Welkom in de **Digital Decade**

Johnny R.F. Honing – ICTRecht – j.honing@ictrecht.nl

ICTRECHT

Digitale Decade

- 2020 – aankondiging Digital Decade door de EU
- Reden:
  - Maatschappij en economie steeds afhankelijker van het digitale domein
  - Toename cyberdreigingen
  - COVID-19 versnelde de digitale transformatie
- Doelen:
  - Veiligheid en digitale soevereiniteit
  - Betere bescherming van privacy en rechten van de burger
  - Stimuleren van economische groei en innovatie
  - Inclusiviteit en gelijke toegang

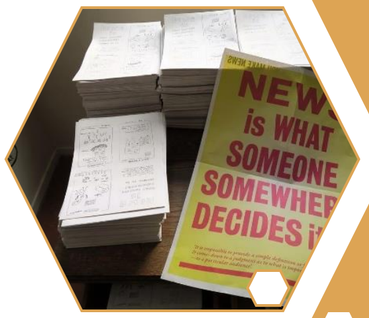
ICTRECHT

Table 1: Overview of EU Legislations in the Digital Sector

Applicable law	Published in the Official Journal of the European Union.
In negotation	Proposal by the European Commission entered the legislative process.
Planed initiative	Mentioned by the European Commission as potential legislative initiative.

