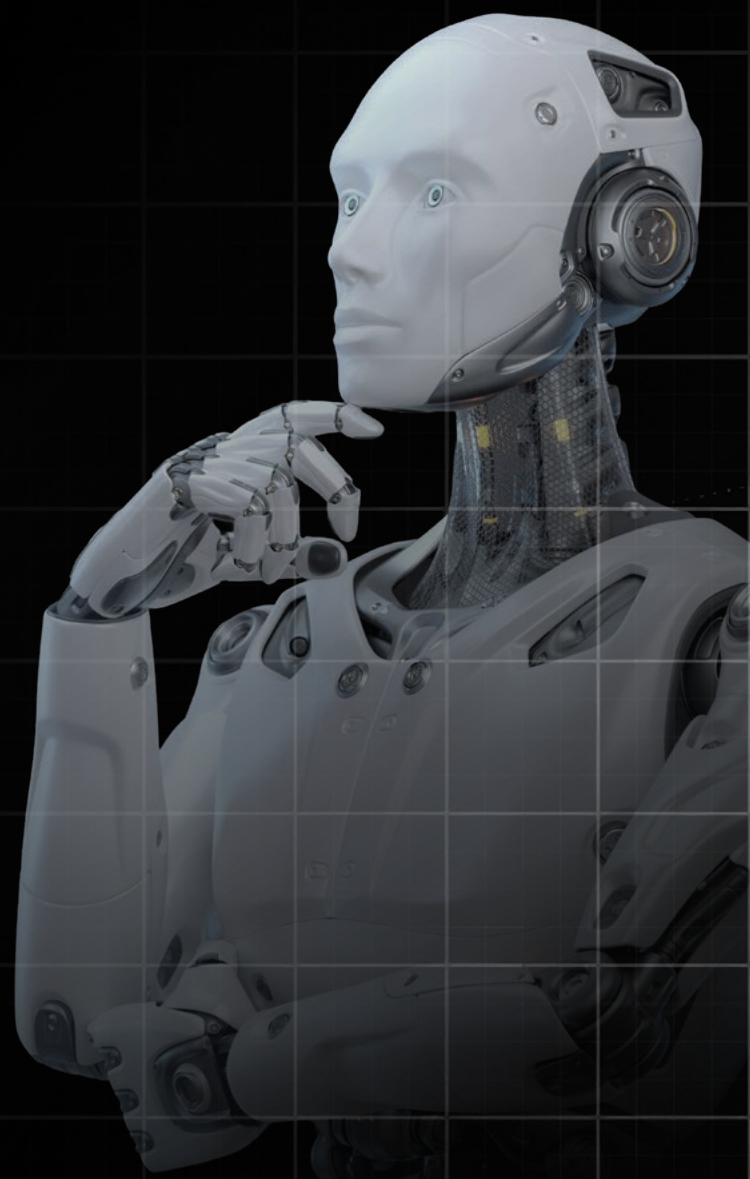


ADVANCED ROBOTICS



ADVANCED ROBOTICS



01 MACHINERY LAW

SAFETY REQUIREMENTS FOR MACHINERY

Due to their movements and direct interaction with people, robots can cause significant physical hazards. Under the Machinery Regulation, these risks, including risks arising from autonomous or self-learning functions, must be assessed at the design stage and reduced through inherently safe design and appropriate protective measures.

[Read More](#)

04 DATA PROTECTION LAW

DATA PROTECTION BY DESIGN AND BY DEFAULT

Environmental sensing by cameras, microphones, voice control or geolocation regularly entails the processing of personal data, such as images, video recordings or voices. As such processing is often unavoidable in practice, GDPR requirements concerning lawfulness, transparency and data protection governance must be considered when the robot is designed.

[Read More](#)

02 GENERAL PRODUCT SAFETY LAW

REQUIREMENTS DEPENDING ON THE INTENDED USE

Robots used in a consumer context are additionally subject to general product safety requirements. Depending on the intended purpose, product-specific requirements may take precedence. Robots with a medical purpose must, for example, meet the Medical Device Regulation requirements for safety, performance and conformity assessment.

[Read More](#)

05 CYBERSECURITY

SECURITY BY DESIGN

Connected robots may be impaired in their operation and safety by vulnerabilities, manipulation or unauthorised access. The Cyber Resilience Act therefore makes cybersecurity a mandatory product characteristic and requires it to be addressed throughout the product lifecycle, from development to vulnerability handling and security updates.

