laissa.
Experienced.
Agile.

AI Act & EHDS Compliance in Healthcare: From Risk to Strategic Advantage

Sandra Liede
Legal Advisor
HealthTech & Life Sciences

Two Game-Changing Regulations Collide

The Perfect Storm

- Artificial Intelligence, AI Act (Aug 2026) + European Health Data Space, EHDS (Mar 2027-2031)
- Healthcare AI is at the epicenter
- Any healthcare AI system developed or deployed during this period must comply with both frameworks from day one.
- Regulatory synergy
- Dual compliance is survival, not optional
- The risk is exclusion from the EU market

Stakeholder Compliance Requirements

AI Developer/Provider (Health Tech Company)

The company must design data governance systems that satisfy both AI Act's data quality requirements and EHDS's health data protection standards simultaneously.

Healthcare Deployer (Hospital)

Hospitals must establish governance frameworks that ensure AI transparency requirements align with patient data rights under EHDS.

Healthcare Professionals

Medical professionals must balance AI Act requirements for human oversight with EHDS requirements for patient data transparency and control.

Patients (Data Subjects)

Patients gain comprehensive protection through both frameworks, with AI Act ensuring algorithmic transparency and EHDS ensuring data control.

AI Developer (Company)

AI Act Obligations:

- Implement comprehensive risk management system
- Ensure training data quality and bias mitigation
- Maintain detailed technical documentation
- Conduct conformity assessment with notified body
- Implement post-market monitoring system
- Ensure human oversight capabilities

EHDS Obligations:

- Comply with health data processing requirements for secondary use
- Implement technical and organizational measures for health data protection
- Ensure interoperability with European health data infrastructure
- Obtain necessary permits for health data processing

Healthcare Deployer (Hospital)

AI Act Obligations:

- Ensure proper human oversight during AI system deployment
- Monitor AI system performance and report serious incidents
- Provide adequate training to medical staff using the AI system
- Maintain logs of AI system usage and decisions

EHDS Obligations:

- Ensure patient consent for health data processing
- Implement data subject rights (access, portability, deletion)
- Comply with health data sharing requirements with other healthcare providers
- Maintain audit trails for health data access

Healthcare Professionals

AI Act Obligations:

- Maintain meaningful human control over AI-assisted diagnoses
- Understand AI system limitations and capabilities
- Report AI system malfunctions or unexpected behavior
- Ensure final diagnostic decisions remain under human responsibility

EHDS Obligations:

- Respect patient data rights when using AI systems
- Ensure proper consent for AI-assisted diagnosis
- Maintain professional confidentiality standards
- Support patient access to their health data and AI-generated insights

Patients (Data Subjects)

AI Act Rights:

- Right to information about AI system use in their healthcare
- Right to human review of AI-assisted medical decisions
- Protection from discriminatory AI outcomes
- Right to understand AI system logic affecting their health