Research & Innovation	Industrial Policy	Connectivity	Data & Privacy	IPR	Cybersecurity	Law Enforcement	Trust & Safety	E-commerce & Consumer Protection	Competition	Media	Finance
Digital Europe Programme Regulation, (EU) 2021/694	Recovery and Resilience Facility Regulation, (EU) 2021/241	Frequency Bands Directive, (EEC) 1987/372	ePrivacy Directive, (EC)2002/58, 2017/0003(COD)	Database Directive, (EC) 1996/9	Regulation for a Cybersecurity Act, (EU) 2019/881, 2023/0108(COD)	Law Enforcement Directive, (EU) 2016/680	Product Liability Directive (PLD), (EEC) 1985/374, 2022/0302(COD)	Unfair Contract Terms Directive (UCTD), (EEC) 1993/13	EC Merger regulation, (EC) 2004/139	Satellite and Cable Directive, (EEC) 1993/83	Common VAT system, (EC) 2006/112, 2022/0407(CNS)
Horizon Europe Regulation, (EU) 2021/695, (EU) 2021/764	InvestEU Programme Regulation, (EU) 2021/523	Radio Spectrum Decision, (EC) 2002/676	European Statistics, (EC) 2009/223, 2023/0237(COD)	Community Design Directive, (EC) 2002/6, 2022/0391(COD)	Regulation to establish a European Cybersecurity Competence Centre, (EU) 2021/887	Directive on combating fraud and counterfeiting of non-cash means of payment, (EU) 2019/713	Toys Regulation, (EC) 2009/48, 2023/0290(COD)	Price Indication Directive, (EC) 1998/6	Technology Transfer Block Exemption, (EU) 2014/316	Information Society Directive, (EC) 2001/29	Administrative cooperation in the field of taxation, (EU) 2011/16
Regulation on a pilot regime for distributed ledger technology, (EU) 2022/858	Connecting Europe Facility Regulation, (EU) 2021/1153	Open Internet Access Regulation, (EU) 2015/2120	General Data Protection Regulation (GDPR), (EU) 2016/679	Enforcement Directive (IPR), (EC) 2004/48	NIS 2 Directive, (EU) 2022/2555	Regulation on interoperability between EU information systems in the field of borders and visa, (EU) 2019/817	European Standardization Regulation, (EU) 2012/1025	E-commerce Directive, (EC) 2000/31	Company Law Directive, (EU) 2017/1132, 2023/0089(COD)	Audio-visual Media Services Directive (AVMSD), (EU) 2010/13	Payment Service Directive 2 (PSD2), (EU) 2015/2366, 2023/0209(COD)
	Regulation on High Performance Computing Joint Undertaking, (EU) 2021/1173, 2024/0016(CNS)	European Electronic Communications Code Directive (EECC), (EU) 2018/1972	Regulation to protect personal data processed by EU institutions, bodies, offices and agencies, (EU) 2018/1725	Directive on the protection of trade secrets, (EU) 2016/943	Cybersecurity Regulation, (EU) 2023/2841	Regulation on terrorist content online, (EU) 2021/784	Radio Equipment Directive (RED), (EU) 2014/53	Unfair Commercial Practices Directive (UCPD), (EC) 2005/29	Market Surveillance Regulation, (EU) 2019/1020	Portability Regulation, (EU) 2017/1128	Digital Operational Resilience Act (DORA Regulation), (EU) 2022/2554
	Regulation on Joint Undertakings under Horizon Europe, (EU) 2021/2085, 2022/0033(NLE)	.eu top-level domain Regulation, (EU) 2019/517	Regulation on the free flow of non-personal data, (EU) 2018/1807	Design Directive, 2022/0392(COD)	Information Security Regulation, 2022/0084(COD)	Temporary CSAM Regulation, (EU) 2021/1232, 2022/0155(COD)	eIDAS Regulation (European Digital Identity Framework), (EU) 2014/910	Directive on Consumer Rights (CRD), (EU) 2011/83	P2B Regulation, (EU) 2019/1150	Satellite and Cable II Directive, (EU) 2019/789	Crypto-assets Regulation (MiCA), (EU) 2023/1114
	Decision on a path to the Digital Decade, (EU) 2022/2481	Roaming Regulation, (EU) 2022/612	Open Data Directive (PSI), (EU) 2019/1024	Compulsory licensing of patents, 2023/0129(COD)	Cyber Resilience Act, 2022/0272(COD)	E-evidence Regulation, (EU) 2023/1543	Regulation for a Single Digital Gateway, (EU) 2018/1724	e-invoicing Directive, (EU) 2014/55	Single Market Programme, (EU) 2021/690	Copyright Directive, (EU) 2019/790	Financial Data Access Regulation, 2023/0205 (COD)
	European Chips Act (Regulation), (EU) 2023/1781	Union Secure Connectivity Programme, (EU) 2023/588	Data Governance Act (DGA Regulation), (EU) 2022/868	Standard essential patents, 2023/0133(COD)	Cyber Solidarity Act (Regulation), 2023/0109(COD)	Digitalisation of cross-border judicial cooperation, (EU) 2023/2844	General Product Safety Regulation, (EU) 2023/988	Regulation on cooperation for the enforcement of consumer protection laws, (EU) 2017/2394	Vertical Block Exemption Regulation (VBER), (EU) 2022/720	European Media Freedom Act, (EU) 2024/1083	Payment Services Regulation, 2023/0210(COD)
	Establishing the Strategic Technologies for Europe Platform (STEP), (EU) 2024/795	Gigabit Infrastructure Act, (EU) 2024/1309	European Data Act (Regulation), (EU) 2023/2854			Directive on combating violence against women, 2022/0066(COD)	Machinery Regulation, (EU) 2023/1230	Geo-Blocking Regulation, (EU) 2018/302	Digital Market Act (DMA Regulation), (EU) 2022/1925	Remuneration of musicians from third countries for recoredd music played in the EU	Digital euro, 2023/0212 (COD)
	European critical raw materials act (Regulation), (EU) 2024/1252	New radio spectrum policy programme (RSPP 2.0)	Interoperable Europe Act, (EU) 2024/903			Directive for combating sexual abuse and child sexual abuse material, 2024/0035(COD)	AI Act (Regulation), 2021/0106(COD)	Digital content Directive, (EU) 2019/770	Regulation on distortive foreign subsidies, (EU) 2022/2560		Regulation on combating late payment, 2023/0323(COD)
	Net Zero Industry Act, 2023/0081(COD)	Digital Networks Act	Regulation on data collection for short-term rental, (EU) 2024/1028			Digitalization of travel documents	Eco-design Regulation, 2022/0095(COD)	Directive on certain aspects concerning contracts for the sale of goods, (EU) 2019/771	Horizontal Block Exemption Regulations (HBER), (EU) 2023/1066, (EU) 2023/1067		
	EU Space Law		European Health Data Space (Regulation), 2022/0140(COD)				AI Liability Directive, 2022/0303(COD)	Digital Services Act (DSA Regulation), (EU) 2022/2065	Platform Work Directive, 2021/0414(COD)		
			Harmonisation of GDPR enforcement procedures, 2023/0202(COD)					Political Advertising Regulation, (EU) 2024/900	Single Market Emergency Instrument (SMEI), 2022/0278(COD)		
			Access to vehicle data, functions and resources					Right to repair Directive, 2023/0083(COD)			
			GreenData4all					Consumer protection: strengthened enforcement cooperation			