[Read More](#)

03 AI REGULATION

AUTONOMOUS DECISION-MAKING PROCESSES IN REAL TIME

The use of AI in robotic systems enables a shift from purely deterministic decision logic to direct, adaptive interaction with the environment. Functions that are regularly classified as high-risk AI are subject to extensive requirements under the AI Act regarding risk management, technical documentation and governance structures.

[Read More](#)

06 OCCUPATIONAL SAFETY

SAFETY IN WORKPLACE USE

Where robots are used in the workplace, occupational health and safety regulations must also be observed in addition to product-related safety requirements. Employers must assess the hazards associated with robot use and implement suitable technical and organisational protective measures for employees.

[Read More](#)

INFOGRAPHIC

[Read More](#)

CONTACT

[Read More](#)

MACHINERY LAW

01

ADVANCED ROBOTICS

ROBOTS ARE MACHINERY WITHIN THE MEANING OF REGULATION (EU) 2023/1230 (MACHINERY REGULATION). THE ESSENTIAL HEALTH AND SAFETY REQUIREMENTS (EHSRS, ANNEX III) APPLY WITH IMMEDIATE EFFECT FROM 20 JANUARY 2027:

- **Risk assessment.** Across the entire lifecycle, including hazards arising from AI-supported perception, path planning and human-robot collaboration (Annex III, no. 1).
- **Inherently safe design.** Design measures take priority. For collaborative robots, this includes power and force limitation before protective devices and user information.
- **Control systems and safety functions.** Safety-related software must remain deterministically controllable. Emergency stop, safe operational stop and prevention of unexpected start-up take precedence over AI decisions (Annex III, no. 1.2).
- **Conformity assessment.** Anyone integrating an AI system into a robot assumes responsibility for the overall system and CE marking. Substantial physical or digital modifications trigger a new conformity assessment procedure.
- **Technical documentation.** Technical documentation, EU declaration of conformity and CE marking. It is advisable to manage this documentation together with the AI documentation under Article 11 of the AI Act.
- **Updates and instructions.** Update capability for safety-related components and instructions specifying the limits and supervision of AI functions, digital provision is permitted.

DEADLINES AND TRANSITION

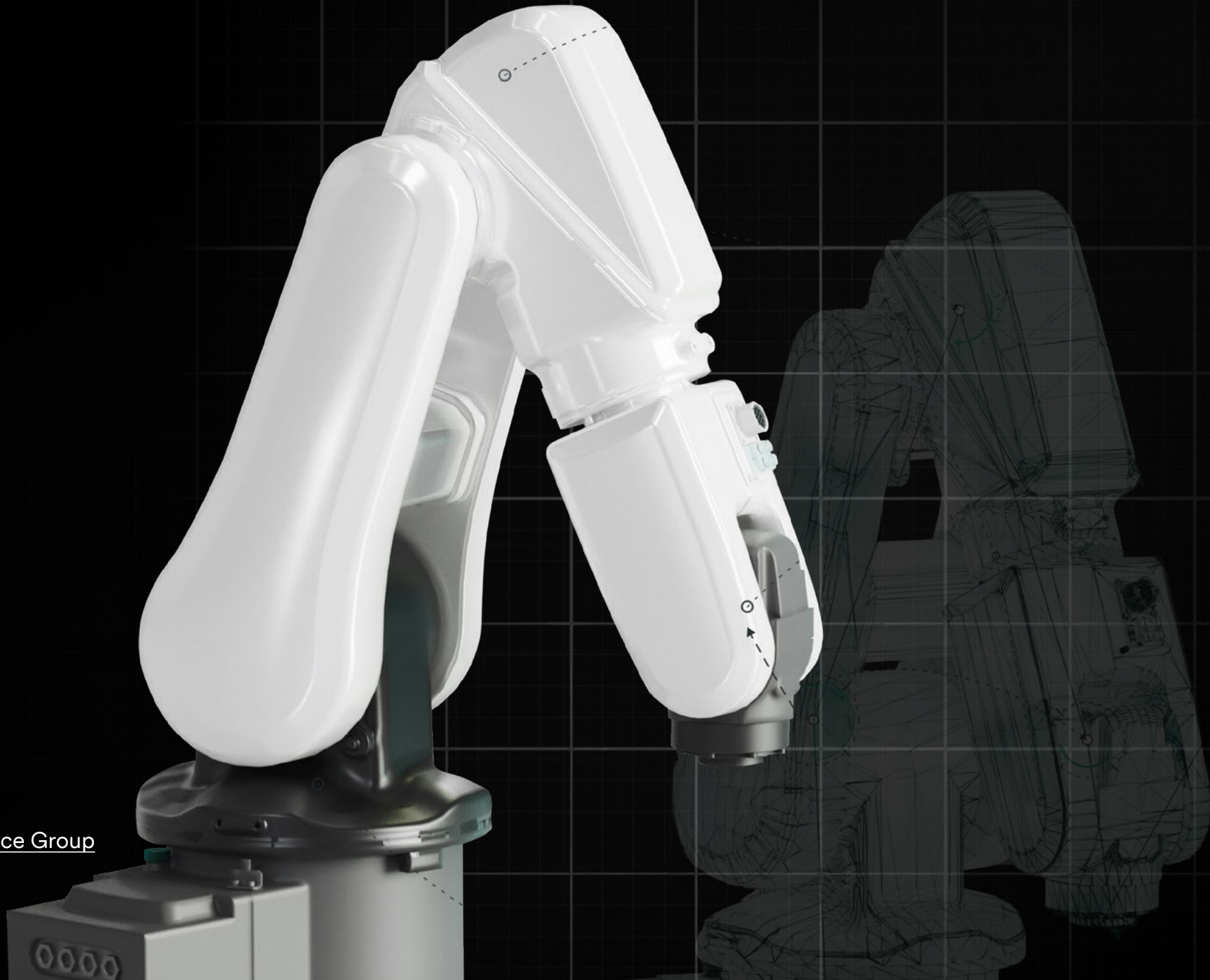
- Applicable from 20 January 2027
- :: Replaces Directive 2006/42/EC
 - :: No grandfathering in the event of a substantial modification

