EUROPEAN
COMMISSION

Brussels, 27.7.2026
C(2026) 5252 final

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 4

1.1 The Cyber Resilience Act 4

1.2 Purpose of the guidance 4

2 Scope 6

2.1 Placing on the market 6

2.2 Software as a product with digital elements 8

2.3 Computer code 9

2.4 Combination of hardware and software forming a product with digital elements 10

2.5 Data connection 11

2.6 Complex systems 11

2.7 Products with digital elements designed before the CRA entered into application 13

3 Free and open-source software 16

3.1 Determining if free and open-source software is under one's responsibility 17

3.2 Determining if free and open-source software is placed on the EU market 18

3.2.1 Charging a price 18

3.2.2 Monetisation of other services or requiring the processing of personal data 19

3.2.3 Support services 20

3.2.4 Donations 21

3.2.5 Financing of free and open-source software 22

3.2.6 Not-for-profit entities set up to achieve not-for-profit objectives 22

3.2.7 Integration by other manufacturers 23

3.3 Open-source software stewards 23

3.3.1 Sustained support and ensuring viability of FOSS 24

3.4 Contributors and downstream uses 26

3.5 Illustrative scenarios 27

4 Substantial modifications and spare parts 30

4.1 Physical repairs 30

4.2 Spare parts 31

4.3 Software updates as substantial modifications 34

4.4 Consequences of a substantial modification 38

4.4.1 Substantial modifications carried out by a person other than the original manufacturer 39

4.4.2 Substantial modifications carried out by the original manufacturer 40

5 Support period 42

5.1 Substantial modifications and the support period 44
6 Important and critical products with digital elements 47
6.1 Core functionality 47
6.2 Conformity assessment for important and critical products with digital elements 52
6.3 Implications for presumption of conformity 54
7 Cybersecurity risk assessment and integration of products with digital elements and components 57
7.1 On the evaluation and treatment of cybersecurity risks 57
7.2 On designing, developing and producing products with digital elements in such a way that they ensure an appropriate level of cybersecurity based on the risks 58
7.3 Risk assessment and due diligence in relation to external dependencies and integrated components 59
7.4 Reuse of risk assessments and conformity documentation for families of products with digital elements 61
8 Remote data processing 63
8.1 What is considered a remote data processing solution for a product with digital elements? 64
8.1.1 The notion of 'at a distance' 64
8.1.2 Would the absence of such data processing prevent the product with digital elements from performing one of its functions? 65
8.1.3 Has the software been designed and developed by the manufacturer, or under its responsibility? 66
8.2 Practical and technical implications of remote data processing solutions and reliance on third-party solutions 68
8.3 Use cases for remote data processing solutions 70
8.3.1 Mobile banking application 70
8.3.2 Smart thermostat 72
8.3.3 e-Reader 72
8.3.4 Industrial robot 73
8.3.5 Cellular network 73
9 Additional elements 74
9.1 Reporting obligations 74
9.2 Vulnerability handling 77
9.2.1 Reporting upstream and sharing security fixes 77
9.2.2 Known exploitable vulnerabilities 78
9.2.3 Effective and regular tests and reviews 80
9.3 Interplay with other legislation 80
9.3.1 Regulation (EU) 2019/2144 and Regulation (EU) No 168/2013 80

9.3.2 Validity of EU type-examination certificates (Article 69(1)) 81

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 the lifecycle of a product with digital elements.

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'.

[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

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].

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 through a public consultation held between 3 March and 13 April 2026[5].

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. Furthermore, the guidance contains a number of examples to illustrate the application of specific provisions. However, these examples are not intended to replace a case-by-case assessment, which 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).

[3] The FAQs can be downloaded via the Commission's CRA implementation website, from the dedicated FAQs webpage.
[4] Expert Group on Cybersecurity of products with digital elements in the register of Commission expert groups and other similar entities.
[5] Public consultation on draft Commission guidance on the Cyber Resilience Act.

2 Scope

2.1 Placing on the market

10. The CRA applies to products with digital elements 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 with digital elements 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')[6], 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 with digital elements covered by the NLF, such as hardware in the form of machinery or radio equipment products with digital elements, 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 with digital elements such as standalone software, further guidance is needed on when such products with digital elements are considered placed on the market. Once the software's manufacturing phase is complete and the product with digital elements is offered to prospective users in the EU market, its manufacturer can be regarded as having manufactured multiple copies of the same software product with digital elements and having supplied them for distribution or use. In fact, unlike tangible products with digital elements, standalone software is not subject to physical production or stock limitations: each act of making the software available for download or distribution 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 EU 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 distribution of this version of the software product with digital elements is therefore

[6] 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.

to be regarded as an instance where this software product with digital elements is made available[7].

14. Therefore, a standalone software product with digital elements 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 multiple copies of the same software product with digital elements at the same time. Therefore, while multiple copies of the same software remain individual products with digital elements, 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. At the same time, where the manufacturer makes software available in different variants that differ in their included components, configurations or enabled functionalities (for example, builds for different operating systems or bundles with differing feature sets), those variants cannot be regarded as multiple copies of the same software product with digital elements. Therefore, they should be treated as distinct products with digital elements for the purposes of placing on the market.