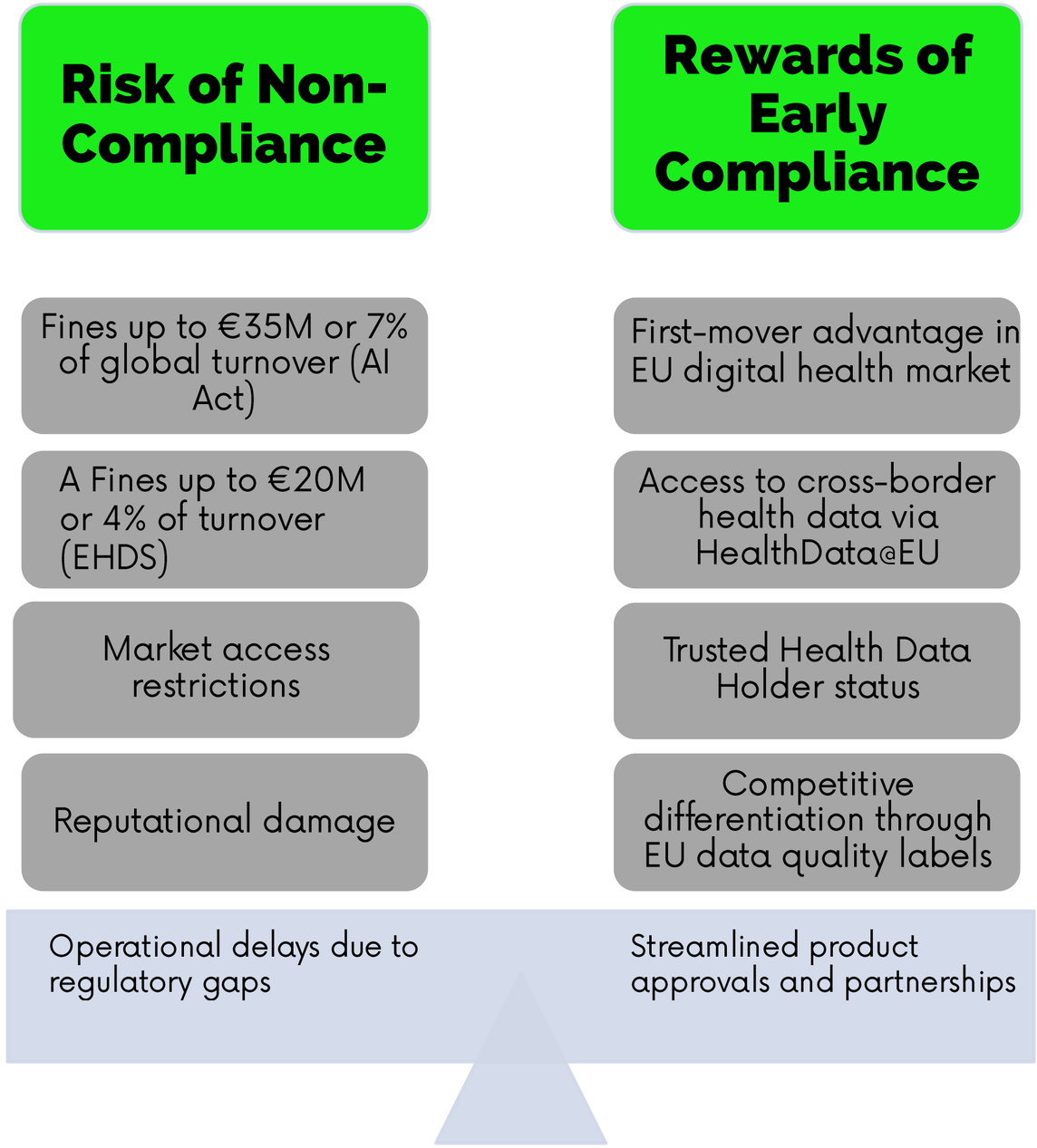
EHDS Rights:

- Enhanced control over health data processing
- Right to data portability across healthcare providers
- Right to access AI-generated health insights
- Right to restrict certain health data processing

Why This Matters

> **Market access depends on compliance**
>
> **Early compliance = competitive edge**

Example of first-mover benefit:
A Finnish health data platform may be designated as a trusted health data holder under EHDS. This status allows it to streamline data-sharing agreements with research institutions and attract EU-wide partnerships. The platform's early compliance with data quality labeling can give it a reputational edge.



Understanding High-Risk Classification

AI System Classification

- Is the system high-risk under the AI Act?

Third-Party Assessment

- Is a notified body required under MDR/IVDR?

Data Governance & Quality

- Is the dataset representative, error-free, and well-documented? (AI Act + EHDS)

Human Oversight & Transparency

- Is the system designed for human intervention? Are users informed they're interacting with AI?

Cybersecurity & Documentation

- Are AI-specific threats addressed? Is technical documentation complete?

Interoperability & Secondary Use

- Do EHR systems support EU formats? Is secondary data use secure and compliant?

Most healthcare AI systems will be classified as high-risk

- **Applies to safety components and medical devices**
- **Requires third-party conformity assessment**
- **Most healthcare AI systems are high-risk**