HARMONISED STANDARDS, ARTICLE 20

- :: No new Machinery Regulation-specific harmonised standards at present
- :: Established EN/ISO machinery standards remain important during transition, but without presumption of conformity

OTHER TECHNICAL STANDARDS

- :: DIN EN ISO 12100 – Risk assessment
- :: DIN EN ISO 10218-1/-2 – Industrial robots
- :: DIN EN ISO 13849-1 – Control systems



GENERAL PRODUCT SAFETY LAW

02

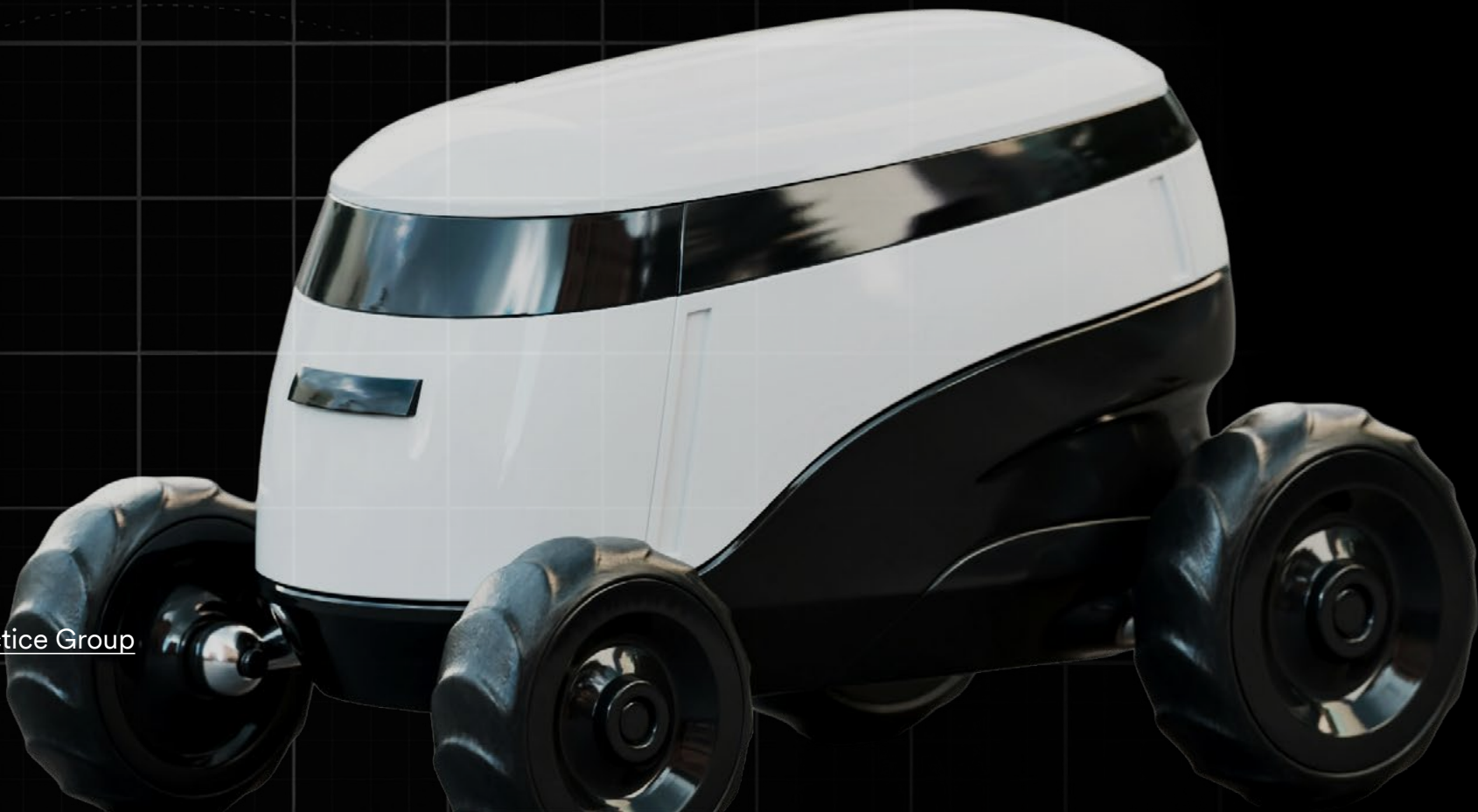
ADVANCED ROBOTICS

IN ADDITION TO THE MACHINERY
REGULATION, HORIZONTAL AND
PRODUCT-SPECIFIC REQUIREMENTS
APPLY, RANGING FROM THE GPSR AND
LOW VOLTAGE AND EMC RULES TO
RADIO EQUIPMENT AND BATTERIES.

- **Risk assessment, GPSR.** Safety, traceability and notification obligations under Regulation (EU) 2023/988 as a safety net for consumer products.
- **Low voltage.** Electrical equipment rated between 50–1,000 V AC or 75–1,500 V DC must meet the safety objectives of Directive 2014/35/EU.
- **Electromagnetic compatibility.** Emissions and immunity under EMC Directive 2014/30/EU.
- **Radio equipment.** Cybersecurity, data protection and fraud protection under Directive 2014/53/EU, including Delegated Regulation (EU) 2022/30.
- **Batteries.** Safety, sustainability, labelling and battery passport requirements under Regulation (EU) 2023/1542.
- **Market surveillance.** Obligations of economic operators and the responsible persons in the EU under Regulation (EU) 2019/1020.

THE USE CASE DETERMINES THE
APPLICABLE FRAMEWORK

- :: Medical devices
- :: Vehicles
- :: Toys



AI REGULATION

03

ADVANCED ROBOTICS

