudvalget 2024–25: Offentligt dokument med høringssvar*. Hentet 26. april 2025, fra https://www.ft.dk/samling/20241/lovforslag/L141/bilag/1/2976178/index.htm

Avgjørelser:

Datatilsynet. (2022, 11. januar). *Overtredelsesgebyr til Østre Toten kommune*. Hentet 5. april 2025, fra https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2022/overtredelsesgebyr-til-ostre-toten-kommune/

Datatilsynet. (2024, 24. januar). *Netcompany indstilles til bøde*. Hentet 24. april 2025, fra https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/jan/netcompany-indstilles-til-boede

Den europeiske menneskerettsdomstolen. (2021). *Big Brother Watch m.fl. mot Storbritannia* (sak nr. 58170/13). Hentet 2. april 2025, fra https://hudoc.echr.coe.int/eng?i=001-210077

EU-domstolen. (2020, 16. juli). *Dom i sak C-311/18: Data Protection Commissioner mot Facebook Ireland Ltd og Maximillian Schrems*. Hentet 2. april 2025, fra https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62018CJ0311

Litteratur:

Aqbal, A. (2013). Kompendium i Retssystemet og juridisk metode. I Kompendium i Retssystemet og juridisk metode. Samfundslitteratur.

Bergo, K. (2000). *Høyesteretts forarbeidsbruk*. Cappelen akademisk forlag

Berrefjord, V. R. Og Lund, M. S. (2024) *Cybermakt - En tverrfaglig innføring.* Oslo: Universitetsforlaget

Boe, E. M. (2010) *Innføring i juss - Juridisk tenkning og rettskildelære* (3. utgave). Oslo: Universitetsforlaget

Eckhoff, T. (2001). Rettskildelære. (5. utgave ved Jan E. Helgesen). Oslo: Universitetsforlaget

Jarbekk, E. og Sommerfeldt, S. (2019) *Personvern og GDPR i praksis* (1. utgave, 1. opplag) Oslo: Cappelen Damm Akademisk

Munk-Hansen, C. (2022). Retsvidenskabsteori (3. udgave). København: Djøf Forlag

Siems, M. (2022). *Comparative Law* (3. utg.). Cambridge University Press

Tvarnø, C. D. og Nielsen, R. (2021) Retskilder og retsteorier, (6. utgave, 1. opplag), Djøf Forlag

Artikler:

Bekkedal, T., og Andenæs, M. (2024) "*EØS-avtalen og kontinentalsoklene*. Lov og Rett 63, nr. 1 (2024): 7-33, https://doi.org/10.18261/lor.63.1.3

Brilingaitė, A., Bukauskas, L., Juozapavičius, A., Kutka, E., (2022) *Overcoming information-sharing challenges in cyber defence exercises*, Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyac001, https://doi.org/10.1093/cybsec/tyac001

Glenstrup, P. (2024, 2. juni). *NIS2 handler om én eneste ting: Overvåkning. Holistisk, fantastisk dataovervåkning*. Digi.no. Hentet 21. april 2025, fra https://www.digi.no/artikler/debatt-nis2-handler-om-en-eneste-ting-overvakning-holistisk-fantastisk-dataovervakning/547269

Graver, H. P. (2008). *Vanlig juridisk metode? Om rettsdogmatikken som juridisk sjanger*. Tidsskrift for Rettsvitenskap*, 121*(2), 149–178. Hentet 1. mai 2025 fra https://doi.org/10.18261/ISSN1504-3096-2008-02-01

Juliussen, B. A., Rui, J. P., & Johansen, D. (2024). *Developing with compliance in mind: Addressing data protection law, cybersecurity regulation, and AI regulation during software development*. UiT Norges arktiske universitet. Hentet 16. april 2025, fra https://munin.uit.no/bitstream/handle/10037/36399/article.pdf

Koiava, A. (2023). Legal aspects of vulnerability disclosure: Navigating GDPR and NIS Directive obligations for data protection and cybersecurity. *L'Europe Unie, 20*, 36–43. Hentet 21. april 2025 fra https://www.ceeol.com/search/article-detail?id=1201602