Examples

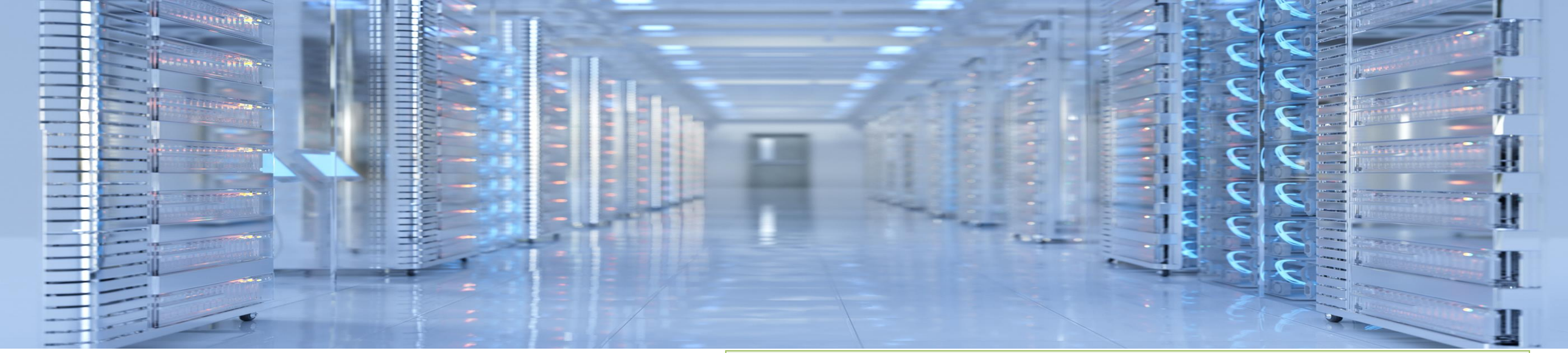
If your AI is a safety component or a medical device, and it requires third-party conformity assessment, you're in scope.

A company developing an AI-based triage assistant for emergency departments

Must classify its system as high-risk under the AIA. Because the tool influences clinical decision-making and is integrated into a CE-marked medical device, it requires third-party conformity assessment and documentation aligned with MDR and AIA standards.

A company developing an AI-powered diagnostic tool for detecting early-stage cancer

Must comply with AIA because the system is classified as high-risk. It functions as a safety component of a medical device and requires third-party conformity assessment under MDR. Company has to redesign its model to include human oversight and bias mitigation protocols before market entry.



Transforming Health Data Access

2031

EHDS – The Data Revolution

Example:
Hospital begins preparing its EHR systems to support the EHDS exchange format. This will involve upgrading legacy systems to ensure interoperability for patient summaries and prescriptions, which will be mandatory by 2029. The hospital can collaborate with Finnish vendors to align with EU technical specifications.

2027 - Foundation Phase
26 March 2027 - General Application Date
• Digital health authorities designated
• National contact points established
• Technical specifications adopted
• MyHealth@EU infrastructure ready
2029 - Phase 1 Implementation
26 March 2029 - Priority Data Categories (a-c)
• Patient summaries, ePrescriptions, medical images
• EHR systems for priority categories
• Secondary use provisions active
2031 - Phase 2 Implementation
26 March 2031 - Extended Data Categories (d-f)
• Laboratory results, discharge reports, rare disease registries
• Full EHR system compliance
• Complete Chapter III provisions
2035 - Final Phase
26 March 2035 - Full Implementation
• All Article 75(5) provisions active
• Complete EHDS ecosystem operational

Dual Compliance is the New Normal

Scenario	Applicable Regulations	Key Compliance Requirements
AI-Powered Diagnostic Software	AI Act + MDR	High-risk AI classification + medical device software classification
EHR System with Medical Device Functions	MDR + EHDS	Medical device requirements + health data interoperability
AI Health Data Analytics	AI Act + EHDS	AI risk assessment + health data access compliance
AI Medical Device in EHR System	AI Act + MDR + EHDS	Triple compliance: AI risk management, medical device safety, and health data interoperability

AIA complements MDR/IVDR

Example:
A U.S.-based health tech firm offering AI-based imaging analysis in Europe has to comply with both AIA and EHDS. Although headquarted outside the EU, their product is used in European hospitals. Must implement secure data processing environments and revise documentations to meet EU standards. Location doesn't exempt companies from compliance.

EHDS adds data access and interoperability

Example:
A Finnish startup offering AI-powered radiology analysis to hospitals across Europe has to comply with both AIA and EHDS. Although its operations are local, its AI outputs are used in other EU countries, triggering cross-border compliance obligations. Need to implement secure data environments and revise its documentation to meet both frameworks.

