Cyber Resilience Act

Document Information

Document ID:	**Doc ID**	Document Owner:	**Lukas Tranholm Olesen**
Document Version	**1.0**	Created by:	**Lukas Tranholm Olesen**
Date:	**16 April 2026**	Approved by:	**Jakob Bjørn Sørensen**

Table of Contents

1 Important notice

This whitepaper is intended to provide customers, partners, and other stakeholders with a high-level overview of how Admin By Request approaches compliance with the EU Cyber Resilience Act (hereinafter 'CRA'). It is written for transparency and information purposes and should not be understood as legal advice or as an exhaustive interpretation of Regulation (EU) 2024/2847. The authentic legal text is the Regulation published in the Official Journal of the European Union, and the European Commission has also published implementation summaries and guidance materials to support understanding.

2 Executive Summary

At Admin By Request, cybersecurity is a core product responsibility. The EU Cyber Resilience Act establishes a harmonized EU-wide framework for the cybersecurity of products with digital elements and requires manufacturers to address cybersecurity across the product lifecycle, from design and development to post-market vulnerability handling and customer information. The CRA entered into force on 10 December 2024; reporting obligations apply from 11 September 2026, and the full regulation applies from 11 December 2027.

This whitepaper explains how Admin By Request addresses the requirements of the CRA and highlights key CRA provisions relevant to our products, operations, and customers. It is intended to create transparency around our governance, secure development practices, vulnerability handling, customer communication, and conformity activities.

3 Purpose of This Whitepaper

The purpose of this whitepaper is to provide customers with greater transparency into Admin By Request's approach to meeting the requirements of the CRA, including how cybersecurity, compliance, and product lifecycle responsibilities are addressed in practice. The CRA was adopted to improve the cybersecurity of products with digital elements, reduce widespread vulnerabilities, improve the provision of security updates, and give users better information about cybersecurity properties and support periods.

4 Scope of This Whitepaper

This whitepaper covers Admin By Request's approach to CRA compliance for products with digital elements that are made available on the EU market under our name or trademark. Under the CRA, a product falls within scope when its intended purpose or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network. The CRA applies to both hardware and software products, including components placed on the market separately, and it also includes remote data processing solutions where these are designed by, or under the responsibility of, the manufacturer and are necessary for one of the product's functions.

5 How the CRA Applies to Admin By Request

For the purposes of this whitepaper, Admin By Request assumes the role of manufacturer under the CRA for the products we develop, have developed, or place on the EU market under our own name or trademark. Under the CRA, the main obligations are directed at manufacturers, who are responsible for ensuring that products with digital elements meet the essential cybersecurity requirements during design, development, production, and the time the products are expected to be in use.

6 CRA Provisions Relevant to Admin By Request

Because we place products with digital elements on the EU market, the following CRA provisions are the ones most relevant to Admin By Request.

6.1 Scope and Product Qualification

The CRA applies to products with digital elements made available on the market where the intended purpose or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network. In practice, this means that connected hardware, software, and certain related remote processing components may fall within scope.

6.2 Essential Cybersecurity Requirements

The CRA requires manufacturers to ensure that products meet the essential cybersecurity requirements set out in Annex I. According to the European Commission's summary, this includes requirements that apply during design, development, and production, as well as requirements for vulnerability handling during the support period of the product. The Commission's manufacturer guidance further highlights examples such as security by design, security by default, access control, cryptography where appropriate, and automatic updates.

6.3 Cybersecurity Risk Assessment

Manufacturers must perform a cybersecurity risk assessment that informs how the essential cybersecurity requirements are implemented. The Commission states that this assessment needs to be taken into account during the planning, design, development, production, delivery, and maintenance phases of the product, and that the assessment must be reflected in the technical documentation.

6.4 Technical Documentation, Conformity Assessment, EU Declaration of Conformity, and CE marking

Before a product is placed on the market, the manufacturer must carry out an appropriate conformity assessment procedure, prepare the technical documentation, draw up the EU declaration of conformity, and affix the CE marking if the product meets the applicable requirements. Chapter III of the CRA covers these conformity mechanisms and the related technical documentation requirements, and the Commission explains that manufacturers may in some cases use internal control (self-assessment), while certain categories of products require stricter assessment routes through a notified body or, where applicable, an eligible European cybersecurity certification scheme.

6.5 Product Categorization: Important and Critical Products

Where a product has the core functionality of an important or critical product category, stricter conformity assessment requirements may apply. These categories are listed in Annexes III and IV to the CRA, and their technical descriptions are further specified by the Commission Implementing Regulation (EU) 2025/2392. Whether this affects a particular product depends on its core functionality and classification.

For the purposes of this whitepaper, our products are categorized under Annex III as identity management systems and privileged access management software and, accordingly, as Important Products with digital elements (Class I) under the CRA.

6.6 Customer Information and Support Periods

The manufacturer must provide information and instructions to users and clearly indicate the support period, including the end date of the support period, at the time of purchase. The Commission highlights that customers should be able to understand how long the product will be supported and that manufacturers remain responsible for vulnerability handling during the time the product is expected to be in use.

6.7 Vulnerability Handling and Incident Reporting

After a product has been placed on the market, manufacturers are required to handle vulnerabilities for the support period and to report actively exploited vulnerabilities and severe incidents affecting the security of the product. Under Article 14 and the Commission's reporting guidance, manufacturers must submit an early warning within 24 hours, a main notification within 72 hours, and a final report within the applicable deadlines through the CRA Single Reporting Platform, with ENISA and the relevant CSIRT involved in the process. Manufacturers must also inform affected users - and, where appropriate, all users - of such vulnerabilities or incidents and, where applicable, any mitigation or corrective measures available to users. These reporting obligations apply from 11 September 2026.

