EUROPEAN
COMMISSION

Brussels, XXX
[…](2026) XXX draft

ANNEX

ANNEX

Communication to the Commission

Approval of the content of the draft Communication from the Commission - Commission guidance on the application of Regulation (EU) 2024/2847 (Cyber Resilience Act)

Contents

1 Introduction

1.1 The Cyber Resilience Act

1. 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) 2019/1020 and Directive (EU) 2020/1828 (the Cyber Resilience Act)[1] entered into force on 10 December 2024. The Regulation aims to strengthen the EU's approach to cybersecurity, address cyber resilience at EU level and improve the functioning of the internal market by laying down a uniform legal framework for essential cybersecurity requirements for placing products with digital elements on the EU market, as well as during a product's lifecycle.

2. The Cyber Resilience Act (CRA) is built upon the EU's New Legislative Framework (NLF) set out in Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 and Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC.[2]

3. Market surveillance and enforcement is carried out by national market surveillance authorities. Products with digital elements that fall within the scope of the CRA are covered by Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011. The Commission and the European Union Agency for Cybersecurity (ENISA) support economic operators and Member States in the application of the CRA.

1.2 Purpose of the guidance

4. Article 26(1) of the CRA requires the Commission to publish guidance to assist economic operators in applying the Regulation, with a particular focus on facilitating compliance by microenterprises and small and medium-sized enterprises (SMEs). Article 26(2) sets out minimum aspects that should be addressed in the guidance. These include: (i) the scope of the CRA (particularly remote data processing solutions and free and open-source software); (ii) the notion of 'support periods'; (iii) the interplay between the CRA and other EU legislation; and (iv) the concept of 'substantial modification'.

5. On 3 December 2025, the Commission published a series of frequently asked questions (FAQs), which are intended to help economic operators prepare for the implementation of the CRA.[3]

[1] OJ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj

[2] The Commission's 2026 work programme envisages the presentation of a "European Product Act", updating the NLF and the rules on market surveillance and on standardisation: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025DC0870

[3] The FAQs can be downloaded via the Commission's CRA implementation website, from the dedicated FAQs webpage.

6. This guidance is intended to help economic operators comply with the CRA and to support the activities of market surveillance authorities, notifying authorities and notified bodies, with a view to ensuring the harmonised enforcement of the CRA across the Union. This guidance is not intended to cover the CRA in its entire scope, but rather to provide clarifications on the rationale of certain key provisions and how they could be implemented in practice. This guidance concerns the CRA and is not applicable to other EU laws.

7. Stakeholders were extensively consulted in the preparation of this guidance, including the Expert Group on Cybersecurity of Products with Digital Elements[4] and [via a public consultation].

8. This guidance is not binding for economic operators or other actors subject to the CRA. An authoritative interpretation of the CRA may only be given by the Court of Justice of the European Union. Nevertheless, these guidelines set out the Commission's interpretation of the CRA, with a view to supporting compliance and contributing to the effective implementation of the Regulation. A case-by-case assessment will always be necessary to account for the specifics of each individual case.

9. In line with Article 26 of the CRA, the Commission may consider issuing further guidance, including guidance targeted at manufacturers subject to the CRA and other Union harmonisation legislation or to other related Union legal acts. This guidance may, for example, address questions on interplay between the CRA and Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (AI Act), and Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA).

[4] Expert Group on Cybersecurity of Products with Digital Elements in the register of Commission expert groups and other similar entities

2 Scope

2.1 Placing on the market

10. The CRA applies to products with digital elements (or simply 'products') that are made available on the EU market. The concept of making available on the market is defined in Article 3(22) of the CRA as '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'. In accordance with Article 3(21), a product is placed on the EU market the first time it is made available.

11. The latest edition of the 'Blue Guide on the implementation of EU product rules' published in 2022 (henceforth, 'the Blue Guide')[5], provides guidance facilitating the understanding of the EU product rules and their uniform application across the different sectorial legal frameworks aligned to the new legislative framework (NLF), such as the CRA. The Blue Guide indicates that the concepts of 'placing on the market' and of 'making available' are to be understood as referring 'to each individual product, not to a type of product, and whether it was manufactured as an individual unit or in series' (Section 2.3).

12. For more 'traditional' products covered by the NLF, such as hardware in the form of machinery or radio equipment products, the concept of 'placement on the market' is well established, and the Blue Guide provides further guidance to clarify when such products are considered to be placed on the market. The 'summary examples' contained in the Blue Guide's Section 2.12 provide further examples of the concept of 'placing on the market'.

13. However, given the nature of intangible products such as standalone software, which is supplied via digital means, further guidance is needed on when such products are considered placed on the market. Once the software's manufacturing phase is complete and the product is offered to prospective users in the EU market, its manufacturer can be regarded as having manufactured a virtually infinite number of copies of the same software product and having supplied them for distribution or use. In fact, unlike tangible products, software supplied via digital means is not subject to physical production or stock limitations: each act of making the software available for download or remote access results in a new identical copy being created for the user. As long as this version of the software is not modified in a way that affects compliance with the CRA, the placing on the market is to be considered to have occurred at the moment of the first offering for distribution or use. The possibility of subsequent download or remote access to this version of the software product is therefore to be regarded as an instance where this software product is made available.

14. Therefore, a standalone software product should be considered to have been placed on the market when its manufacturing phase is complete and that software is first supplied for distribution or use on the EU market in the course of a commercial activity. The manufacturer should be considered to have placed on the market a virtually infinite

[5] Commission notice - The 'Blue Guide' on the implementation of EU product rules 2022 (Text with EEA relevance) 2022/C 247/01, OJ C 247, 29.6.2022, pp. 1–152.

number of copies of the same software product at the same time. Therefore, while multiple copies of the same software remain individual products, they are considered to be placed on the market at the same time, regardless of when possession or use of each individual copy is transferred to another natural or legal person.

Example 1: On 1 January 2028, company A first supplies for distribution via its website version 1.0.0 of its software X. On the same day, customer 1 purchases a copy of version 1.0.0 of software X. On 15 January 2028, customer 2 purchases a copy of version 1.0.0 of software X. Both copies of version 1.0.0 of software X are placed on the market on 1 January 2028.

15. Given the iterative nature of software development, it should be further clarified that subsequent iterations of a software product are considered as newly placed on the market when those iterations qualify as a 'substantial modification' of a software product already placed on the market, as indicated in recital 41 of the CRA. Iterations that do not qualify as substantial modifications do not require the manufacturer to perform a new conformity assessment procedure and therefore do not modify that software's date of placement on the market. For more guidance on the concept of substantial modifications see Section *4 Substantial modifications*.

Example 2: On 1 January 2028, company A first supplies for distribution via its website version 1.0.0 of software X. On the same day, customer 1 purchases a copy of version 1.0.0 of software X. On 15 January 2028, company A issues an updated version 1.0.1 of software X that does not constitute a substantial modification. On 30 January 2028, customer 2 purchases a copy of version 1.0.1 of software X. Both copies of version 1.0.0 and 1.0.1 of software X are considered to be placed on the market on 1 January 2028.

16. The guidance laid down in points 13, 14 and 15 applies exclusively insofar as the product is standalone software provided via digital means. This is not the case, for example, where software is provided via physical means (e.g. a USB flash drive), as the USB flash drive with the software on it is the product supplied for distribution, or when the software is combined with hardware, as discussed in Section *2.2 Combination of hardware and software forming a product*.

2.2 Combination of hardware and software forming a product

17. Article 3(1) of the CRA defines a product with digital elements as 'a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately'. Such products fall within the scope of the CRA where their intended purpose or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network.[6]

18. The CRA therefore can cover standalone software, such as (i) apps and computer programs; (ii) hardware with embedded software (e.g. Internet-of-Things devices); (iii) standalone hardware (e.g. integrated circuits, motherboards); and (iv) any combination of hardware and software supplied separately but intended to operate together.

[6] See Article 2(1) of the CRA.

19. Whether software forms part of a product should be determined not by how or when that software is delivered to the user, but by whether, in light of the product's intended purpose and reasonably foreseeable use, the software is necessary for the product to perform its intended functions. Where a hardware device is designed to operate together with specific software in order to perform its functions, the hardware and that software together constitute the product placed on the market. Software that is necessary to operate, configure, control or meaningfully use a device is therefore part of the product, even if it is obtained through a separate channel (e.g. an app store, a download link or another digital channel after the hardware has been placed on the market).

Example 3: A network printer is placed on the market as hardware, while the software drivers required to send print jobs, configure the device and manage its operation are made available for download from the manufacturer's website. Although the printer and the drivers are supplied through different channels, they together constitute a single product with digital elements, because the printer cannot fulfil its intended purpose without the drivers.

Example 4: A fitness wearable is placed on the market to measure a user's heart rate and activity, while a smartphone application provided by the manufacturer is required to display the measurements, show history and allow configuration of the device. Although the application is downloaded separately from an app store, the wearable and the application together constitute a single product, because they are designed and intended to operate together to deliver the product's functionality.

2.3 Source code

20. It is also useful to clarify what constitutes a software product. The CRA defines software as 'the part of an electronic information system which consists of computer code' (Article 3(4)). Computer code can generally mean either (i) machine code, which is the set of instructions directly executed by a computer's processor, written in binary format; or (ii) source code, i.e. the set of instructions and statements written in a programming language, which must be compiled or interpreted to be executed by a computer.

21. Whether computer code is uncompiled, compiled or interpreted is not relevant to determining whether such software is within the scope of the CRA. The CRA applies to products when they are made available on the EU market in the course of a commercial activity. A natural or legal person that shares free and open source computer code on publicly accessible repositories is not considered to be placing that code on the EU market (for more guidance on the topic, see Section *3 Free and open-source software*). Unfinished code shared during a product's design and development phase (e.g. for testing or review) is also not considered to be placed on the market, as its manufacturing phase is not completed. Similarly, sample or demo code provided as part of tutorials or training materials is also not considered placed on the market.[7]

[7] It should also be recalled that Article 4(3) allows manufacturers to make available on the market unfinished software which does not comply with the Regulation, such as alpha versions, beta versions or release candidates, provided that the unfinished software is made available only for the time necessary to test it and gather feedback.

22. On the other hand, where a manufacturer provides its customers with computer code as part of its commercial activity, that code is considered to be placed on the market, regardless of whether it is machine code or source code.[8]

Example 5: Company A licences source code to company B for a customisable internal platform, and provides that source code in a text file. Even if that source code requires further adaptation and compilation by company B before being used, company A is responsible for the source code it has developed, when licensing it to company B (i.e. at the moment that code is placed on the market). Company A is not responsible for company B's subsequent adaptations and compilation of that code.

2.4 Data connection

23. Article 2(1) states that the CRA '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'. The definition of 'product with digital elements' ultimately relies on the definition of electronic information system, i.e. 'a system, including electrical or electronic equipment, capable of processing, storing or transmitting digital data' (Article 3(7)). The scope of the CRA is therefore anchored not in the mere presence of electronics, but in a product's capacity to exchange digital information.

24. While the terms 'logical connection' and 'physical connection' are defined in Article 3, the CRA does not define 'data connection' or 'digital data'. It is therefore useful to set out an interpretation of what a data connection is, in order to clarify the boundary of the CRA's scope. This boundary is particularly important to distinguish products that merely use electrical signals from those that participate in digital communication and are therefore exposed to cybersecurity risks.

25. At its most basic level, a data connection involves transmitting information in binary form, i.e. as a sequence of 0s and 1s. Simply switching an output on and off (i.e. 0/1) does not by itself constitute a data connection if those states are not intended to represent data or are not read by a digital input. For a data connection to exist, the binary states must be deliberately encoded as information by a source and must be capable of being decoded as information at the destination. In other words, there must be a sender that deliberately generates digital symbols according to a defined scheme, and a receiver capable of interpreting those symbols as data. Where electrical or electronic signals are used solely to trigger or power a function, without conveying digitally encoded information, no data connection exists for the purposes of the CRA.

[8] On the other hand, it should be noted that for the purposes of product liability law, computer code itself does not constitute a product and therefore manufacturers that place such code on the market cannot be held liable under Directive (EU) 2024/2853 (the Product Liability Directive). Recital 13 of that Directive states that "information is not, however, to be considered a product, and product liability rules should therefore not apply to the content of digital files, such as media files or e-books or the mere source code of software". This does not preclude that manufacturers may be liable under national tort law.

2.5 Complex systems

26. Products within the meaning of the CRA may consist not only of single devices or software components, but also of complex systems, including systems composed of multiple hardware and software elements that operate together to perform a certain function. Where such a system is placed on the market as a single product, it constitutes a product for the purposes of the CRA.

27. Such complex systems are often characterised by long design and development cycles, with contracts that may have been signed before the CRA applies, extended operational lifetimes and a high degree of technical and organisational complexity. Such systems may rely on components placed on the market before the CRA entered into application, on established architectures or on widely used interoperability standards, including standards referred to in other EU legislation or sector-specific frameworks. As a result, certain technical characteristics of those systems may be difficult or disproportionate to modify without affecting their intended purpose, safety, reliability or interoperability with existing infrastructure.

28. These characteristics do not in themselves exclude complex systems from the CRA's scope. Rather, they illustrate the application of the CRA's risk-based approach, which allows compliance to be demonstrated in different ways depending on the product's characteristics and constraints, in accordance with Article 13(3) of the CRA. Those characteristics form part of the product's intended purpose and operating context and are therefore relevant when assessing compliance with the essential cybersecurity requirements. In particular, recital 55 explicitly recognises that certain essential requirements may not be fully compatible with the nature of a product. For example, this may be the case where compliance would undermine mandatory interoperability requirements or the system's proper functioning.

29. Accordingly, manufacturers are required to address cybersecurity risks on the basis of the cybersecurity risk assessment referred to in Article 13(2). As also explained in recital 55, in some cases, specific essential cybersecurity requirements are not applicable or cannot be fulfilled via the implementation of state-of-the-art security measures due to, for example, the system's intended purpose, which requires the product to interact with existing dependencies or to follow certain interoperability requirements. In such cases, manufacturers should identify and document those specific constraints, assess the associated risks, and implement appropriate alternative or compensatory risk mitigation measures, so as to not undermine the product's security. For these purposes, both the technical documentation referred to in Article 31 and the information and instructions to the user referred to in Annex II play a key role in transparently describing the identified constraints, the associated cybersecurity risks and the risk mitigation measures implemented. In accordance with the obligation to keep the risk assessment updated during the support period, manufacturers should also periodically reassess whether such constraints continue to exist. Where such constrains can be lifted or reduced over time, manufacturers should update the product accordingly so that it can move towards state-of-the-art cybersecurity.

Example 6: A manufacturer places on the market a product that communicates with external systems using a network protocol. As part of the application of the essential cybersecurity requirements, the manufacturer determines, on the basis of the cybersecurity risk assessment, that the use of a secure communication protocol is necessary to ensure the confidentiality and integrity of data exchanged by the product.

However, the product's intended purpose includes interoperability with existing systems that only support an older or less secure protocol. In such cases, the manufacturer may implement that protocol where this is necessary to achieve interoperability, provided that the associated cybersecurity risks are identified and mitigated through other means.
Where it is technically feasible for the product to support both the secure protocol and the less secure protocol, the manufacturer is expected to implement the secure protocol and to enable its use by default. The less secure protocol would be allowed only where required for interoperability.

2.6 Products designed before the CRA entered into application

30. In some cases, a manufacturer will place on the market a product manufactured in accordance with a type or model designed and developed before the date of application of the CRA. In such cases, compliance with this Regulation does not necessarily require that the product be redesigned. The manufacturer is required to carry out a cybersecurity risk assessment in accordance with Article 13(2) of the CRA in order to determine whether the product, on the basis of its intended purpose and reasonably foreseeable use, meets the essential cybersecurity requirements set out in Part I of Annex I.

31. Where the outcome of that risk assessment demonstrates that the product already incorporates appropriate and effective security measures addressing the relevant risks, the manufacturer may rely on those existing measures to demonstrate compliance with the CRA. The CRA does not in itself impose an obligation to introduce new security features or to redesign the product where this is not necessary to address the identified risks.

32. Nevertheless, the manufacturer remains subject to the obligations laid down in the CRA. These include making sure, before the product is placed on the market, that the applicable conformity assessment procedure has been carried out, the EU declaration of conformity has been drawn up and the CE marking affixed. Compliance with those requirements is independent of whether the product design required modification as a result of the risk assessment. For products designed prior to the application of the CRA, when it is not possible for the manufacturer to demonstrate how the risk assessment has been taken into account during the design and development phase of the product, the obligation of Article 13(2) should be understood as requiring manufacturers to perform a cybersecurity risk assessment and demonstrate on that basis that the product incorporates adequate security measures with a view to minimising cybersecurity risks, preventing incidents and minimising their impact, including in relation to the health and safety of users.

33. Accordingly, products designed before the CRA entered into application might be placed on the market under the CRA without redesign, provided that the manufacturer can demonstrate, through the cybersecurity risk assessment and the technical

documentation, that the product achieves an appropriate level of cybersecurity in light of its intended purpose and reasonably foreseeable use and complies with the cybersecurity essential requirements.

34. Furthermore, it is necessary to clarify the application of conformity assessment obligations for manufacturers of products that are manufactured in accordance with a type or model designed and developed before the date of application of the CRA. In accordance with Article 13(12), the manufacturer is required to demonstrate via the relevant conformity assessment procedure that its product is in conformity with the applicable essential cybersecurity requirements and to include evidence to that effect in the product's technical documentation (point 6 of Annex VII).

35. However, the application of such requirements needs to be interpreted in light of the cybersecurity risk assessment and the risk profile of the product. Particularly in the case of products designed before the CRA applied and subject to the conformity assessment procedures of Article 32(1), where the risk assessment demonstrates that the product already incorporates appropriate and effective security measures addressing that product's risks, the obligation to provide evidence as part of the conformity assessment procedure should not be understood as requiring the manufacturer to provide test results covering the original design and development phases of such products. This would not be necessary as it would not be contributing to increasing the security of the product itself. Where tests may nonetheless be necessary, manufacturers are not expected to provide evidence of tests carried out on all product variants, but can group such tests across product families, as further discussed in Section *7.4 Re-use of risk assessments and conformity documentation for product families*.

36. Nonetheless, the manufacturer should provide evidence of how it complies with the vulnerability handling processes laid down in Part II of Annex I, it should keep its risk assessment updated in line with Article 13(3), as well as fulfil all other obligations laid down in the CRA, including by providing users with information and instructions in accordance with Article 13(18).

Example 7: A manufacturer places on the market a microcontroller that was designed and developed before the date of application of the CRA. The microcontroller is intended to be integrated into a range of electronic products, including products with connectivity functionalities.
Before placing new units of the microcontroller on the market after the CRA applies, the manufacturer carries out a cybersecurity risk assessment in accordance with Article 13(2). On the basis of the intended purpose of the microcontroller and its reasonably foreseeable use, the manufacturer identifies relevant cybersecurity risks, such as unauthorised access, manipulation of software or data, and misuse of available interfaces.
The outcome of the risk assessment shows that the microcontroller, as originally designed, already incorporates appropriate and effective security measures addressing the identified risks. The manufacturer therefore concludes that the product meets the relevant essential cybersecurity requirements set out in Part I of Annex I and that no redesign or introduction of additional security functionalities is necessary.

