

**Velkommen til nyhedsbrev fra Rådet for Digital Sikkerhed, februar 2026****Vinterens digitaliseringsdebat****Henning Mortensen og Anne Dorte Bach, Rådets formandskab**

Vinteren er nærmest et billede på den geopolitiske situation, som bedst kan betegnes som ustabil. I Danmark og Europa står barometeret på store forandringer, som vi tålmodigt og vedholdende skal håndtere på kort og lang sigt, alt imens det raser og råber derude. På den digitale front er det ikke meget anderledes.

**National cybersikkerhedsstrategi**

Den var længe ventet, og sidst i januar kunne regeringen endelig fremlægge en politisk aftale om 'Strategi for national cyber- og informationssikkerhed 2026-2029'. Strategien har særligt fokus på de områder, der ikke er omfattet af NIS2-lovgivningen. Der er navnlig fokus på borgernes it-sikkerhed og sikkerheden hos de danske små- og mellemstore virksomheder.

Fra Rådets side glæder vi os særligt over, at det pågående arbejde med sikkerhedsanbefalinger målrettet de mindre virksomheder er nævnt som indsatsområde.

Rådet varetager pt. formandshvervet for den arbejdsgruppe, der har til opgave at opstille anbefalingerne med ledsagende vejledning, og vi ser frem til lancering senere på foråret. Ved offentliggørelsen udtrykte Rådet dog samtidig bekymring for, om de afsatte midler til gennemførelse af strategien er tilstrækkelige.

Læs mere på Rådets hjemmeside [her](#)

**Trump dekret om aflysning af AI-regulering**

Det gik det nærmest ubemærket hen, at Trump i december 2025 aflyste de amerikanske delstaters lovgivning på AI-området. Det skete - nærmest selvsagt - med et dekret og til trods for, at næsten alle 50 delstater (både demokratiske og republikanske) allerede har lovgivning, der lægger vægt på ansvarlighed, gennemsigtighed og beskyttelse af borgerrettigheder i tilknytning til AI. Dekretet er indtil videre en sejr for de store amerikanske tech-virksomheder, der har lobbyet for deregulering; men samtidig er det tvivlsomt, om dekretet vil virke efter sin hensigt. Det er i hver fald stødt på stor kritik internt i USA.

Læs mere på Rådets hjemmeside [her](#)

**EU's Digitale Omnibus Pakke med ændringer i GDPR**

Deregulering er også et centralt kodeord for EU's forslag til den såkaldte 'Digital Omnibus Package' fra november 2025 om end, det efter vanlig EU-procedure blot er et forslag fra kommissionen til politisk behandling i medlemslandene og EU-

organerne.

Omnibuspakken rummer mange forslag, der tilsammen skal spare administration og booste innovation i det europæiske erhvervsliv.

På vegne af Rådets bestyrelse har Rådet her i februar 2026 fremsendt sine bemærkninger om den del af Omnibus-pakken, der omhandler ændring af GDPR, til justitsministeren og digitaliseringsministeren.

Rådet giver udtryk for, at kommissionens forslag ikke er ambitiøst nok, hvis byrderne for alvor skal lettes inden for administration og compliance på GDPR-feltet. Samtidig lægger Rådet afgørende vægt på, at der ikke bør rokkes ved selve definitionen af personoplysninger, som udover at være hængt op det Europæiske Charter for grundlæggende rettigheder, er kernen i GDPR.

Læs mere på Rådets hjemmeside [her](#)

Sidst i februar 2025 afholder Rådet et medlemsarrangement om EU's forslag til ændringer i GDPR med oplæg fra Datatilsynets direktør Cristina Gulisano og præsentation af Rådets ændringsforslag.

Læs mere om Rådets arrangementer [her](#)

### **Cyber Security Package med forslag til ændringer af Cyber Security Act og NIS2**

EU Kommissionen har i januar 2026 foreslået en samlet gennemgang af NIS2 og Cyber Security Act (CSA) under overskriften 'Cyber Security Package', som er et element i EU's samlede digitale omnibus strategi. Formålet er navnlig af forenkle reglerne om cybersikkerhed, risikostyring, strømline hændelsesrapporteringen og styrke ENISAs koordinerende rolle.

Med pakken foreslås en række mindre justeringer af NIS2, hvor visse typer enheder undtages og andre nye snævre typer enheder tilføjes. Videre får EU Kommissionen mulighed for at udstede delegerede retsakter i forhold til de konkrete krav til cybersikkerhedsforanstaltninger, som nævnes i artikel 21.

