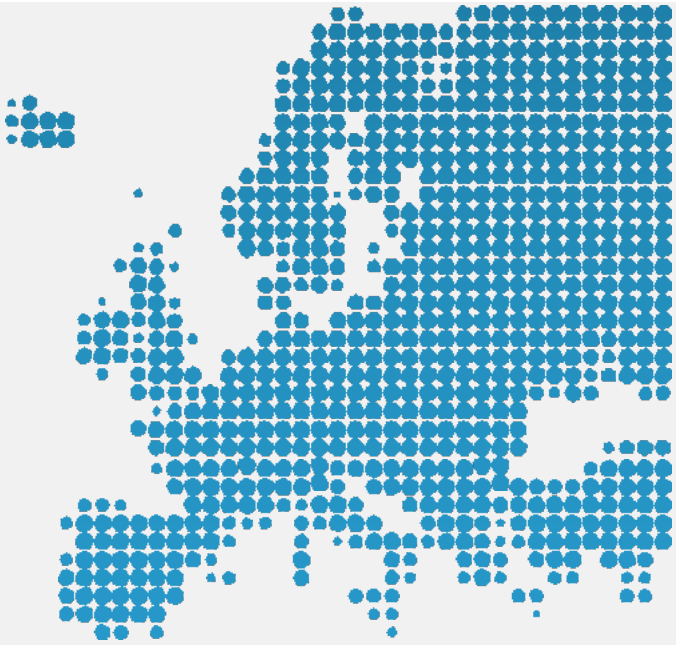
Cyber Resilience Act (CRA) and Artificial Intelligence Act (AIA) – a distant vision of the future?

Status: July 2026



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 (AI ACT)

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

This document provides an overview of what manufacturers can expect following the introduction of the Cyber Resilience Act (CRA) and the Artificial Intelligence Act (AIA).

Both 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. For door manufacturers, these requirements are no longer a distant prospect. As digitalisation, connectivity and artificial intelligence continue to evolve rapidly, manufacturers should begin preparing now for the forthcoming regulatory obligations.

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

The Three Waves Coming to the Door Industry

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

The CRA is not an IT law.

It is de facto a product right for digital products; a CE marking is the result.

We know CE-marking so far for:

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

and we will learn how to relate the CE marking to these new topics as well:

- CE = also Cybersecurity

The decisive change is:

It is not the operator, but the manufacturer who must systematically prove cybersecurity.

For example, for a door manufacturer, this means:

- Secure standard configuration
- Secure remote maintenance
- Vulnerability Management
- Updateability
- Security documentation
- Security over the product lifecycle

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

(Usage)Data is now primarily used for:

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

Who actually owns the data?

The EU's answer is simplified: "The user is entitled to far-reaching access rights to the data generated."

For example, for a door manufacturer, this means:

- How do the new requirements affect the service and business model and what do I have to do – now?

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

For the door industry, the AI Act is currently not yet a major compliance issue. But attention: this is often only partially true.

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

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.
Therefore, in the future, the following questions will be asked:

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

Strategically, CRA + Data Act + AI Act belong together:

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)

And the final key question: "How much software, data and AI are already in the products 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: July 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