Where it is not possible to demonstrate how a cybersecurity risk assessment was taken into account during the original design and development phase, the manufacturer documents a current cybersecurity risk assessment and explains how the existing design and measures mitigate the identified risks. The manufacturer is not required to recreate historical design or test documentation, as this would not contribute to enhancing the cybersecurity of the product. Where several variants of the microcontroller are based on the same design and share the same risk profile, the manufacturer may also rely on representative evidence covering the relevant product family.

The manufacturer also ensures compliance with the vulnerability handling requirements laid down in Part II of Annex I, including by maintaining processes to address and remediate vulnerabilities and by keeping the cybersecurity risk assessment under review in accordance with Article 13(3).

In these circumstances, the microcontroller designed before the date of application of the CRA may be placed on the market without redesign, provided that the manufacturer can demonstrate, through the cybersecurity risk assessment and the technical documentation, that it achieves an appropriate level of cybersecurity in light of its intended purpose and reasonably foreseeable use and complies with the applicable essential cybersecurity requirements.

3 Free and open-source software

37. As recalled in Section *2.1 Placing on the market*, the CRA applies to products that are made available on the EU market for the first time (i.e. 'placed on the market'), as well as to any subsequent instance that constitutes making that same product available on the market. The Blue Guide (Section 2.2) clarifies that 'commercial activity' is to be understood as providing goods, in return for payment or free of charge, in a business-related context and can only be appreciated on a case-by-case basis, taking into account the regularity of the supplies, the product's characteristics, the intentions of the supplier, etc.

38. Supply in the course of a commercial activity is characterised by a range of circumstances, amply documented in the Blue Guide and recalled in recital 15 of the CRA. These can include directly charging a price, as well as 'charging a price for technical support services where this does not serve only the recuperation of actual costs, by an intention to monetise, for instance by providing a software platform through which the manufacturer monetises other services, by requiring as a condition for use the processing of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software, or by accepting donations exceeding the costs associated with the design, development and provision of a product with digital elements' (recital 15).[9]

39. The CRA, however, recognises the specificities in the different ways of developing and publishing 'free and open-source software' (FOSS) and offers some guidance to help identify whether a FOSS is a product placed on the market (i.e. in the course of a commercial activity) within the meaning of the CRA. As explained in recital 18, 'the mere circumstances under which the product with digital elements has been developed, or how the development has been financed, should […] not be taken into account when determining the commercial or non-commercial nature of that activity'. More specifically, 'to ensure that there is a clear distinction between the development and supply phases, the provision of products with digital elements qualifying as free and open-source software that are not monetised by their manufacturers should not be considered to be a commercial activity'.

40. It is therefore useful to (i) clarify what FOSS is; (ii) when it is deemed to fall under the responsibility of a natural or legal person; and (iii) to provide examples to help stakeholders understand when the distribution of FOSS constitutes a placement on the market. Where FOSS is not placed on the market, it falls outside the scope of the CRA, unless the entity publishing it is a legal person that meets the definition of 'open-source software steward' (henceforth, 'steward') under Article 3(14). In that case, it is subject only to the obligations laid down in Article 24.

[9] It should also be recalled that, while often products are monetised (also) via the processing of personal data, protection of personal data is a fundamental right and therefore personal data cannot be considered as a commodity, as indicated in recital 24 of Directive 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, *OJ L 136, 22.5.2019, pp. 1–27,* ELI: http://data.europa.eu/eli/dir/2019/770/oj.

41. Article 3(48) defines FOSS as 'software the source code of which is openly shared and which is made available under a free and open-source licence which provides for all rights to make it freely accessible, usable, modifiable and redistributable'. While this guidance does not identify specific free and open-source licences that are compatible with the definition laid down in Article 3(48), it follows from the wording of that provision that only software that cumulatively fulfils two conditions qualifies as FOSS for the purposes of the CRA: (i) the software must be made available under a free and open-source licence granting the full set of rights referred to in Article 3(48); and (ii) its source code must be openly shared.

42. The requirement that the licence provide for the software to be 'freely accessible, usable, modifiable and redistributable' reflects the traditional understanding of FOSS, namely that users must be able to access the source code, use it without undue restriction, modify it and redistribute original or modified versions. Access to the source code is therefore a necessary precondition for the exercise of the other rights: without access to the source code, it is not practically possible to modify or meaningfully reuse the software.

43. However, Article 3(48) goes beyond referring only to the licence terms, as it expressly requires that the source code 'is openly shared'. Recital 18 substantiates this further by adding that FOSS is developed, maintained and distributed openly. The notion of 'openly shared' indicates that the source code must be made publicly available, and not merely provided on a restricted or conditional basis. Accordingly, Software distributed under a free and open-source licence but whose source code is only shared (or allowed to be shared) with paying customers or a limited group of users is not to be considered FOSS within the meaning of Article 3(48). For the purposes of the CRA, only software whose source code is publicly available and licensed under a free and open-source licence granting the full set of rights referred to in Article 3(48) should therefore be considered to qualify as FOSS.

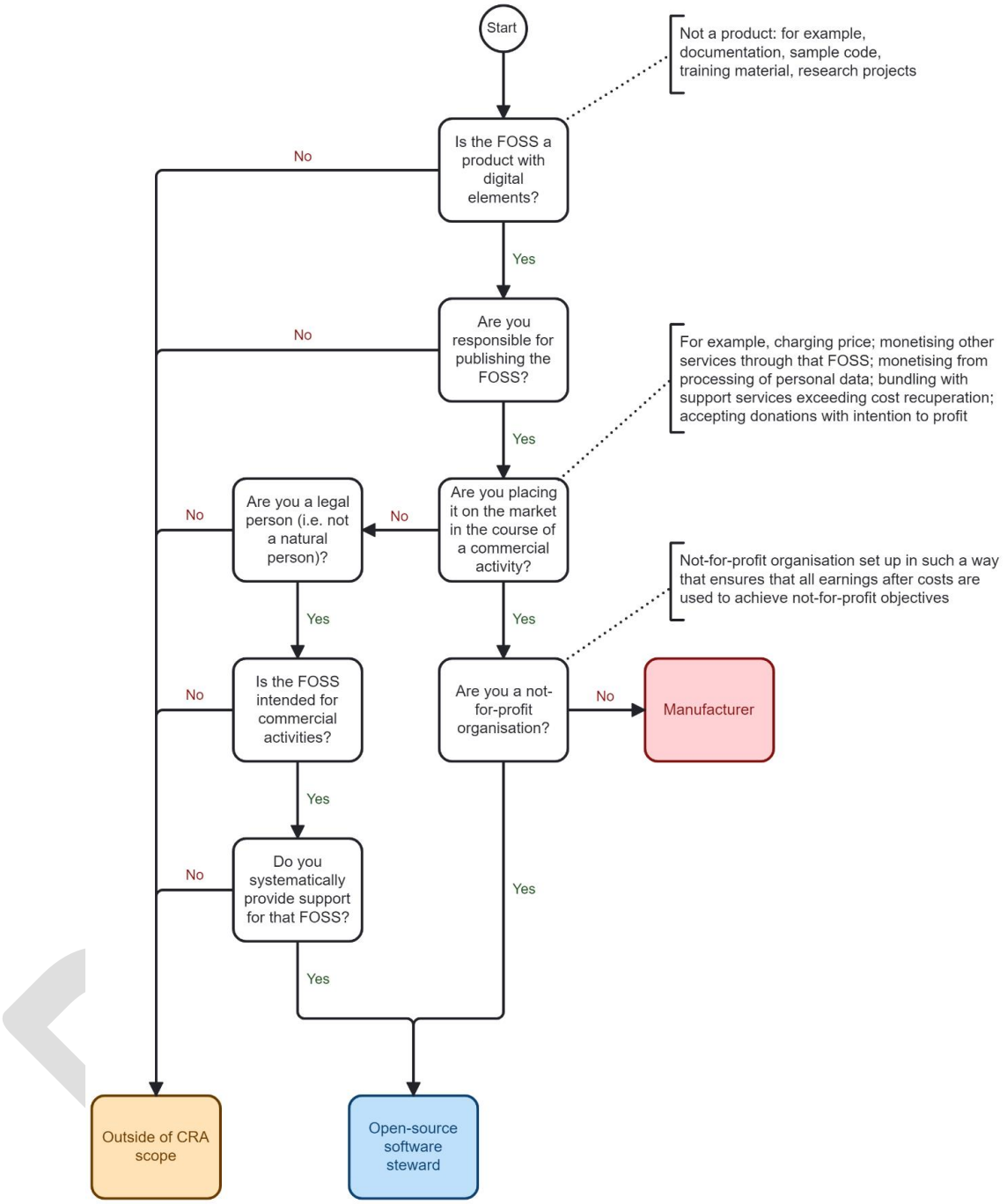

Figure 1: Stylised flowchart for CRA coverage of free and open-source software

3.1 Determining if free and open-source software is under one's responsibility

44. The CRA places key responsibilities on economic operators that supply products in the EU market. It defines the manufacturer as the natural or legal person that supplies a product under its name or trademark, and that does so in the course of a commercial activity (thereby placing it on the market). Similarly, an importer is the natural or legal person established in the EU that supplies the product of a person established outside of the EU, and that does so in the course of a commercial activity (thereby placing it on the market).

The obligations of stewards apply to the legal person that supplies a FOSS intended for commercial activities,[10] but does not place it on the market within the meaning of the CRA.

45. Therefore, to determine whether a natural or legal person is placing FOSS on the EU market, first it needs to be clarified whether that natural or legal person is actually supplying the FOSS. To correctly establish the applicable obligations under the CRA, it is essential to determine whether the the natural or legal person is indeed performing the action of supplying a FOSS. In fact, as recalled in recital 18, the CRA does not apply to natural or legal persons who contribute source code to products with digital elements qualifying as FOSS that are not under their responsibility.

46. Given the specificities of the development of FOSS, which often involves multiple contributors, decentralised collaboration models and a separation between contribution and decision-making, it is useful to clarify that FOSS is considered to be 'under the responsibility' of natural or legal persons who publish it and exercise primary control over its development, releases, and distribution decisions (often referred to as ‘maintainers’). Persons who contribute source code but do not control releases, roadmaps, or governance decisions are considered ‘contributors’; in such cases, the FOSS is not under their responsibility, even though they contributed code to it. The mere existence of technical permissions, such as commit access, is not sufficient to establish responsibility; responsibility lies with those who publish and control the FOSS.

3.2 Determining if free and open-source software is placed on the EU market

47. Once it is established that that a FOSS is under the responsibility of a natural or legal person, it needs to be established whether that person supplies it in the course of a commercial activity, thereby constituting a placement on the market.

3.2.1 Charging a price

48. Where the natural or legal person that supplies a FOSS charges a price for its use, either for the full product or certain of its features, that person is placing a product on the market. The person that places a FOSS on the market is therefore a manufacturer under the CRA.

49. Often, manufacturers of FOSS supply versions for free of that software (often called ‘community’ versions), whose codebase is (almost) identical to the paid version. Those products, however, are different products: the paid version is monetised in some way (e.g. either by charging a price or via other means as discussed in this section) and therefore considered to be placed on the market, triggering the manufacturers’ obligations. The version provided for free (or community version) is not monetised and therefore is not considered to be placed on the market.

[10] This is a necessary but not sufficient condition for a legal person to qualify as an open-source software steward, as the definition set out in Article 3(14) lays down additional conditions for a legal person to qualify as steward.

50. If the person supplying the community version is a legal person, that legal person is also subject to the obligations on stewards for the version it supplies for free (the community version). If the entity is a natural person, the version provided for free (the community version) is not within the scope of the CRA.

3.2.2 Monetisation of other services or requiring the processing of personal data

51. A natural or legal person publishing a FOSS may also be placing it on the market (i.e. supplying it in the course of a commercial activity) where it provides the software through which it monetises other products or services, or where it requires as a condition for use the processing of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software.

Example 8: A natural or legal person publishes a free and open-source marketplace application. The application is available free of charge, but it enables users to purchase goods or services through it. The app allows that person to monetise other products and services offered through it, therefore the application is considered placed on the market in the course of a commercial activity.

Example 9: A natural or legal person publishes a free and open-source VPN. The application is available free of charge, but it enables users to pay to access additional servers or dedicated IP addresses. That application allows that person to monetise other services offered through it, therefore it is considered placed on the market in the course of a commercial activity.

Example 10: A natural or legal person publishes a free and open-source fitness tracking application. The application is available free of charge, but its use is conditional upon the processing of users' personal data for purposes such as targeted advertising or analytics unrelated to the security, compatibility or interoperability of the software. By requiring such data processing as a condition for use, the application is therefore considered placed on the market in the course of a commercial activity.

3.2.3 Support services

52. The mere fact that a natural or legal person publishing a FOSS also offers support services related to it does not, as such, mean that the product is supplied in the course of a commercial activity.

53. The decisive factor is whether access to the FOSS itself (i.e. the provision of the product), including its maintenance and support, is conditioned on remuneration, rather than the mere offering of support services around a freely available product, as indicated in recital 18 of the CRA ('the provision of products with digital elements qualifying as free and open-source software that are not monetised by their manufacturers should not be considered to be a commercial activity'). Where the FOSS can be downloaded and installed freely, and users can optionally choose to purchase support or other services separately, that FOSS is not considered to be placed on the market.

54. By contrast, in somes cases access to a specific version of the product including certain benefits such as technical assistance or performance optimisation, is conditioned on

remuneration. In such cases, that provision constitutes a monetised provision of a product supplied in the course of a commercial activity and is therefore considered placed on the market. This includes cases where a paid edition or enterprise version is made available under a commercial agreement, irrespective of whether functionally equivalent software is also available free of charge under a free and open-source licence.

Example 11: A natural or legal person publishes a free and open-source operating system, offering a paid version of that operating system which includes support services, such as technical assistance or performance optimisation. The operating system is considered placed on the market in the course of a commercial activity.

Example 12: A natural or legal person publishes a free and open-source command line tool. The tool is freely accessible and anyone can download and install it. That natural or legal person separately offers optional consultancy services to train users and support them in installing and using the tool. That FOSS is not considered placed on the market within the meaning of the CRA.

55. Particularly in the case of natural persons publishing FOSS, offering support services directly bundled with access to the product would still not qualify as a commercial activity if, as indicated by recital 15 of the CRA, the price charged serves only the recuperation of actual costs. Such actual costs include a variety of costs related to that software's design, development and maintenance, including the person's reasonable living expenses. Therefore, a natural person publishing a FOSS and offering technical support services to cover their costs and obtain fair remuneration is not to be considered, on that basis alone, as placing that software on the EU market.

56. A natural or legal person offering technical support services related to a FOSS not under its responsibility is not deemed to be placing that software on the market, unless that person substantially modifies the FOSS, in accordance with Article 22, as part of their delivery of such support services.

Example 13: A service provider does not publish a FOSS, but helps a customer install it on the customer's on-premises server. It does so without performing a substantial modification of that FOSS. The service provider is therefore not deemed to beplacing the FOSS on the market.

3.2.4 Donations

57. Natural or legal persons publishing FOSS projects routinely include ways for users of that software to voluntarily donate money to thank the project's publisher(s) and also to ensure that the project remains actively maintained.

58. As indicated in recital 15 of the CRA 'accepting donations without the intention of making a profit should not be considered to be a commercial activity'. The mere fact of including a link to a donation platform or similar tools to collect donations should not be viewed as an intention to make a profit, even where the amount collected via donations exceeds the mere costs associated with the design, development and provision of a product This includes reasonable compensation for the contributors hired by a legal person, and/or a natural person's reasonable living expenses. Donations, by their very nature, fluctuate over time, and therefore a degree of flexibility is to be exercised when assessing whether

a FOSS monetised exclusively through donations is deemed to be placed on the market. A FOSS supported only through donations is therefore unlikely to be deemed placed on the market within the meaning of the CRA.

Example 14: A natural or legal person publishes a FOSS tool in a public online repository, allowing anyone to download, use, modify and redistribute it under a free and open-source licence. The publisher invites users to make voluntary donations via a donation platform to support the project's continued development and maintenance. Access to the software, its source code and its updates is not conditional on making a donation. That FOSS is not deemed to be supplied in the course of a commercial activity and is not deemed placed on the market within the meaning of the CRA.

59. Nonetheless, there are instances where a FOSS supported through donations may be deemed to be placed on the market. This is the case where, based on an overall assessment of the circumstances, the donations are de facto equivalent to charging a price to access the product or certain of its functionalities. This may be the case, in particular, where: (i) access to the FOSS, to essential functionalities, or to updates is conditioned in practice on making a donation; (ii) donations are associated with contractual benefits or exclusive advantages that go beyond community perks; or (iii) the organisation of donations demonstrates an intention to systematically generate profit rather than ensure the software's sustainability and fair remuneration for its contributors.

Example 15: A natural or legal person publishes a software product under a free and open-source licence, but provides downloadable releases and security updates only to users who make a donation. Users who do not make a donation do not have access to the software's current version.
In this case, the donations are de facto a condition for access to the product and therefore amount to charging a price. That FOSS is therefore deemed to be placed on the market within the meaning of the CRA.

Example 16: A natural or legal person makes the source code of a FOSS publicly available, but provides pre-compiled binaries, regular updates and guaranteed security fixes only to donors. In this case, the donations are linked to access to essential aspects of the product and constitute remuneration for the product's supply. That FOSS is therefore deemed to be placed on the market in the course of a commercial activity.

3.2.5 Financing of free and open-source software

60. The mere fact that a third party has paid for, sponsored or otherwise financed the development of a FOSS does not in itself determine whether that FOSS is placed on the market. It is common practice in the FOSS ecosystem for individual developers, foundations or communities to receive funding from companies, public bodies or other sponsors in order to work on specific features, fix bugs or maintain critical components. This funding may take many forms, including grants, bug bounties, sponsorships, service contracts or paid development work.

61. As indicated by recital 18 of the CRA, however, 'the mere circumstances under which the product with digital elements has been developed, or how the development has been financed, should […] not be taken into account when determining the commercial or non-commercial nature of that activity'.

62. Therefore, where the FOSS is openly shared and made freely available for all to access, use, modify and redistribute, the fact that a commercial entity may have paid for that project should not contribute to determining whether the software is placed on the market. In fact, if that FOSS is not otherwise monetised, it is not to be considered as placed on the market. Where the company that funded the FOSS's development (as well as any other company) integrates it into its product, it is to exercise due diligence in accordance with Article 13(5) of the CRA.

Example 17: An individual developer publishes a FOSS project and actively maintains it. Manufacturer A requests that the individual developer add a specific feature for that FOSS, and funds that development. The developer adds the feature to the FOSS code base, openly sharing it and making it freely available for all to access, use, modify and redistribute. The individual developer is not deemed to have placed that FOSS on the market. If the manufacturer integrates the FOSS into its product, it needs to exercise due diligence in accordance with Article 13(5).

3.2.6 Not-for-profit entities

63. Where a legal person publishing a FOSS is a not-for-profit organisation 'set up in such a way that ensures that all earnings after costs are used to achieve not-for-profit objectives' (recital 18 of the CRA), the FOSS it publishes is not considered to be placed on the market. Where that legal person meets the definition of 'steward', it is subject to the corresponding obligations (Article 24 of the CRA).

Example 18: A legal person publishes a free and open-source browser that is directly monetised via search engine partnerships, but all its earnings after costs are used for not-for-profit objectives. The browser is not deemed to be placed on the market within the meaning of the CRA.

3.2.7 Integration by other manufacturers

64. In some cases, a FOSS is published by a clearly identifiable natural or legal person, but that FOSS is 'intended for integration by other manufacturers into their own products with digital elements'. In such cases, that FOSS is not considered to be placed on the EU market, unless it is also monetised by the person that publishes it (i.e. the original manufacturer), in line with previous sections of this guidance.

