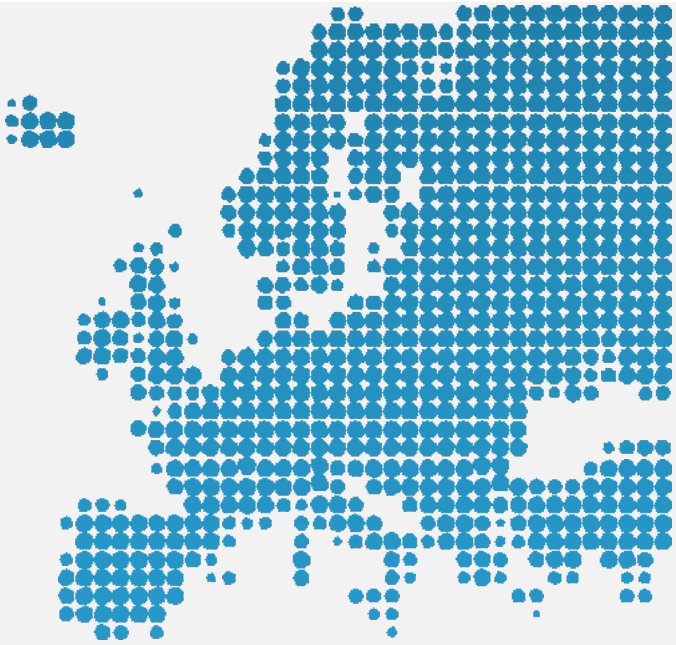
Cyber Resilience Act (CRA), Data Act and Artificial Intelligence Act (AIA)– a distant vision of the future?

Status: October 2026



Cyber Resilience Act (CRA), Data Act and Artificial Intelligence Act (AIA) – a distant vision of the future?



Contents

1 I Wave 1: Cybersecurity becomes a product requirement (CRA)

2 I Wave 2: Data becomes a customer right (Data ACT)

3 I Wave 3: AI is regulated (AIA)

Cyber Resilience Act (CRA), Data Act and Artificial Intelligence Act (AIA) – a distant vision of the future?

This document provides an overview of what manufacturers can expect from three major elements of the European Union's evolving digital regulatory framework: the Cyber Resilience Act (CRA), Regulation (EU) 2024/2847[1]; the Data Act, Regulation (EU) 2023/2854[2]; and the Artificial Intelligence Act (AI Act), Regulation (EU) 2024/1689[3].

All three regulations are expected to have a significant impact on the development and design of products. For manufacturers of doors, it is therefore important to understand the forthcoming requirements and to prepare for their implementation at an early stage. These requirements are no longer a distant prospect for the door industry. As digitalisation, connectivity and artificial intelligence continue to evolve rapidly, manufacturers should begin preparing now for the forthcoming regulatory obligations.

These regulations form part of the European Union's broader response to the rapid digitalisation of products and services. The CRA emerged from the EU's cybersecurity strategy and introduces horizontal cybersecurity requirements for products with digital elements throughout their lifecycle. The Data Act is a key pillar of the European strategy for data and responds to the growing volume of data generated by connected products by establishing rules for fair access to and use of that data. The AI Act developed from the EU's policy objective of promoting trustworthy, human-centred artificial intelligence and introduces a risk-based framework intended to protect safety, fundamental rights and other public interests. Together, the three regulations address complementary questions

[1] Official text: Regulation (EU) 2024/2847 (Cyber Resilience Act), EUR-Lex: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng
[2] Official text: Regulation (EU) 2023/2854 (Data Act), EUR-Lex: https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng
[3] Official text: Regulation (EU) 2024/1689 (Artificial Intelligence Act), EUR-Lex: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

concerning the security of digital products, access to product-generated data and the responsible use of artificial intelligence.

This guideline is not intended to provide a detailed legal interpretation of the CRA, the Data Act or the AI Act. Instead, it offers a practical and accessible overview of the expected requirements, highlights key aspects that manufacturers should consider and identifies actions that should be initiated as early as possible.

