



08:00	Registrering og lett servering
08:30	Åpning med Hege Svendsen, daglig leder i Den Norske Dataforening
08:45	DEL 1: MULIGHETER OG UTFORDRINGER FOR MYNDIGHETENE • Tor Jørgen Bergbye, seniorrådgiver i NSM: <i>NIS-direktivene og lov om digital sikkerhet</i> • Janne Stang Dahl, dir. for kommunikasjon og samfunnskontakt i Datatilsynet <i>Implementerings- og håndheving utfordringer - hva kan vi lære av GDPR?</i> • Olav Johannessen, Seksjonssjef tilsyn IT og betalingstjenester i Finanstilsynet <i>Fra IKT-forskriften til DORA</i> • Catharina Nes, avdelingsleder i Digitaliserings- og forvaltningsdepartementet <i>Om KI og implementering av forordningen</i> • Paneldebatt moderert av Audun Jøsang, professor UiO
09:30	DEL 2: MULIGHETER OG UTFORDRINGER FOR VIRKSOMHETENE • Hanne Tangen Nilsen, administrerende direktør i Sykehuspartner: <i>Risikobasert tilnærming</i> • Martin Sværen, Managing Director Cybersecurity i Accenture <i>Implementering av DORA, utfordringer og erfaringer</i> • Trond Sundby, CISO i Bærum kommune <i>Cybersikkerhet og utfordringer for kommunene</i> • Kristian Foss, partner i BULL advokater <i>Om ledelsens og styrets ansvar for cybersikkerhet</i> • Paneldebatt moderert av Audun Jøsang, professor UiO
10:20	Pause
10:50	DEL 3: KONSEKVENSER OG MARKEDSEFFEKTER • Lee Bygrave, professor på UiO, senter for rettsinformatikk <i>Cybersikkerhet: Fremdeles et "lemons market"?</i> • Aina Slinning, sikkerhetsdirektør i Aker ASA <i>Hvilke effekter kan vi vente av regelverkene?</i> • Håkon Styri, seniorrådgiver i Norsk Sikkerhetsmyndighet <i>Innebygd sikkerhet i hele verdikjeden</i> • Sverre Stoltz, programdirektør i DFØ <i>Markedsplassen for skytjenester: Formål og noen betraktninger</i> • Paneldebatt moderert av Audun Jøsang, professor UiO
11:50	Avslutning og oppsummering
12:00	Mingling og kaffe

Arrangementskomitéen har bestått av: Audun Jøsang, Renate Thoreid, Håkon H. Hansen, Willy Domaas, Lone Bekkeheien, Torkjell Dahl, og Haakan Dyrseth.



EUs cyber-rettsakter - kort oversikt

NIS2-direktivet (+ CyClone)

Vedtatt i EU 14.12.2022, og trådte i kraft 24.10.2024, da NIS1-direktivet fra 2016 opphørte. Lov om digitalsikkerhet som følger NIS1 ble i Norge vedtatt 20.12.2023 men vil ikke tre i kraft før forskriften er plass. Når NIS2 innlemmes i EØS-avtalen vil det medføre oppdatering av lov om digitalsikkerhet. NIS2 spesifiserer bl.a. å etablere EU-CyCLONe (European Cyber Crisis Liaison Organisation Network) der Norge vil delta.

DORA (Digital Operational Resilience Act – Lov om operasjonell sikkerhet i finans)

DORA-forordningen ble vedtatt i EU 14.12.2022 og trer i kraft 17.01.2025. DORA regnes å være EØS-relevant, slik at forordningen antagelig vil gjelde i Norge innen 2026.

CRA (Cyber Resilience Act – Cyberresiliensforordningen)

EU-kommisjonen foreslo 15.09.2022 en ny forordning om krav til cybersikkerhet i produkter med digitale elementer og programvare. Omfanget av produkter som dekkes av forslaget til regulering er svært bredt og vil gjelde alt fra eksempelvis smartklokker og leketøy til wifi-rutere og brannmurer samt programvare som benyttes i produktene. CRA ble vedtatt av Europarådet 10.10.2024, og vil antagelig tre i kraft EU i 2027. CRA regnes å være EØS-relevant, slik at forordningen antagelig vil gjelde i Norge innen 2028.

Cybersecurity Act (Cybersikkerhetsforordningen)

Forordningen som trådte i kraft i EU 27.06.2019 gir permanent status til ENISA (EU Agency for Cyber Security) med hovedkvarter Athen. Forordningen etablerer også et rammeverk for frivillig sertifisering av IKT-produkter, tjenester og prosesser, der ENISA skal administrere rammeverket. Forordningen ble tatt inn i EØS-avtalen 03.02.2023, med grunnet budsjettmessige konsekvenser tar Norge forbehold om innlemmelse.

Cyber Solidarity Act (Cybersolidaritetsforordningen)

Foreslått av EU-kommisjonen 18.04.2023 og vedtatt av EU-parlamentet 05.03.2024. Cybersolidaritetsforordningen har som mål å styrke EUs cyberberedskap. Forordningen inkluderer et europeisk integrert cybervarslingssystem og responsmiljø for å styrke EUs cybermotstandskraft. Forordningen er EØS-relevant, men videre tidsplan for EØS er ikke bestemt.

Data Act (Dataforordningen)

Foreslått 23.02.2022 og trådte i kraft i EU 11.01.2024. De fleste av bestemmelsene vil gjelde fra 12.09.2025. Dataforordningen legger til rette for at forbrukere og virksomheter får tilgang til data som genereres ved deres bruk av tilkoblede produkter og relaterte tjenester. Forordningen er til vurdering i EØS.

Product Liability Directive (Produktansvarsdirektivet) (oppdatering)

Foreslått 28.9.2022 som oppdatering av tidligere direktiv fra 1985 som i utilstrekkelig grad dekker moderne digitale produkter. Oppdatert direktiv er tenkt å også dekke skade som følge av feil i programvare mm. Forslaget er til vurdering i EU, og vil deretter vurderes i EØS.

AI Act (KI-forordningen)

Foreslått av EU-kommisjonen 21.04.2021, og iverksatt 13.06.2024. Beskriver fire risikokategorier for KI, der høyeste risiko representerer forbudt KI, som skal håndheves fra desember 2024. Håndhevelse av de lavere risikokategoriene skjer trinnvis frem til 2027. KI-forordningen er EØS-relevant og kommer til Norge i 2025.

AI Liability Directive (KI-ansvarsdirektivet)

Foreslått av EU-kommisjonen 28.09.2022, og gjelder sivilrettslig erstatningsansvar utenfor kontrakt når skaden forårsakes av KI. En utredning fra 2024 anbefaler å utvide det foreslåtte virkeområdet. EØS har ikke tatt stilling til om direktivet er relevant. Oppdateringer forventes i 2025.

eIDAS Regulation (electronic IDentification And trust Services)

Vedtatt i EU i 2014, iverksatt mellom 2016 og 2018. Forordningen ble i Norge iverksatt 15.06.2018 som lov om elektroniske tillitstjenester. Oppdatert som eIDAS 2.0 11.04.2024. Innebærer at myndighetene i hvert land oppretter en ordning for «digital lommebok» for innbyggerne og en statlig eID-ordning på nivå HØYT.

GDPR (General Data Protection Regulation - Personvernforordningen)

Innført i EU 25.05.2018. Forordningen ble i Norge iverksatt 20.07.2018 som personopplysningsloven. *Artikkel 32: Sikkerhet ved behandlingen* setter krav om cybersikkerhet ved behandling av persondata.