Koops, B.-J. (2014). *The trouble with European data protection law*. *International Data Privacy Law, 4*(4), s. 250–261. https://doi-org.zorac.aub.aau.dk/10.1093/idpl/ipu023

Kun, Eyup. (June 15, 2021) *Strengthening the Supervision and Enforcement in the EU Cybersecurity Law: Are All Organisational Measures Created Equally?* Hentet 16. april fra: http://dx.doi.org/10.2139/ssrn.3933680

Küfeoğlu, S., og Akgün, A. T. (2023). *Critical infrastructure and cyber resilience frameworks*. (1 utg.): CRC Press. Hentet 17. april fra https://doi-org.zorac.aub.aau.dk/10.1201/9781003449522-1

Lov&Data. Hentet 17. april 2025, fra https://lod.lovdata.no/article/2024/06/Logging%20som%20sikkerhetstiltak%20etter%20GDPR

Maglaras, L., Kantzavelou, I., & Ferrag, M. A. (2021). *Digital transformation and cybersecurity of critical infrastructures*. Applied Sciences*, 11*(18), 8357. Hentet 8. mars 2025 fra https://doi.org/10.3390/app11188357

Nweke, L. O., & Wolthusen, S. D. (2020). *Legal issues related to cyber threat information sharing among private entities for critical infrastructure protection*. Jančárková, L. Lindström, M. Signoretti, I. Tolga & G. Visky (Red.), *12th International Conference on Cyber Conflict: 20/20 Vision: The Next Decade* (s. 63–78). NATO Cooperative Cyber Defence Centre of Excellence. Hentet 7. april 2025 fra https://ccdcoe.org/uploads/2020/05/CyCon_2020_4_Nweke_Wolthusen.pdf

Rajamäki, J., Jarzemski, D., Kucera, J., Nyman, V., Pura, I., Virtanen, J., Herlevi, M., & Karlsson, L. (2024). *Implications of GDPR and NIS2 for Cyber Threat Intelligence Exchange in Hospitals*. WSEAS TRANSACTIONS ON COMPUTERS, *23*, 1–11. https://doi.org/10.37394/23205.2024.23.1

Schmitz-Berndt, S. (2023) *Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive*, Journal of Cybersecurity, Volume 9, Issue 1, 2023, tyad009, https://doi.org/10.1093/cybsec/tyad009

Sverdrup, U. (2004). *Compliance and conflict management in the European Union: Nordic exceptionalism.* Scandinavian Political Studies*, 27*(1), 23–43. Hentet 16. april 2025 fra: https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1467-9477.2004.00098.x

Symantec Threat Hunter Team. *Attacks Against Critical Infrastructure: A Global Concern*. Hentet 8. mars 2025 fra https://symantec.broadcom.com/hubfs/Attacks-Against-Critical_Infrastructrure.pdf

Vostoupal, J., Stupka, V., Harašta, J., Kasl, F., Loutocký, P., & Malinka, K. (2024). *The legal aspects of cybersecurity vulnerability disclosure: To the NIS 2 and beyond*. Computer Law & Security Review, *53*, 105988-. https://doi.org/10.1016/j.clsr.2024.105988

Internett:

Center for Cybersikkerhed. (2024). *Cybertruslen mod Danmark 2024*. Hentet 12. april 2025, fra https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/cfcs---cybertruslen-mod-danmark-2024.pdf

Center for Cybersikkerhed. *Implementering av NIS2 i dansk rett*. Hentet 19. mars 2025, fra https://www.cfcs.dk/da/opgaver/nis2/implementering-af-nis2/

Center for Cybersikkerhed. *Om oss*. Hentet 12. mars 2025, fra https://www.cfcs.dk/da/om-os/

Center for Cybersikkerhed. *Sektoransvarlige myndigheter*. Hentet 19. mars 2025, fra https://www.cfcs.dk/da/opgaver/nis2/sektoransvaligemyndigheder/

Center for Cybersikkerhed. *Underretning til CFCS*. Hentet 24. april 2025, fra https://www.cfcs.dk/da/om-os/indberetning/

Danmarks Statistik. *Digitalisering*. Hentet 6. mars 2025, fra https://www.dst.dk/da/Statistik/temaer/digitalisering

