RMF document

All digital products (HW & SW)

Applicability of Cyber Resilience Act to ADLINK

1.0 TABLE OF CONTENT

2.0 GENERAL DOCUMENT INFORMATION

As ADLINK products are all somehow “digital” and cyber threats increase day by day, ADLINK customers more and more request information about the corresponding resilience against such threats for their own (internal) risk management.

Based on these requests and forced by current regulations, ADTW and especially ATG(D) needs to consider and follow the European Cyber Resilience Act 2024/2847.

Now the upcoming questions to be answered in this document shall be: ***What ADLINK products are concerned in which way? What timelines need to be followed and milestones kept? What measures need to be taken?***

Note: This document cites one or more reference documents. These text passages are indicated by a different font. `This example sentence is now marked as such a citation.`

2.1 Acronyms and abbreviations

The following abbreviations and acronyms are used throughout this document:

Acronym/abbreviation	Description/meaning
ADTW	ADLINK Technology Inc., TaiWan
ATG	ADLINK Technology GmbH
ATGD	ADLINK Technology GmbH, Deggendorf
ATGM	ADLINK Technology GmbH, Mannheim
BSI	Bundesamt für Sicherheit in der Informationstechnik i.e. Federal Office for Information Security
CRA	Cyber Resilience Act (see [REF1])
CSIRT	Computer Security Incident Response Team
ENISA	European Network and Information Security Agency
HW	According to [REF1]: `(5) 'hardware' means a physical electronic information system, or parts thereof capable of processing, storing or transmitting digital data;`
RMF	Risk Management File
SW	According to [REF1]: `(4) 'software' means the part of an electronic information system which consists of computer code;`

2.2 Definitions

Term/Phrase	Definition
ADLINK	ADTW and/or ADT(G), please observe the context
Configuration	General term denoting the modification(s) of a basic device. Such modification(s) are related to RAM size, CPU type, HDD or/and SSD type, WLAN, RFID, isolated COMports, other customizations but changes of SW/FW as well. Note: The reduction or removal of functions is also a configuration.
Model	General term denoting various types of basic and modified devices.

Term/Phrase	Definition
	Product families typically consist of defined (basic) devices. Each device differing significantly (e.g. by size, function, etc.) is then a model of this product family and needs an UDI-DI.
Shall	Means in the context of this document a “must have” or is a mandatory requirement or compliance.

2.3 Additional documents & references

REF#	Document ID/file name	Remark(s)
[REF1]	2024_2847_CRA.pdf	**REGULATION (EU) 2024/2847** OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 **(Cyber Resilience Act)** Note: Current available corrections C1, C2 and C3 are not relevant for ADLINK
[REF2]	2019_881_CyberSec_regulation.pdf	**REGULATION (EU) 2019/881** OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 **on ENISA** (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
[REF3]	BSI-TR-03183-1_v0_10_0.pdf	**Technical Guideline TR-03183**: Cyber Resilience Requirements for Manufacturers and Products issued by the German Federal Office for Information Security (i.e. BSI) in version 0.10.0 on 12-Sept-2025
[REF4]	FAQs_on_the_CRA_v12.pdf	**FAQ of the EU Commission** in version 1.2 from 16-Jan-2026
[REF5]	EU CRA landing page	Web page of the European Union with links to the legal text ([REF1]) and the FAQ document (in EN), see [REF4]

3.0 INFORMATION COLLECTION

3.1 [REF1]: Article 1 Subject matter

[REF1] defines in Article 1 the purpose of the CRA in four points. While the first two of them are linked to products or devices, the last both document requirements to processes.

This Regulation lays down:

(a) rules for the **making available on the market of products with digital elements** to ensure the cybersecurity of such products;

(b) **essential cybersecurity requirements for the design, development and production** of products with digital elements, **and obligations for economic operators** in relation to those products with respect to cybersecurity;

(c) **essential cybersecurity requirements for the vulnerability handling processes put in place by manufacturers** to ensure the cybersecurity of products with digital elements during the time the products are expected to be in use, and obligations for economic operators in relation to those processes;

(d) rules on market surveillance, including monitoring, and enforcement of the rules and requirements referred to in this Article.

So the CRA lays down rules and cybersecurity requirements for products with digital elements for various stake holders in the course of putting in place as well as making available them on the market.

3.2 [REF1]: Article 3 Definitions

[REF1] provides in Article 3 various definitions which are directly listed below for convenient understanding.