Styring af forsyningskæderisici fylder også en del i justeringen af CSA. Her får Kommissionen mulighed for at udstede delegerede retsakter, hvorefter de kan udpege lande, som udgør en trussel mod ICT supply chains, udpege leverandører som high-risk suppliers og udpege visse dele af NIS2 enheders infrastruktur som kritisk. På den baggrund kan de forbyde NIS2-omfattede enheder at bruge bestemte leverandører eller overføre data ud af EU. Rådet er generelt skeptisk overfor brug af delegerede retsakter, da disse dels har et demokratisk underskud ved ikke at være politisk behandlet og dels kan skabe usikkerhed og dermed omkostninger for de omfattede enheder.

Læs mere om EU kommissionens Cyber Security Package [her](#)

### **Cyber Resilience Act får snart virkning**

EU's CRA-forordning (Cyber Resilience Act (EU) 2024/2847) blev vedtaget af EU-landene i oktober 2024. Formålet er at sikre, at produkter med digitale elementer har god sikkerhed, inden de slippes løs på det europæiske marked. De første dele af forordningen får virkning allerede til september 2026, herunder navnlig bestemmelserne om indberetning af sårbarheder og alvorlige hændelser.

Til december 2027 træder forordningen i kraft i sin helhed, hvor alle produkter med digitale elementer (hardware og software), der markedsføres i EU, skal overholde de nye cybersikkerhedskrav og bære CE-mærket. Fabrikanter, importører og distributører får tildelt forskellige roller i forordningen.

Virksomhederne skal derfor i gang med at sikre en passende produktudvikling, have en proces for opdatering, sikre passende dokumentation og kommunikation til kunder. Det er et omfattende arbejde, som tager tid. RfDS satte derfor fokus på området sammen med Gorrissen-Federspiel på et medlemsarrangement i januar måned. Fra dagens præsentation var der gode råd at hente til dem, der skal i gang med arbejdet.

Læs mere på Rådets oversigt over arrangementer [her](#)

Opmærksomheden henledes også på, at EU-Kommissionen og ENISA som led i implementeringen af CRA-forordningen har iværksat en undersøgelse om CRA-forordningens relevans i forhold til EU små- og mellemstore virksomheder (under 250 ansatte).

Gå til ENISAs undersøgelse om CRA i forhold til de mindre virksomheder [her](#) (den tager ca. 5 minutter)

Læs mere om ENISAs indsats i forhold til cybersikkerhed for små- og mellemstore virksomheder [her](#)

### **Folketinget nedsætter en privatlivskommission**

I december 2025 vedtog et enigt Folketing et beslutningsforslag om nedsættelse af en privatlivskommission. Forslaget har været undervejs siden maj 2025, hvor flere organisationer, herunder Rådet for Digital Sikkerhed udtrykte kritik i forhold til hastebehandling af regeringens forslag til at give PET øgede beføjelser til at indsamle og overvåge data.

Læs mere om kritikken og forslaget om nedsættelse af en privatlivskommission på Rådets hjemmeside [her](#)

Kritikken af regeringens forslag førte til, at justitsministeren satte lovforslaget om ændring af PET-loven i bero. Lovforslaget, som blev fremsat april 2025, fremgår fortsat af [Folketingets hjemmeside](#).

I henhold til resumeet for beslutningsforslaget fra december nedsættes *"... en uafhængig privatlivskommission, der har til formål at beskæftige sig med udviklingen i overvågning, databehandling og indgreb i borgernes privatliv i Danmark og komme med anbefalinger til, hvordan balancen mellem tryghed, sikkerhed og retten til privatliv bedst sikres i fremtiden."*

Læs mere om beslutningsforslaget [her](#):

### **Kompromis om EU-indsats til bekæmpelse af materiale med seksuelt misbrug af børn**

Sidst i november 2025 lykkedes det for det danske EU-formandskab at skabe opbakning til den kommende såkaldte Child Sexual Abuse Directive, der skal bekæmpe udbredelsen af materiale med seksuelt misbrug af børn. Forslaget har

været flere år undervejs og har stødt på omfattende kritik fra politikere og eksperter, fordi det oprindeligt – som kritikken lød – åbnede for en generel scanning borgernes private online kommunikation.

Det var en kritik, som Rådet tilsluttede sig sammen med en lang række andre organisationer.

Læs mere om kritikken på Rådets hjemmeside [her](#)

Et af de værktøjer, der indgår i det foreliggende kompromisforslag, er en permanentgørelse af den frivillige opsporing af overgrebsmateriale, som hidtil har været baseret på en tidsbegrænset undtagelsesbestemmelse til EU-retten. Herudover indeholder det foreliggende kompromis en række forpligtelser for udbydere af kommunikationstjenester til at risikobegrænse og bekæmpe udbredelse af materiale med seksuelt misbrug af børn.