65. Where that FOSS is not placed on the market, the legal person publishing it would be subject to the obligations of stewards, if it provides support on a sustained basis, in line with the definition of 'steward'.

Example 19: A legal person publishes a free and open-source JavaScript library for building user interfaces. It does not monetise the supply of that library, but integrates it into another of its products (which is in turn monetised). The JavaScript library is not considered placed on the market within the meaning of the CRA, but the legal person that publishes it is its steward.

Example 20: A legal person places an operating system on the market, and also publishes FOSS libraries to serve as reference implementations for users of that operating system. The legal person does not monetise the FOSS libraries. The legal person that publishes them is a steward to those FOSS libraries.

3.3 Open-source software stewards

66. The CRA introduces the novel legal category of 'open-source software steward' in light of 'the importance for cybersecurity of many products with digital elements qualifying as free and open-source software that are published, but not made available on the market within the meaning of the [CRA]' (recital 19 of the CRA).

67. In some cases, a FOSS is published but not made available on the market within the meaning of the CRA by a legal person who 'has the purpose or objective of systematically providing support on a sustained basis for the development of [FOSS] […] intended for commercial activities, and that ensures the viability of those products' (Article 3(14) of the CRA). In such cases, that legal person is subject to the obligations of stewards.

68. A steward is defined as 'a legal person, other than a manufacturer' because a manufacturer, by definition, is the natural or legal person who places products with digital elements on the market ('markets them') under its own name or trademark. A legal person can be a steward only to products qualifying as FOSS that are published, but not made available on the market within the meaning of the CRA. The concept of steward, therefore, applies to specific instances of FOSS that 'are ultimately intended for commercial activities, such as for integration into commercial services or into monetised products with digital elements' (recital 19 of the CRA[11]) but not made available on the market within the meaning of the CRA, and for which the legal person publishing that FOSS ensures systematic support.

69. Being a steward for one specific FOSS does not mean that that legal person is necessarily also a steward for other FOSS that it publishes. Similarly, being a manufacturer for one specific FOSS does not mean that the legal person may not be a steward for other FOSS, This includes providing 'community' versions of the same FOSS, as described in Section *3.2.1 Charging a price*.

70. A legal person may therefore simultaneously be a steward for one specific FOSS (where the steward systematically provides support on a sustained basis and ensures the software's viability) and a manufacturer for another specific FOSS (where it places it on the market). In other words, the same legal entity can be required to fulfil different roles for different FOSS projects.

71. For each specific FOSS that it publishes, the legal person will need to ascertain whether that FOSS is considered to be placed on the market within the meaning of the CRA. If so,that makes the legal entity the software's manufacturer. If the FOSS is not deemed placed on the market, the legal person may be the steward to it, if the software is intended for commercial activities and if the legal person is sustaining it in line with the definition of steward.[12]

[11] This notion is also contained in the formulation 'intended for commercial activities' included in the definition of 'open-source software steward' set out in Article 3(14) of the CRA.

[12] The legal person may also not be subject to any obligations under the CRA, in cases where: (i) a specific FOSS is not placed on the market within the meaning of the CRA; and (ii) the legal entity does not meet the definition of steward in relation to that specific FOSS.

3.3.1 Sustained support and ensuring viability of FOSS

72. Recital 19 explains that the provision of sustained support to the development of a product includes (but is not limited to): (i) the hosting and managing of software development collaboration platforms; (ii) hosting source code or software; (iii) governing or managing products qualifying as free and open-source software; and (iv) steering the development of such products.

73. This may be the case, for example, for a legal entity that develops FOSS for integration into its own products and then publishes it without placing it on the market. This is also discussed in Section *3.2.7 Integration by other manufacturers*. In this case, the legal entity is not a manufacturer of the software, but may be a steward to it. Additionally, as also explained in previous sections, a legal entity that publishes a free (or community) version and a monetised version of the same FOSS, is deemed a steward to the free (or community) version (and a manufacturer to the monetised version).

74. Similarly, a legal entity that monetises a FOSS but is a not-for-profit entity whose earnings after costs are used to achieve not-for-profit objectives (and therefore its FOSS is not made available on the market within the meaning of the CRA, as discussed in Section *3.2.6 Not-for-profit entities*) is a steward to the FOSS it publishes.

75. Furthermore, certain foundations offer collaboration platforms with various forms of governance that enable manufacturers to contribute regularly to the development of FOSS and/or that are regularly financed by manufacturers. Such foundations are to be considered stewards in relation to specific FOSS which are intended for commercial activities and for which the foundation offers sustained support. However, as explained in Section *3.3 Open-source software stewards*, such a foundation may not be subject to any obligations under the CRA for other specific FOSS that it hosts, in cases where it does not provide systematic support for a specific FOSS, it does not ensure its viability, and/or that specific software is not intended for commercial activities.

76. The type of 'sustained support' that foundations and similar organisations provide to specific FOSS projects can vary greatly. For example, certain legal entities only provide non-technical support, such as managing the branding of projects, laying down governance rules, organising community events or collecting donations. Other entities also provide the underlying IT infrastructure necessary to run the project, such as hosting source code repositories, providing version control systems, or generating signing keys. Others go further in the type of support they provide by actively contributing engineering resources to the project, for example by employing developers, coordinating development work, reviewing or merging code, managing releases, or handling vulnerability reports and security patches. While all legal entities that qualify as stewards under the CRA are required to comply with the obligations in Article 24(1) and (2), how far the obligations laid down in Article 14(1), (3) and (8) apply to those legal entities varies depending on the type of support they provide, in accordance with Article 24(3).

77. For example, a steward that only provides non-technical support is, by definition, not involved in the product's development, and is therefore not required to report actively exploited vulnerabilities. That steward also does not provide any network and information

systems for the development of such products, and therefore is not required to report severe incidents to ENISA and the CSIRTs or to impacted users. Nonetheless, where the steward becomes aware of an actively exploited vulnerability (e.g. via a report from external sources, such as security researchers), it should share the information with the product's maintainers, in accordance with its cybersecurity policy. The maintainers of the products and/or the stewards should also consider reporting the vulnerability on a voluntary basis, in accordance with Article 15.

78. On the other hand, where a steward provides the underlying IT infrastructure for certain products, it is required to notify ENISA and the CSIRTs, in accordance with Article 14(3) of any severe incidents that have an impact on the security of products. It is also required, where appropriate, to inform all users (e.g. via a general announcement). As indicated in the previous point, while the steward is not required to report actively exploited vulnerabilities it becomes aware of, it should foster the correct handling of vulnerabilities and should consider voluntary reporting in accordance with Article 15.

79. Finally, where an entity also provides engineering resources to specific products, it is required to: (i) notify, in accordance with Article 14(1), of actively exploited vulnerabilities that it becomes aware of; and (ii) where appropriate, to inform all users. To the extent that the steward also has a direct relationship with impacted users, it is also required to inform them directly, in accordance with Article 14(8).

3.4 Contributors and downstream uses

80. As already mentioned in Section *3.1 Determining if free and open-source software is* under one's responsibility, the CRA clarifies that it does not apply 'to natural or legal persons who contribute with source code to products with digital elements qualifying as free and open-source software that are not under their responsibility' (recital 18).

81. Manufacturers of products with digital elements that integrate FOSS components into their own products also do not become responsible for such components' individual compliance with the CRA, even where the manufacturers contribute source code to their maintenance.

82. Similarly, the mere fact that manufacturers integrate FOSS components into their own (monetised) products has no impact on the status of that FOSS component under the CRA. Whether the CRA applies to that FOSS component depends solely on whether the entity that publishes it places it on the market.

83. Nonetheless, manufacturers of products with digital elements that integrate FOSS components are required to comply with the CRA for their own products with digital elements They also have a due diligence obligation, in accordance with Article 13(5), towards the FOSS components that they integrate. In addition, they are required to report vulnerabilities in integrated components and share security fixes with the person maintaining those components, in accordance with Article 13(6). For more guidance on this topic, see Section *9.2.1 Reporting upstream and sharing security fixes*.

3.5 Illustrative scenarios

84. The examples listed below are completely hypothetical and only meant to illustrate different cases as explained in the sections above.

Example 21: Individual developer A has developed a FOSS. Developer A publishes that FOSS under its own name or trademark, but does not charge a price for its use. The software is openly shared and freely available for all to access, use, modify and redistribute. Developer A also includes a link to a platform to collect voluntary donations.
Companies B, C and D integrate that FOSS into their own products. To support ongoing maintenance, companies B, C and D make voluntary donations to developer A. These donations enable developer A to keep the project actively maintained.
That FOSS is not placed on the market. Developer A has no obligations under the CRA. Companies B, C, and D are to exercise due diligence in accordance with Article 13(5) when integrating that FOSS into their own products with digital elements.

Example 22: Not-for-profit foundation F publishes a FOSS component for integration into other commercial products. Foundation F commits to providing sustained support to that FOSS, to ensure its viability and uptake. Companies A, B and C integrate that FOSS into their own products with digital elements. Companies A and B voluntarily contribute some of their developers' time to development and maintenance of FOSS projects within foundation F, including for that FOSS.
As foundation F is a not-for-profit entity set up in such a way that its earnings after costs are used to achieve not-for-profit objectives, the FOSS is not deemed to be placed on the market. Foundation F is the FOSS steward and is subject to the corresponding obligations laid down in Article 24. Companies A, B and C are to exercise due diligence in accordance with Article 13(5) when integrating that FOSS into their own products.

Example 23: Company A has developed a FOSS component for integration into its own products with digital elements. It also publishes that FOSS separately under its own name or trademark and actively maintains it, However, it does not charge for its use or monetise in other ways. Companies B, C and D integrate that FOSS into their own products with digital elements, and voluntarily contribute some of their developers' time to its maintenance.
That FOSS is not deemed to be placed on the market. Company A is not its manufacturer, but is its steward. Companies B, C, and D are to exercise due diligence in accordance with Article 13(5) when integrating the FOSS into their own products.

Example 24: Company A publishes a FOSS under its own name or trademark and offers it as a paid version, which includes certain benefits such as technical assistance or performance optimisation. Developers from companies B, C and D contribute to the FOSS's maintenance, but it remains under the control of Company A.
Company A is deemed a manufacturer to that FOSS.[13] Companies B, C and D are not subject to obligations under the CRA for that specific FOSS. If they integrate that FOSS into their own products with digital elements, they are required to exercise due diligence in accordance with Article 13(5).

[13] Unless company A is a not-for-profit entity set up in such a way that ensures that all earnings after costs are used to achieve not-for-profit objectives, in which case it would be the steward to that FOSS.

Example 25: Company A publishes a FOSS under its own name or trademark and provides ongoing maintenance to ensure its long-term viability, to enable that software to be integrated into other companies' products with digital elements. Company A does not charge for its use, process personal data it collects through the product, or sell support services associated with publishing the FOSS.
Company B contributes code and developers' time to the FOSS's maintenance, but does not distribute it commercially. Company B offers technical support services independently from the FOSS's distribution. Company A is deemed to be the steward for that FOSS, whereas company B has no obligations under the CRA for that FOSS.

Example 26: A FOSS component is published by a not-for-profit entity set up in such a way that ensures that all earnings after costs are used to achieve not-for-profit objectives. The entity provides sustained support to ensure the project's long-term viability. Maintenance is financed through public funding, such as research grants. Additional developments, including new features, are funded through donations and specific projects, carried out in partnership with manufacturers that integrate that FOSS into their products. Such features are incorporated into the FOSS's code base.
The not-for-profit entity that publishes the FOSS is deemed the steward for that FOSS component. A manufacturer that has contributed to the development of certain features does not become the manufacturer of that FOSS component. Where the manufacturer integrates that FOSS component into its own product with digital elements, it needs to exercise due diligence in accordance with Article 13(5).

Example 27: A not-for-profit entity set up in such a way that ensures that all earnings after costs are used to achieve not-for-profit objectives publishes a FOSS software development kit (SDK) and ensures its ongoing maintenance. The SDK is openly shared and is freely available for all to access, use, modify and redistribute. Funding is provided through membership fees paid to the not-for-profit entity, and developers employed by member organisations contribute code and other resources to the SDK's development. Manufacturers use the SDK as a component to build other products.
The not-for-profit entity that publishes that SDK is the steward for it. The foundation's members are not responsible for the SDK's compliance with the CRA. Where manufacturers use the SDK to build their own product, they need to exercise due diligence in accordance with Article 13(5).

Example 28: An individual developer publishes a FOSS library on a public package repository for a given programming language and actively maintains it. In the package documentation, the developer adds a link to collect donations. A manufacturer downloads that library from the repository for free and integrates it into its own product with digital elements.
The individual developer and the package repository do not have any obligations under the CRA. The manufacturer that integrates the library needs to exercise due diligence in accordance with Article 13(5).

4 Substantial modifications and spare parts

85. Article 3(30) of the CRA defines a 'substantial modification' as a change to the product with digital elements following its placing on the market, which (i) affects the product's compliance with the essential cybersecurity requirements set out in Part I of Annex I; or (ii) results in a modification to the intended purpose for which the product has been assessed.

86. The notion of substantial modification is relevant for ascertaining CRA obligations in a number of cases, including the following:

a. in accordance with Article 21, an importer or distributor that carries out a substantial modification of a product already placed on the market is considered to be its manufacturer;

b. in accordance with Article 22, any natural or legal person that carries out a substantial modification of a product and makes it available on the market is considered to be its manufacturer;

c. in accordance with Article 69(2), any natural or legal person that carries out a substantial modification after 11 December 2027 of a product placed on the market before 11 December 2027 and places it on the market is considered to be its manufacturer;

d. for manufacturers of products placed on the market after 11 December 2027, in order to ascertain whether a product is required to undergo a new conformity assessment procedure due to changes made after that date, particularly in light of the iterative nature of software development.

87. Therefore, it is important to provide guidance to help economic operators understand when hardware or software modifications qualify as substantial modifications.

4.1 Physical repairs

88. As stated in recital 42 of the CRA, 'where a product with digital elements is subject to 'refurbishment', 'maintenance' and 'repair' as defined in Article 2, points (18), (19) and (20), of Regulation (EU) 2024/1781 of the European Parliament and of the Council, this does not necessarily lead to a substantial modification of the product, for instance if the intended purpose and functionalities are not changed and the level of risk remains unaffected. However, an upgrade of a product with digital elements by the manufacturer might lead to changes in the design and development of that product and might therefore affect its intended purpose and compliance with the requirements set out in this Regulation'. This is consistent with Section 2.1 of the Blue Guide, which recalls that 'a product subject to important changes or overhaul after it has been put into service must be considered as a new product if: i) its original performance, purpose or type is modified, without this being foreseen in the initial risk assessment; ii) the nature of the hazard has changed or the level of risk has increased in relation to the relevant Union harmonisation legislation; and iii) the product is made available (or put into service if the applicable legislation also covers putting into service within its scope). This has to be assessed on a

case-by-case basis and, in particular, in view of the objective of the legislation and the type of products covered by the legislation in question'.

89. Operations of refurbishment, maintenance or repair which result in physical modifications of products already placed on the market do not necessarily amount to substantial modifications. A case-by-case assessment should therefore be performed, to ascertain whether such physical modification affects the product's compliance with the essential requirements of Part I of Annex I, or results in a change to the product's intended purpose covered by the cybersecurity risk assessment.

90. Replacing defective parts or worn items by parts that perform better (e.g. because of technical progress or because the old part is no longer produced) does not in itself trigger a substantial modification of the repaired product. It only does so if the performance change or the way the repaired product operates (i) affects the product's compliance with the essential requirements or (ii) results in a change to the intended purpose that was not covered by the original risk assessment.

Example 29: The manufacturer of a computer server performs a repair operation, switching out a defective RAM with a new, better performing one. The server's compliance with the essential requirements is not affected. The server performs better, but its new performance remains within the server's intended use as considered in the cybersecurity risk assessment. The computer server is not considered to be substantially modified.

Example 30: The manufacturer of the computer server performs a similar operation as in example 1, but the operation leads to a significant change in the server's behaviour by altering the way core functions are executed. The manufacturer had not considered the server's new behaviour in its original risk assessment, thereby potentially affecting the product's compliance with the essential requirement. The computer server is considered to be substantially modified.

4.2 Spare parts

91. Article 2(6) of the CRA establishes that spare parts intended to replace identical components and manufactured according to the same specifications as those components are not subject to the CRA. Recital 29 further states that the exemption covers both spare parts for products made available before the CRA entered into application, and spare parts that have already undergone a conformity assessment procedure as laid down in the Regulation.

92. Accordingly, where a spare part is identical to a component already included in a product either placed on the market before the CRA's date of application or that has been placed on the market in compliance with the CRA, that spare part is not itself subject to the CRA.

93. By contrast, where a spare part is not identical to the original component, that spare part constitutes a product in its own right and is therefore subject to the CRA. In such cases, compliance with the essential cybersecurity requirements must be assessed in light of the spare part's intended purpose. Of particular relevance is the spare part's function of ensuring compatibility or interoperability with an existing product, including where that product is a product placed on the market before the CRA entered into application. Where certain essential requirements cannot reasonably be met due to that intended

purpose or technical constraints, the manufacturer must reflect this in the cybersecurity risk assessment and implement appropriate alternative or compensatory risk-mitigation measures, in order not to undermine the product's security. As also discussed in Section *2.5 Complex systems*, both the technical documentation and the information and instructions to the user play a key role in transparently describing the identified constraints, the associated cybersecurity risks and the risk mitigation measures implemented.

94. As explained in Section *4.1 Physical repairs*, replacing defective parts or worn items by parts that perform better does not in itself trigger a substantial modification of the repaired product.

Example 31: A manufacturer placed a connected industrial controller on the EU market in 2026, before the date of application of the CRA. In 2028, a digital communication module in that controller fails. The manufacturer supplies a replacement module that is identical and manufactured according to the same specifications as the original.
In this case, the replacement module falls within the scope of the exemption in Article 2(6). The spare part is not itself subject to the CRA, even though it is a product with digital elements, because it replaces an identical component in a product placed on the market before the CRA applied. The repair does not constitute a substantial modification of the product.

Example 32: A manufacturer placed a connected industrial controller on the EU market in 2026, before the date of application of the CRA. In 2028, a communication chip in that controller fails. As the manufacturer no longer manufactures that chip, it supplies a newer chip with equivalent functionality, but with a different design or firmware, in order to maintain compatibility and continued operation.
In this case, the replacement chip does not benefit from the exemption in Article 2(6) because it is not identical and not manufactured according to the same specifications. It therefore constitutes a product subject to the CRA. Compliance of the replacement part must be assessed in light of its intended purpose, including its role in ensuring interoperability with the product placed on the before the CRA entered into application. However, the repair of the controller does not in itself amount to a substantial modification, provided that the intended purpose and cybersecurity risk profile of the controller remain unchanged.

Example 33: A manufacturer places on the market a smart building controller in 2028 in compliance with the CRA. In 2029, a defective digital interface board is replaced with a board that is identical and manufactured according to the same specifications.
In this case, the replacement board falls within the scope of the exemption in Article 2(6). The spare part is not itself subject to the CRA, even though it is a product with digital elements, because it replaces an identical component in a product already placed on the market. The repair does not constitute a substantial modification of that product.

Example 34: A manufacturer places on the market a smart building controller in 2028 in compliance with the CRA. In 2029, the wireless module in that controller fails. As the manufacturer no longer manufactures that module, it supplies a new module that performs the same function using the same communication protocols and security mechanisms, but based on a different chipset or updated firmware in order to maintain availability.