For the purposes of this Regulation, the following definitions apply:

(1) **'product with digital elements'** means a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately;

(2) **'remote data processing'** means **data processing at a distance for which the software is designed and developed by the manufacturer**, or under the responsibility of the manufacturer, **and the absence of which would prevent the product with digital elements from performing one of its functions**;

(3) **'cybersecurity'** means cybersecurity as defined in Article 2, point (1), of Regulation (EU) 2019/881;

The related definitions for cybersecurity and additionally cyber threat from [REF2] are these:

(1) **'cybersecurity'** means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats;

(8) **'cyber threat'** means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons;

Back to the CRA, which provides in article 3 in total 51 definitions. The next both are the root cause for ADLINK products to be concerned by the CRA:

(7) **'electronic information system'** means a system, including electrical or electronic equipment, **capable of processing, storing or transmitting digital data;**

(9) **'physical connection'** means a **connection between electronic information systems or components implemented using physical means,** including through electrical, optical or mechanical interfaces, wires or radio waves;

Following [REF1] definition (1) **all ADLINK products are concerned by the CRA** which is confirmed by definitions (7) and (9). ADLINK products are either

- SW capable to transmit and receive data via a physical connection or
- HW capable to process, store or transmit digital data and building (or are already) a physical electronic information system

Note: Chapter 2.1 Acronyms and abbreviations provides the definitions for SW and HW from the CRA.

The following three CRA definitions are important for ADLINK as they influence timelines and requested activities later:

(21) **'placing on the market'** means **the first making available of a product** with digital elements on the Union market;

(22) **'making available on the market'** means **the supply of a product** with digital elements **for distribution or use on the Union market in the course of a commercial activity,** whether in return for payment or free of charge;

(30) **'substantial modification'** means a **change to the product** with digital elements **following its placing on the market,** which affects the compliance of the product with digital elements with the essential cybersecurity requirements set out in Part I of Annex I or **which results in a modification to the intended purpose** for which the product with digital elements has been assessed;

3.3 [REF1]: Article 2 Scope

The concernment of ADLINK products is derived from the applicable CRA definitions in chapter 3.2 [REF1]: Article 3 Definitions. This article sequence is changed for better understanding as the prior CRA chapter Article 2 Scope uses already later following definitions. Nevertheless this article 2 underpins the relevance for ADLINK and its products:

1. This Regulation applies to **products with digital elements** made available on the market, **the intended purpose or reasonably foreseeable use of which includes a direct or indirect logical or physical data connection** to a device or network.

Thereafter following scope exclusions do not list or define ADLINK products except Medical Devices underlying the MDR (EU) 2017/745. So (again;-) MDs are exempt from the CRA.

3.4 [REF1]: Article 71 Entry into force and application

[REF1] article 71 provides a timeline for partly and full application of the CRA:

2. This Regulation shall apply from 11 December 2027.

However, Article 14 shall apply from 11 September 2026 and Chapter IV (Articles 35 to 51) shall apply from 11 June 2026.

The following table lists these timelines together with the referenced chapters (including the articles if relevant) for a brief overview.

Appliance date	**CRA Chapter & Article**	**CRA chapter or article title** **Incl. remark(s)**
11th June 2026	Chapter IV Article (35..51)	NOTIFICATION OF CONFORMITY ASSESSMENT BODIES *Does NOT concern ADLINK > concerns member states and notified bodies*
11th September 2026	Article 14	Reporting obligations of manufacturers *Concerns ADLINK > especially ADLINK Taiwan as manufacturer and in the following ATG*
11th December 2027	***CRA complete***	***REGULATION (EU) 2024/2847 (Cyber Resilience Act)*** ***Applies to all ADLINK products placed after this date, as well as previously placed products that have undergone significant changes.***

3.5 [REF1]: Article 69 Transitional provisions

[REF1] gives in in Article 69 rules for products which are placed on the market before 11th December 2027. The applicable paragraphs are

2. Products with digital elements that have **been placed on the market before 11 December 2027 shall be subject to the requirements set out in this Regulation only if, from that date, those products are subject to a substantial modification.**

3. By way of derogation from paragraph 2 of this Article, **the obligations laid down in Article 14 shall apply to all products** with digital elements that fall within the scope of this Regulation that have been placed on the market before 11 December 2027.

All ADLINK products placed on the market (i.e. made available in the Union for the first time) until 11th December 2027 do **NOT need to comply** with the CRA. This exemption is valid only, if no substantial modification is applied to these products (see chapter 3.2 [REF1]: Article 3 Definitions).

