Digital compliance

En virksomheds data er guld. Guld repræsenterer en værdi, og ejer du guld, passer du naturligvis godt på det. Du låser uden tvivl dørene, benytter alarm m.v.

I denne digitaliserede verden skal vi passe på virksomhedens data og placere dataene bag "lås og slå" og gøre det til en vanskelig opgave for de cyberkriminelle at få adgang til dem, for de vil gerne have fat i dem, viser nyeste statistikker [1]. De sidste 25 år er fysisk kriminalitet faldet med 50 procent. Cyberkriminaliteten er derimod drastisk stigende og den kriminalitetsform, der vokser hurtigst og overhaler alle andre former for kriminalitet.

GDPR sikrer ansvarlig anvendelse af data i et digitaliseret samfund, så GDPR betyder også, at virksomheder skal have et vist teknisk sikkerhedsniveau, som er med til at beskytte data.

GDPR var i 2018 grundstenen for ansvarlig brug af data, men området inden for dataregulering er foranderligt, og hvis du ikke allerede har hørt om NIS2-direktivet (se faktaboks nedenfor), vil du nok snart høre om det:

Mens GDPR regulerer mennesket, har NIS2 til formål at regulere og dermed opnå et fælles cybersikkerhedsniveau i EU og sikre at tjenester og systemer [2], som bruges til at kommunikere og behandle data via, er tilgængelige, så samfundskritiske tjenester kan fortsætte deres drift trods et cyberangreb, supply chain-svigt, IT-nedbrud, hacking osv. NIS2-direktivet vil få en afsmittende effekt på hele forsyningskæden, idet de omfattede organisationer forventeligt vil videreføre kravene helt/delvist til leverandører og kunder, så de virksomheder, der endnu ikke har fået styr på deres IT-sikkerhed, bliver indirekte presset til at få det bragt i orden. Det samme gælder også deres behandling af persondata.

GDPR var således kun starten inden for dataregulering, og ligesom GDPR forsvinder NIS2 ikke. "Digital compliance" er kommet for at blive og har ingen slutdato, da samfundet skal være rustet og modstandsdygtigt ift. cyberangreb og andre IT-relaterede trusler.

Budskabet fra Rådet for Digital Sikkerhed er også klart. Rådet (…) "opfordrer virksomhederne til at opdatere risikovurderinger, politikker og tekniske foranstaltninger for at beskytte sig samt blive bedre til at dele erfaringer og data om hændelser" [3].

Hos Roesgaard står vi klar til at hjælpe dig med at forstå digital compliance, og her kommer lidt gode råd:

- Kortlæg IT-miljøet, og hav overblik over data, og hvad de bruges til samt jeres anvendte leverandører
- Hav en procedure for forretningskontinuitet i tilfælde af, at I bliver ramt af en cyberhændelse, herunder en beredskabsplan og styr på fysisk sikkerhed
- Anvend sikker software, og hav styr på den tekniske sikkerhed
- Skol medarbejderne, inkl. ledelsen, i GDPR og NIS2
- Hav skriftlige politikker/procedurer samt risikovurderinger for ovenstående

Husk, at data er et springbræt ift. vækst, og en forudsætning for at udnytte dette springbræt er, at behandlingen af data foregår dataansvarligt og i overensstemmelse med digital compliance.

Hvad er NIS2-direktivet?

- Direktivet vedrører beskyttelse af net- og informationssystemer (NIS2) og er en fortsættelse af NIS-direktivet fra 2016