In this case, the replacement module does not benefit from the exemption in Article 2(6) because it is not identical and not manufactured according to the same specifications. It therefore constitutes a product with digital elements subject to the CRA. Compliance of the replacement part must be assessed in light of its intended purpose, including its role in ensuring interoperability with the existing product. However, the repair of the controller does not in itself amount to a substantial modification, provided that the intended purpose and cybersecurity risk profile of the controller remain unchanged.

4.3 Software updates as substantial modifications

95. Software development is iterative in nature, with software products already placed on the market being frequently and continuously updated. In this context, it is useful to provide more guidance to ascertain when software is to be considered substantially modified. Such guidance is intended in particular to help manufacturers of software products who make changes to their own products determine whether those changes amount to a substantial modification.

96. As stated above, Article 3(30) of the CRA establishes that a change qualifies as a substantial modification where it:

    a. affects the product's compliance with the essential cybersecurity requirements; or

    b. results in a modification to the intended purpose for which the product was originally assessed.

97. Recital 39 further indicates that a product is substantially modified where a change alters the level of cybersecurity risk, and where such altered or additional risk has not been considered by the manufacturer in its risk assessment and, consequently, in its implementation of the essential requirements. A manufacturer should therefore assess, on a case-by-case basis, whether a software update introduces new or increased cybersecurity risks, and whether such risks were already addressed in its original risk assessment.

98. Where a product introduces new functionalities that result in a change to the product's intended purpose as a whole, it is likely that the manufacturer did not consider such changes in its original risk assessment. In such circumstances, the change would generally qualify as a substantial modification.

    Example 35: A manufacturer places on the market a dashboard that collects data from machines and displays trends and alerts, without having the ability to control such machines. The manufacturer subsequently develops a new version of that dashboard, introducing functionalities that enable it to control the machines, including by adjusting operating parameters and restarting machines following fault conditions. As a result of these changes, the dashboard's intended purpose has evolved beyond what was envisaged in the original risk assessment, shifting from a situational awareness tool to a product intended to exercise operational control over other devices. The dashboard has therefore been substantially modified.

    Example 36: A manufacturer places on the market a consumer software application intended to organise and display personal data, such as emails, messages, or documents, and to support basic search and filtering functions. The manufacturer subsequently

introduces an update that enables the application to automatically analyse user content in order to generate behavioural profiles and make automated decisions affecting the prioritisation, suppression, or recommendation of content without user intervention. As a result of this change, the software's intended purpose shifts from a user-controlled information management tool to an automated decision-making system, which was not envisaged in the original risk assessment. The application has therefore been substantially modified.

99. At the same time, however, it is possible that a manufacturer progressively introduces new functionalities already included in its original risk assessment. The manufacturer has anticipated the development of those functionalities, has already described and assessed the associated risks, and has implemented appropriate mitigation measures to ensure continued compliance with the essential requirements. Updates of this nature should therefore not be regarded as substantial modifications.

Example 37: A messaging application is initially released with functionality limited to one-to-one messaging. The manufacturer's original risk assessment covers the later introduction of group messaging, including for example the increased complexity of message routing. In a subsequent update, the manufacturer adds a group chat functionality together with administrator controls and moderation tools that were already foreseen and assessed in the original design. The update implements functionalities that fall within the scope of the original intended purpose and risk assessment. The messaging application has therefore not been substantially modified.

Example 38: A production monitoring system is placed on the market with read-only dashboards enabled, while automated control features are present in the system architecture but remain disabled. The manufacturer's original risk assessment explicitly covers the future activation of automated control loops, including the cybersecurity risks associated with closed-loop control, as well as safeguards such as operator override mechanisms and fail-safe states. In a later update, the manufacturer enables the automated control features and activates the safeguards as originally assessed. The production monitoring system has therefore not been substantially modified.

100. Conversely, even limited or seemingly minor new functionalities may introduce significant cybersecurity risks, if such risks were not included in the original risk assessment and may impact compliance with the essential requirements. The assessment of substantial modification should therefore not be based on the scale or complexity of the change, but on its potential effect on the product's cybersecurity risk profile.

Example 39: A manufacturer introduces an update to a software application adding a 'remember me' or persistent login feature that stores authentication tokens locally to improve user convenience. Although the functionality is limited in scope, it introduces new risks related to token theft, unauthorised access, and session hijacking that were not considered in the original risk assessment. The update therefore affects compliance with the essential requirements. The software application has been substantially modified.

Example 40: A manufacturer adds a new logging and diagnostics feature to an existing software product, enabling detailed system logs to be exported for troubleshooting purposes. While the functionality appears minor, it results in the collection and storage of sensitive operational data in an unencrypted format, introducing risks of data exposure

that were not previously assessed or mitigated. The change may therefore have a significant impact on the product's cybersecurity risk profile. The software product has been substantially modified.

101. In line with recital 39 of the CRA, security updates are generally not to be regarded as substantial modifications, as their primary purpose is to reduce the level of cybersecurity risk associated with the product. A security update that does not modify the product's intended purpose and does not introduce new cybersecurity risks should therefore not be considered a substantial modification. This includes where certain functionalities are modified or constrained solely for the purpose of mitigating identified vulnerabilities and ensuring continued compliance with the essential requirements.

Example 41: A manufacturer deploys a security update to address a vulnerability in the product's code base by correcting an input validation error that could lead to a buffer overflow, or by fixing a logic flaw allowing authentication bypass through improper session token validation. The update modifies the internal implementation of the software without affecting the product's intended purpose or introducing new exposure. Such an update is intended exclusively to reduce the cybersecurity risk. The security update should not be considered a substantial modification.

Example 42: A manufacturer introduces a security update that strengthens existing security configurations, such as tightening firewall rules, disabling unused network ports, changing default administrator password policies, or making multi-factor authentication mandatory where such functionality was already available or foreseen. Although the update may affect how users configure or access the product, it does not alter the product's intended purpose and serves solely to enhance its security posture. The security update should not be considered a substantial modification.

Example 43: A manufacturer places on the market a software product that secures communications using a configurable encryption framework supporting multiple cryptographic algorithms and key sizes, as described in the product's technical documentation and original risk assessment. The risk assessment covers all the cryptographic options provided in the product and anticipates the future deprecation of certain algorithms. The risk assessment also includes mitigation measures, such as cryptographic agility, internal key management, and compatibility testing. In response to emerging cryptographic guidance, the manufacturer deploys a security update that disables a deprecated algorithm and activates a stronger, already supported alternative, without introducing new external dependencies or altering data flows. As the update implements a security measure that was foreseen and assessed as part of the original design, and it does not alter the product's intended purpose or trust model, the security update should not be considered a substantial modification.

102. By contrast, a security update may qualify as a substantial modification where, notwithstanding its security objective, the update results in the product's intended purpose being modified beyond what was originally foreseen or introduces cybersecurity risks not foreseen in the original risk assessment.

Example 44: A manufacturer places on the market a software product intended to provide local file encryption for data stored on a user's device, enabling users to encrypt and decrypt files on demand. Following the discovery of a vulnerability in the encryption

workflow, the manufacturer deploys a security update that removes local encryption functionality and instead requires all files to be uploaded to, stored in, and processed by a remote encryption service operated by the manufacturer. As a result of this change, the product no longer performs local encryption as originally intended, instead functioning as a remote encryption and data processing service. Although the update is introduced for security reasons, it fundamentally alters the product's intended purpose in a manner not foreseen in the original risk assessment and therefore qualifies as a substantial modification.

Example 45: A manufacturer places on the market a software product that relies on an established encryption protocol and an internally managed key lifecycle to secure communications between components of the product. In response to newly identified cryptographic weaknesses, the manufacturer introduces a security update that replaces the existing encryption mechanism with a different protocol requiring the use of an external key management service operated by a third party. As a result of this change, the product's trust model, dependency structure, and data flows are materially altered, introducing new external interfaces and reliance on third-party services not considered in the original risk assessment. Although the update is security-driven, it introduces new cybersecurity risks, and therefore qualifies as a substantial modification.

103. As stated in point 97 above, whether a software update constitutes a substantial modification should be assessed on a case-by-case basis. When performing this assessment, manufacturers may consider, in a non-exhaustive manner, whether the software update:

a. introduces new threat vectors, such as additional interfaces, communication channels, execution environments, or external dependencies through which threats could materialise;

b. enables new attack scenarios, including for example new ways in which unauthorised access, manipulation, interference or misuse of the product, or of data processed by it, could plausibly occur;

c. changes the likelihood of previously identified attack scenarios, for example by lowering the effort or expertise required to exploit them, increasing exposure to untrusted actors, or weakening existing safeguards;

d. changes the potential impact of previously identified attack scenarios, including for example the scope of affected data or functions, the severity of operational, safety or economic consequences, or the ability to detect, contain or recover from an incident.

104. In some cases, a software update does not introduce new threat vectors, does not enable new attack scenarios, and does not materially alter the likelihood or impact of previously identified attack scenarios. This may indicate that the update does not introduce new or increased cybersecurity risks, provided that the assumptions and mitigation measures relied upon in the original risk assessment remain valid and effective. It is therefore likely that the update does not qualify as a substantial modification.

105. Conversely, a software update may introduce new threat vectors, enable new attack scenarios, or materially alter the likelihood or impact of existing attack scenarios. In such cases, the manufacturer should reassess the product's cybersecurity risks and determine

whether the essential requirements continue to be met, including whether the update introduces new or increased risks not foreseen in the original risk assessment.

106. Whether a software update qualifies as a substantial modification is relevant when determining whether certain obligations under the CRA apply, as set out in point 86. However, irrespective of that qualification, manufacturers remain responsible for ensuring the security of software updates and of their product with digital elements during its support period, in accordance with the vulnerability handling requirements set out in Annex I, Part II of the CRA. Furthermore, regardless of whether software updates qualify as substantial modifications or not, manufacturers are required to keep the risk assessment and the technical documentation accurate, complete and continuously up to date, in accordance with Articles 13(7) and 31(2).

4.4 Consequences of a substantial modification

107. Where a product modification qualifies as a substantial modification, the modified product is to be treated as a new product for the purposes of the CRA. As a result, the act of making the substantially modified product available on the market constitutes a new placing on the market.

108. In such cases, the natural or legal person who carries out the substantial modification, or has the modification carried out, is to be regarded as the modified product's manufacturer, irrespective of whether that person was involved in the original design or placing on the market of the product. Where the substantial modification is carried out by the original manufacturer, including in the context of iterative development of software products, that manufacturer remains the manufacturer for the purposes of the CRA. However, the substantially modified product is to be considered as newly placed on the market.

109. In accordance with Section 2.1 of the Blue Guide, '*the technical documentation has to be updated in as much as the modification has an impact on the requirements of the applicable legislation. It is not necessary to repeat tests and produce new documentation in relation to aspects not impacted by the modification. It is up to the natural or legal person who carries out changes or has changes carried out to the product to demonstrate that not all elements of the technical documentation need to be updated. The natural or legal person who carries out changes or has changes carried out to the product shall be responsible for the conformity of the modified product and draw a declaration of conformity, even if they use existing tests and technical documentation*'.

110. Therefore, the natural or legal person placing the substantially modified product on the market may re-use existing documentation and tests for aspects of the product that are not impacted by the substantial modification. Particularly where the manufacturer places substantially modified versions of the same product on the market, the conformity assessment procedure should focus on the substantially modified parts of the product with digital elements. Similarly, where a third-party conformity assessment is performed, the conformity assessment body should focus its assessment on the substantially modified parts. For unchanged parts of the product, it may re-use existing documentation and test results.

111. In accordance with Article 69(2) of the CRA, products that were placed on the market before 11 December 2027 are subject to the Regulation only if, from that date, they undergo a substantial modification.

112. For products that were placed on the market before 11 December 2027, manufacturers who did not apply the CRA at the time of initial placement on the market must be able to demonstrate upon request of a market surveillance authority that subsequent updates do not constitute a substantial modification. Carrying out a cybersecurity risk assessment that covers the elements of Article 13(2), including documented demonstration of compliance with the essential cybersecurity requirements should make it easier to establish that a software update does not affect the intended purpose, the cybersecurity risk profile or the compliance of the product, and therefore does not amount to a substantial modification within the meaning of Article 69(2).

113. Where the update constitutes a substantial modification, the manufacturer is required to comply with the CRA in its entirety before placing the substantially modified product on the market, as well as for the duration of the product's support period.

5 Support period

114. Article 13(8) of the CRA requires manufacturers to determine the support period during which the vulnerabilities of the product, including its components, are handled effectively and in accordance with the essential cybersecurity requirements set out in Part II of Annex I. Article 13(8) also sets out criteria that the manufacturer is required to take into account when determining the support period, as well as additional criteria that it may take into account. Overall, such criteria are to be taken into account in a manner that ensures proportionality in determining the support period.

115. Article 13(8) further requires that the support period be at least five years, unless the product is expected to be in use for less than five years, in which case the support period shall correspond to the expected use time. The minimum support period therefore operates only as a safeguard, ensuring that vulnerabilities are handled for a sufficiently long period, while allowing manufacturers to take into account products with genuinely shorter expected use times. Recital 60 provides more guidance in this respect, clarifying that products reasonably expected to be in use for longer than five years should accordingly have longer support periods. A support period of five years is therefore not to be considered as the default for all products. Instead, the manufacturer should determine the appropriate support period in light of the criteria referred to in Article 13(8).

116. Article 13(19) requires manufacturers to indicate at the time of purchase, in a clear and understandable manner, the end date of the support period (at least the month and year). It also requires manufacturers to display a notification to users once the support period expires, where this is technically feasible in light of the nature of the product. This obligation is intended to provide transparency to users as regards the duration for which security support can be expected.

117. In the case of software products, which are often developed and released iteratively and where substantially modified versions may be placed on the market frequently over time, the support period must be understood in light of this development model. Each version of a software product placed on the market has to have a declared support period that complies with Article 13(8). This includes the minimum support period of at least five years, unless the expected use time of that version is demonstrably shorter, as also clarified in recital 60.

118. Article 13(10) provides flexibility for software products by allowing manufacturers, under certain conditions, to ensure compliance with the vulnerability handling requirement set out in Part II, point (2), of Annex I (addressing and remediating vulnerabilities) only for the version of the software product last placed on the market. This is permitted where users of previously placed versions have access to the version last placed on the market free of charge and do not incur additional costs to adjust the hardware and software environment in which they use that product's original version.

119. For the purposes of Article 13(10), the concept of 'additional costs' should be interpreted in a practical and proportionate manner, taking into account normal and expected practices in software maintenance and operation. It does not encompass reasonable

operational effort that is inherent to applying software updates or maintaining a secure operating environment, such as personnel time, routine testing, configuration adjustments or upgrades of underlying software dependencies that are necessary to address end-of-life components or known security vulnerabilities. By contrast, 'additional costs' refers burdens that go beyond what can normally be expected in the context of software updates, such as mandatory purchases of new hardware, infrastructure replacement or fundamental changes to the operating environment.

120. For continuously evolving software products, manufacturers may place successive substantially modified versions on the market over relatively short intervals and expect users to upgrade regularly. In such cases the declared support period for each substantially modified version must comply with Article 13(8) at the time it is placed on the market. In other words, the manufacturer must declare a new support period for that substantially modified version. However, manufacturers may rely on Article 13(10) to discontinue addressing and remediating vulnerabilities for earlier versions once users are able to upgrade to a later version free of charge and without incurring additional costs as referred to above, even if this results in a shorter effective support period for those earlier versions.[14] The manufacturer remains subject to the other vulnerability-handling requirements. As also explained in recital 40, these include, for all subsequent substantially modified versions of the software product placed on the market: (i) maintaining a policy on coordinated vulnerability disclosure; and (ii) measures to facilitate the sharing of information about potential vulnerabilities.

Example 46: A manufacturer places a smartphone model on the EU market and declares a support period of eight years from the date of placement on the market, during which it will provide security updates addressing vulnerabilities in the operating system and key software components. During that period, the manufacturer releases regular software updates and substantially modified versions of the operating system, which users can install free of charge without requiring new hardware.
The manufacturer may, in accordance with Article 13(10), address and remediate vulnerabilities for the latest version of the operating system made available for that smartphone model, provided that earlier versions can be upgraded free of charge and without additional costs. For the duration of the support period, the manufacturer remains subject to the other vulnerability handling requirements, such as coordinated vulnerability disclosure and information-sharing measures.

Example 47: A manufacturer places an enterprise software product on the market and releases substantially modified versions every few months, reflecting security improvements, new features and compatibility with updated operating systems and platforms. Each version is placed on the market with a declared support period in accordance with Article 13(8). The manufacturer expects users to upgrade regularly as part of normal operation and provides access to the latest version free of charge. Applying

[14] It should be recalled that Article 13(9) requires manufacturers, where technically feasible in light of the nature of the product, to display a notification to users informing them that their product has reached the end of its support period. Therefore, where addressing and remediating vulnerabilities for earlier versions is discontinued, it is expected that users who have not upgraded to the newest version are informed.

updates may require reasonable operational effort, such as testing or configuration adjustments, but does not require additional costs, such as the purchase of new hardware or fundamental infrastructure changes. In this context, the manufacturer may rely on Article 13(10) to discontinue addressing and remediating vulnerabilities for earlier versions once users can upgrade to the latest version, while continuing to comply with the other vulnerability-handling requirements for all subsequent substantially modified versions.

6 Important and critical products

121. Article 7(1) of the CRA establishes that products that have the core functionality of a product category set out in Annex III to the Regulation are considered to be 'important products'. Annex III further divides important products into class I and class II. Similarly, Article 8(1) establishes that products that have the core functionality of a product category set out in Annex IV to the CRA are considered to be 'critical products'.[15]

122. The classification of a product as important or critical or, conversely, as belonging to the 'default' category[16], is of relevance when determining the conformity assessment procedure the manufacturer needs to follow, in accordance with Article 32, before it can place that product on the market. Notably, products in the default category can always rely on the internal control procedure based on module A ('self-assessment').[17] Important products of class I or II and critical products are subject to more stringent conformity assessment procedures. This does not include important products of class I or II qualifying as free and open-source software, for which, in accordance with Article 32(5), manufacturers are allowed to follow the procedures of the default category.

123. The concept of core functionality is therefore essential for the manufacturer to determine the applicable conformity assessment regime. However, this concept is not explicitly defined in the CRA.Products can perform a range of functions, some of which may be ancillary to the product's core functionality, and should not impact the product's classification as default/important class I/important class II/critical. It is therefore useful to provide more guidance to help manufacturers correctly perform the relevant conformity assessment procedures, and to assist market surveillance authorities in ensuring the harmonised enforcement of the CRA across the EU.

6.1 Core functionality

124. A product's core functionality refers to the product's main features and technical capabilities, without which it would not be able to meet its intended purpose. It can be ascertained in light of the product's specific context and conditions of use, as specified in the information the manufacturer supplies in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation.

Example 48: A software product provides an abstraction layer over the underlying hardware and manages the execution of software components. Its main features include hardware and peripheral initialization, process and memory management, input–output control, scheduling, resource allocation, and the exposure of system services and application programming interfaces (APIs) through which applications interact with device resources. The technical documentation indicates that the product orchestrates

[15] Commission Implementing Regulation (EU) 2025/2392 sets out the technical description of the categories of important and critical products.

[16] The term 'default' category is not a term defined in the CRA. This expression refers to products that do not have the core functionality of a product category set out in Annexes III or IV to the CRA, and that consequently are subject to the conformity assessment regime set out in Article 32(1).