6.8 Market Surveillance and Enforcement

The CRA is enforced through national market surveillance authorities, supported by EU coordination mechanisms. These authorities can request technical documentation, assess products that may pose significant cybersecurity risks, and require corrective or restrictive actions. CRA compliance is therefore not only a design-time exercise but also an ongoing regulatory obligation after a product has been placed on the market.

7 Our Approach to CRA Compliance

7.1 Governance and Accountability

We treat CRA readiness as a cross-functional responsibility involving product, engineering, security, legal/compliance, quality assurance, and customer-facing teams. This reflects the CRA's lifecycle-based approach, which places responsibility on manufacturers throughout planning, design, development, maintenance, and post-market placement vulnerability handling.

At a governance level, our objective is to ensure that CRA-related responsibilities are assigned, documented, and reviewed on a continuing basis. This includes maintaining internal ownership for product scoping classification, technical documentation, conformity activities, vulnerability handling, and customer communications. These activities align with the Commission's description of manufacturer obligations and the need to keep relevant documentation available for market surveillance authorities.

7.2 Product Scoping and Role Assessment

For each relevant offering, we assess whether the product qualifies as a product with digital elements under the CRA and whether Admin By Request acts as manufacturer, importer, distributor, or in another relevant capacity. This scoping exercise includes reviewing connectivity, intended use, remote data processing dependencies, and supply chain roles, because these factors influence which CRA obligations apply.

7.3 Secure Design and Development

Our compliance approach is built around secure design and secure development principles. In line with the CRA, we integrate cybersecurity early in the product lifecycle and implement controls informed by risk assessment, including appropriate security-by-design and security-by-default measures. The Commission's manufacturer guidance specifically points to measures such as access control, use of cryptography where appropriate, and automatic updates as examples of the type of foundational security expected under the CRA.

7.4 Third-Party Components and Supply Chain Due Diligence

Where our products rely on third-party software, hardware, or other components, we apply due diligence to reduce the risk that external components compromise the cybersecurity of the overall product. The European Commission's CRA summary explicitly states that where a manufacturer integrates third-party components, it must exercise due diligence, so those components do not undermine the security of the product with digital elements. We're actively

reviewing third parties providing us services as part of our ISMS. We also maintain an inventory of open-source components used in our products.

7.5 Technical Documentation and Evidence of Conformity

We maintain and update technical documentation intended to demonstrate how applicable CRA requirements are addressed. In line with the Commission's summary, this includes documenting the cybersecurity risk assessment and the means used to implement relevant requirements and keeping such documentation available for competent authorities where required. Before placing an in-scope product on the market, we follow the applicable conformity assessment route and complete the necessary compliance steps for EU declaration of conformity and CE marking, where applicable.

7.6 Vulnerability Handling, Updates, and Support Periods

We maintain processes for identifying, assessing, prioritizing, and remediating vulnerabilities during the support period of relevant products. We also work to define and communicate support periods in a way that is clear to customers, as the CRA requires the end date of the support period to be clearly specified at the time of purchase and expects manufacturers to handle vulnerabilities effectively during that period.

7.7 Incident and Vulnerability Reporting

We are preparing our reporting process for the CRA reporting regime that applies from 11 September 2026. Where required by law, this includes the capability to assess whether an actively exploited vulnerability or a severe incident affecting the security of a product triggers notification obligations and, if so, to make the necessary notifications and submissions, including submissions through the CRA Single Reporting Platform within the prescribed timelines.

7.8 Customer Transparency and Communication

A key goal of our CRA work is transparency for customers. The CRA was designed not only to improve product cybersecurity but also to make it easier for businesses and consumers to understand cybersecurity characteristics and support periods when selecting and using products. In line with that objective, we aim to provide clear information on support periods, relevant security information and instructions for use, and the way we handle cybersecurity throughout the lifecycle of relevant products.

8 What our Customers Can Expect

Customers can expect Admin By Request to approach CRA compliance as an ongoing product and lifecycle commitment rather than as a one-time certification exercise. In practical terms, this means working to ensure that relevant products are appropriately scoped, designed with cybersecurity in mind, supported through defined support periods, documented for conformity purposes, and backed by processes for vulnerability handling and regulatory reporting where required. A part of the compliance preparations entails updates to our Terms and Conditions to reflect our commitments directly in our agreements with our customers.

Customers can also expect continued transparency from Admin By Request as our CRA compliance matures. The European Commission, ENISA, and Member States are continuing implementation work on standards, conformity assessment, reporting infrastructure, and guidance. As those materials develop, we expect to continue refining our own internal processes and customer-facing communications accordingly.

9 CRA Implementation Timeline Relevant to Our Customers

The CRA entered into force on 10 December 2024. Provisions on the notification of conformity assessment bodies apply from 11 June 2026. Reporting obligations under Article 14 apply from 11 September 2026. The main CRA obligations apply from 11 December 2027. These milestone dates are part of the Commission's published implementation timeline and are relevant to how companies, customers, and conformity assessment infrastructure prepare for full CRA application.

10 Closing Statement

The EU Cyber Resilience Act is reshaping how software and connected products are designed, documented, supported, and monitored across the EU market. At Admin By Request, we support the objective of improving cybersecurity, strengthening transparency, and promoting trustworthy digital products. The whitepaper reflects our commitment to giving customers visibility into our approach and to continuing our CRA readiness efforts in line with the evolving implementation framework.