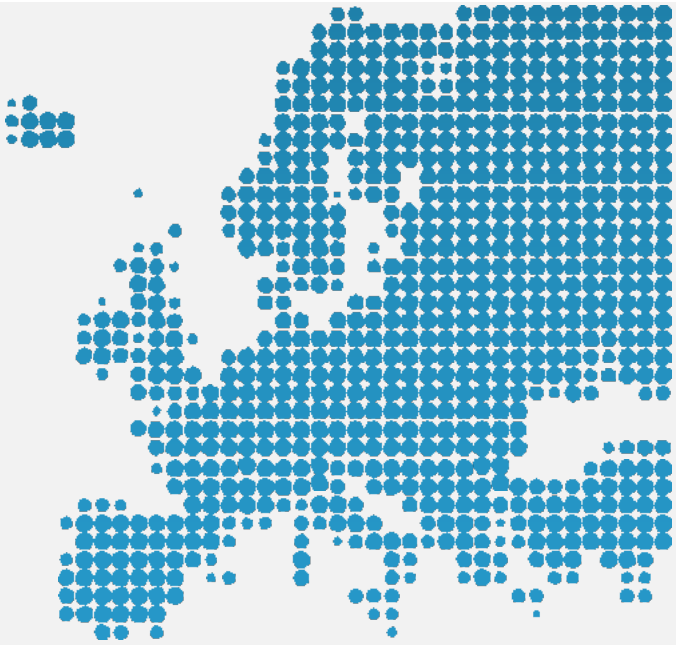
CRA, AIA, DA – What to do?

Status: October 2026



CRA, AIA and DA – what to do?



Contents

1 I Cyber Resilience Act: cyber security becomes a product requirement

2 I Data Act: prepare for user access to product-generated data

3 I AI Act: classify AI functions before defining the compliance route

4 I A combined implementation programme

5 I What happens if preparation is delayed?

6 I 90-day starting checklist

CRA, AI Act and Data Act – what should door manufacturers do now?

Cybersecurity, artificial intelligence and access to product-generated data are no longer matter for the IT department alone.
They increasingly determine how connected doors, gates, controls, locks and service platforms must be designed, documented, placed on the market and supported through-out their lifecycle.

This guideline builds on E.D.S.F. Guideline 10, which introduced the Cyber Resilience Act (CRA), the Artificial Intelligence Act (AI Act) and the Data Act.
The present document goes one step further. It helps manufacturers translate the three regulations into practical questions, responsibilities and work packages. It is intended as an implementation aid, not as a substitute for product-specific legal advice.

This guideline is relevant in particular to manufacturers and integrators of automatic and industrial doors, fire and safety doors, access-control systems, smart locks, connected controllers, service apps, cloud portals and remote-maintenance solutions.

A product may be affected even if the manufacturer does not regard itself as a software company: embedded firmware, a network interface, an app, a cloud service or an AI-supported function may be sufficient to trigger new obligations.

The practical starting point is therefore simple: identify where software, connectivity, product-generated data and AI are already present in the portfolio. Then determine which company acts as manufacturer, provider, deployer, data holder or user, and allocate the necessary technical, contractual and organisational tasks.

How to use this guideline

Each section first explains why the regulation matters to the door industry, then identifies concrete actions and concludes with a short example. The recommended approach is iterative: start with a portfolio inventory, prioritise the products and services with the greatest regulatory or safety relevance, record decisions and close identified gaps through the normal product-development and quality-management processes.

1. Cyber Resilience Act: cybersecurity becomes a product requirement

The CRA applies to products with digital elements whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network.
For the door industry, this may include connected door controls, smart locks, access-control systems, gateways, cloud portals, service apps and remote-maintenance access. The decisive question is not whether the product looks like an IT product, but whether hardware or software can exchange data with another device or network.

The CRA introduces cybersecurity requirements throughout the product lifecycle.
Before placing a product on the market, the manufacturer must assess cybersecurity risks, implement the applicable essential requirements, prepare technical documentation and complete the appropriate conformity-assessment procedure.
At market placement, the manufacturer must provide the required information, indicate the support period and draw up the EU declaration of conformity. During the support period, vulnerabilities must be monitored, assessed and remedied.