[17] The manufacturer can nonetheless always choose to apply a more rigorous conformity assessment procedure, opting for a third-party assessment as set out in Article 32(1).

computing resources, enforces system configurations, and provides standardised interfaces for software modules and connected peripherals. The manufacturer highlights these capabilities as enabling the platform to serve as the central software environment on which applications can reliably run. The product has the core functionality of an operating system, as described in Annex I, point 11 to Implementing Regulation (EU) 2025/2392.

125. A product's functionality is rarely restricted exclusively to its core functionality, as products often – if not always – perform additional functions that do not contribute to the product's core functionality. This may also include incorporating components that have themselves the functionality of another important or critical product. However, the fact that a product performs functions other than or additional to those detailed in the technical descriptions of important or critical products does not in itself prevent the product from having one such core functionality.

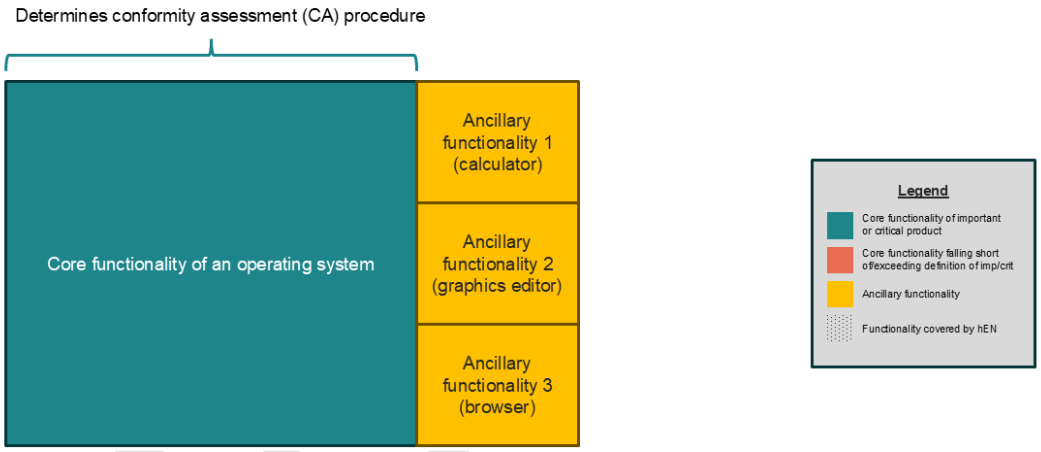

Figure 2: Illustration of core functionality

126. A product may have the ability to perform the functions of an important or critical product category, but nonetheless have a core functionality different from that of such a product category. In those cases, that product would not qualify as an important or critical product. As stated explicitly in Article 7(1) of the CRA for important products (and applying the same logic for critical products), the mere integration of an important or critical product does not in itself render the product an important or critical product.

Example 49: A smartphone integrates an operating system that provides the functionalities described in Annex I, point 11 to Implementing Regulation (EU) 2025/2392. While the operating system enables the management of hardware resources and execution of software applications, the smartphone as a whole has a different core functionality (e.g. that of enabling users to communicate, access information and services, and run third-party applications). The mere integration of an operating system does not mean that the smartphone has the core functionality of an operating system.

127. Some products may be similar to an important or critical product category, or belong to the same general product, yet their core functionality substantially exceeds or substantially falls short of the core functionality of that category. Partial similarities in domain, purpose or deployment context are not sufficient grounds to conclude that two

products share the same core functionality. In such circumstances, the assessment should focus on the product's features and technical capabilities, as reflected in its intended purpose, rather than on vague product groupings or partially overlapping functionalities.

Example 50: A security orchestration, automation and response (SOAR) software often has the ability to perform the functions of products with digital elements in the category of 'security information and event management (SIEM) systems', i.e. collect data from multiple sources, analyse and correlate that data and present it as actionable information for security-related purposes. However, the software's core functionality substantially exceeds that of a SIEM, including services such as incident response. Therefore, SOAR software is generally not considered to have the core functionality of SIEM systems.

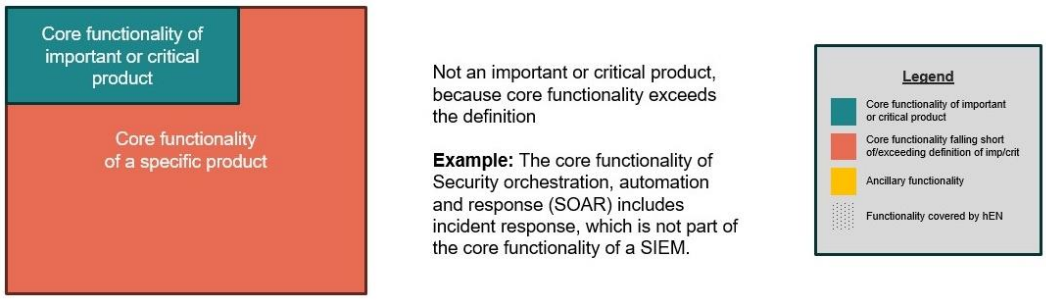

Figure 3: Illustration of core functionality exceeding the definition

Example 51: Certain log collection and visualisation tools have the ability to ingest log data and present basic dashboards showing system events. While these tools can support security monitoring activities, their core functionality falls short of that of SIEM systems, as they do not perform data correlation, nor do they provide actionable security insights. Therefore, such tools are generally not to be considered to have the core functionality of SIEM systems.

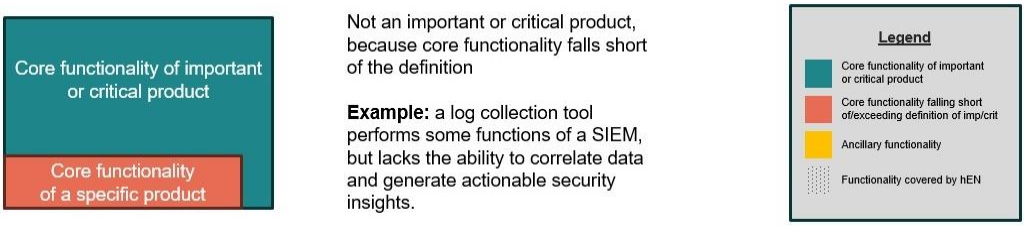

Figure 4: Illustration of core functionality falling short of the definition

128. A product may not have more than one core functionality for the purposes of determining the applicable conformity assessment regime. In accordance with Annex VII of the CRA, as part of a product's technical documentation, manufacturers are required to describe their product's intended purpose and the conformity assessment procedure they have followed. The product's core functionality should therefore be clearly identified. This enables the correct identification of the applicable conformity assessment regime and allows market surveillance authorities to supervise and check that the Regulation is being applied correctly.

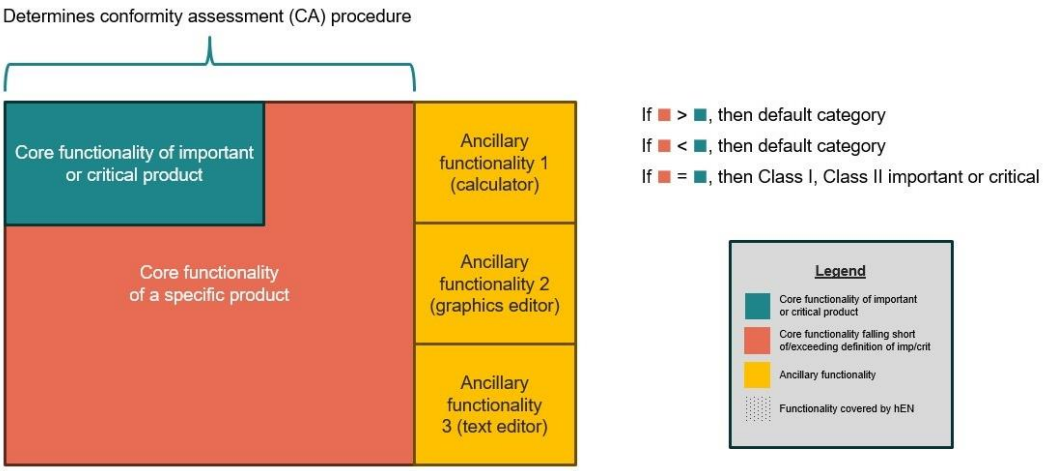

Figure 5: Illustration of how core functionality determines product class

129. A manufacturer may not misrepresent its product's core functionality in such a way as to escape the conformity assessment regime applicable to important or critical products, e.g. by overly emphasising or downplaying the role of certain functionalities, so that the product exceeds or falls short of a given core functionality. This would be the case, for example, where there are clear inconsistencies between promotional materials, instructions for use, and technical documentation.

130. Non-compliance with the obligations set out in Article 32 of the CRA may trigger administrative fines in accordance with Article 64(3).

6.2 Conformity assessment for important and critical products

131. Once the manufacturer has determined its product's core functionality, it needs to perform one of the applicable conformity assessment procedures. The manufacturer needs to ensure that the product as a whole undergoes the conformity assessment procedure, in order to demonstrate that it meets the essential cybersecurity requirements, considering, as appropriate, the security of the components or functionalities integrated into it.

132. A third-party conformity assessment procedure is mandatory for important products of class II (with the exception of those qualifying as free and open source software, in accordance with Article 32(5)) and for critical products, whereby a notified body checks compliance with the essential cybersecurity requirements of the product as a whole.[18] By contrast, important products of class I (with the exception of those qualifying as free and open source software, in accordance with Article 32(5)) are required to undergo a third-party conformity assessment only if the manufacturer has not applied or has applied only in part relevant harmonised standards the references of which have been published in the *Official Journal of the European Union* (henceforth, 'harmonised standards'), common specifications or European cybersecurity certification schemes at assurance level at least 'substantial'.

[18] This is also the case when making use of a European cybersecurity certification scheme with an assurance level at least 'substantial', as the involvement of a third-party certification body is required.

133. Therefore, for an important product to be eligible for the internal control procedure, (i) all the applicable requirements of a relevant harmonised standard need to be applied; and (ii) the standard's scope needs to cover at least all the risks related to the product's core functionality.

134. The product's scope may be broader than the scope foreseen by the relevant harmonised standard, and such additional functions may present different or additional cybersecurity risks. When using a harmonised standard, the manufacturer is always required to carry out a risk assessment and to check whether that standard covers all risks associated with the product. Where the standard does not cover all risks, the manufacturer should ensure via other means that its product is in compliance with the essential cybersecurity requirements.

135. Therefore, if the manufacturer of a product of important class I has applied a relevant harmonised standard that covers the product's core functionality, it can decide to make use of the internal control procedure to demonstrate its product's conformity. As part of its conformity assessment activities, the manufacturer will still be required to demonstrate that all risks applicable to its product are addressed. Hence, where there is a gap between the coverage of the harmonised standard and the scope of the product as a whole, the manufacturer still needs to document which additional measures it has put in place to treat those risks.

Example 52: An antivirus software has the core functionality of software that searches for, removes, or quarantines malicious software, as described in Annex I, point 4 to Implementing Regulation (EU) 2025/2392. That product also includes additional features, namely a disk-cleaning function and an anti-tracking function protecting the user when navigating on the web. The manufacturer carries out a risk assessment covering the product in its entirety, including the antivirus's core functionality, the disk-cleaning and the anti-tracking functions. It applies a harmonised standard covering the antivirus's core functionality, and additional measures to deal with risks stemming from additional functions. The manufacturer is allowed to make use of the internal control procedure for its conformity assessment, covering the product as a whole, including the disk-cleaning and the anti-tracking functions.

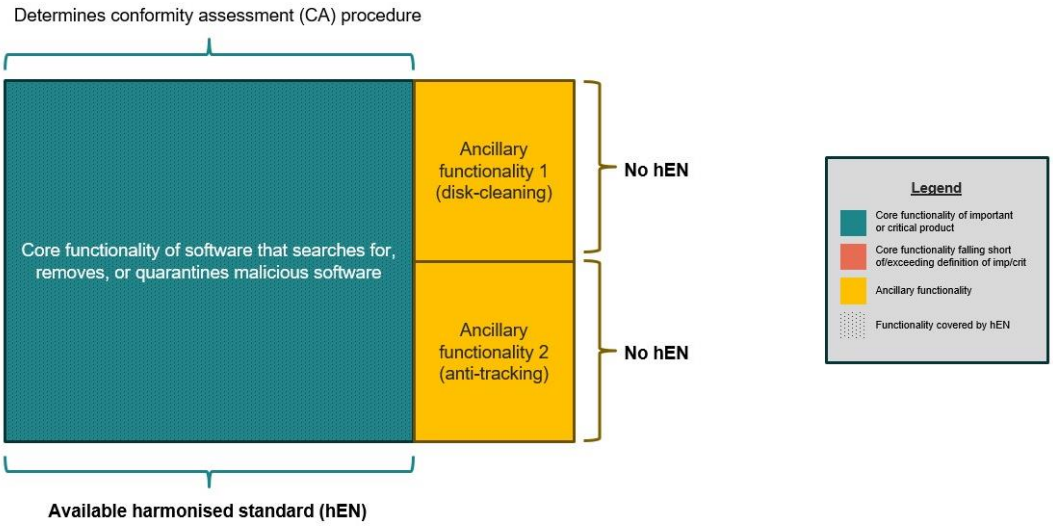

Figure 6: Illustration of harmonised standard covering only core functionality

136. This is also the case where the product integrates an additional function that is itself that of another important or critical product. In fact, it is the core functionality of the product as a whole, and not the functionality of the integrated components taken in isolation, that determines whether the product is important or critical (and therefore determines the applicable conformity assessment regime). For example, if a product has the core functionality of an important product of class I, the product as a whole is subject to the conformity assessment regime applicable to important products of class I, even though it integrates a component that is itself a critical product. Where the manufacturer applies a harmonised standard covering its product's core functionality, it is allowed to make use of the internal control procedure.

Example 53: A hardware product has the core functionality of a router, as described in Annex I, point 12 to Implementing Regulation (EU) 2025/2392. That product also includes additional functionalities, including firewalling capabilities, as it integrates a firewall component. The manufacturer carries out a risk assessment covering the product in its entirety, including the router's core functionality and the firewall functionality. It applies a harmonised standard covering the router's core functionality, and additional measures to deal with risks stemming from additional functions. The manufacturer is allowed to make use of the internal control procedure for its conformity assessment, covering the product as a whole, including the firewall functionality.

6.3 Implications for presumption of conformity

137. Article 27(1) of the CRA establishes that products and processes put in place by the manufacturer which are in conformity with harmonised standards or parts thereof, the references of which have been published in the *Official Journal of the European Union (OJEU)*, are presumed to be in conformity with the essential cybersecurity requirements of the CRA covered by those standards or parts thereof.[19] Article 27(5) extends the same

[19] As clearly stated in Section 4.1.2.2 of the Blue Guide, 'in risk related harmonisation legislation [...] manufacturers always, even when using harmonised standards the references of which are published in the

presumption of conformity to products and processes put in place by the manufacturer which are in conformity with common specifications adopted by the Commission via implementing acts, and Article 27(8) establishes the presumption of conformity for products and processes put in place by the manufacturer for which an EU statement of conformity or certificate has been issued under a European cybersecurity certification scheme adopted pursuant to Regulation (EU) 2019/881, if this has been specified via delegated acts in accordance with Article 27(9).[20]

138. Therefore, where the manufacturer has applied a harmonised standard whose references have been published in the OJEU, and which addresses all the relevant cybersecurity risks associated with its product, it benefits from a presumption of conformity. This could be the case, for example, where the referenced harmonised standard covers the full scope of an important product of class I and there are no additional functionalities that present cybersecurity risks.

139. In the cases discussed in points 135 and 136, the manufacturer is allowed to use the internal control procedure because the harmonised standard covers the product's core functionality. However, the products described in those examples may be broader than the scope of the harmonised standards, and additional functionalities may present cybersecurity risks that are not addressed by such harmonised standard. The product may therefore not benefit from a presumption of conformity, which only covers the parts of the product whose risks are covered by the harmonised standard.

Example 54: An antivirus software has the core functionality of software that searches for, removes, or quarantines malicious software, and that core functionality is covered by the harmonised standard. That product also includes additional functionalities, namely a disk-cleaning function and an anti-tracking functionality protecting the user when navigating on the web, which are not covered by the harmonised standard. If the harmonised standard is applied, the manufacturer is allowed to make use of the internal control procedure for its conformity assessment. It will benefit from a presumption of conformity for the product's core functionality, but not for the additional functionalities.

OJEU, remain fully responsible for assessing all the risks of their product in order to determine which essential (or other) requirements are relevant. After this assessment a manufacturer may then choose to apply technical specifications given in harmonised standards the references of which are published in the OJEU to implement 'risk reduction measures' which are specified by harmonised standards'.

[20] For brevity and clarity, the remainder of this section only refers to harmonised standards the references of which have been published in the OJEU. However, the same guidance extends to common specifications adopted in accordance with Article 27(2) and European cybersecurity certification schemes where specified by the Commission via delegated acts in accordance with Article 27(9).

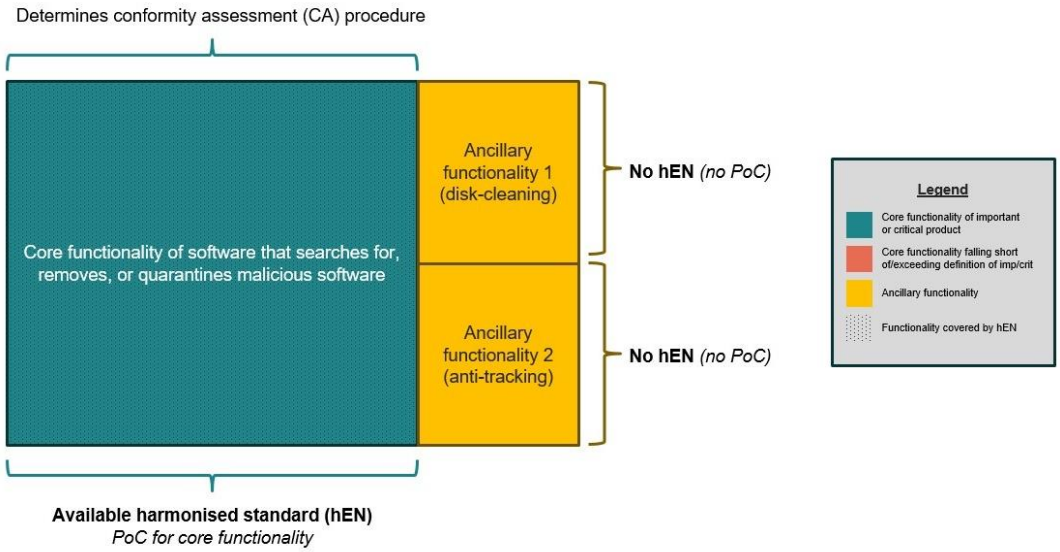

Figure 7: Harmonised standard grants presumption of conformity (PoC) for core functionality

Example 55: In the same scenario as the previous example, the harmonised standard has now been updated to also cover one of the additional functionalities, namely the disk-cleaning function, but not the other (i.e. the anti-tracking function). If the harmonised standard is applied, the manufacturer is allowed to make use of the internal control procedure for its conformity assessment. It will benefit from a presumption of conformity for the product's core functionality and for the disk-cleaning function, but not for the anti-tracking function.