ADAPTIVE AI FUNCTIONS IN ROBOTICS ARE REGULARLY CLASSIFIED AS HIGH-RISK AI WITHIN THE MEANING OF REGULATION (EU) 2024/1689 AND REGULATION (EU) 2026/1744 (AI ACT), ENTAILING EXTENSIVE OBLIGATIONS FOR PROVIDERS.

- **Risk management.** Ensure continuous risk management throughout the lifecycle, including adaptive behaviour, to control risks to safety, health or fundamental rights.
- **Data governance.** Ensure the quality and suitability of training, validation and test datasets.
- **Documentation.** Technical documentation demonstrating compliance with the requirements of Annex IV.
- **Logging.** Automatic recording of relevant events throughout the AI system's lifetime.
- **Traceability.** Transparency requirements for design and development, together with instructions for use.
- **Human oversight.** Effective human supervision during operation, enabled by suitable human-machine interfaces.
- **Technical reliability.** Accuracy, robustness and cybersecurity against manipulation.
- **Quality management.** A quality management system for quality control and quality assurance.

HARMONISED STANDARDS, ARTICLE 40

- :: EN 18286:2026 – AI quality management
- :: prEN 18228 – Risk management (draft)
- :: prEN 18229-1 – Trustworthy AI framework (draft)
- :: prEN 18282 – Human oversight (draft)

OTHER TECHNICAL STANDARDS

- :: ISO/IEC 42001 – AI management system
- :: ISO/IEC 23894 – AI risk management
- :: ISO/IEC 24028 – AI trustworthiness
- :: ISO/IEC 24029-1 – AI robustness

THE AI ACT AND THE MACHINERY REGULATION INTERLOCK AT KEY POINTS, INCLUDING ARTICLE 9 PARA. 10 AND ARTICLE 11 PARA. 2 OF THE AI ACT. IN PRACTICE, THESE OVERLAPS SHOULD BE SPECIFICALLY REVIEWED FOR SYNERGIES AND EFFICIENCY GAINS.