ICTRECHT



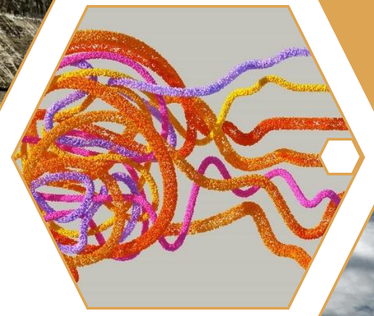
Digitale identiteit

Cyber en weerbaarheid

Infrastructuur en toegang

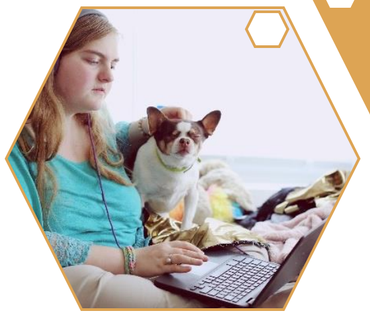
Digitale economie en markten

Data en privacy



Inhoud en expressie

Mensgericht en inclusief



Digitale soevereiniteit

ICTRECHT

Certificering en keuring

Cybersecurity Act

Sectorspecifieke security

NIS2 / CER

Cyber Resilience Act

DORA

Cybersecurity en weerbaarheid

Digitale weerbaarheid

Cyber Solidarity Act

Data-eigendom

Data Act

GDPR

EHDS

Photo by Bikram Bezbaruah, Pexels

Doel en reikwijdte (NIS2)

1. Europese Richtlijn gericht op kritieke en belangrijke infrastructuur met strengere eisen voor cybersecurity maatregelen.
2. Nederlandse implementatiewet is de Cyberbeveiligingswet.
3. Gericht op het vergroten van de cyberweerbaarheid van organisaties.
4. Van toepassing op verschillende sectoren en er wordt een onderscheid gemaakt tussen ”grote”, ”middelgrote” en ”kleine” organisaties.

Bijlage I (Zeer kritieke sectoren)	Bijlage II (Andere kritieke sectoren)
Energie	Post- en koeriersdiensten
Vervoer	Afvalstoffenbeheer
Infrastructuur voor de financiële markt	Productie, verwerking en distributie van levensmiddelen
Gezondheidszorg	Vervaardiging
Drinkwater	Digitale aanbieders
Afvalwater	Onderzoek
Digitale infrastructuur	
Beheer van ICT-diensten (business-to-business)	
Overheid	
Ruimtevaart	

Belangrijkste verplichtingen

1. **Governance:** Van het bestuur wordt meer betrokkenheid verwacht. Zo moet er meer kennis zijn op het gebied van cyberbeveiliging en kunnen zij aansprakelijk gesteld worden.
2. **Registratieplicht:** Essentiële en belangrijke organisaties moeten zich registreren als NIS2-plichtig op mijn.ncsc.nl.
3. **Zorgplicht:** 10 maatregelen waar een organisatie aan moet voldoen:
   - Beleid inzake risicoanalyse en beveiliging van informatiesystemen.
   - Incidentbehandeling.
   - Bedrijfscontinuïteit, zoals back-up beheer en noodvoorzieningenplannen, en crisisbeheer;
   - Beveiliging van de toeleverancierskеten.
   - Beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen.
   - Beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen.
   - Cyberhygiëne en training op het gebied van cybersecurity.
   - Beleid en procedure inzake het gebruik van cryptografie en, in voorkomend geval, encryptie.
   - Beveiligingsaspecten, t.a.v. personeel, toegangsbeleid en beheer van activa.
   - Multifactor-authenticatie (wanneer gepast).
4. **Meldplicht:** Wanneer een organisatie vermoed dat er een (significant) incident plaatsvindt moet de organisatie dit melden bij de toezichthouder plus het C-SIRT.