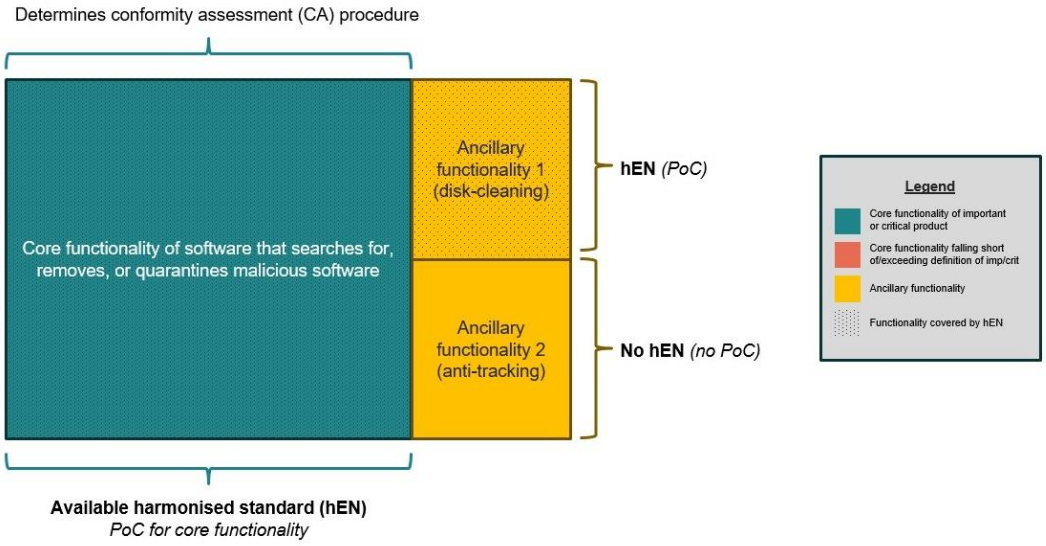

Figure 8: Harmonised standard grants PoC for core functionality and ancillary functionality 1

7 Cybersecurity risk assessment and integration of products and components

7.1 On the evaluation and treatment of cybersecurity risks

140. The cybersecurity risk assessment provided for in Article 13(2) of the CRA requires manufacturers to identify relevant risks and assess their potential impact on the product. Manufacturers also need to implement appropriate measures to address those risks, in accordance with the essential requirements of Annex I.

141. In organisational risk management, risks are commonly evaluated against acceptance criteria derived from the organisation's internal objectives or risk appetite. By contrast, under the CRA, residual cybersecurity risk is assessed against a regulatory threshold: the product placed on the market needs to ensure an appropriate level of cybersecurity based on the risks, taking into account its intended purpose and reasonably foreseeable use.

142. Accordingly, the manufacturer's internal risk tolerance, commercial strategy or cost considerations are not relevant in determining whether the essential cybersecurity requirements are met. For the purposes of Articles 13(2) and (3), manufacturers must be in a position to determine whether identified cybersecurity risks have been sufficiently addressed to meet the essential requirements of Part I of Annex I, in light of the product's intended purpose, reasonably foreseeable use and conditions of use, including, where relevant, the operational environment and the assets to be protected, taking into account the length of time the product is expected to be in use.

143. Residual cybersecurity risk is an inherent outcome of risk assessment and risk treatment. It is recognised that cybersecurity risks cannot, in practice, be entirely eliminated. However, the existence of residual risk does not imply that any risk may be accepted at the manufacturer's discretion. A product may only be placed on the market where the residual risks, once appropriate measures have been taken, have been sufficiently addressed to meet the essential cybersecurity requirements, taking into account the product's intended purpose and reasonably foreseeable use.

144. In accordance with Article 13(3), where cybersecurity risks are identified, manufacturers are required to address them through appropriate measures implemented at product level. Depending on the circumstances, this may involve for example reducing the attack surface, implementing technical safeguards, limiting or adapting functionality, or defining the product's intended purpose and reasonably foreseeable use more precisely, in order to ensure compliance with the essential cybersecurity requirements.

145. The CRA does not provide for the transfer of cybersecurity risk or responsibility to users or third parties. The obligation to place a secure product on the market and to demonstrate conformity with the essential cybersecurity requirements remains with the manufacturer.

146. Nonetheless, information and instructions provided to users may be used to support the product's secure deployment and operation, including where the manufacturer has chosen to restrict the intended purpose of the product to trusted environments, and to inform users of residual risks. Such information cannot be used to compensate for

shortcomings in product design or to justify leaving cybersecurity risks unaddressed where those risks are incompatible with the essential requirements.

147. Where the cybersecurity risk assessment identifies risks that cannot be adequately addressed through appropriate measures, compliance with the CRA may require changes to the product's design, functionality or intended purpose. Considerations relating solely to cost or commercial feasibility do not constitute sufficient grounds for leaving such risks untreated where this would prevent the product from meeting the essential cybersecurity requirements.

7.2 On designing, developing and producing products in such a way that they ensure an appropriate level of cybersecurity based on the risks

148. The essential cybersecurity requirement referred to in point 1 of Part I of Annex I of the CRA provides that products are designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.

149. This essential requirement is aimed at also addressing additional cybersecurity risks that may have been identified by the cybersecurity risk assessment and that are not otherwise adequately addressed as part of the implementation of the essential requirements of Part I of Annex I other than point 1.

150. Accordingly, where all relevant cybersecurity risks related to a product are treated by implementing adequate measures to address the applicable essential requirements other than point 1, the essential requirement referred to in point 1 of Part I of Annex I is deemed to be fulfilled. Conversely, where the cybersecurity risk assessment identifies additional risks not fully addressed by such measures, manufacturers are required to implement appropriate measures on the product to address those risks, so that they comply with the essential requirement referred to in point 1 of Part I of Annex I. In practice, in most cases, compliance with the other essential requirements is expected to result in compliance with this requirement.

7.3 Risk assessment and due diligence in relation to external dependencies and integrated components

151. The CRA establishes two distinct but complementary obligations for manufacturers in relation to cybersecurity risk management. First, Article 13(2) requires manufacturers to carry out a cybersecurity risk assessment for the product itself. Second, Article 13(5) imposes the obligation to exercise due diligence with respect to integrated components. Together, these two obligations are designed to ensure that the product remains secure, including where it relies on remote data processing solutions, cloud-based services, networks, or third-party software or hardware components.

152. The cybersecurity risk assessment concerns the identification and management of relevant risks that may affect the product, including risks that originate outside the product itself, such as external networks, environmental factors, or other external aspects which might affect the product or on which the product relies. For such external risks, the

CRA does not require manufacturers to control or govern the external environment. Rather, manufacturers are required to identify such risks and to mitigate them through the design and development of the product itself. This will involve implementing the appropriate essential cybersecurity requirements set out in Part I of Annex I, including where necessary providing information and instructions to users on integration or deployment risks.

153. For example, a manufacturer may identify a risk that unauthorised persons may gain access to back-end systems while the product is in operation and attempt to send malicious commands to the product. In such cases, the CRA requires the manufacturer to address that risk through product-level measures, such as by requiring cryptographic authentication of remote commands, verifying the integrity of configuration changes, or generating security-relevant logs or alerts when abnormal behaviour is detected. Similarly, where a manufacturer identifies a risk that a remote service may become unavailable due to power outages or failures of the infrastructure, the CRA may require product-level mitigations such as ensuring that the outage does not cause the product to enter into insecure states. In such cases, the CRA regulates how the product responds to those risks; it does not impose obligations on how the back-end infrastructure is organised, staffed or operated.

154. Due diligence relates to elements that form part of the product itself, in particular integrated software or hardware components provided by a third-party. Manufacturers are required to take appropriate measures to ensure that such components do not undermine the product's compliance with the essential cybersecurity requirements. This can only be achieved by determining what the product requires from its components in order to meet its cybersecurity objectives, and verifying, in a risk-based manner, that those components are in line with the product's needs, as also indicated in recital 34.

155. The manufacturer has to identify as part of its cybersecurity risk assessment what those requirements should be. For example, if the risk assessment shows that the product relies on cryptographic functions, update mechanisms or secure communications provided by a component, the manufacturer must, as part of its due diligence, identify those needs and verify that the component satisfies them. Evidence for this purpose may consist of documentation obtained from the component manufacturer, such as technical specifications, security documentation or relevant conformity or assurance documentation. Where appropriate, the manufacturer may also carry out functional tests on those components to ensure stated aims are met. While due diligence is a separate legal obligation, it supports and underpins the manufacturer's ability to demonstrate compliance with the essential cybersecurity requirements for the product as a whole.

156. When assessing the risks to the product as a whole, elements outside of the product, such as environmental elements, external infrastructure, other systems or networks, must be considered in the cybersecurity risk assessment and, where relevant, addressed to ensure that the essential requirements are implemented within the product itself. Components that are physically or logically inside the product but supplied by a third party must also be considered as part of the risk assessment. Howevever, for compliance purposes these are treated as external inputs whose external properties must be verified upon integration

through due diligence, as they cannot be re-designed or re-developed by the manufacturer.

157. The same logic applies during the development and integration of components. Where the manufacturer develops functionalities itself, it must directly implement the essential cybersecurity requirements. Where the manufacturer integrates components developed by others, it must ensure through due diligence, that those components can be used in a way that enables the product as a whole to comply. In both cases, the objective remains the same: that the product, as placed on the market, achieves an adequate level of cybersecurity as required by the CRA, taking into account the risks identified in the cybersecurity risk assessment.

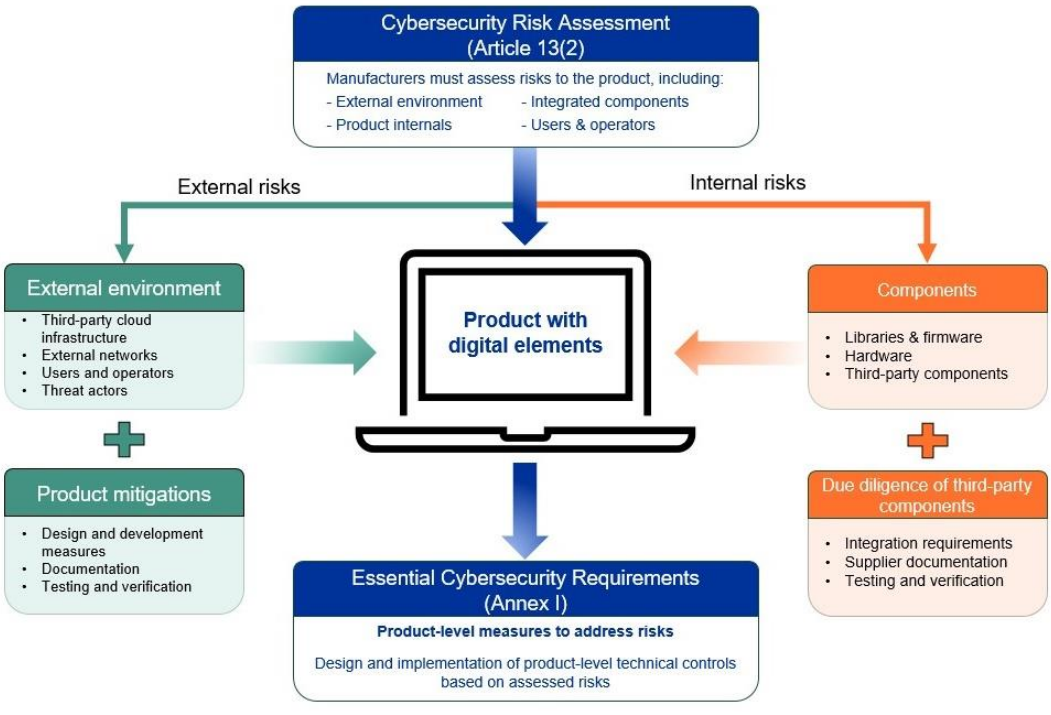

Figure 9: Risk assessment and due diligence in the CRA

7.4 Re-use of risk assessments and conformity documentation for product families

158. Manufacturers may place on the market products that are similar, for example different variants, models or configurations of the same product family. Where such products share the same architecture, security-relevant design and intended purpose, and are exposed to the same cybersecurity risks, the CRA does not require manufacturers to treat each variant as an entirely separate product for the purposes of risk assessment and conformity assessment.

159. In such cases, provided that all variants concerned are adequately covered in terms of relevant risks and essential requirements, manufacturers may rely on: (i) a single cybersecurity risk assessment carried out in accordance with Article 13(2) of the CRA; (ii) a single set of technical documentation; and (iii) a single conformity assessment

procedure. This also allows a single EU declaration of conformity to be issued for the group of products, as long as it clearly identifies the product variants to which it applies.

160. The decisive factor is whether the differences between the variants are relevant to cybersecurity. Variations that do not affect the product's cybersecurity properties, such as differences in physical housing, colour, form factor, memory size, or other non-security-relevant characteristics, do not require separate risk assessments or conformity assessments. Conversely, in some cases variants may differ in ways that affect exposure to threats or the implementation of essential cybersecurity requirements, for example through different communication interfaces, different software stacks, different update mechanisms or different remote connectivity. In such cases, those differences must be reflected in the risk assessment and, where necessary, in the conformity assessment and technical documentation.

161. Manufacturers remain responsible for ensuring that the risk assessment and the related documentation accurately reflect the products placed on the market. Where a new variant introduces new cybersecurity risks or changes the way essential requirements are implemented, the existing risk assessment and conformity documentation must be updated accordingly. Reliance on a single conformity assessment is only possible to the extent that the products do not present differences with regards to their cybersecurity properties.

8 Remote data processing

162. Article 3(1) of the CRA defines a product as 'a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately'. In this light, the manufacturer must consider the product as a whole, including its remote data processing solutions (RDPS). For instance, when demonstrating that the product complies with the essential requirements laid out in Annex I, RDPS must be taken into account, starting with the risk assessment (Article 13(2)). The same is valid when considering lifecycle obligations, such as reporting of actively exploited vulnerabilities and severe incidents (Article 14).

163. The purpose of this guidance is to provide further support to manufacturers in determining whether their product has RDPS as defined in the CRA and how to fulfil their compliance obligations in this regard. After an initial analysis of the definitions and recitals laid down in the CRA, this guidance will provide questions to guide manufacturers in clarifying if their product includes RDPS (see Section *8.1 What is considered a remote data processing solution for a product with digital elements?*). Subsequently, it will elaborate on the technical implications of RDPS and how to assess compliance with the CRA (see Section *8.2 Practical and technical implications of remote data processing solutions and reliance on third-party solutions*).

164. In fact, Article 3(2) defines the concept of 'remote data processing' as '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'. RDPS is therefore defined as the software elements ('the part of an electronic information system which consists of computer code', as defined in Article 3(4)) of data processing at a distance. It is not meant to include, as part of the scope of the product, the hardware that remote data processing may rely upon.

165. Recitals 11 and 12 give further explanations on how this concept should be interpreted. Recital 11 clarifies that the goal of covering remote data processing solution is that 'products are adequately secured in their entirety by their manufacturers, irrespective of whether data is processed or stored locally on the user's device or remotely by the manufacturer'. It also states that 'requirements concerning the remote data processing solutions falling within the scope of this Regulation do therefore not entail technical, operational or organisational measures aiming to manage the risks posed to the security of a manufacturer's network and information systems as a whole.'

166. Therefore, it results from recital 11 that the intent is not for the CRA requirements to cover the whole IT infrastructure of an organisation, but only software components that allow for the execution of the data processing solution. For example, internal systems relating to the manufacturer's own human resources, payrolls, customer relationship management, continuous integration/continuous delivery (CI/CD) pipelines, the distribution of security updates to edge locations, should not be considered as RDPS. Likewise, systems linked to auditing and testing activities, such as penetration testing, threat hunting and red teaming are outside the scope of a product as covered by the CRA. It is important to note that while applying effective and regular tests and reviews of the security of the product is an essential requirement laid down in point 3 of Part 2 of Annex

I of the CRA, this does not mean that such activities are to be considered RDPS for the product.

167. Recital 12 focuses on cloud services and elaborates on the circumstances under which cloud services might be considered RDPS. The recital concludes by recalling that cloud computing services and cloud service models fall within the scope of Directive (EU) 2022/2555 (NIS 2)[21], which establishes cybersecurity risk-management requirements for cloud computing service providers. Those requirements are further specified by Commission Implementing Regulation (EU) 2024/2690[22].

8.1 What is considered a remote data processing solution for a product with digital elements?

168. The definition of remote data processing laid down in Article 3(2), thus, relies on three elements: (i) whether data processing is 'at a distance'; (ii) whether the absence of such data processing would prevent the product from performing one of its functions; and (iii) whether the software is designed and developed by the manufacturer, or under its responsibility. The next three subsections address each of these elements in more detail.

8.1.1 The notion of 'at a distance'

169. The notion of 'at a distance' referred to in Article 3(2) is relevant but not sufficient to determine whether a product includes RDPS. Furthermore, given the variety of solutions that might fall under this concept, it is not possible to provide an exhaustive definition of 'at a distance'. A case-by-case assessment by the manufacturer is needed.

170. Recital 11 of the CRA mentions data processed or stored 'remotely by the manufacturer' as opposed to data processed or stored 'locally on the user's device'. Remote data processing typically takes place outside the product's user environment or an organisation's operational environment (for a professional user). This, however, does not prevent processing from also taking place close to the device ('at the edge'). The transmission of data may be wired (e.g. ethernet cable) or wireless (e.g. Wi-Fi, Bluetooth). Cloud computing, including edge computing, is a typical example of data processing taking place 'at a distance'. For instance, in the case of a cloud-based function accessed by the user from a mobile application, part of the data processing takes place on the cloud, outside of the user's environment.

[21] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJ L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/2022-12-27

[22] Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers, OJ L, 2024/2690, 18.10.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj

171. It is important to note that RDPS are not necessarily operated on third-party cloud infrastructure. Remote data processing running on local servers on the manufacturer's premises can also constitute RDPS. In other words, a solution run on-premises and on a private cloud is just as likely to qualify as RDPS as a solution run on a public cloud and off-premises.

172. The two decisive and cumulative questions that determine whether data processing is covered by CRA as remote data processing solution are set out below, in sections *8.1.2* and *8.1.3*. If both questions are answered in the affirmative, the remote data processing qualifies as RDPS.

8.1.2 Would the absence of such data processing prevent the product from performing one of its functions?

173. As laid down in the definition of 'remote data processing' included in Article 3(2), for data processing at a distance to qualify as a RDPS, its absence would need to prevent the product from performing one of its functions. The notion of 'functions' included in this definition is not limited to the product's 'core functionality' or 'intended purpose', as the CRA does not impose such a limitation. The functions within the scope of the CRA are both functions that directly fulfil the intended purpose of the product as experienced by users and functions that support the product's overall performance.

174. Examples of functions where data processing at a distance may happen and that would prevent a product from performing one of its functions would include: (i) sending commands to a device; (ii) synchronising files; (iii) onboarding the user; (iv) configuration (personalisation of the product); (v) receiving updates, including feature update and security patching; (vi) identity and access management.

175. In some cases, the user can use a function both remotely and manually (e.g. switching a light bulb with an app or manually). Having this option does not exclude qualification as RDPS of the data processing associated with the remote performance of the function. Performing this function remotely is also considered part of the functions the product offers.

176. By contrast, where the absence of a certain data processing does not prevent the product from performing one of its functions, such processing is not considered as a RDPS within the meaning of the CRA. This includes, for example, remote analysis of telemetry data collected purely for statistical purposes or future product development.