DATA PROTECTION LAW

04

ADVANCED ROBOTICS

SENSORS, CAMERAS AND VOICE CONTROL REGULARLY ENTAIL THE PROCESSING OF PERSONAL DATA. THE GDPR THEREFORE ALREADY CONSTITUTES A DESIGN REQUIREMENT FOR ROBOTIC SYSTEMS. OPERATIONAL AND SENSOR DATA MAY ALSO QUALIFY AS PRODUCT DATA UNDER THE DATA ACT.

DIGITAL OMNIBUS

- :: Adjustments to consent and access to terminal equipment
- :: Facilitations for AI training based on legitimate interests
- :: Deadlines and final wording remain open

RELEVANT LEGISLATION

- :: GDPR – Regulation (EU) 2016/679
- :: Data Act – Regulation (EU) 2023/2854
- :: ePrivacy Directive 2002/58/EC and TDDDG

OTHER TECHNICAL STANDARDS

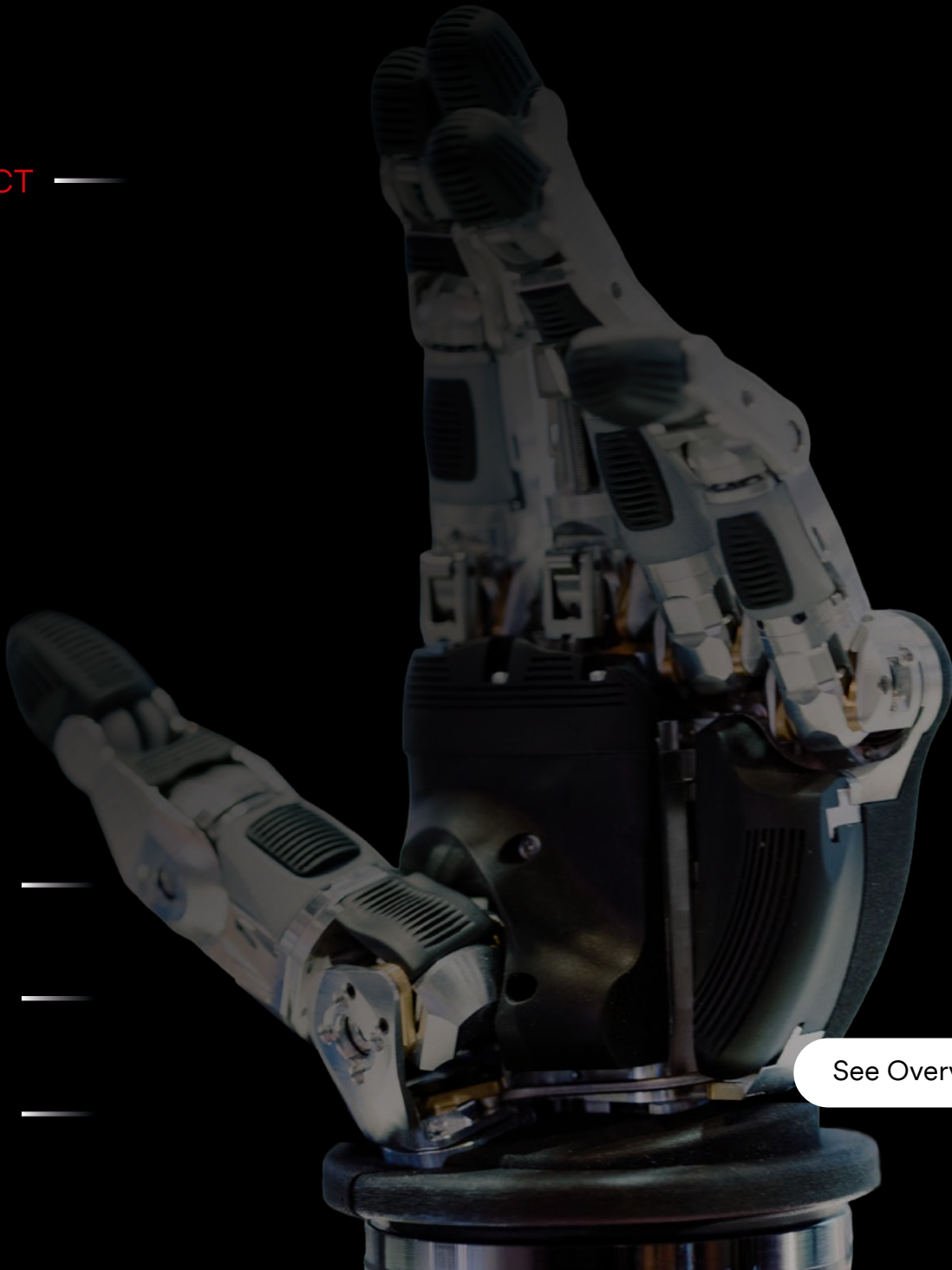
- :: ISO/IEC 27701 – PIMS
- :: ISO/IEC 27001 – ISMS
- :: ISO/IEC 29100 – Privacy framework
- :: EDPB Guidelines 3/2019 – video devices
- :: ISO/IEC 24029-1 – AI robustness

