Haavind

Launching software/digital services in Europe?

Fluid market dynamics should be factored in at every stage of software development:

→ A wave of new tech regulations (such as the Data Act and DSA and AI act) impact design, data practices, and user interactions

→ Security expectations keep rising, accelerated by EUs cybersecurity laws and political tension

→ Innovation moves fast, especially in AI. Flexible systems that can adapt quickly and at the same time meet legal standards can be competitively advantageous

Haavind

Mapping legal requirements across the software lifecycle

Some abbreviations to be used

AI Act
=
Artificial Intelligence Act
(*Regulation 2024/1689)*

Partly applicable in the EU

Data Act
=
Regulation 2023/2854

Applicable in the EU from 12.09.25

CRA
=
Cyber Resilience Act
(*Regulation 2024/2847)*

Applicable in the EU from 11.12.27

NIS2
=
Network and Information Security Directive
(*2022/2555)*

Applicable in the EU**

DSA
=
Digital Services Act
(*Regulation 2022/2065)*

Applicable in the EU

DORA
=
Digital Operational Resilience Act
(*Regulation 2022/2554)*

In force in Norway

Omnibus
=
Enforcement and modernisation directive
(*2019/2161)*

In force in Norway

* "ish" – most member states have not yet transposed the directive

** "Fun" fact: Norway is currently implementing the NIS1 directive, NIS2's predecessor

Mapping legal requirements should be an integral

NIS2 assumes **early** threat modeling, secure coding practices, vulnerability management, testing, and changes in a way that the security controls are traceable to risk decisions.

The CRA requires assessments of cybersecurity risk for products with digital elements to be taken into account **during planning, design and development**

To implement appropriate technical and organizational measures under the GDPR, risk assessments must be conducted and documented **prior to** processing personal data

Risk assessment & documentation

NIS2 requires **risk management to extend to suppliers**, requiring assessing supplier security practices, contractual security requirements, and maintaining evidence of controls across the supply chain

The CRA requires a **formal record** containing details and supply chain relationships of components included in the software elements of a product with digital elements

Processing of personal data by sub-contractors assumes **being able to document** them providing sufficient guarantees to meet requirements under the GDPR

Supply Chain Management

Depending on the product, the AI Act demands a "by design" approach where risk categorization, transparency, and human oversight **shape your architecture from day one**