177. Nevertheless, even when data processing does not support a product function, manufacturers may need to consider if those remote communications introduce risks to the product as part of their cybersecurity risk assessment, and mitigate such risks accordingly (e.g. through product-level mitigations).

178. Websites are a specific case that deserves further clarification. Websites are not within the scope of RDPS if they do not support a product function, as explained in recital 11 of the CRA. It is not sufficient for a website to contain information about a product to be considered within the scope of RDPS, even if the product redirects to such website. For example, redirecting users to an external webpage that provides information and instructions to users is not a RDPS. By contrast, a website may be within the scope of RDPS if it enables or supports a product function. For example, an authentication portal that

issues credentials/tokens required for the product to operate would be considered RDPS (provided that the other criteria of the definition are also met).

8.1.3 Has the software been designed and developed by the manufacturer, or under its responsibility?

179. The definition of 'remote data processing' of Article 3(2) of the CRA further specifies that the software of such data processing at a distance needs to be designed and developed by the manufacturer, or under its responsibility. Remote data processing entirely developed and designed by the manufacturer (in-house) would naturally qualify as RDPS. This would also be the case if manufacturers rely on an external service provider for the development and design of a solution (i.e. 'under its responsibility'). The phrase 'under the responsibility of the manufacturer' refers to remote processing solutions that are tailor-made for the manufacturer. These are cases where the manufacturer is not merely licensing an existing product or service that a service provider offers to its customers or slightly modified versions thereof. '[U]nder the responsibility of the manufacturer' entails that the software is built solely on behalf of the manufacturer, based on designs and specifications provided by it. In other words, these are situations where the technology developed by the service provider is owned, not licensed, by the manufacturer.

180. In understanding RDPS, the notion of 'who operates the solution' is not a decisive factor, as the CRA definition only refers to the design and development of the RDPS. This is consistent with the CRA approach whereby requirements and obligations are on manufacturers, and not on the operation of the product. If manufacturers design and develop solutions, which are then operated by a third party, they remain responsible for compliance with the CRA's essential requirements for the product that they place on the market.

181. It is necessary to differentiate between the cases where design and development are done by manufacturers (or under their responsibility) and cases of reliance on third-party solutions not designed and developed by manufacturers (or under their responsibility). As an example, it is helpful to consider the most common cloud service models that provide different degrees of user control and that are also cited in recital 12 of the CRA, namely Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

182. In the case of a third-party IaaS solution, the manufacturer does not manage or control the underlying physical and virtual resources (such as the underlying hardware and the cloud service provider's hypervisor), but is able to deploy and run arbitrary software using such resources, such as operating systems and applications. Such software is designed and developed by the manufacturer, or under its responsibility, and may therefore qualify as RDPS (if it fulfils the other elements of the definition).[23]

183. In the case of a third-party PaaS solution, the manufacturer deploys its own (created or acquired) application using programming languages and execution environments provided by the cloud service provider and integrates the application into its product. The manufacturer has control over the application and possibly over configuration settings for the execution environment. The application is therefore designed and developed by the

[23] Where such components are sourced from third parties, as often the case for example for the operating system running on the IaaS, the manufacturer is to exercise due diligence in accordance with Article 13(5).

manufacturer, or under its responsibility, and may therefore qualify as RDPS (if it fulfils the other elements of the definition).

184. In the case of a third-party SaaS solution, the SaaS provider offers the manufacturer a fully developed application to be integrated into the manufacturer's product. The manufacturer has limited ability to manage user-specific application configuration settings. The application is therefore not designed and developed by the manufacturer, or under its responsibility.

185. Nonetheless, where certain elements do not qualify as RDPS (e.g. the hypervisor in the case of a third-party IaaS infrastructure, the operating system in the case of a third-party PaaS solution, or the third-party SaaS application), such solutions should be considered similar to third-party components as they are integrated in the product, hence they might compromise its security. The manufacturer is required to identify and assess risks linked to the integration of those components and to address them by implementing the essential requirements on the product itself. Additionally, the manufacturer is expected to exercise a similar obligation to the obligation to perform due diligence referred to in Article 13(5) related to the security of these components.

186. Therefore, it can be summarised that:

a. For data processing to qualify as RDPS, the answer to the questions posed in Sections *8.1.2 Would the absence of such data processing prevent the product from performing one of its* functions? and *8.1.3 Has the software been designed and developed by the manufacturer, or under its responsibility?* needs to be affirmative.

b. Manufacturers should treat the third-party solution as a component if the answer to the question in Section *8.1.2 Would the absence of such data processing prevent the product from performing one of its* functions? is affirmative but the answer to the question in *8.1.3 Has the software been designed and developed by the manufacturer, or under its responsibility?* is negative. As part of the risk assessment, manufacturers should assess the risks stemming from the integration of such solution and mitigate them accordingly. Additionally, manufacturers should exercise due diligence.

c. If the answer to the question in Section *8.1.2 Would the absence of such data processing prevent the product from performing one of its* functions? is negative, manufacturers should assess the risks stemming from the existence of such data processing as part of their risk assessment.

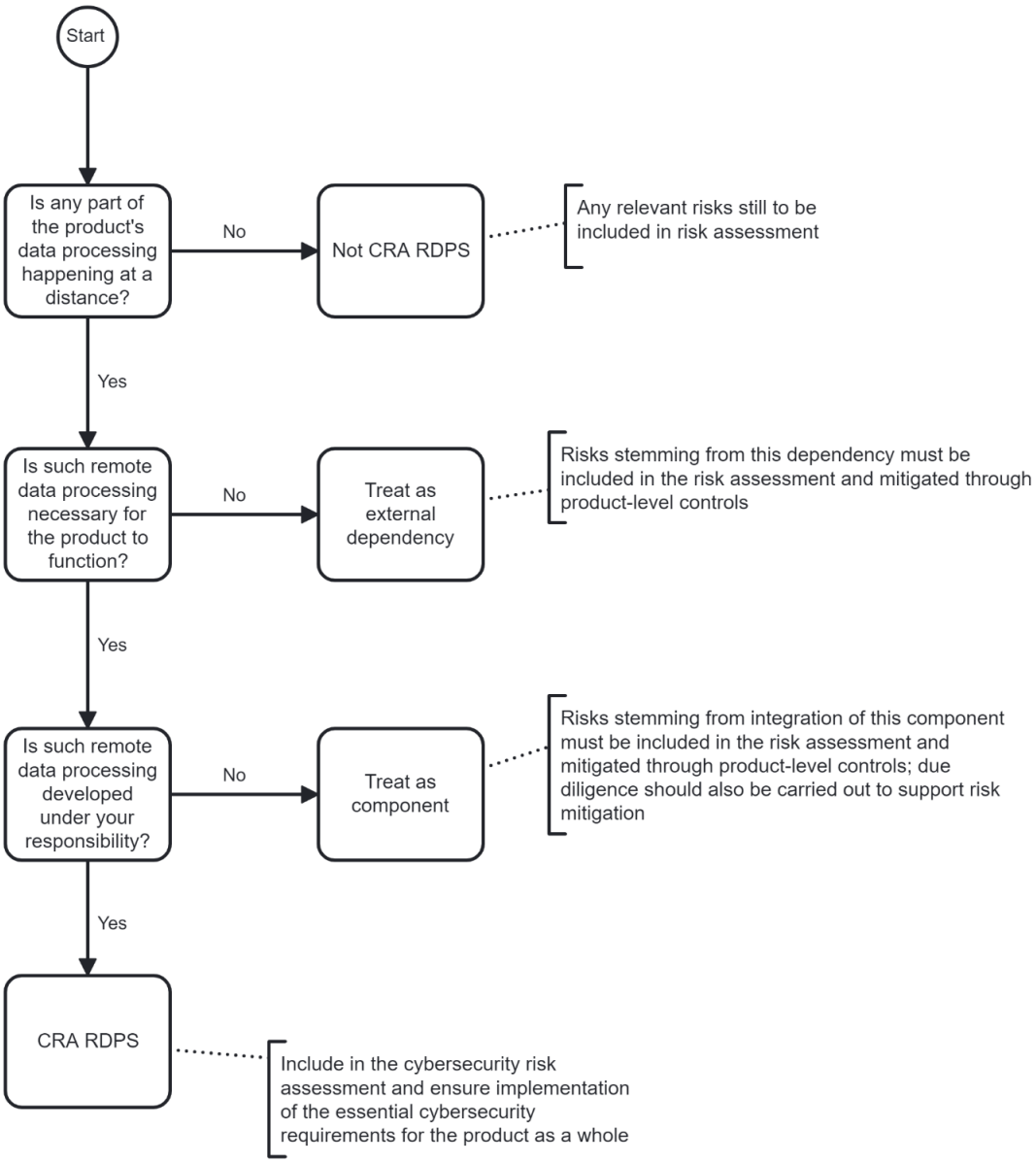

Figure 10: Sylised flowchart to determine if product contains RDPS

8.2 Practical and technical implications of remote data processing solutions and reliance on third-party solutions

187. The CRA follows a risk-based approach, which is enshrined in Article 13(2) and (3), as well as in the first essential requirement of Part I of Annex I, whereby 'products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks'. Consequently, a risk-based approach should be considered when applying the CRA requirements to the RDPS and the treatment of risks stemming from third-party services integrated into the product.

188. First, manufacturers should (i) indicate in the technical documentation that their product has RDPS or relies on third-party cloud solutions and (ii) describe such solutions. If the same RDPS supports several products, the RDPS needs to be declared in each product's

technical documentation. The documentation concerning RDPS serving several products may be re-used from one product conformity assessment to another.

189. It appears appropriate to delineate the part of the system that would be within the scope of the conformity assessment. Segregation of systems and data may make it easier to identify relevant parts of the RDPS. CRA requirements should only apply to those parts of the system where data intended for the provision of product functions is stored or processed. For instance, when a banking application interacts with the financial entity's environment, the intent of the CRA is not to cover the entire entity's environment but only those parts of the system that directly interact with the product, i.e. where the data processing and storage necessary for the product to perform one of its functions takes place. More information on this use case may be found in Section *8.3.1 Banking application*. In all cases, the underlying hardware infrastructure should be considered outside the scope of the product. However, relevant risks should be assessed as part of the risks assessment.

190. Second, the risk assessment performed by the manufacturer should consider: (i) risks related to RDPS;; (ii) and risks related to reliance on third-party cloud solutions (similar to third party components), (iii) risks related to the product environment (e.g. underlying hardware). Manufacturers should implement security controls on the product itself to mitigate those risks.

191. Third, as part of the conformity assessment and/or the fulfilment of due diligence obligations related to third-party cloud services, the following-elements can be re-used in support of the manufacturer's assessment:

    a. as applicable, the CE marking of components provided they are within their support period;

    b. evidence of fulfilment of obligations under Commission Implementing Regulation (EU) 2024/2690;

    c. evidence of fulfilment of obligations under Regulation (EU) 2022/2554 (DORA);

    d. statement of conformity or certificate obtained under a European cybersecurity certification scheme (adopted under Regulation (EU) 2019/881 – the Cybersecurity Act);

    e. Evidence of conformity with ISO/IEC 27017:2015 or ISO/IEC 27001:2022.

192. Finally, in their interactions with third-party cloud service providers, manufacturers need to implement the most appropriate security measures based on their risk assessment. Those mitigation measures should include security controls implemented at product level and the verification of security measures provided by the third-party providers themselves (due diligence). A tool to mitigate such risks can be to embed security guarantees in their service level agreements (SLAs) with third-party providers, including assurances that providers adequately handle vulnerabilities. A major change in the solutions provided by the third-party cloud services providers should not qualify as a substantial modification of the product, as these elements are not under the manufacturer's responsibility. However, as part of their due diligence obligations and to correctly mitigate risks stemming from the use of third-party providers, manufacturers are encouraged to ensure that their third-party could service providers keep them adequately informed about changes they implement on their solutions. Based on such

information, manufacturers may need to revise their risk assessment. The updated risk assessment should consider whether the third-party service providers still provide sufficient guarantees in terms of cybersecurity and whether the product-level security controlsare still adequate. In some cases, manufacturers may need to modify such controls or change third-party service providers.

8.3 Use cases for remote data processing solutions

In order to provide additional practical guidance for manufacturers, this section introduces a series of fictional use cases, describing archetypal products that rely on remote data processing and illustrating whether such procesing qualifies as remote data processing solutions within the meaning of the CRA.

8.3.1 Banking application

A financial entity places a banking application on the market. The app's back-end systems - support, among others, authentication, authorisation, account management, and payments. The financial entity uses a hybrid strategy relying on in-house infrastructure as well as third-party cloud solutions to support the app's functionalities. These include:

Self-hosted servers to support financial transactions:

- The customer initiates a transfer via the mobile app.
- The request is submitted to the banking application programming interface (API) layer, which has been developed by the financial entity and self-hosted; the API authenticates the customer's identity by quering the account management system and submits a request to the ledger system.
- The account management system and ledger system, which are also self-hosted but are logically segregated from the banking API layer, are used to record the transaction.
- The ledger system returns the transaction status to the banking API layer, which ultimately presents the result to the customer.

Implications for RDPS:

- The banking API layer is necessary for the app to perform its functions (i.e. supporting financial transactions). It is designed and developed under the responsibility of the manufacturer. As the answer to both questions presented in earlier sections is affirmative, the banking API is to be considered a RDPS. It must therefore be included in the cybersecurity risk assessment and in the implementation of the essential cybersecurity requirements for the product as a whole.
- The account management system and the ledger system do not qualify as RDPS for the banking application. Although they are part of the financial entity's environment, they do not interact directly with the app and do not support one of its functions. They therefore fall outside the definition of RDPS for the purposes of the CRA. However, those systems remain external dependencies that may give rise to significant cybersecurity risks for the product. For example, compromise of the ledger system could allow an attacker to influence transaction results that are subsequently displayed in the application. The manufacturer is therefore required to identify and assess those risks as part of the cybersecurity risk assessment and to mitigate them through product-level measures, such as strong authentication of backend interfaces, integrity protection of transaction data, secure communication channels and verification of responses received by the app.

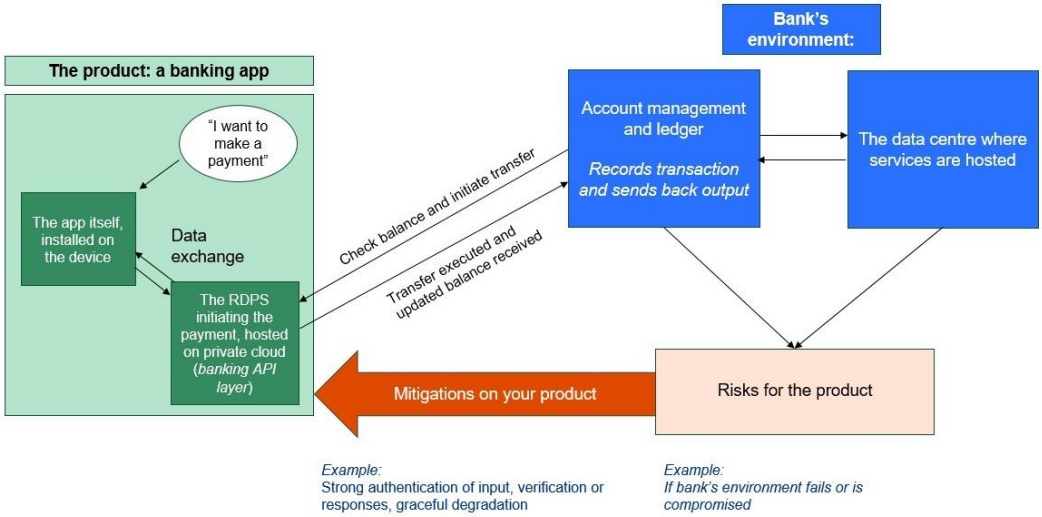

Figure 11: Representation of a banking app relying on RDPS

Third-party SaaS for customer support:

- The financial entity integrates into its app a customer support chat solution developed and operated by a third party provider; the third party provider has written the chat server code, built the user interface and operates the infrastructure where the chat is deployed (i.e. SaaS model).
- When the customer initiates a request for support, the app connects the customer to the third-party service to establish a chat session and handle the messaging flow, without providing the third party with access to core banking systems.

Implications for RDPS:

- The support chat solution is necessary for the product to perform one of its functions, but is not designed and developed by the financial entity, or under its responsibility; it therefore is not a RDPS. However, it should be treated like a third-party component. The reliance on that third-party service may create cybersecurity risks for the banking application, for example if an attacker were to use the chat channel to impersonate the bank or to deliver malicious content to users. The financial entity must take those risks into account in its cybersecurity risk assessment and mitigate them through product-level measures, such as isolating the chat function from core banking features, controlling data flows and validating content. Due diligence on the SaaS should also be exercised.

Reliance on third-party PaaS for transaction notifications:

- The banking app provides real-time notifications when money moves in or out of an account.
- This function relies on a cloud service provider's PaaS, which provides the execution environment and underlying physical and virtual infrastructure; the financial entity has itself developed and deploys the application code responsible for the notification logic and message generation, on top of the cloud service provider's PaaS.

Implications for RDPS:

- The application code responsible for the notification is necessary for the app to perform its function (i.e. pushing transaction notifications). It is designed and developed under the responsibility of the manufacturer. It therefore is to be considered a RDPS.

- The functions provided by the third-party PaaS provider are not designed or developed by the manufacturer or under its responsibility; they are therefore not to be considered RDPS. Nonetheless, the financial entity should treat the PaaS like a component. The use of that PaaS may still give rise to cybersecurity risks, such as unauthorised access to the notification service or disruption of message delivery. Those risks must be identified in the cybersecurity risk assessment and mitigated through product-level measures, such as strong authentication of the service, integrity protection of messages and resilience against service outages. Due diligence on the PaaS provider should also be exercised.

8.3.2 Smart thermostat

A smart thermostat enables users to control the temperature of their homes via a mobile application. The mobile application and the smart thermostat rely on remote data processing to exchange data (e.g. request to increase the temperature) and store data (e.g. user preferences). These functions were developed and designed under the responsibility of the manufacturer but run on an underlying physical and virtual infrastructure provided by a third-party (third-party IaaS).

As the smart thermostat would not work without this remote data processing, its absence would prevent the product from performing one of its functions. Additionally, the software was developed and designed under the responsibility of the smart thermostat manufacturer. Therefore, the remote data processing qualifies as RDPS as defined in the CRA.

For the purpose of CRA compliance, the manufacturer of the smart thermostat needs to document the RDPS as well as the reliance on the third-party IaaS in the product's technical documentation, including details of the contracted service. The manufacturer needs to consider those elements in the risk assessment, which includes the product's intended purpose and reasonably foreseeable use. The manufacturer implements the CRA's essential requirements based on the risks on the RDPS. For the third-party IaaS, the manufacturer needs to ensure that the security measures provided by the third-party provider are appropriate and/or take relevant measures vis-à-vis the infrastructure. For the former, the manufacturer could, for example, ask for evidence that NIS 2 obligations have been met.

8.3.3 e-Reader

The manufacturer of an e-Reader software uses a third-party SaaS storage service to store electronic books purchased by customers and enable them to access their books. The absence of this storage service would prevent the product from performing one of its functions, but the third-party SaaS storage service is not developed by or under the responsibility of the manufacturer; the SaaS provider makes it available to customers for any use case.

The SaaS storage service does not meet the definition of RDPS. However, the e-Reader manufacturer relies on that external service for the functioning of its product and must therefore take the associated risks into account in its cybersecurity risk assessment. The e-Reader manufacturer should treat the SaaS like a component. The manufacturer must implement appropriate product-level security measures, such as secure authentication, encryption and integrity protection of communications with the storage service. Due diligence when selecting and integrating the SaaS provider will also support the manufacturer's obligations, so that the product as a whole can comply with the essential cybersecurity requirements.