- **Legal basis.** Collection by camera, microphone or geolocation requires a legal basis. Biometric and health data additionally require compliance with Article 9.
- **Privacy by design and by default.** Technical and organisational measures must be incorporated during development, with privacy-friendly default settings.
- **Data minimisation.** Prefer on-device processing, anonymise recordings and apply short retention periods.
- **Transparency and data subject rights.** Inform third parties in the operating environment. Access, erasure and objection rights must be practically implementable.
- **Data protection impact assessment.** Regularly required for systematic monitoring of public areas or automated data processing, including profiling.
- **Automated decision-making.** Limits apply to decisions without human intervention, linked to oversight under the AI Act.
- **Security and notification obligations.** State-of-the-art protection and notification of personal data breaches within 72 hours.

GDPR

- **On-device data access.** Control, sensor and status data must, where possible, be directly accessible to the operator on the robot (access by design).
- **Aftermarket and maintenance.** Operational and fault data must be provided, at the operator's request, to independent service and maintenance providers.
- **Protection of manufacturer know-how.** Data access does not extend to design and process knowledge. Trade secrets may be disclosed only subject to agreed safeguards, and data may not be used to develop a competing product.

DATA-ACT



See Overview

CYBER- SECURITY

05

ADVANCED ROBOTICS

CONNECTED ROBOTS ARE PRODUCTS WITH DIGITAL ELEMENTS. REGULATION (EU) 2024/2847 (CYBER RESILIENCE ACT) MAKES CYBERSECURITY A MANDATORY PRODUCT CHARACTERISTIC THROUGHOUT THE LIFECYCLE. DIRECTIVE (EU) 2022/2555 (NIS2) AND THE BSIG ADDITIONALLY ADDRESS TECHNICAL AND ORGANISATIONAL SECURITY REQUIREMENTS AT OPERATOR LEVEL.

CRA DEADLINES

- :: Article 14 reporting obligations from 11 September 2026
- :: Full applicability from 11 December 2027
- :: Observe transitional periods when products are modified

HARMONISED STANDARDS, ARTICLE 27 CRA

- :: No harmonised CRA standards published in the EU Official Journal yet
- :: Initial drafts available, especially horizontal EN 40000 and product-specific ETSI standards
- :: Further standards under development for OT products, semiconductors and critical products

OTHER TECHNICAL STANDARDS

- :: IEC 62443 – Industrial communication networks
- :: ISO/IEC 27001 / TISAX – ISMS
- :: EN 18031 series – Radio equipment

CRA

- **Security by Design.** Cybersecurity must be considered during concept development, design and production and is not merely a downstream protective measure.
- **Vulnerability Management.** Identify, address and document vulnerabilities throughout the support period.
- **Security updates.** Provide security updates free of charge, generally for at least five years.
- **Notification obligations.** Notify actively exploited vulnerabilities and severe incidents to ENISA and the BSI within 24/72 hours.
- **Software bill of materials.** Document components and dependencies as a basis for vulnerability management.

NIS2

- **Risk management.** State-of-the-art technical and organisational measures, including business continuity and crisis management.
- **Supply-chain security.** Contractually secure and monitor security requirements imposed on suppliers and service providers.
- **Reporting.** Early warning within 24 hours, incident notification within 72 hours and final report to the BSI within one month.