Unified Data Governance is Key

Both regulations demand strong data governance

Key Differences:

- Scope: AI Act covers all high-risk AI systems across sectors; EHDS specifically focuses on health data
- Data Categories: AI Act defines technical data types (training, validation, testing); EHDS defines 17 specific health data categories
- Prohibited Uses: AI Act focuses on biometric and emotion recognition restrictions; EHDS emphasizes insurance/employment discrimination prevention
- Governance: AI Act relies on market surveillance authorities; EHDS establishes specialized health data access bodies
- Secondary Use Framework: EHDS has comprehensive secondary use provisions for research and innovation; AI Act has more limited research provisions

AI Act: Bias mitigation, dataset quality

EHDS: Data quality labels, metadata standards

Action: Implement unified governance across both frameworks

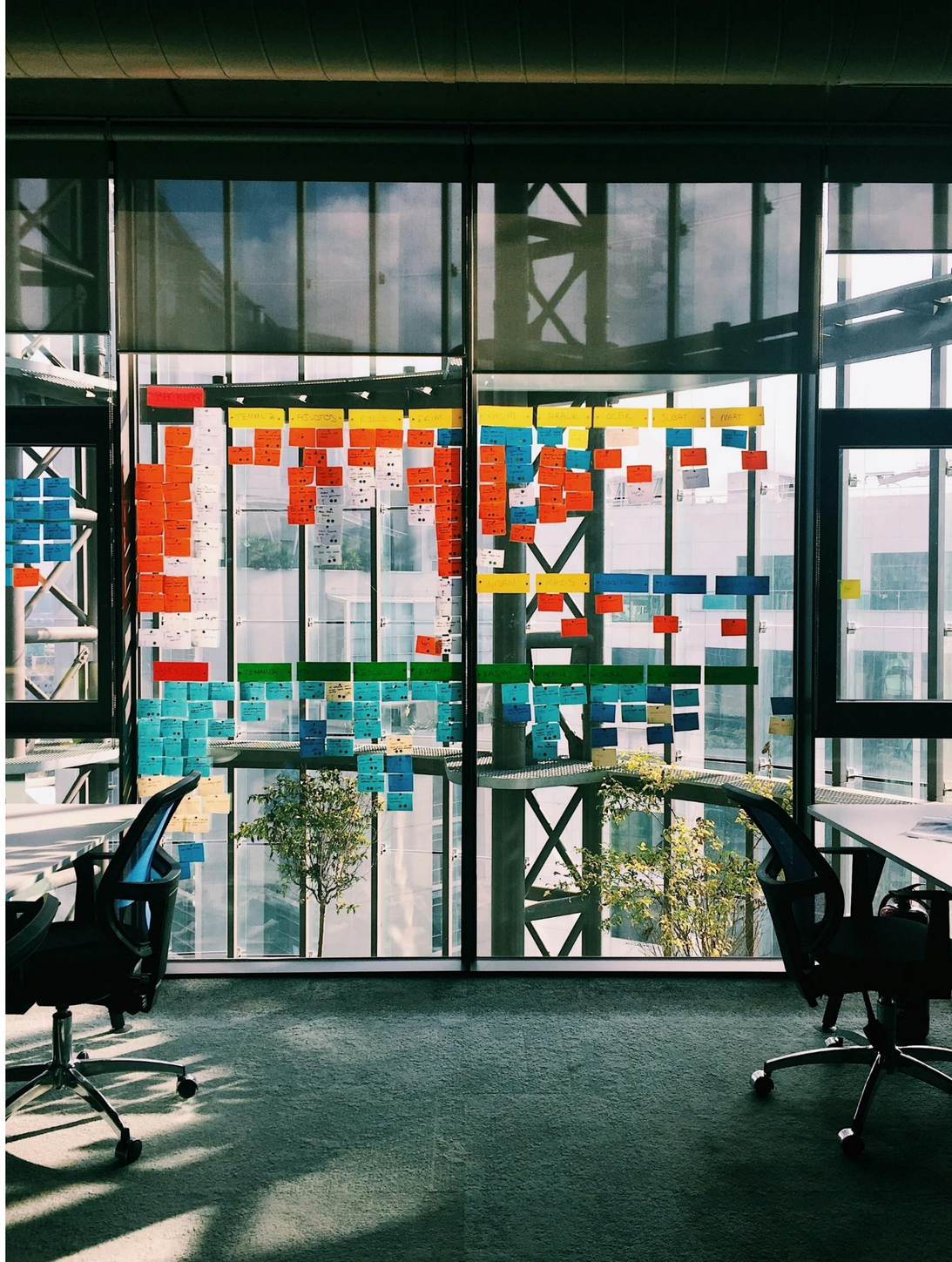
Compliance as a Catalyst for Innovation – a Gateway to Growth

Business Opportunities

- EHDS creates a harmonized EHR market, reducing fragmentation.
- Secondary use of health data opens doors for research, innovation, and AI training.
- HealthData@EU will support cross-border access.