8.3.4 Industrial robot

An industrial robot has the task of picking up parts. The robot sends information collected via cameras to a remote service designed and developed by the manufacturer. This service runs on an underlying

physical and virtual infrastructure provided by a third party service provider (third-party IaaS). The cloud service calculates the position of a part based on the camera feeds and sends commands back to the robot to pick up the parts.

The absence of this data processing would prevent the industrial robot from picking up parts, hence from performing one of its functions. Furthermore, the software running on top of the infrastructure has been designed and developed by the manufacturer. The software designed and developed by the manufacturer meets the definition of RDPS.

The manufacturer of the industrial robot needs to document the RDPS as well as the reliance on the third-party IaaS in the product technical documentation (including details of the contracted service). The manufacturer also needs to consider those elements in the risk assessment, which includes the product's intended purpose and reasonably foreseeable use. The manufacturer implements the CRA's essential requirements on the product, including its RDPS, on the basis of the risks. Due diligence when selecting the PaaS provider will also support the manufacturer's obligations. For example, the manufacturer could ask for evidence that NIS 2 obligations have been met.

8.3.5 Cellular network

A smartphone relies on a 5G network to provide internet connection, phone calls and messages to its users (mobile connectivity). The cellular network is developed and designed by telecommunication operators. The network comprises small cells and cell towers, and other network equipment.

The product should be able to connect to a network correctly; this is one of its functions. However, whether that network is in operation or not is not relevant to ascertain if the product is working correctly. The network is only a communication channel and is not necessary for the product to perform its function of 'connecting to a network correctly'. Likewise, an ethernet cable, a router or Wi-Fi signal is not considered data processing whose absence would prevent the product from performing one of its functions, but rather an enabler of communication/connectivity.

Consequently, the cellular network does not meet the definition RDPS. The network should not be considered like a third-party component, as there is no software integrated into the product, the product instead merely relying on this network. As such, it is not necessary for the manufacturer to exercise due diligence obligations towards the network provider.

9 Additional elements

9.1 On reporting obligations

193. Under Article 14(1) and (3) of the CRA, a manufacturer is required to notify simultaneously to the CSIRT designated as coordinator and to ENISA of (i) any actively exploited vulnerability contained in its product that it becomes aware of; and (ii) any severe incident having an impact on the security of the product that it becomes aware of. The obligation to notify such events applies once the manufacturer becomes aware that a vulnerability is being actively exploited or that a severe incident has occurred and has led to the security of its product being compromised. Therefore, guidance on when a manufacturer is deemed to have become aware should help manufacturers determine the moment when the applicable reporting deadlines start.

194. Manufacturers that may be subject to comparable reporting obligations under different EU acts. To ensure the concept of 'becoming aware' is interpreted consistently and to facilitate manufacturers' compliance with those obligations, this guidance is aligned with recital 31 of Commission Implementing Regulation (EU) 2024/2690 and Section II(A) of the Guidelines 9/2022 on personal data breach notification under the GDPR.

195. In some cases, a manufacturer will detect a suspicious event, or a third party, such as an individual, a customer, an entity, an authority, a media organisation or other source will bring a potential incident or vulnerability to its attention. In such cases, the manufacturer should assess the suspicious event immediately to determine whether it constitutes an actively exploited vulnerability or a severe incident having an impact on the security of the product. The manufacturer is therefore to be regarded as having become aware when, after such an initial assessment, it has a reasonable degree of certainty that: (i) a vulnerability contained in its product is being actively exploited; or (ii) a severe incident has occurred and has led to the security of its product being compromised.

196. Therefore, the point in time at which a manufacturer can be considered to be aware will depend on the circumstances of the specific actively exploited vulnerability or severe incident. In some cases, it will be relatively clear from the outset that a vulnerability is being actively exploited or that a severe incident is impacting the security of a product with digital elements. In others, it may take some time to establish whether a product is affected by a vulnerability and whether that vulnerability is being exploited by a malicious actor, or whether an incident is impacting the security of a product. However, the emphasis should be on prompt action to carry out the initial assessment to determine whether such conditions are indeed met, particularly where the vulnerability may pose a significant risk, and if so, to take remedial action and notify in accordance with the CRA.

197. Furthermore, the structure of the reporting obligations requires manufacturers to update their notifications progressively, as their internal investigations advances and their knowledge of the actively exploited vulnerability or incident becomes more detailed. In particular, manufacturers are required to submit an early warning notification containing limited information without undue delay and in any event within 24 hours of becoming aware. Additional information is subsequently required as part of the notification to be

submitted without undue delay and in any event within 72 hours of becoming aware ('72-hour notification'). The complete report needs to be submitted within 14 days after a corrective or mitigating measure is available for actively exploited vulnerabilities, or within one month after the 72-hour notification for severe incidents.

198. After becoming aware of an actively exploited vulnerability or a severe incident, manufacturers are required, in accordance with Article 14(8), to inform impacted users and, where appropriate, all users. Where they fail to do so in a timely manner, the CSIRTs that received the notification may provide such information to users when this is considered proportionate and necessary to prevent or mitigate the impact of that vulnerability or incident.

199. In line with the CRA's risk-based approach, the obligation to inform users laid down in Article 14(8) is to be applied in a risk-based and proportionate manner. In particular, the provision of information about an actively exploited vulnerability or a severe incident does not imply that such information must be made public or disclosed indiscriminately. Where appropriate, and in light of the product's nature, the affected users and the vulnerability or incident's potential impact, manufacturers may limit the disclosure of detailed information to the relevant users or customers concerned. This is particularly the case for products used in sensitive or essential environments, where public disclosure of technical details could itself increase cybersecurity risks or facilitate further exploitation.

200. Once the vulnerability has been adequately addressed or mitigated, broader disclosure may be appropriate. This would be the case, for example, where disclosure contributes to raising general awareness or enables users to verify that their products are no longer affected. In such cases, the level of detail and the timing of any broader disclosure should remain proportionate and take into account the residual risks of exploitation, the product's nature and the interests of the users concerned.

9.2 On vulnerability handling

9.2.1 Reporting upstream and sharing security fixes

201. Article 13(6) of the CRA requires manufacturers to report vulnerabilities in integrated components to the person or entity manufacturing or maintaining that component ('reporting upstream').

202. Manufacturers are required to report upstream only in respect of the version of the component that they integrate. Furthermore, manufacturers are required to report upstream only those vulnerabilities that exist in the integrated component itself, and not vulnerabilities that exist as result of the integration between the component and other code developed by the manufacturer or by the integration of other components. Nonetheless, there may be situations in which a component's integration into a specific product reveals certain behaviours, interactions or security-relevant characteristics of that component that were not apparent, or not readily identifiable, in isolation. In such cases, manufacturers are encouraged to communicate this information to the person or entity manufacturing or maintaining the component, in order to foster good vulnerability-

handling practices aimed at facilitating effective remediation and improving the overall security of the component ecosystem.

203. Finally, manufacturers are also not required to report the vulnerability upstream where the component no longer has a maintainer, or when the manufacturer has itself duplicated ('forked') the free and open-source component and no longer relies on the original maintainer for new versions or security fixes.[24]

204. Furthermore, under Article 13(6) manufacturers that have developed a software modification to address a vulnerability in an integrated component are required to share that software modification ('security fix') with the person or entity manufacturing or maintaining the component ('sharing upstream').

205. It is considered that manufacturers are required to share that fix, where appropriate, in a machine-readable format, such as via a merge request containing the necessary changes to the codebase, in a manner that can be easily verified and, where appropriate, integrated by the person or entity manufacturing or maintaining the component. Where the component is a free and open-source component, the security fix should be shared in a manner compatible with that component's licence, for example by sharing it under the same licence or under a licence that allows the maintainer to distribute the fix under its own licence. Generally, where the maintainer of that component has guidelines on how security fixes should be shared, the manufacturer should follow those guidelines.

206. However, manufacturers are not required by the CRA to ensure that their security fixes are necessarily accepted by the person or entity manufacturing or maintaining the component. Nor are they required to ensure that those fixes are necessarily integrated into the component's code repository, for instance where the maintainer may prefer a different option to fix the issue. Similarly, manufacturers are not required to accept a proposed fix developed by the component maintainer, and may prefer to mitigate the issue in other suitable ways.

207. In some cases, the person or entity manufacturing or maintaining the component may have already provided a security fix to address the vulnerability, but a manufacturer implements a different mitigation strategy (for example by changing a different configuration). In such cases, the CRA does not require the manufacturer to share the modification of another part of the system upstream.

9.2.2 Known exploitable vulnerabilities

208. One of the essential cybersecurity requirements of Part I of Annex I of the CRA provides that, on the basis of the cybersecurity risk assessment referred to in Article 13(2), and where applicable, products must be made available on the market without known exploitable vulnerabilities.

[24] A manufacturer integrating a free and open-source component should not be considered to be maintaining an independent fork, and therefore not be required to comply with Article 13(6), where it continues to rely on the upstream project for new versions or security fixes. This may be the case, for example, where the manufacturer regularly synchronises local copies of the component with the upstream project.

209. Article 3(41) defines 'exploitable vulnerability' as 'a vulnerability that has the potential to be effectively used by an adversary under practical operational conditions'. Not all vulnerabilities are exploitable under practical operational conditions, and some vulnerabilities can only be exploited in theoretical conditions (e.g. in a lab or in a simulation) and/or not under conditions which would occur in a product's operational environment.

210. The CRA requires manufacturers to have appropriate policies and procedures to handle and remediate potential vulnerabilities reported from internal or external sources (Article 13(8)). However, it does not explicitly specify when an exploitable vulnerability should be considered to be known by the manufacturer, thereby triggering the obligation to comply with this essential requirement at the moment of placement on the market.

211. An exploitable vulnerability should be regarded as known when it is listed in relevant publicly accessible vulnerability databases, such as the European vulnerability database established by Article 12(2) of Directive (EU) 2022/2555 or other prominent vulnerability databases, such as the Common Vulnerability and Exposures (CVE) List maintained by the MITRE Corporation.

212. Additionally, an exploitable vulnerability may also be known when the manufacturer has been made aware of it via non-public information, for example via coordinated disclosure by a security researcher or through the manufacturer's own internal testing and analysis. Likewise, an exploitable vulnerability may be known when it has been publicly and prominently reported in reliable media outlets, including specialised cybersecurity publications or general mass media.

213. Nevertheless, the mere fact that a vulnerability is reported as exploitable does not, in itself, mean that it is exploitable in practice or applicable to the specific product concerned. The manufacturer will need to investigate it and confirm the veracity of such information and applicability to its own product. Accordingly, a limited period of time may elapse between the first report of the vulnerability and its confirmation. As indicated in Section *9.1 On reporting obligations*, the emphasis should be on prompt action to investigate and react.

214. Furthermore, the obligation for manufacturers to comply with the essential cybersecurity requirements set out in Part I of Annex I applies at the moment of placement on the market, in accordance with Article 13(1). In practice, it may be the case that new potentially exploitable vulnerabilities are discovered during the final stages of the product development lifecycle, including shortly before it enters the distribution chain (and is therefore placed on the market).

215. As the obligation to place products on the market without known exploitable vulnerabilities is a risk-based obligation, it falls upon the manufacturer to determine whether, on the basis of the cybersecurity risk assessment, the product can be securely placed on the market, in compliance with the CRA. Alternatively, the manufacturer may determine that a new vulnerability that may have become known needs to be fixed before the product can be placed on the market. In making that determination, manufacturers should take into account the severity, exploitability and potential impact

of the vulnerability, as well as the risks arising for the product itself once in use. In any case, once a product is placed on the market, the manufacturer remains subject to the obligation to handle vulnerabilities effectively and in accordance with the vulnerability handling requirements set out in Part II of Annex I.

9.3 Interplay with other legislation

9.3.1 Regulation (EU) 2019/2144 and Regulation (EU) No 168/2013

216. Point (c) of Article 2(2) of the CRA establishes that the Regulation does not apply to products to which Regulation (EU) 2019/2144 applies. Regulation (EU) 2019/2144 applies to 'vehicles of categories M, N and O, as defined in Article 4 of Regulation (EU) 2018/858, and to systems, components and separate technical units designed and constructed for such vehicles'.

217. Similarly, products with digital elements falling within the scope of Regulation (EU) No 168/2013 have been excluded from the scope of the CRA by Commission Delegated Regulation (EU) 2025/1535. Regulation (EU) 168/2013 applies to L-category vehicles and 'to systems, components and separate technical units, as well as parts and equipment, designed and constructed for such vehicles' (Article 2(1)).

218. Vehicles to which those Regulations apply are not subject to the CRA. Furthermore, additional clarifications are necessary as regards the scope of the exemption for systems, components, separate technical units, parts and equipment (for the sake of this section, 'components') designed and constructed for such vehicles that are deemed to be products within the meaning of the CRA.

219. It is considered that such components are not subject to the CRA, provided that they are exclusively designed and constructed for integration into vehicles covered by Regulations (EU) 2019/2144 and No 168/2013. This is the case regardless of whether the manufacturer of that component sells it directly to the vehicle manufacturer or to another economic operator in the automotive supply chain, as long as the component is clearly intended and suitable only for ultimate integration within those vehicles.

220. By contrast, a manufacturer that sells generic components that are products with digital elements that can be integrated into different types of product, and not exclusively into vehicles covered by those Regulations, is subject to the CRA.

221. The assessment of whether a component is placed on the market within the meaning of the CRA must be based on the objective conditions under which it is made available. Where a manufacturer offers a component that is not exclusively suitable for ultimate integration within those vehicles through distribution channels that are open to customers outside the automotive supply chain, such as general retail outlets or online sales channels accepting orders from the general public, that component falls within the scope of the CRA, irrespective of any statements concerning its intended use. In such circumstances, the component cannot be considered as being designed and constructed exclusively for integration into vehicles covered by Regulations (EU) 2019/2144 and No 168/2013, and the manufacturer is required to comply with the CRA. By contrast, the use

of restricted, business-to-business distribution channels limited to the automotive supply chain may indicate that it is designed and constructed exclusively for such integration.

9.3.2 Validity of EU type-examination certificates (Article 69(1))

222. Article 69(1) of the CRA states that 'EU type-examination certificates and approval decisions issued regarding cybersecurity requirements for products with digital elements that are subject to Union harmonisation legislation other than this Regulation shall remain valid until 11 June 2028, unless they expire before that date, or unless otherwise specified in such other Union harmonisation legislation, in which case they shall remain valid as referred to in that legislation'.

223. The continued validity of such certificates and approval decisions should be understood as being limited to the cybersecurity risks and corresponding requirements that are covered by the respective Union harmonisation legislation on the basis of which they were issued. For those risks, manufacturers are not required to reassess or re-demonstrate compliance solely for the purposes of the CRA during the period of validity referred to in Article 69(1) for products they intend to place on the market on or after 11 December 2027 and until 11 June 2028.[25] This is the case for certificates and approval decisions issued where the applicable Union harmonisation legislation requires the manufacturer to perform the conformity assessment procedure via a notified body, as well as where the manufacturer has voluntarily chosen to do so.

224. Accordingly, the existence of a valid certificate or approval decision under other Union harmonisation legislation does not exempt manufacturers from carrying out a comprehensive cybersecurity risk assessment under the CRA (or from other obligations under it). Instead, it allows them to rely on existing certifications as evidence of compliance for their conformity assessment procedure, to the extent that the corresponding cybersecurity risks are already covered. Where the certificate or approval decision has validity under other Union harmonisation legislation extending beyond 11 June 2028, the manufacturer may nonetheless rely on such certificate or decision for the purposes of the CRA only until 11 June 2028.

225. Where the cybersecurity risk assessment carried out in accordance with Article 13(2) identifies additional risks not covered by the cybersecurity requirements underpinning the existing certificate or approval decision, manufacturers remain responsible for addressing those risks in accordance with the CRA. In such cases, compliance requires that the identified gaps be assessed and mitigated, irrespective of the continued validity of the existing certificate or approval decision.

226. This can be illustrated by considering the case where a product is subject to the cybersecurity requirements laid down in Commission Delegated Regulation (EU) 2022/30 supplementing Directive 2014/53/EU (the Radio Equipment Directive (RED) Delegated

[25] Products placed on the market before 11 December 2027 are subject to Union legislation applicable at the time of their placing on the market and, if they were compliant, they can be sold and put into operation, unless they are, on or after 11 December 2027, subjected to substantial modifications. For the concept of 'placing on the market' and 'making available on the market', see also Section *2.1 Placing on the market* of this document as well as Chapter 2 of the Blue Guide.

Act), and where an EU type-examination certificate or approval decision has been issued on the basis of those requirements. In that case, the certificate or decision remains valid, in accordance with Article 69(1), for the cybersecurity risks that are covered by that certificate and related to the cybersecurity essential requirements of Directive 2014/53/EU (the Radio Equipment Directive, or 'RED').

227. In such cases, manufacturers are not required, for the purposes of the CRA, to reassess or re-demonstrate compliance in respect of those risks already addressed by those certificates, for as long as the relevant certificate or approval decision remains valid and, in any event, not beyond 11 June 2028. This includes, for example, cybersecurity risks related to network protection, protection of personal data and privacy or prevention of fraud (to the extent that those risks are covered by that certificate) related to the RED cybersecurity requirements and reflected in the conformity assessment.

228. However, where the cybersecurity risk assessment carried out in accordance with Article 13(2) of the CRA identifies additional cybersecurity risks not covered by those certificates, manufacturers remain responsible for addressing those risks in accordance with the CRA. This may include, for example, risks related to vulnerability handling processes, data minimisation, and reduction of the attack surface, or other product-specific cybersecurity aspects not addressed by those certificates or, in any case, not covered by the RED cybersecurity essential requirements.

229. Accordingly, the existence of a valid EU type-examination certificate or approval decision under the RED for its essential requirements relating to cybersecurity does not, in itself, demonstrate full compliance with the CRA. Instead, it allows manufacturers to rely on that certificate or decision as evidence of compliance for the corresponding risks, while ensuring that any remaining or newly identified risks are assessed and mitigated in accordance with the CRA.

230. Similarly, where a product is subject to the cybersecurity-related essential health and safety requirements laid down in Regulation (EU) 2023/1230 (the Machinery Regulation), fully applicable as of 20 January 2027, and where an EU type-examination certificate or approval decision has been issued on the basis of those requirements, that certificate or approval decision remains valid, in accordance with Article 69(1) of the CRA, for the cybersecurity risks covered by the Machinery Regulation.

231. In particular, this concerns cybersecurity aspects related to the protection against corruption and the safety and reliability of control systems, as set out in Sections 1.1.9 and 1.2.1 of Annex III to the Machinery Regulation. For those risks, manufacturers are not required, for the purposes of the CRA, to reassess or re-demonstrate compliance for as long as the relevant certificate or approval decision remains valid and, in any event, not beyond 11 June 2028. This applies insofar as those risks have been addressed as part of the conformity assessment under the Machinery Regulation.

232. As with the RED cybersecurity essential requirements mentioned above, where the cybersecurity risk assessment carried out pursuant to Article 13(2) of the CRA identifies additional cybersecurity risks that are not covered by the relevant certificate issued pursuant to the Machinery Regulation and that are related to the cyber-safety

requirements of that Regulation, manufacturers remain responsible for addressing those risks in accordance with the CRA.