[REF4] provides this example to clarify the term `substantial modification´:

For example, a manufacturer places on the market a smart TV in mid-2027. The manufacturer is not required to comply with the CRA for this product with digital elements. In 2028, it releases a software update, which does not qualify as a substantial modification, to fix a bug that causes apps running on the TV to crash after some usage time. The manufacturer is not required to bring the smart TV in conformity with the CRA, as it would not be substantially modifying it. In 2029, that manufacturer releases a software update that qualifies as a substantial modification, for example because it modifies the original intended functions by enabling the smart TV to control smart home systems. In that case, the manufacturer is required to bring the smart TV into compliance with the CRA.

Nevertheless the reporting obligations as specified by article 14 (see chapter 3.6) need to be followed by ADLINK in any case for all products, beginning with 11th September 2026.

3.6 [REF1]: Article 14 Reporting obligations of manufacturers

The upcoming obligations for ADLINK, documented in the CRA article 14, create near future tasks and responsibilities to be observed. Therefore the whole article is cited in the following.

[REF3] is an official German BSI guideline and very handy in explaining and commenting the CRA. Fortunately this guideline is available in English.

Note: Some cited paragraphs are followed by relevant information/clarification or by action requests. The latter are indicated by the key phrase @ADLINK. Some paragraphs are no concern for ADLINK and are therefore commented as such.

1. A manufacturer shall notify any actively exploited vulnerability contained in the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to ENISA. The manufacturer shall notify that actively exploited vulnerability via the single reporting platform established pursuant to Article 16.

@ADLINK to **report actively exploited vulnerability** contained in the product to a designated CSIRT and ENISA

2. For the purposes of the notification referred to in paragraph 1, the manufacturer shall submit:

(a) an **early warning notification** of an actively exploited vulnerability, without undue delay and in any event **within 24 hours** of the manufacturer becoming aware of it, indicating, where applicable, the Member States on the territory of which the manufacturer is aware that their product with digital elements has been made available;

(b) unless the relevant information has already been provided, a **vulnerability notification**, without undue delay and in any event **within 72 hours** of the manufacturer becoming aware of the actively exploited vulnerability, which shall provide general information, as available, about the product with digital elements concerned, the general nature of the exploit and of the vulnerability concerned as well as any corrective or mitigating measures taken, and corrective or mitigating measures that users can take, and which shall also indicate, where applicable, how sensitive the manufacturer considers the notified information to be;

(c) unless the relevant information has already been provided, a **final report, no later than 14 days** after a corrective or mitigating measure is available, including at least the following:

(i) a description of the vulnerability, including its severity and impact;

(ii) where available, information concerning any malicious actor that has exploited or that is exploiting the vulnerability;

(iii) details about the security update or other corrective measures that have been made available to remedy the vulnerability.

Contains details and deadlines of information to be reported.

3. A manufacturer shall notify any severe incident having an impact on the security of the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to ENISA. The manufacturer shall notify that incident via the single reporting platform established pursuant to Article 16.

@ADLINK to **report severe incidents** impacting the security of a product to a designated CSIRT and ENISA

4. For the purposes of the notification referred to in paragraph 3, the manufacturer shall submit:

(a) an **early warning notification** of a severe incident having an impact on the security of the product with digital elements, without undue delay and in any event **within 24 hours** of the manufacturer becoming aware of it, including at least whether the incident is suspected of being caused by unlawful or malicious acts, which shall also indicate, where applicable, the Member States on the territory of which the manufacturer is aware that their product with digital elements has been made available;

(b) unless the relevant information has already been provided, an **incident notification**, without undue delay and in any event **within 72 hours** of the manufacturer becoming aware of the incident, which shall provide general information, where available, about the nature of the incident, an initial assessment of the incident, as well as any corrective or mitigating measures taken, and corrective or mitigating measures that users can take, and which shall also indicate, where applicable, how sensitive the manufacturer considers the notified information to be;

(c) unless the relevant information has already been provided, a **final report, within one month** after the submission of the incident notification under point (b), including at least the following:

(i) a detailed description of the incident, including its severity and impact;

(ii) the type of threat or root cause that is likely to have triggered the incident;

(iii) applied and ongoing mitigation measures.

Contains details and deadlines of information to be reported.

5. For the purposes of paragraph 3, an **incident having an impact on the security of the product** with digital elements shall be considered to be severe where:

(a) it negatively affects or is capable of negatively affecting the ability of a product with digital elements to protect the availability, authenticity, integrity or confidentiality of sensitive or important data or functions; or

(b) it has led or is capable of leading to the introduction or execution of malicious code in a product with digital elements or in the network and information systems of a user of the product with digital elements.