Læs mere på Justitsministeriets hjemmeside [her](#)

### **EU-vejledning om digital suverænitet**

I oktober 2025 offentliggjorde EU-Kommissionen en vejledning om, hvordan man som kunde kan vurdere sin leverandørs digitale suverænitet. Tanken er, at en kunde kan evaluere sit behov for suverænitet for en given IT-løsning ud fra otte forskellige suverænitetsparametre. Først fastlægger kunden sit krav til suverænitet på en skala fra 0 til 4 på de otte parametre. Sideløbende hermed beder kunden leverandøren give sin egen vurdering af it-løsningens suverænitet på de otte parametre. Når kunden modtager leverandørens svar, scorer kunden leverandørens svar igen på skalaen fra 0-4. Til sidst vejes vurderingerne sammen med vægte givet fra EU-Kommissionen. Kunden får dermed en suverænitets score for hver IT-løsning – hvilket kan bruges til at sammenligne leverandører eller vise hvilke systemer, der måske skal lægges om for at øge suverænitetsscoren.

Du kan læse mere om EU Kommissionens vejledning [her](#)

### **NIS2-implementeringen fortsætter i Danmark**

Det hører med til Rådets vinterstatus, at NIS2-implementeringen fra den centrale myndighed Styrelsen for Samfundssikkerhed (SAMSIK) er ved at finde form. På SAMSIKs hjemmeside findes 4 tværgående vejledninger samt en vejledning målrettet kommunerne.

Der er endvidere etableret et såkaldt 'NIS2tjek', hvor en virksomhed kan få hjælp til at afklare, om man er omfattet af NIS2.

Læs mere på SAMSIKs hjemmeside [her](#)

Det hører dog også med til billedet, at Rådet tilbage i oktober 2025 afholdt et seminar med oplæg fra Bech-Bruun, hvor det blev betonet, at den danske NIS2-implementering hænger noget i bremsen med hensyn til virksomhedernes klarhed over reglerne og forankring af risikostyringen i organisationen. Rådet vil selvsagt følge op på NIS2-implementeringen i den kommende tid.

### **Rådets hjemmeside er blevet trimmet**

Afslutningsvis vil vi henlede opmærksomheden på, at Rådets hjemmeside har fået en overhaling. I kan læse mere om

- Rådets nyheder [her](#)
- Rådets arrangementer [her](#)
- Rådets fokusområder [her](#)

Fortsat god vinter – foråret er lige om hjørnet!



## Bliv medlem af Rådet for Digital Sikkerhed

Hvis du ikke allerede er medlem, så kan vi kun opfordre!

Rådet for Digital Sikkerhed er et uafhængigt netværk med eksperter fra it-verdenen, erhvervslivet, advokatbureauer, forskningen, erhvervs- og forbrugerorganisationer samt Institut for Menneskerettigheder. Rådet tæller i dag ca. 70 medlemmer, der mødes online og til arrangementer for at gøre hinanden klogere på de brændende digitale temaer.

Rådets rødder går snart 15 år tilbage, men fokus er det samme: Et trygt og frit digitalt samfund for alle. Det er en vision for en digital udvikling, der er i konstant forandring med nye banebrydende teknologier og nye udfordringer for privatlivet, samfundets sikkerhed, samspillet mellem borgerne og det offentlige, virksomhedernes innovation samt ikke mindst vores kritiske forståelse af forholdet mellem mennesker og teknologi.

Rådet har gennem årene manifesteret sig som en fagligt velfunderet stemme i forhold til den offentlige debat. Vi deltager i statslige råd og arbejdsgrupper og er fast høringspart omkring nye lovtag på det digitale felt.

Rådet ledes af en bestyrelse, der afspejler Rådets sammensætning. Bestyrelsen mødes 5-6 årligt.

Hvis du vil høre mere eller ønske at melde dig ind, så kontakt venligst Rådets sekretariatschef Claus Hjorth på [claus.hjorth@digitalsikkerhed.dk](mailto:claus.hjorth@digitalsikkerhed.dk) / mobil 5334 2522.

Tjek også [Rådets hjemmeside](#).

/Anne Dorte Bach og Henning Mortensen

Rådet for Digital Sikkerhed - Vester Farimagsgade 37B, 1. Th - 1606 København V  
- [digitalsikkerhed.dk](https://digitalsikkerhed.dk)  
Du modtager denne mail, da du har tilmeldt dig vores nyhedsbrev. [Afmeld.](#)