Each of the following three sections follows the same practical approach: it explains the regulatory change in simple terms, indicates why it matters for door manufacturers and identifies the questions that companies should begin addressing. The purpose is not to provide a complete legal analysis, but to help manufacturers recognise where their products, services and internal processes may be affected.

The Three Waves Coming to the Door Industry

1. Wave 1: Cybersecurity becomes a product requirement (CRA)

The CRA should not be understood merely as another piece of IT legislation. In practice, it introduces cybersecurity as a product requirement for products with digital elements. Manufacturers will therefore have to consider cybersecurity as part of product design, conformity assessment and CE marking.

Until now, door manufacturers have mainly associated CE marking with mechanical and electrical safety, machinery legislation and construction product requirements:

- CE = Mechanics
- CE = electrical safety
- CE = Machinery Directive / Regulation
- CE = Construction Product Requirements

Under the CRA, this familiar understanding must be expanded: for products with digital elements, CE marking will also indicate that the applicable cybersecurity requirements have been addressed:

- CE = also Cybersecurity

The decisive change is that responsibility for demonstrating cybersecurity no longer rests primarily with the operator. The manufacturer must systematically address and document cybersecurity throughout the product lifecycle.

For door manufacturers, this creates practical requirements in several areas of product development, operation and support:

- Secure standard configuration
- Secure remote maintenance
- Vulnerability Management
- Updateability
- Security documentation

- Cybersecurity must be maintained throughout the supported product lifecycle, including through appropriate updates, vulnerability handling and security documentation.

2. Wave 2: Data becomes a customer right (Data Act)

Connected products already generate usage and operational data that manufacturers use for maintenance contracts, service portals, remote monitoring, predictive maintenance and other service-related activities:

- Maintenance contracts
- Service portals
- Remote Monitoring
- Predictive Maintenance
- Operational data collection

The central question is not simply who owns the data, but who is entitled to access and use data generated by a connected product. In simplified terms, the Data Act gives users extensive rights to obtain and use data generated through their use of the product.

For door manufacturers, the practical task is to determine how this access and use rights affect existing service arrangements, digital platforms and data-based business models.

- Manufacturers should therefore examine what product-generated data is available, who is entitled to receive it, how it can be provided and whether existing contracts, interfaces and service processes need to be adapted.

3. Wave 3: AI is regulated (AI Act)

For many door manufacturers, the AI Act may not yet appear to be an immediate compliance priority. However, this assessment can change as soon as AI-based functions are integrated into products, safety systems, access-control solutions or service applications.

3.1 Where AI is already emerging in the industry

Today, AI applications can already be found in:

- Video analysis for access control (e.g. automated door systems)
- License plate recognition (e.g. barrier systems in parking garages)
- Person detection (e.g. for safety devices for doors / gates)
- Anomaly detection
- Predictive Maintenance
- Service Assistant
- Chatbots
- Automatic fault diagnostics

3.2 What does the AI Act regulate?

The AI Act does not only regulate the developer of an AI model. Integrators, providers and some operators may also have obligations.
Manufacturers should therefore clarify the following questions when assessing AI-based functions and their possible obligations under the AI Act:

- Where is AI in the product?
- What decisions or recommendations does the AI-based function make or support?
- What data does it use?
- How is it monitored?
- How are risks documented?

From a strategic perspective, the CRA, the Data Act and the AI Act should be considered together because connected products may simultaneously raise questions about cybersecurity, access to generated data and the responsible use of AI.

For example, for a door manufacturer, this means:

- CRA Is the digital product secure? ("Cybersecurity")
- Data Act Who is allowed to use the data? (Data access)
- AI Act How is AI used responsibly? (AI use)

The final strategic question for every manufacturer is therefore: how much software, product-generated data and artificial intelligence are already present in our products and related services today?

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