Paragraph (5) is a definition for the phrase **incident having an impact on the security of the product**

6. Where necessary, the CSIRT designated as coordinator initially receiving the notification may request manufacturers to provide an intermediate

report on relevant status updates about the actively exploited vulnerability or severe incident having an impact on the security of the product with digital elements.

Specifies the permission of the designated CSIRTs for information requests.

7. The notifications referred to in paragraphs 1 and 3 of this Article shall be submitted via the single reporting platform referred to in Article 16 using one of the electronic notification end-points referred to in Article 16(1). The notification shall be submitted using the electronic notification end-point of the CSIRT designated as coordinator of the Member State where the manufacturers have their main establishment in the Union and shall be simultaneously accessible to ENISA.

Defines the reporting path via a platform to the designated CSIRT and ENISA for European manufacturers.

For the purposes of this Regulation, a manufacturer shall be considered to have its main establishment in the Union in the Member State where the decisions related to the cybersecurity of its products with digital elements are predominantly taken. If such a Member State cannot be determined, **the main establishment shall be considered to be in the Member State where the manufacturer concerned has the establishment with the highest number of employees in the Union.**

Specifies the German CSIRT as designated CSIRT (and reporting platform) because ATG has the highest number of employees in the Union and is therefore considered the main establishment for this purpose.

Where a manufacturer has no main establishment in the Union, it shall submit the notifications referred to in paragraphs 1 and 3 using the electronic notification end-point of the CSIRT designated as coordinator in the Member State determined pursuant to the following order and based on the information available to the manufacturer:

(a) the Member State in which the authorised representative acting on behalf of the manufacturer for the highest number of products with digital elements of that manufacturer is established;

(b) the Member State in which the importer placing on the market the highest number of products with digital elements of that manufacturer is established;

(c) the Member State in which the distributor making available on the market the highest number of products with digital elements of that manufacturer is established;

(d) the Member State in which the highest number of users of products with digital elements of that manufacturer are located.

In relation to the third subparagraph, point (d), a manufacturer may submit notifications related to any subsequent actively exploited vulnerability or severe incident having an impact on the security of the product with digital elements to the same CSIRT designated as coordinator to which it first reported.

Not relevant as ADLINK related CSIRT is defined previously.

8. After becoming aware of an **actively exploited vulnerability or a severe incident having an impact on the security of the product** with digital elements, **the manufacturer shall inform the impacted users of the product** with

digital elements, and where appropriate all users, of that vulnerability or incident and, where necessary, of any risk mitigation and corrective measures that the users can deploy to mitigate the impact of that vulnerability or incident, where appropriate in a structured, machine-readable format that is easily automatically processable. Where the manufacturer fails to inform the users of the product with digital elements in a timely manner, the notified CSIRTs designated as coordinators may provide such information to the users when considered to be proportionate and necessary for preventing or mitigating the impact of that vulnerability or incident.

@ADLINK to **inform users of concerned products** (e.g. in a machine-readable form) and in a timely manner; additionally **information about possible mitigations**.

9. By 11 December 2025, the Commission shall adopt delegated acts in accordance with Article 61 of this Regulation to supplement this Regulation by specifying the terms and conditions for applying the cybersecurity-related grounds in relation to delaying the dissemination of notifications as referred to in Article 16(2) of this Regulation. The Commission shall cooperate with the CSIRTs network established pursuant to Article 15 of Directive (EU) 2022/2555 and ENISA in preparing the draft delegated acts. 10. The Commission may, by means of implementing acts, specify further the format and procedures of the notifications referred to in this Article as well as in Articles 15 and 16. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2). The Commission shall cooperate with the CSIRTs network and ENISA in preparing those draft implementing acts.

Permission for the (European) Commission to adopt further delegated acts and “letter of intent” to collaborate with CSIRTs and ENISA.

3.7 Future ADLINK obligations starting 11-Dec-2027

ADLINK products need to comply with the CRA if placed on the market after 11-Dec-20207.