OCCUPATIONAL SAFETY

06

ADVANCED ROBOTICS

WHEN ROBOTS ARE USED IN THE WORKPLACE, OCCUPATIONAL SAFETY OBLIGATIONS, IN PARTICULAR UNDER THE “ARBSCHG” AND “BETRSICHV”, APPLY ALONGSIDE PRODUCT-RELATED REQUIREMENTS. RESPONSIBILITY LIES WITH THE EMPLOYER AS OPERATOR.

- **Risk assessment.** Assess hazards arising from robot use and human-robot collaboration before commissioning and update the assessment when changes occur.
- **Protective measures.** Technical measures take precedence over organizational measures, which in turn take precedence over personal protective measures. Protective measures include safeguards, emergency stop functions, and speed and force limitation mechanisms.
- **Work equipment and inspections.** Robots are work equipment. They must be provided safely, inspected by competent persons and maintained.
- **Instruction and qualification.** Regularly instruct employees on operation and troubleshooting.
- **Participation and documentation.** Involve occupational safety specialists, company physicians and the works council. Document the assessment.
- **AI-supported systems.** For adaptive behaviour, additionally consider oversight and operator obligations under the AI Act.

PRODUCT AND OPERATION INTERFACE

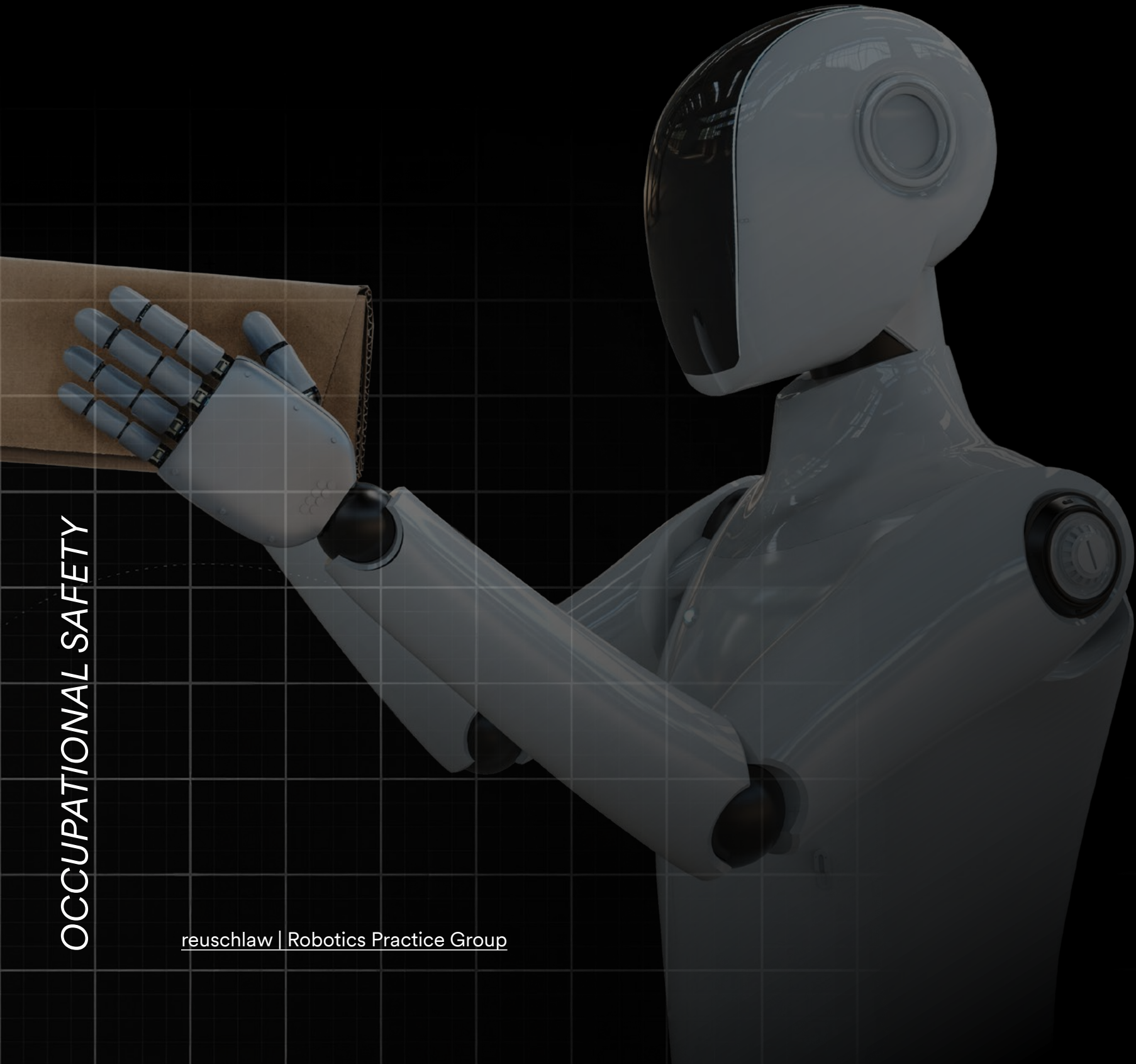
- :: Product law addresses the manufacturer; occupational safety law addresses the employer
- :: CE conformity does not replace the risk assessment
- :: A substantial modification may trigger manufacturer obligations