1.1 Immediate CRA work packages

a) **Define the product and its digital boundaries.** Document the hardware, firmware, software, communication interfaces, mobile applications, cloud functions and remote data-processing solutions that form part of the product or support its functions.

b) **Assign the economic-operator role**[1]**.** Clarify who places the final product on the market and who controls its design. Buying a controller or software component does not automatically transfer the final manufacturer's responsibility to the supplier.

c) **Carry out a cybersecurity risk assessment.** Consider foreseeable attack paths, safety-relevant effects, unauthorised access, manipulation of settings, loss of availability, data exposure and dependencies on external services.

d) **Apply security by design and by default.** Examples include unique or user-defined credentials, least-privilege access, protected update mechanisms, secure communication, logging, secure recovery and disabling unnecessary interfaces.[2]

[1] Under Article 3 CRA, 'economic operator' includes the manufacturer, authorised representative, importer, distributor or another person subject to obligations relating to the manufacture or making available of products with digital elements. The applicable role depends on the company's activities in the supply chain; placing a product on the market under one's own name or trademark may result in manufacturer obligations.
[2] For machinery-related products, the cybersecurity risk assessment and security-by-design process may be supported by prEN 50742, EN ISO 12100 and, where appropriate, the EN IEC 62443 series, in particular EN IEC 62443-4-1 and EN IEC 62443-4-2.

e) **Establish component transparency.** Maintain an inventory of software and relevant dependencies, including open-source components. An SBOM (Software Bill of Materials) can support vulnerability monitoring, but it should be embedded in a wider configuration and supplier-management process.

f) **Define the support period and update process.** Decide how long security support will be provided, how updates will be tested and distributed, how customers will be informed and how products that cannot be updated will be handled.

g) **Prepare vulnerability handling and reporting.** Establish an intake channel for vulnerability reports, responsibilities for triage and remediation, escalation criteria and evidence of decisions. Reporting obligations for actively exploited vulnerabilities and severe incidents apply from 11 September 2026; the main CRA obligations apply from 11 December 2027.

1.2 Practical example: remote maintenance

An industrial door controller can be accessed remotely by a service company. The manufacturer should not treat the remote gateway as an external IT accessory. It should determine whether the gateway and cloud service form part of the product with digital elements, assess the consequences of stolen credentials or service compromise, require secure authentication and access logging, define how vulnerabilities are reported and patched, and ensure that contractual responsibilities with the gateway or cloud supplier are documented.

1.3 Useful official sources

Consult the official CRA text, the European Commission's manufacturer guidance and the Commission's information on CRA reporting obligations. These sources should be checked regularly because guidance, harmonised standards and implementing measures continue to develop.

1.4 NIS2 and product liability: additional business pressure

NIS2 does not replace the CRA and does not automatically apply to every door manufacturer.
However, customers in sectors such as energy, transport, healthcare, digital infrastructure and other critical activities may impose stronger cybersecurity requirements on their supply chain.
Manufacturers should therefore be able to explain how connected products are secured, supported and monitored.

A cyber weakness may also have physical and commercial consequences. If compromised remote access causes an uncontrolled opening, production interruption, property damage or injury, the manufacturer may be asked to show whether cyber risks were assessed, known vulnerabilities were addressed and an effective update and incident process existed. Cybersecurity evidence should therefore be integrated into product safety, quality and liability management rather than maintained as a separate IT file.

2. Data Act: prepare for user access to product-generated data

The Data Act has applied since 12 September 2025. It gives users of connected products greater control over data generated through the use of those products. In the door industry, relevant data may include operating cycles, status messages, error codes, energy consumption, maintenance information, sensor values and event logs.
The Data Act does not simply declare that the user "owns" all data; it establishes rights and obligations concerning access, use and sharing.