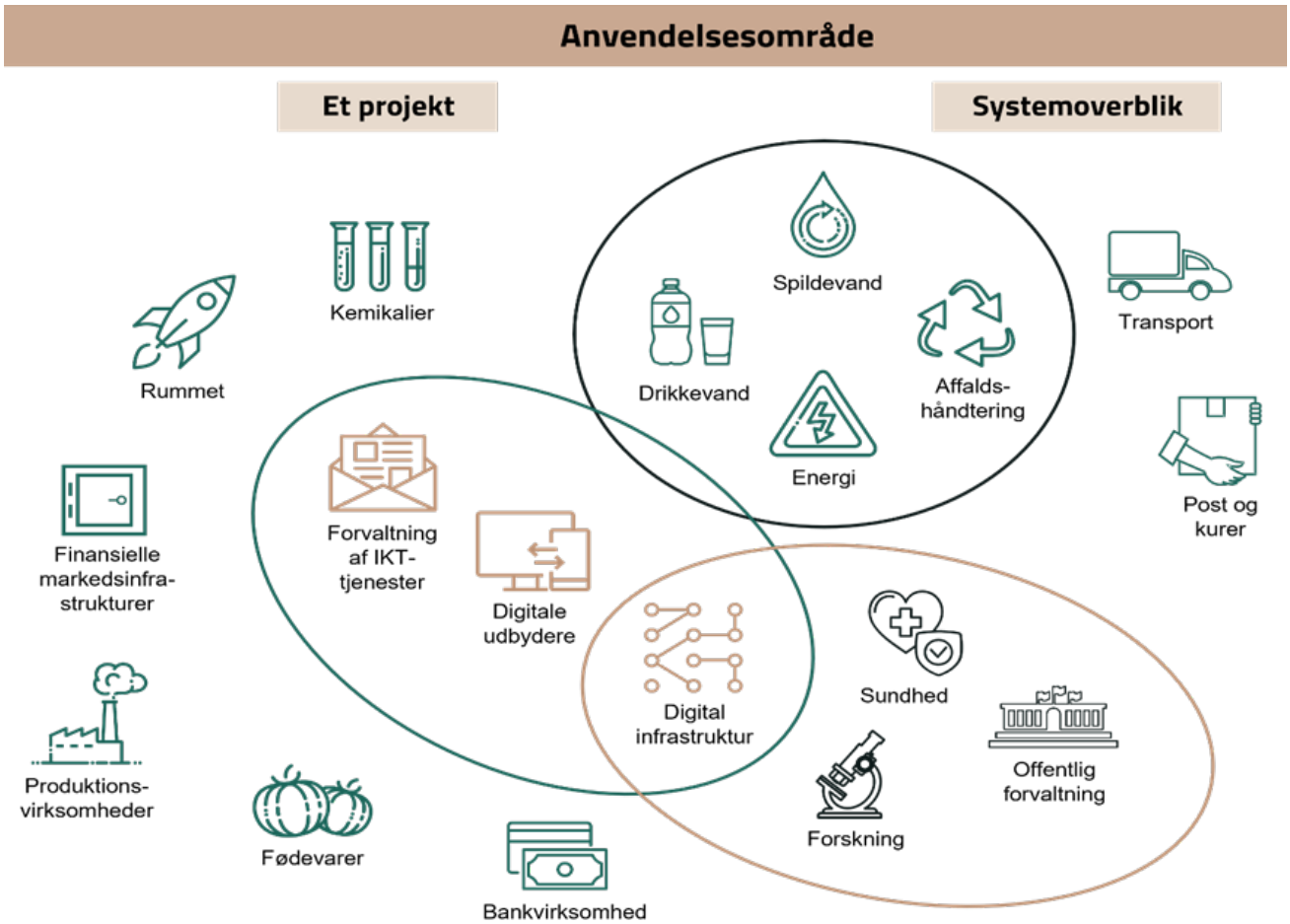
Hvad er formålet med NIS2-direktivet?

- At højne beskyttelsen af den digitale infrastruktur så samfundskritiske funktioner kan fortsætte deres drift trods f.eks. et cyberangreb. Direktivet har således fokus på tilgængeligheden af tjenester

Hvad er konsekvenserne ved manglende overholdelse af NIS2?

- Bøder på op til 75 mio. kr. eller 2 procent af omsætningen
- Ledelsen kan gøres ansvarlig for manglende overholdelse af NIS2

Hvem er direkte omfattet af NIS2-direktivet?



Virksomheder, der har under 50 ansatte og en årlig omsætning eller samlet årlig balance på under 10 mio. euro, er som udgangspunkt ikke omfattet af NIS2-direktivet.

---

[1] Chrome-xtension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvur

mod-danmark-2023.pdf

[2] Alle fysiske og ikke fysiske komponenter og kommunikationstjenester

[3] https://www.linkedin.com/feed/update/urn:li:activity:7081185567308218368/

<

Mette Reeberg Delfs
Cand. jur.
20 81 19 04 · mrd@roesgaard.dk