RELEVANT LEGISLATION

- :: ArbSchG – general employer obligations and risk assessment
- :: BetrSichV – provision and use of work equipment
- :: DGUV Regulation 1 and DGUV rules

OTHER TECHNICAL STANDARDS

- :: DIN EN ISO 10218-1/-2 – Industrial robots and robot systems
- :: DIN ISO/TS 15066 – Collaborative robot applications
- :: DIN EN ISO 13849-1 – Safety-related parts of control systems
- :: DIN EN ISO 12100 – Risk assessment and risk reduction



INFOGRAPHIC

**MSR – Regulation
(EU) 2019/1020**

Applies where the Machinery Regulation does not take precedence; governs market surveillance.

**GPSR – Regulation
(EU) 2023/988**

Applies where the Machinery Regulation does not take precedence; establishes general product safety requirements.

LEX
GENERALIS

TDDDG

Telecommunications Digital Services Data Protection Act; national implementation relating to the ePrivacy framework.

**GDPR –
Regulation (EU)
2016/679**

Fundamental requirements governing the processing of personal data.

**Data Act –
Regulation (EU)
2023/2854**

Access to and use of data from connected products and related services.

**ePrivacy Directive –
Directive
2002/58/EC**

Protection of the confidentiality of electronic communications.

BDSG

Federal Data Protection Act; national supplement to the GDPR.

**Machinery Regulation –
Regulation (EU)
2023/1230**

Specific requirements for machinery and safety components.

**Annex III to
the Machinery
Regulation – EHSRs**

Contains the essential health and safety requirements under the Machinery Regulation.

*DIN EN ISO
10218-1 / -2*
Industrial robots

ISO 13849:2023
Safety of
machinery —
Safety-related
parts of control

ISO/IEC 42001

Artificial
Intelligence
Management
System (AIMS)

**AI Act – Regulation
(EU) 2024/1689**

Regulation of
AI systems.

ISO/IEC 23894
Standardized risk
management for AI.

DIN EN

18286:2026-09

Quality management
system for regulatory
purposes under the
EU AI Act.

ADVANCED ROBOTICS

PRODUCT SAFETY
(VERTICAL
REGULATION)

DATA
PROTECTION /
DATA LAW

AI

PRODUCT SAFETY
(HORIZONTAL
REGULATION)

HUMAN-MACHINE-
INTERACTION (HMI)

CYBERSECURITY /
IT SECURITY

**Low Voltage
Directive**

Requirements
for electrical
equipment.

EMC Directive

Requirements for
electromagnetic
compatibility.

*DIN EN IEC
61000-6-2*

Immunity
requirements.

*DIN EN IEC
61000-6-4*

Emission requirements
within specified
frequency ranges.

ArbSchG

General obligations
of the employer
when robots are
used as work
equipment.

BetrSichV

Specific obligations
relating to the
provision and use
of work equipment.

*DIN EN ISO 10218-
2:2025*

Safe human-robot
collaboration,
including collaborative
applications.

**CRA – Regulation
(EU) 2024/2847**

Cybersecurity
requirements for
products with
digital elements.

**NIS2 – Directive (EU)
2022/2555**

Cybersecurity
requirements
for essential and
important entities.

IEC 62443

Security for industrial
communication networks.

BSIG

Protection of information
security.

CONTACT



DANIEL WUHRMANN

Attorney-at-law
Head of Mobility

Saarbruecken office
Stengelstraße 1
66117 Saarbruecken

T +49 681 / 859 160 0
E daniel.wuhrmann@reuschlaw.de



DR. VOLKER HARTMANN

Attorney-at-law
Of Counsel

Berlin office
Joachimsthaler Straße 20
10719 Berlin

T +49 30 / 2332 895 0
E volker.hartmann@reuschlaw.de