Cyber Resilience Act (CRA) Compliance Statement

Signify | General corporate statement | 9 October 2026

Signify is committed to complying with the applicable requirements of the European Cyber Resilience Act (Regulation (EU) 2024/2847) for products with digital elements placed on the European Union market.

Product security programme

To support this objective, Signify maintains a comprehensive product security programme covering the lifecycle of connected products and services. This programme includes security governance, security-by-design principles, security testing and validation activities, vulnerability management, coordinated vulnerability disclosure processes, and security incident management. These activities support the cybersecurity requirements relating to product properties and vulnerability handling set out in Annex I, Parts I and II of the CRA.

Signify continuously reviews and enhances its product security processes to align with evolving regulatory requirements, industry standards, and threat landscapes. CRA implementation activities are underway across relevant products and services, including the establishment and maintenance of technical documentation in line with Annex VII, information and instructions for users in line with Annex II, vulnerability handling processes, Software Bills of Materials (SBOMs), and incident reporting capabilities. Product-specific applicability, conformity assessment and supporting evidence are determined for the relevant product with digital elements.

Manufacturer and reporting obligations

In accordance with the manufacturer obligations in Article 13, Signify takes cybersecurity into account in the planning, design, development, production, delivery and maintenance of relevant products with digital elements, including through risk-based product security activities and vulnerability handling throughout the applicable support period.

Signify maintains incident reporting capabilities and procedures to assess actively exploited vulnerabilities and severe cybersecurity incidents affecting relevant products and, where required, report them to the designated CSIRT and ENISA in accordance with Article 14 of the CRA. This includes the applicable staged notifications and final reporting within the timelines prescribed by the CRA.

Vulnerability reporting and communication

Signify maintains channels through which security researchers, customers, suppliers and partners can report potential product security issues. Reported vulnerabilities are assessed and handled through established processes, supporting the coordinated vulnerability disclosure and vulnerability handling activities referenced in Annex I, Part II.

Further information

Additional information regarding Signify's product security programme, governance framework, vulnerability disclosure process and security practices is available at:

Signify Professional Systems and Services Product Security

For product security matters, vulnerability reports or CRA-related security communications, please contact:

productsecurity@signify.com

About this statement
This is a general corporate statement describing Signify's CRA implementation approach. It is not a product-specific EU declaration of conformity and does not replace product-specific compliance documentation, conformity assessment or contractual commitments.

Key CRA references

Article 13 - manufacturer obligations | Article 14 - reporting obligations

Annex I - essential cybersecurity requirements | Annex II - user information | Annex VII - technical documentation