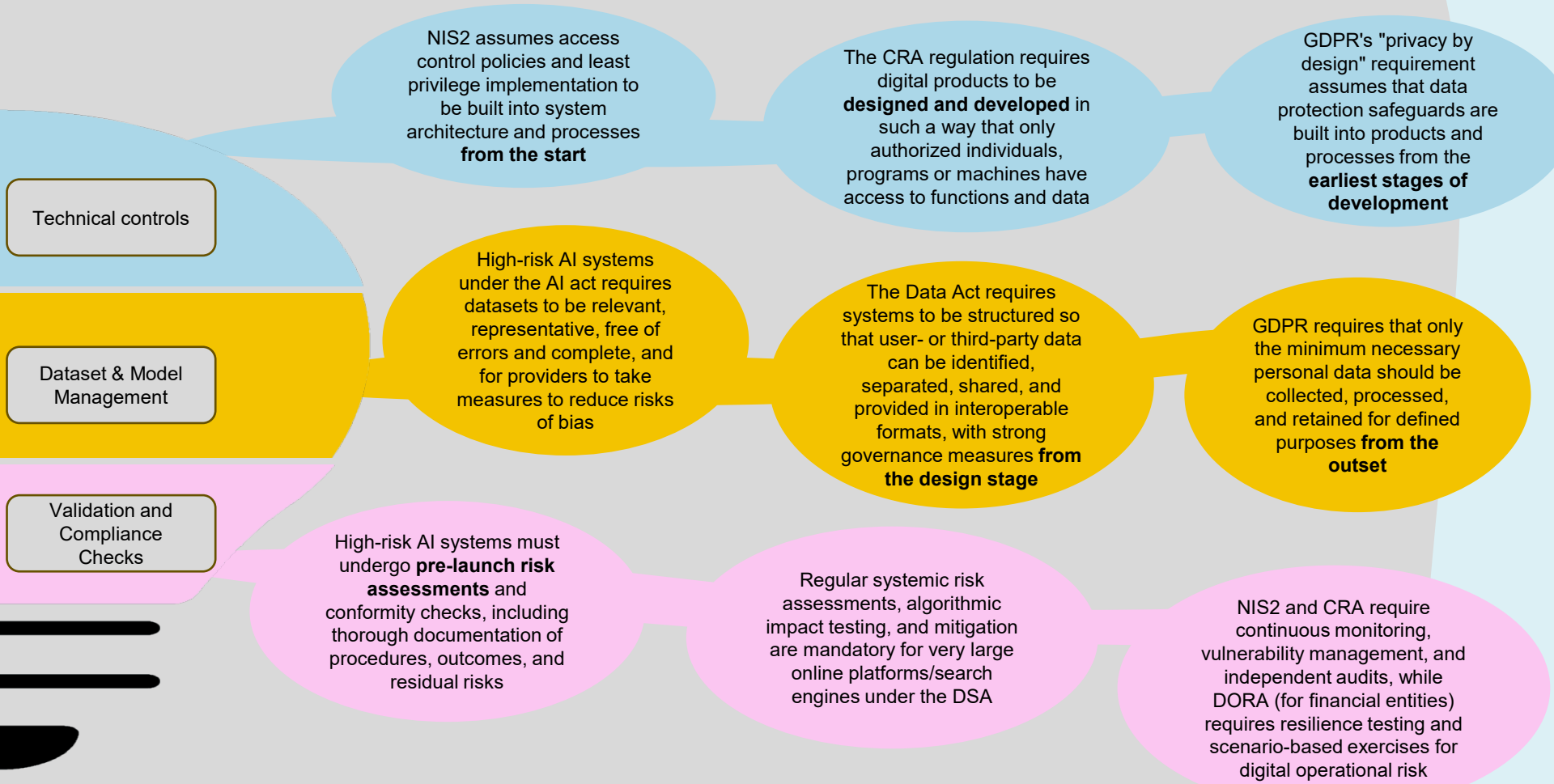
The AI Act assumes use of lawful training data, minimization of bias, and a **clear audit trail**. System logs, technical documentation, and clear instructions for use should be built into your development process

Data sharing obligations under the Data Act requires **established processes** for access management and interoperability. Your system architecture will determine how easy it is to grant, restrict, or trace access to data later

AI transparency & Data Governance

Applicable to IoT providers and "related services"

part of software design&development



Getting ready

Compliance documentation should now be established, up-to-date and cross-regulation ready

AI Act

- Comprehensive description of AI system
- Documented process of risk/benefit analysis
- Audit trails

NIS2

- Documented ISMS
- Incident response and business continuity plans
- Staff training records on security
- Software vulnerability handling procedure

CRA

- Comprehensive technical file for each product
- EU Declaration of Conformity
- Policy and process for issuing security updates

DORA

- Contractual documentation for all ICT third-party service relationships
- Disaster recovery plans and evidence of regular testing

Data Act

- Documentation of safeguards for trade secrets and personal data
- Described measures for preventing international governmental access to data held in the EU.

New transparency obligations also apply in B2B-service offerings

- Information that a user interacts with an AI System and detailed summary of datasets used for training the model (also GenAI)
- High risk: Purpose of system, conditions for proper use, how the system was trained and what data was used etc.

- Clear instructions & cybersecurity info, such as default security settings, supported lifetime, known residual risks
- Security update policy with timeframes
- Contact points for vulnerability reporting

- Information to users/third parties on how to access, share, or control their data
- Information on available switching and porting methods and formats as well as restrictions and technical limitations

for market

Providing software to consumers? Get the new information obligations right from the start

Omnibus

Right of withdrawal and information obligations now applies explicitly to digital services and online marketplaces, e.g:

- Main product features, including functionality and technical protection measures
- Existence of right to withdrawal
- Compatibility and interoperability (with hardware or software)
- Online marketplaces: Parameters that determine the ranking of offers in search results, and the relative importance of these parameters compared to others

DSA

All Intermediary Services

- Clear, plain-language terms about content moderation policies, restrictions, and user rights
- Establish process for annual transparency report

Hosting&Online Platforms

- Mechanism for and information about how to report illegal content
- Statement of reasons for restrictions on users, e.g. visibility of specific items (hosting services)
- Mechanism to contest user restrictions and clear and user-friendly information about how to seek redress.