Obligations for this compliance are specified in [REF1] chapter II OBLIGATIONS OF ECONOMIC OPERATORS AND PROVISIONS IN RELATION TO FREE AND OPEN-SOURCE SOFTWARE. For a brief overview, the following list includes the titles of the articles 13..26 from this chapter. ADLINK concerning and relevant articles are marked bold and italic:

Article 13 ***Obligations of manufacturers***

Article 14 ***Reporting obligations of manufacturers***

Article 15 Voluntary reporting

Article 16 Establishment of a single reporting platform

Article 17 Other provisions related to reporting

Article 18 ***Authorised representatives***

Article 19 ***Obligations of importers***

Article 20 ***Obligations of distributors***

Article 21 ***Cases in which obligations of manufacturers apply to importers and distributors***

Article 22 Other cases in which obligations of manufacturers apply

Article 23 ***Identification of economic operators***

Article 24 Obligations of open-source software stewards

Article 25 Security attestation of free and open-source software

Article 26 Guidance

Most important tasks and responsibilities for ADLINK derived from the marked entries are

1. to observe the essential cybersecurity requirements as set out in [REF1] Annex I part I
2. to handle vulnerabilities as set out in [REF1] Annex I part II
3. to conduct a risk assessment inclusive appropriate documentation for concerned products as set out in [REF1] Article 13 paragraphs 2. and 3.
4. to create and maintain a technical documentation for each concerned product as set out in [REF1] Article 13 paragraphs 4
   Note: Annex VII provides a minimum requirements list for that purpose

Of course a conformity assessment process resulting in a corresponding Declaration of Conformity and the affixing of the CE mark is mandatory. Be aware that this is depending on the products “risk class”, documented in [REF1] Annexes III and IV, which shall be determined in the mentioned risk assessment. Depending on this classification, ADLINK is allowed to apply the CE mark on its own responsibility or needs a certification by a conformity assessment body for that.

4.0 SUMMARY AND CONCLUSION

This chapter shall now compare the questions from chapter 2.0 General document information with found information from relevant chapter passages (cited or commented) above.

4.1 What ADLINK products are concerned in which way?

Mainly the definitions cited in chapter 3.2 [REF1]: Article 3 Definitions and corresponding comments together with chapter 3.3 [REF1]: Article 2 Scope underpin the CRA regulations applicability to ALL ADLINK products.

Products already placed on the market need NOT to comply with the CRA. Only a reporting obligation will exist from 11th September 2026.

Products placed on the market or substantially modified after 11th December 2027 need to comply with the CRA completely.

4.2 What timelines need to be followed and milestones kept?

See previous chapter 4.1 and for details chapters 3.4 [REF1]: Article 71 Entry into force and application and 3.5 [REF1]: Article 69 Transitional provisions.

4.3 What measures need to be taken?

Besides creating and establishing internal procedures and tasks including the appropriate documentation, key measures are

- Reporting to official contacts by assigned ADLINK persons and recommended under a substitution policy as timelines to be kept are in some cases 24h only.
  Details to be found in chapter 3.6 [REF1]: Article 14 Reporting obligations of manufacturers

- Creating and maintaining a technical documentation for all future ADLINK products
  Details to be found in chapter 3.7 Future ADLINK obligations starting 11-Dec-2027

- Creating and maintaining a risk assessment
  Details to be found in chapter 3.7 Future ADLINK obligations starting 11-Dec-2027

4.4 Recommended actions

4.4.1 Other regulations and countries

The CRA is an EU regulation applicable only there. It is expected that other countries follow this approach and create (or already have created) their own legislation regarding cyber resilience in the coming years. That should lead into an international observation procedure executed by ADLINK to be informed about such developments in time.

4.4.2 OS and SW responsibility

ADLINK should take over only the required and necessary obligations. As most ADLINK products need an Operating System (OS) to provide the intended functionality and is shipped in some cases with the products (e.g. upon customers request), the OS is NOT considered as part of these products. ADLINK should exclude its responsibility therefore via risk assessment or similar documentation.

Otherwise, ADLINK needs to inform about already covered vulnerabilities and incidents, see Microsoft® updates etc.

The same exclusion shall apply to 3rd party SW, not developed or maintained within ADLINK.

4.4.3 Responsibility for drivers

It is to be discussed if drivers, commonly supplied by 3rd party vendors and used with ADLINK products, shall be covered by ADLINK. A reason for this could be, that such vendors are selected by ADLINK with no customer influence possible. Additionally some vendors might not offer an interface or even a communication channel, as they are e.g. located outside the EU. On the other hand, vendors such as Intel® will offer a much more professional and timely service, an additional ADLINK action regarding the same issue could confuse more than help.

4.4.4 ADLINK CSIRT

ADLINK should follow the CSIRT (Computer Security Incident Response Team) idea as a central handling and management group, especially for the reporting obligations. As one of these are to inform customers and as customers will be the most probable reporting channel for vulnerabilities and especially incidents, this team should be located close to customers in terms of organisation.