European Union (EU) Radio Equipment Directive (RED) Product Security Whitepaper

Version 1.0 (July 2025)

Document Version: 1.0 (July 2025).

Contents

1. Introduction

Purpose

The European Union's (EU) Radio Equipment Directive (RED) mandates that radio equipment, particularly internet-connected devices, must meet specific security standards, including those related to network protection, data privacy, and fraud prevention if they are to be sold in the EU. This whitepaper outlines the strategy and attestation for Xerox.

Target Audience

The target audience for this document is Xerox manufacturing partners and customers concerned with IT security.

Disclaimer

The content of this document is provided for information purposes only. The performance of the products referenced herein is exclusively subject to the applicable Xerox Corporation terms and conditions of sale and/or lease. Nothing stated in this document constitutes the establishment of any additional agreement or binding obligations between Xerox Corporation and any third party.

2. RED Directive

The radio equipment directive 2014/53/EU (RED) establishes a regulatory framework for placing radio equipment on the market. It ensures a single market for radio equipment by setting essential requirements for safety and health, electromagnetic compatibility, and the efficient use of the radio spectrum. It also provides the basis for further regulation governing some additional aspects such as:

- Protection of personal data
- Protection against fraud
- Interoperability
- Access to emergency services
- Compliance of combined radio software and equipment

The EU RED cybersecurity requirements apply to a wide range of products, including internet-connected radio equipment, childcare products, toys, and wearable data collection equipment.

Network Protection (Article 3.3(d))

"Radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service."

Data Protection and Privacy (Article 3.3(e))

"Radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected".

Fraud Prevention (Article 3.3(f))

"Radio equipment supports certain features ensuring protection from fraud"

Harmonized Standards and Compliance

A harmonized standard is a European standard developed by a recognized European Standards Organization: CEN, CENELEC, or ETSI. It is created following a request from the European Commission to one of these organizations. Manufacturers, other economic operators, or conformity assessment bodies can use harmonized standards to demonstrate that products, services, or processes comply with relevant EU legislation. The references of harmonized standards must be published in the Official Journal of the European Union (OJEU)

The Commission services provide this summary for information purposes only. Although they take every possible precaution to ensure that the summary is updated regularly and is correct, errors may occur, and the summary may not be complete at a certain point in time: Directive 2014/53/EU on radio equipment - Summary list (xlsx).

3. Compliance Assessment

While the new cybersecurity requirements took effect in February 2022, compliance becomes mandatory on August 1, 2025.

Failure to comply can result in severe penalties and damage to a company's reputation.

Compliance Assessment and Certification

Xerox has elected to use the self-declaration option for certification in the form of a Declaration of Conformity.

Cybersecurity Best-Practices

Xerox follows industry standards and best practices throughout the Secure Development Life Cycle (SDLC) by integrating security scanning, testing, consultation, and analysis throughout the product development timeline from concept initiation through post launch support.

4. Xerox and the Secure Development Lifecycle (SDLC)

Secure Development by Design

Xerox integrates security into all levels of the development processes including but not limited to annual employee and partner training on best coding practices, regular scans and analysis using industry standard appliances, and continuous improvement to process.

Relevant Security Controls

Xerox features technologies including but not limited to secure data storage and transmission, encrypted data at rest, digitally signed software updates, and robust access control mechanisms that reduce the attack surface and improve security posture.

Risk Assessment and Mitigation

Xerox employs a product risk registry to analyze and track risks associated with products, services, and applications as well as regular security assessments of Common Vulnerabilities and Exploits (CVEs) as compiled by the National Institute of Standards and Technology (NIST) in the NVD Database.

5. EU RED Cybersecurity Compliant Products

Product Support Table

The table below includes Xerox products considered “internet connected radio equipment”. These products are fully compliant with EU RED, including the new cybersecurity requirements.

For specific information related to security controls and recommendations, reference the safety documentation compliance sheets for each model in the links below.

AltaLink / VersaLink	B / C Series	PrimeLink	Xerox
AltaLink B82xx MFP	Xerox B225 MFP	PrimeLink C92xx	Phaser 3020
AltaLink C82xx MFP	Xerox B230 Printer		WorkCentre 3025
VersaLink B415 MFP	Xerox B235 MFP		
VersaLink B620 MFP	Xerox B305 MFP		
VersaLink B625 MFP	Xerox B310 Printer		
VersaLink C415 MFP	Xerox B315 Printer		
VersaLink C620 Printer	Xerox C230 Printer		
VersaLink C625 Printer	Xerox C235 Printer		
VersaLink C7000	Xerox C320 Printer		
VersaLink B71xx	Xerox C325 MFP		
VersaLink C71xx			

6. Additional Information and Resources

Security @ Xerox®

Xerox maintains an evergreen public web page that contains the latest security information pertaining to its products. Please see https://www.xerox.com/security

Responses to Known Vulnerabilities

Xerox has created a document which details the Xerox Vulnerability Management and Disclosure Policy used in discovery and remediation of vulnerabilities in Xerox software and hardware. It can be downloaded from this page: https://www.xerox.com/information-security/information-security- articles-whitepapers/enus.html

Additional Resources

Below are additional resources.

Security Resource	URL
Frequently Asked Security Questions	https://www.xerox.com/en-us/information-security/frequently-asked-questions
Common Criteria Certified Products	https://security.business.xerox.com/en-us/documents/common-criteria/
Current Software Release Quick Lookup Table	https://www.xerox.com/security
Bulletins, Advisories, and Security Updates	https://www.xerox.com/security
Security News Archive	https://security.business.xerox.com/en-us/news/
Xerox Zero Trust Security	https://www.xerox.com/en-us/about/security-solutions/zero-trust-security