2.1 Immediate Data Act work packages

a) **Create a data inventory.** For each connected product and related service, record what data are generated, where they are stored, in which format, at what frequency and who currently receives them.

b) **Identify the user and data holder.** In a typical installation, the purchaser, building owner, tenant, operator, installer, service company and platform provider may have different roles. These roles should not be assumed; they should be analysed for the relevant business model and contract.

c) **Design a practical access route.** Determine whether data can be made directly accessible from the product or must be supplied on request. The route should be secure, proportionate and usable, with appropriate metadata and without avoidable technical barriers.

d) **Review pre-contract information.** Customers should understand what data the connected product generates, how they can access it, whether the manufacturer intends to use it and whom they should contact.

e) **Review contracts and permissions.** Maintenance, platform, remote-monitoring and dealer agreements should clearly address authorised uses, third-party sharing, confidentiality, trade secrets, personal data and security controls.

f) **Separate Data Act and GDPR questions.** Data access under the Data Act does not remove obligations under data-protection law.[3] Event logs or access records may contain personal data and require a distinct legal and technical assessment.

2.2 Practical example: predictive maintenance portal

A manufacturer operates a portal that analyses door cycles and fault codes to offer predictive maintenance.
The manufacturer should identify which raw and pre-processed data are within the Data Act scope, explain the data generation and access arrangements before contracting, provide the user with an appropriate access or request mechanism, and define how the user can authorise a third-party maintenance provider to receive eligible data.

[3] The Data Act and data-protection law apply in parallel. The Data Act governs access to and use of data generated by connected products, including non-personal data. Where such data are personal data, the GDPR continues to apply in full; the Data Act does not create a separate legal basis for processing personal data and does not override the rights and safeguards of data subjects. Data sets may contain both personal and non-personal data and should therefore be assessed accordingly.

Trade-secret and cybersecurity safeguards should be designed into the process rather than used as a blanket reason to refuse access.

2.3 Useful official sources

Consult the official Data Act text and the European Commission's Data Act explainer. The Commission's material includes practical explanations of connected-product data, user rights, data sharing and contractual issues.

3. AI Act: classify AI functions before defining the compliance route

Not every advanced algorithm is an AI system, and not every AI system is high-risk. The first task is therefore technical and functional classification.

Manufacturers should identify systems that generate predictions, recommendations, decisions or content with a degree of autonomy, then determine the intended purpose, their own role and the applicable risk category.

Potential applications in the door sector include video-based access control, licence-plate recognition, person or obstacle detection, anomaly detection, predictive maintenance, automatic fault diagnosis, service assistants and chatbots.

An AI function that is used as a safety component of a regulated product may require particular attention, especially where the product is subject to third-party conformity assessment.

3.1 Immediate AI Act work packages

a) **Compile an AI use-case register.** Include AI embedded in products and AI used in associated services or internal processes. Record the intended purpose, supplier, model or system version, input data, outputs and affected decisions.

b) **Determine the company's role.** A company may be a provider, deployer, importer or distributor. Integrating a third-party AI system under the company's own name or substantially modifying it can affect the role and obligations.

c) **Classify the risk.** Check prohibited practices first, then determine whether the system may be high-risk under Article 6 and the relevant annexes. Document why a system is or is not considered high-risk and review the decision when the intended purpose changes.

d) **Define human oversight and fallback.** For safety- or access-relevant functions, specify who can review, override or disable an AI output and how the product behaves when confidence is low, sensors fail or the AI service is unavailable.

e) **Control data and performance.** Record the origin and suitability of training, validation and operational data where relevant; define performance limits, foreseeable misuse, monitoring and change control.

f) **Manage suppliers.** Obtain sufficient documentation, performance information, update notices and contractual rights from AI suppliers. A black-box procurement model may leave the final product manufacturer unable to demonstrate compliance.

g) **Provide AI literacy.** Ensure that staff who develop, integrate, sell, operate or monitor AI systems understand the relevant capabilities, limitations and risks.

3.2 Practical example: AI-supported person detection

A camera system classifies whether a person is present in the movement area of an automatic door. The manufacturer should define whether the AI output has a safety function or only supplements conventional protective equipment. It should document the intended operating conditions, performance limitations, foreseeable lighting and occlusion problems, human or technical fallback, change control for model updates and the allocation of responsibilities with the camera or software supplier. The classification must be revisited if the AI output later becomes safety decisive.

3.3 Useful official sources

Consult the official AI Act text, the Commission's AI Act overview and the available guidance on high-risk classification. Because the implementation framework and timelines continue to evolve, the latest consolidated legal text and Commission material should be checked before relying on a deadline or classification.