Datatilsynet. (2021, 22. april). *Nasjonale samarbeidsrelasjoner – Årsrapport for 2020*. Hentet 23. mars 2025 fra https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/datatilsynets-arsrapporter/arsrapport-for-2020/nasjonale-samarbeidsrelasjoner/

Datatilsynet. (2023, 7. november). *Kontrol af medarbejdere*. Hentet 23. mars 2025 fra https://www.datatilsynet.dk/Media/638348919997326341/Kontrol%20af%20medarbejdere.pdf
Datatilsynet. (2023, 7. november). *Logning af brugernes anvendelser af personoplysninger*. Hentet 26. april 2025, fra https://www.datatilsynet.dk/regler-og-vejledning/behandlingssikkerhed/katalog-over-foranstaltninger/logning-af-brugernes-anvendelser-af-personoplysninger
Datatilsynet. (2024, 23. oktober). *Nasjonale samarbeidsrelasjoner – Årsrapport for 2023*. Hentet 23. mars 2025 fra https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/datatilsynets-arsrapporter/arsrapport-for-2023-2/nasjonale-samarbeidsrelasjoner/
Datatilsynet. *Anmeld sikkerhedsbrud*. Hentet 24. april 2025, fra https://www.datatilsynet.dk/sikkerhedsbrud/anmeld-sikkerhedsbrud
Datatilsynet. *Datatilsynets oppgaver*. Hentet 17. april 2025, fra https://www.datatilsynet.no/om-datatilsynet/oppgaver/
Datatilsynet. *Om personopplysningsloven med forordning og når den gjelder*. Hentet 8. april 2025 fra https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/om-personopplysningsloven-og-nar-den-gjelder/
Datatilsynet. *Personvernprinsippene*. Hentet 11. mars 2025, fra https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/
Digitaliserings- og forvaltningsdepartementet. (2024). *Fremtidens digitale Norge: Nasjonal digitaliseringsstrategi 2024–2030*. Hentet 24. mars 2025 https://www.regjeringen.no/contentassets/c499c3b6c93740bd989c43d886f65924/no/pdfs/nasjonal-digitaliseringsstrategi_ny.pdf
Digitaliseringsdirektoratet. (2025, 27. januar). *Veileder i kompetanse- og kulturutvikling innen digital sikkerhet*. Hentet 30. mars 2025, fra https://www.digdir.no/media/4981/download
Energistyrelsen. (2024, 3. mai). *Lov om styrket beredskab i energisektoren er vedtaget*. Hentet 7. mars 2025, fra https://ens.dk/presse/lov-om-styrket-beredskab-i-energisektoren-er-vedtaget
Europalov. *EU-rettsaktene*. Hentet 2. april 2025, fra https://europalov.no/laer-mer/eu-rettsaktene
European Commission. (2020). *Commission Staff Working Document: Impact Assessment Report Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148* (SWD(2020) 345 final). Hentet 2. april 2025, fra https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020SC0345
European Commission. *Legal framework of EU data protection*. Hentet 4. mars 2025, fra https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en
European Commission. *NIS2 Directive: new rules on cybersecurity of network and information systems*. Hentet 6. april 2025, fra https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
European Commission. *What the European Commission does in law*. Hentet 8. mars 2025, fra https://commission.europa.eu/about/role/law_en
Folketingets EU-Oplysning. (2024, 14. oktober). *EU-ret i Danmark*. Hentet 29. april 2025 fra https://www.eu.dk/da/danmark-i-eu/eu-ret-i-danmark
Gisle, J. *Komparativ rett*. I Store norske leksikon. Hentet 3. mars 2025, fra https://snl.no/komparativ_rett
Hagen, J., Hermansen, O., Toftegård, Ø., Pettersen, J.-M., Steen, R., & Paulen, S. L. (2017). *Regulering av IKT-sikkerhet: Et helhetlig og fremtidsrettet sikkerhetsregime for forsyningssikkerhet i en digitalisert energisektor* (NVE Rapport nr. 26/2017). Norges vassdrags- og energidirektorat. Hentet 9. mars 2025, fra https://publikasjoner.nve.no/rapport/2017/rapport2017_26.pdf
Hansen, T. (2025, 24. februar). *Desentralisering*. I *Store norske leksikon*. Hentet 3. mars 2025, fra https://snl.no/desentralisering
Juridika. *Lovforarbeidet*. Hentet 5. mars 2025, fra https://juridika.no/innsikt/lovforarbeidet