Aansprakelijkheid en gevolgen

Aansprakelijkheid:

- Bestuur/Sr. Management -> Persoonlijke aansprakelijkheid bij nalatigheid.

Sancties:

- Boetes: max 10 mln. Euro / 2% wereldwijde omzet.
- Toezicht: (o.a.) RDI en IGJ houdt toezicht en handhaaft.

Best practice:

Governance & toezicht aantoonbaar maken:

- Notulen waarbij risicomanagement en cybersecurity vast topics zijn
- Audits/assessments
- Oefeningen & trainingen

Gevolgen bij niet-naleving:

- Imagoschade
- Juridische claims
- Bestuurswissels

In de kern – Verantwoordelijkheden van de top

Verantwoordelijkheid voor risicobeheer

Bestuur blijft eindverantwoordelijk voor de implementatie en het toezicht op cybersecuritymaatregelen.

Bevoegde kennis en vaardigheden

Verplichting om voldoende kennis van cybersecurity op bestuursniveau te waarborgen (bijv. door opleiding en externe ondersteuning).

Actieve betrokkenheid bij risicobeheersmaatregelen

Niet delegeren zonder toezicht: bestuur moet betrokken zijn bij keuzes en prioriteiten van beveiligingsmaatregelen.

Aansprakelijkheid bij nalatigheid

Persoonlijke sancties mogelijk bij onvoldoende betrokkenheid of grove nalatigheid.

Bevorderen continuïteit en weerbaarheid

Integratie van cyberweerbaarheid in bedrijfscontinuïteitsplannen en crisismanagement.

Van wet naar compliance – hoe nu verder in de praktijk?

Start met een 0-meting en een GAP-analyse – Waar staan we nu?

Doel: Inzicht krijgen in de huidige situatie.

Wat je kunt doen:

- Verzamel bestaande documentatie (beleid, procedures, incidentenregisters).
- Interview sleutelfunctionarissen (Sr. Management, IT, Compliance, Security, Operations).
- Gebruik een maturity model of checklist (bijv. NIS2 maturity model of ISO/IEC 27001/ NEN7510-1/2 als basis).

Praktische tools:

- Zelfevaluatietool NIS2 (of vergelijkbaar op het gebied van CRA/DORA).
- GAP-analyse checklist per wetgeving.
- Noodzakelijke vragen: *Welke processen zijn al ingericht? Wat is nog onbekend terrein?*

ICTRECHT

Stel een roadmap op

Doel: Concrete stappen plannen richting compliance.

Fasering in de roadmap:

- **Quick wins** (bijv. Opstellen van beleid, awareness training, rollen en verantwoordelijkheden beleggen).
- **Structurele acties** (bijv. opzetten ISMS, risicoanalyses, leveranciersbeoordeling).
- **Langetermijnplanning** (bijv. auditvoorbereiding, scenario-oefeningen, technische maatregelen).

Praktisch:

- Maak een tijdslijn van max. 12 maanden.
- Benoem voor elke stap: *wie*, *wat*, *wanneer*, *welke wetgeving raakt dit?*

Bouw een Compliance-toolkit

Essentiële onderdelen:

- **Risicobeoordeling-template** (IRAM2, ISO 31000).
- **Incident response plan** (NIS2, DORA, NEN7510).
- **Leverancierbeoordeling** (voor CRA en DORA-ketenverantwoordelijkheid).
- **Awareness materiaal** (voor medewerkers en management).

Praktisch:

- Gebruik bestaande frameworks (NIST, ISO, NEN, OWASP).
- Open-source tools en templates kunnen veel werk besparen (bijv. CIS Controls).

Takeaways

1. **Begin met inzicht**
   Je hoeft niet meteen alles op orde te hebben. Een 0-meting maakt duidelijk waar de gaten zitten.
2. **Gebruik bestaande (maturity) modellen**
   Ze helpen om pragmatisch en gestructureerd te groeien richting compliance.
3. **Wees een bruggenbouwer**
   Jij kunt IT, business en wetgeving met elkaar verbinden.
   Durf klein te beginnen
   Quick wins zoals awarenesscampagnes en basale risicobeoordelingen maken al veel verschil.
4. **Blijf leren**
   De wet –en regelgeving verandert snel. Volg updates en blijf kritisch kijken naar processen en verantwoordelijkheden.