Online Platforms

- Identification of adverts and display main parameters used for targeting, including who paid for the ad
- Explain to users when content is recommended using recommender systems and give information about the main parameters that influence their recommendations
- "Compliance by design" traders must be enabled to comply with pre-contractual information obligations (marketplaces)
- Internal complaint-handling system
- Prohibition on "dark patterns"

Very large Online Platforms (45M+ EU users)

- More detailed and frequent public reporting requirements
- Maintain publicly accessible ad repositories with targeting criteria and reach
- Perform and publish independent audits of systemic risks and mitigation measures
- Transparency about risk management processes for illegal/harmful content and impact on fundamental rights

Selling &

Clear, compliant contracts build

New legislation will influence B2B contract drafting

Data Act

Mandatory data sharing requirements for **connected products and related services:**

- Specify how and when users (and in some cases their third parties) can access data generated from products or related services
- Contract terms regarding data access/use cannot be unilaterally imposed by stronger parties, incl. prohibition of unfair contractual terms towards SMEs

Mandatory portability and data export requirements in **cloud service agreements:**

- Right to export data, incl. metadata
- Description of the export process (format, means of transfer, timeline, and support)
- Functional equivalence and obligation to supply all necessary information for the customer to make use of data
- Switching charges **banned** from Jan 2027
- Maximum notice period for switching process not exceeding two months

AI Act

No mandatory contract requirements, but AI software contracts should:

- Clarify roles and responsibilities ("provider", "deployer" etc.)
- Indicate contractual limitations on the customer's use of the AI system to prevent unlawful or unintended uses
- Clarify who is responsible for end-user transparency obligations (e.g. informing end users when interacting with an AI system)
- Detail what information and instructions businesses (deployers) will receive to enable proper human oversight, as required for high-risk AI uses
- Clarify what responsibility you are willing to take if an AI system causes loss, e.g. if outputs are faulty or discriminatory
- Clarify rights to use Customer's **input** data and define the ownership and permitted use of **AI outputs**

Cybersecurity laws

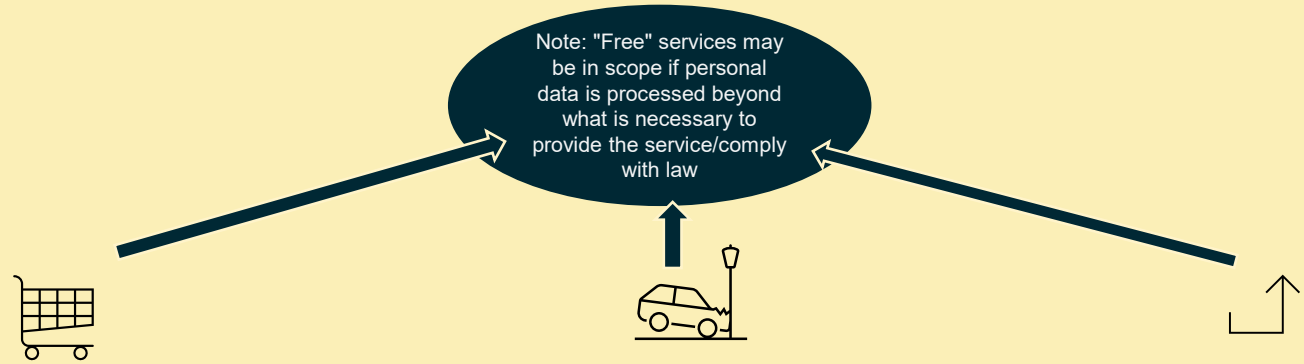
Cybersecurity laws such as NIS2, DORA and CRA will impact your contracts whether or not you are subject to such laws, as parts of your customer base will be. Contracts should:

- Define technical and organisational measures applicable to the service (if you do not define a standard, your customer will)
- Clear and realistic timeframes for notifying customers of security incidents and data breaches
- Commercial consequences of audit rights and assistance to the customer's internal compliance reviews
- Mandatory DORA requirements such as service description and locations, cooperation obligation with authorities, service level requirements, transition assistance and exit planning
- CRA:
  - Specify delivery method timing and timing for updates, at no cost to the customer
  - Support period: Minimum 5 years vulnerability handling, unless justified and agreed for tailor-made product
  - Subcontractors: Flow-down of security requirements

Contracting

lasting trust and legal certainy

Incorporate new mandatory requirements in consumer contracts



The **Digital Content Directive** imposes mandatory requirements to digital content/services in B2C relations:

- Minimum 2-year legal guarantee
- Remedies (repair, replacement, compensation) cannot be excluded
- General service guarantees unless **explicitly** deviated from, such as "fit-for-purpose", qualities and performance features normal for similar digital content or digital services
- Necessary updates free of charge
- Modifications presume valid reason, no extra cost, advance notification and (often) right to terminate

The **Revised Product Liability Directive** explicitly includes software and AI systems

- Manufacturers are strictly liable for death or personal injury, property damage and destruction or corruption of non-professional data resulting from defective software
- Defect is defined as software that does not provide the safety a person is entitled to expect (malfunctions, security failures, loss/corruption of data, etc.)
- You cannot limit or exclude product liability through software contracts
- Manufacturers of defective software integrated or connected with another product may also be liable

The **Omnibus Directive:**

- Explicitly includes digital services in the scope of the right of withdrawal, providing for a 14-day withdrawal right for digital services bought at a distance
- Obliges online marketplaces to disclose professional/trader status of sellers
- Advertised price reductions must be the lowest price you have used for the software product in the past 30 days
- If you publish reviews, you must state whether and how you verify reviews or ratings
- Provide clear contact details and instructions for making complaints or exercising consumer rights

Complying with legal requirements during ongoing delivery

Security & Updates (CRA, NIS2)

- Proactively release security patches and updates without delay
- Implement risk management and incident response (NIS2, CRA) throughout the software life cycle
- Maintain a vulnerability handling process and notify users of significant risks or fixes

Operational resilience (NIS2, DORA)

- Ensure business continuity for continued services provision
- Establish contingency, disaster recovery, and incident reporting mechanisms
- Ongoing cybersecurity training and testing, in particular Exit-scenarios under DORA

Data rights (Data Act)

- Allow users (and, in some cases, third parties designated by the user) to access and use data generated by IoT-products in real time and throughout the contract period
- Inform users of any changes regarding data accessibility, formats, and how to exercise data access/export/switching rights etc.

AI Risk Management

- Continuous risk monitoring of AI output, especially for high-risk systems. Use both technical (e.g. logs, automated flagging) and organisational means (e.g. user reporting mechanisms)
- Keep up-to-date records of detected risks, incidents, and corrections
- Supply and update technical documentation for safe use of AI systems

Mandatory consumer requirements

- Notify consumers promptly about available updates and any impact on their use of the software
- Follow mandatory procedures when making changes in software, such as advance notification, information about changes and (when applicable) providing the customer with a right to terminate.

Digital Services (DSA):

Act “expeditiously” on notifications regarding illegal content, removing or disabling access when appropriate → Provide clear information to users about your content moderation policies, including AI/automated tools used → Publish transparency reports on content moderation, use of automated tools, handling of notices → Collect and verify necessary trader information before allowing them to offer products to consumers

Andreas Gard Meyer
Senior Lawyer

a.meyer@haavind.no
+47 988 37 538

Kari Gimmingsrud
Partner

k.gimmingsrud@haavind.no
+47 922 91 006

Stian Hultin Oddbjørnsen
Partner

s.oddbjornsen@haavind.no
+ 47 957 89 414

Haavind