4. A combined implementation programme

The three regulations should not be implemented in isolated projects. The same connected door system may simultaneously require cybersecurity risk management, user access to generated data and governance of an AI-supported function.
A combined programme avoids duplicate inventories and contradictory technical or contractual decisions.

a) **Appoint an accountable sponsor and a cross-functional team.** Product management, development, IT security, quality, legal, service, procurement and sales should have defined responsibilities.

b) **Build one portfolio inventory.** Record software, connectivity, cloud services, data flows, AI functions, suppliers, product roles, expected support periods and relevant customer sectors.

c) **Prioritise.** Start with products that are connected, remotely maintained, safety relevant, widely installed or dependent on cloud and third-party software.

d) **Perform structured gap assessments.** Compare current development, documentation, supplier, update, vulnerability, data-access and AI-governance practices with the applicable requirements.

e) **Convert gaps into product-roadmap tasks.** Assign owners, budgets and deadlines. Distinguish product redesign, process changes, contractual changes and evidence or documentation work.

f) **Integrate controls into the quality system.** Regulatory compliance should become part of design reviews, supplier approval, release management, post-market monitoring and management review.

4.1 Minimum management dashboard

Management should be able to see, at minimum, which products are in scope, which high-priority risks remain open, whether support and reporting processes are operational, whether data-access requests can be handled, whether AI use cases are classified, and whether critical supplier evidence is missing.

5. What happens if preparation is delayed?

The earliest consequences may be commercial rather than regulatory.

Customers and integrators are already asking suppliers for evidence of secure development, vulnerability handling, support periods, data-access capabilities and responsible AI use.
Companies that cannot provide credible answers may face additional audits, tender exclusions, contractual reservations or higher insurance and remediation costs.

Delay also creates technical debt.

Cybersecurity, data access and AI oversight are difficult to add shortly before market placement if the underlying architecture, supplier contracts and documentation were not designed for them.

Retrofitting may require new interfaces, update mechanisms, cloud arrangements, product documentation and validation work.
Where the modification affects safety-related functions, the intended purpose or the risk profile of the machinery, the safety assessment may also need to be reviewed under the Machinery Directive or the Machinery Regulation.[4]

Once the applicable obligations are fully enforceable, insufficient evidence may become a market-access and compliance issue. The practical objective should therefore not be to produce a last-minute legal file, but to embed the new requirements in product development and lifecycle support.

6. 90-day starting checklist

- Nominate a management sponsor and responsible project lead.
- Identify connected products, software components, cloud services, data flows and AI functions.
- Select the highest-priority product family for a pilot assessment.
- Map suppliers and request missing software, security, update, data and AI documentation.

[4] Under Regulation (EU) 2023/1230, a physical or digital modification may constitute a ‘substantial modification’ if it was not foreseen or planned by the manufacturer and affects the safety of the machinery by creating a new hazard or increasing an existing risk. Depending on the date and circumstances of the modification, the Machinery Directive 2006/42/EC or the Machinery Regulation (EU) 2023/1230 should therefore be considered.

- Define a vulnerability intake and escalation route, including CRA reporting responsibilities.
- Test how a user request for connected-product data would be received, verified and fulfilled.
- Record and classify every AI use case, including purchased services.
- Create a remediation roadmap with owners, milestones and management reporting.

The way forward

Manufacturers do not need to solve every detail at once, but they do need a documented starting point, clear responsibilities and a realistic implementation plan. The longer software, data and AI remain outside normal product governance, the more difficult and expensive compliance will become.

Text / Editorial team:

The information on which this publication is based has been researched and processed with the greatest of care. We cannot, however, accept liability for any injuries, expenses or losses incurred which could in any degree be attributed to the use of the information contained in this text. Reprinting or copying in whole or in part is only permitted with the written permission of the publisher and clear reference to the publication source.

Status: October 2026

E.D.S.F.
European Door and Shutter Federation e.V.
Neumarktstr. 2 b
58095 Hagen · Deutschland

Fon +49 2331 2008-0
Fax +49 2331 2008-40
info@edsf.com
www.edsf.com