Example: A biotech startup partners with a national health data holder to access anonymized patient data for training its AI models. Thanks to EHDS provisions, they could use the data for innovation and product development, accelerating their time to market and improving model accuracy.

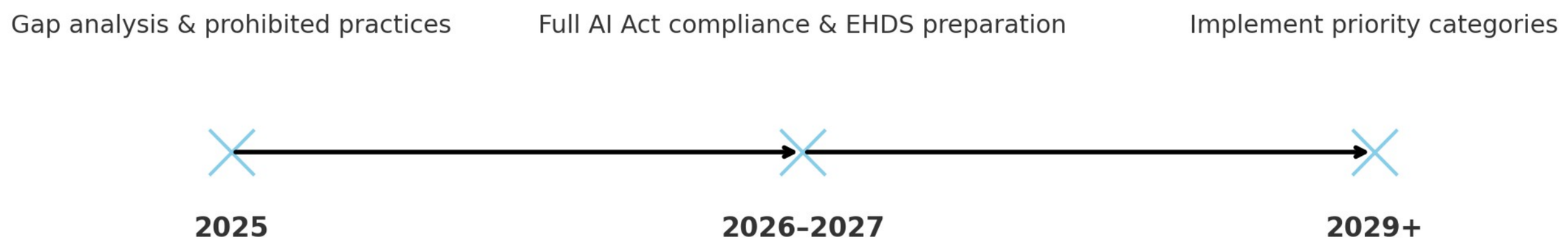
Demonstrates how compliance opens doors to valuable data and partnerships.



Your Roadmap to Compliance

Implementation Strategy

Phased Roadmap for AI Act & EHDS



Invest Smart, Monitor Proactively

Risk Mitigation

Monitor risks continuously and unify documentation systems to meet both AI Act and EHDS requirements.

Resource Allocation

Legal, technical, and training teams must work together.
Use EU testing environments to validate products.

What are you buying?

- Products / Services
- Components
- Manufacturing

Your Company

What are you selling?

- Products
- Software
- Services
- B2B: public/private
- B2C

- Written agreements
- Supply chain liability management
- IPR strategy
- Insurance framework

PRE-CONTRACT:

Vendor Due Diligence & Supply Chain Compliance

- Data protection and cross-border considerations
- Confidential information
- Legal risk assessment
- Dispute resolution

THANK YOU

FOR COMING

Contact:
Sandra.liede@laissa.fi
+358407001658

Let's connect:
https://www.linkedin.com/in/sandra-liede-40120559/

Extra slide

Anticipate the Tough Questions

What if we're not ready?

Penalties, restricted access

Documentation burden?

Templates, integration

Third-country companies?

No escape clause

Can we phase compliance?

Yes, strategically

Designing for Safety and Trust

Human oversight is a legal requirement. In healthcare, patient safety demands even stricter oversight than the regulations require.

Aspect	**AI Act**	**EHDS**
Scope of Human Oversight	Direct operational oversight of AI systems during use to prevent risks to health, safety and fundamental rights	Regulatory oversight of data access and processing compliance
Real-time Control	Humans must be able to intervene, override, or stop AI systems through 'stop' buttons	Limited real-time intervention provisions
Decision Authority	Prohibits solely automated decisions with adverse legal effects	Emphasises human decision-making independence in data access bodies
Competency Requirements	Specific AI literacy, competence, training and authority requirements for human overseers	General professional competency requirements for regulatory staff
Biometric Safeguards	Requires verification by at least two natural persons for biometric identification decisions	No specific biometric oversight provisions
Individual Rights	Right to explanation for AI-based decisions affecting individuals	Right to information about data processing and how to exercise rights