Justis- og beredskapsdepartementet. (2019, 30. januar). *Nasjonal strategi for digital sikkerhet*. Hentet 2. mai 2025, fra https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/nasjonal-strategi-for-digital-sikkerhet.pdf

Justis- og beredskapsdepartementet. (2021, 22. februar). *NIS2-direktivet*. Hentet 9. mars 2025, fra https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2021/feb/nis2-direktivet/id2846097/

Klima-, Energi- og Forsyningsministeriet. (2025, 27. februar). *Ny lovgivning styrker sikkerheden i energisektoren*. Hentet 26. mars 2025 fra https://www.kefm.dk/aktuelt/nyheder/2025/feb/ny-lovgivning-styrker-sikkerheden-i-energisektoren-#:~:text=Ny%20lovgivning%20styrker%20sikkerheden%20i,og%20tekniske%20sikkerhedskrav%20i%20energisektoren

Ministeriet for Samfundssikkerhed og Beredskab. (2024, 14. oktober). *Lovforslag om cybersikkerhed forventes at træde i kraft i Danmark 1. juli 2025*. Hentet 19. april 2025, fra https://mssb.dk/nyheder/2024/oktober/lovforslag-om-cybersikkerhed-forventes-at-traede-i-kraft-i-danmark-1-juli-2025/

Nasjonal sikkerhetsmyndighet. (2020, 4. juni). *Sektormyndighet med tilsynsansvar*. Hentet 6. april 2025, fra https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/veileder-for-tilsyn-med-forebyggende-sikkerhetsarbeid/tilsyn/tilsynsmyndigheter/sektormyndighet-med-tilsynsansvar/

Nasjonal sikkerhetsmyndighet. (2020). *Veileder for virksomheters håndtering av uønskede hendelser*. Hentet 12. mars 2025, fra https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/veileder-for-virksomheters-handtering-av-uonskede-hendelser/

Nasjonal sikkerhetsmyndighet. (2024). *Risiko 2024: Nasjonal sikkerhet – et felles ansvar*. Hentet 24.mars 2025 https://nsm.no/getfile.php/1313477-1719434219/NSM/Filer/Dokumenter/Rapporter/Risiko%202024.pdf

Nasjonal sikkerhetsmyndighet. (2025). *Risiko 2025: Et sikkert Norge i en usikker verden*. Hentet 24. mars 2025, fra https://nsm.no/getfile.php/1314212-1738741587/NSM/Filer/Dokumenter/Rapporter/Risiko%202025.pdf

Nasjonal sikkerhetsmyndighet. *Dette er NSM*. Hentet 12. mars 2025, fra https://nsm.no/om-oss/dette-er-nsm/

Publikasjonskontoret for Den europeiske union. *Forrang for EU-retten (primacy of EU law)*. Hentet 6. april 2025, fra https://eur-lex.europa.eu/legal-content/EN-DA/ALL/?uri=LEGISSUM:primacy_of_eu_law&from=DA

SektorCERT. (2023). *Angrebet mod dansk kritisk infrastruktur*. Hentet 7. mars 2025, fra https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-Angrebet-mod-dansk-kritisk-infrastruktur-TLP-CLEAR.pdf

Styrelsen for Forsyningssikkerhed. (2023). *Erhvervsliv og det offentlige skulder ved skulder om forsyningssikkerhed*. Hentet 17. mars 2025, fra https://sfos.dk/2023/11/13/erhvervsliv-og-det-offentlige-skulder-ved-skulder-om-forsyningssikkerhed/

Styrelsen for Samfundssikkerhed. *Styrelsen for Samfundssikkerhed*. Hentet 26. mars 2025 fra https://mssb.dk/ministeriet/styrelsen-for-samfundssikkerhed/

Utenriksdepartementet. (2025). *Spørsmål og svar om EØS*. Hentet 8. mars 2025 fra https://www.regjeringen.no/no/tema/europapolitikk/fakta-115259/ofte-stilte-sporsmal/id613868/