    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 with digital elements are considered as newly placed on the market when those iterations qualify as a 'substantial modification' of a software product with digital elements 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 with digital elements is standalone software. This is not the case, for

[7] In accordance with Article 13(11), manufacturers may maintain public software archives enhancing user access to historical versions. In such cases, users shall be informed clearly and in an easily accessible manner about risks associated with using unsupported software.

example, when the software is combined with hardware, as discussed in Section *2.4 Combination of hardware and software forming a product*.

2.2 Software as a product with digital elements

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 with digital elements 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.

18. The CRA therefore can cover a range of products with digital elements, including: (i) standalone software, such as apps and computer programs, whether digitally or physically distributed; (ii) hardware with embedded software (e.g. Internet-of-Things devices, laptops, tablets); (iii) standalone hardware (e.g. integrated circuits, motherboards); and (iv) any combination of hardware and software supplied separately but intended to operate together.

19. Standalone software therefore falls in scope of the CRA where it is placed on the market as a product with digital elements. It is helpful to distinguish between software products with digital elements that are subject to the CRA and the remote provision of services that do not fall in scope of the CRA.

20. For software to fall within the scope of the CRA, a software product with digital elements must be provided to a user, obtained by that user and operated on, or as part of, an electronic information system on the user's side. Software that is downloaded, installed or otherwise supplied to the user and that executes on the user's electronic information system meets these criteria, including for example where it takes the form of a browser extension or an application developed using web technologies but supplied for local execution.

21. By contrast, software that executes remotely and is merely accessed by the user is not, on that basis alone, a product with digital elements. Recitals 11 and 12 of the CRA, in fact, draw this distinction, by explaining that processing or storage at a distance is subject to the CRA only to the extent that it is necessary for a product with digital elements to perform its functions (i.e. through the concept of remote data processing as defined in Article 3(2)), and not themselves as products with digital elements. This is typically the case for web applications, including progressive web apps, where they are accessed exclusively through a web browser. The same applies to websites: whilst websites may, to a limited extent, technically run and execute on the user's device, it follows from recital 12 of the CRA that websites are not themselves to be considered as products with digital elements, and fall within the scope of the CRA only where they support the functionality of a product with digital elements, i.e. to the extent that they qualify as remote data processing (as further explained in Section *8* and notably *8.1.2 Would the absence of such data processing prevent the product with digital elements from performing one of its functions?)*.

Example 3: a mobile application that a user downloads from an app store and installs on their smartphone is supplied to the user and executes on the user's device and is therefore a product with digital elements. Where it is placed on the market in the course of a commercial activity, it may fall within the scope of the CRA.

Example 4: a desktop application built using web technologies but packaged for local installation is supplied to the user and executes on the user's device, and is therefore a product with digital elements. Where it is placed on the market in the course of a commercial activity, it may fall within the scope of the CRA.

Example 5: a web application accessed by the user exclusively through a web browser is not a product with digital elements. Unless it supports the functionality of a product with digital elements, it does not fall within the scope of the CRA. By contrast, an application supplied to the user as a locally installed client that executes on the user's device is a product with digital elements. Where it is placed on the market in the course of a commercial activity, it may fall within the scope of the CRA. If that client relies, in order to perform one or more of its functions, on data processing at a distance which meets the definition of remote data processing, that data processing at a distance is also part of the product with digital elements.

Example 6: a website that merely presents information to its visitors and does not support the functionality of a product with digital elements is not itself a product with digital elements. It therefore does not fall within the scope of the CRA.

2.3 Computer code

22. It is also useful to clarify whether source code can constitute a software product with digital elements. The CRA defines software as 'the part of an electronic information system which consists of computer code' (Article 3(4)). Computer code can take the form of (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. The definition of software laid down in the CRA covers both.

23. A separate question is whether a given supply of computer code amounts to placing a product with digital elements on the EU market, which requires a supply in the course of a commercial activity. This may often not be the case for source code. For example, a natural or legal person that shares free and open-source computer code on publicly accessible repositories is generally not considered to be placing that code on the EU market for the purposes of the CRA (as discussed in more detail in Section *3 Free and open-source software*). Unfinished code shared during the design and development phase of a product with digital elements (e.g. for testing or review) is also not considered to be placed on the market for the purposes of the CRA, 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 for the purposes of the CRA[8].

24. On the other hand, where a manufacturer provides its customers with computer code as a product with digital elements, that code is considered to be placed on the market, regardless of whether it is machine code or source code[9].

Example 7: 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 placing that source code on the market and is therefore subject to the CRA. Company A is not responsible for the compliance with the CRA of company B's subsequent adaptations and compilation of that code.

2.4 Combination of hardware and software forming a product with digital elements

25. Whether software forms part of a product with digital elements 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 with digital elements to perform its intended functions. Where a hardware product with digital elements is designed to work together with a specific software provided by the same manufacturer in order to perform its functions, the hardware and that software together constitute the product with digital elements. Software that is necessary to operate, configure, control or use a product with digital elements in accordance with its intended purpose is therefore part of the product with digital elements, even if it is obtained through a separate channel (e.g. an app store, a download link or another digital channel after the hardware product with digital elements has been placed on the market). Its placing on the market thus occurs at the same point in time as units of the hardware products with digital elements are placed on the market.

Example 8: A network printer is placed on the market as a hardware product with digital elements, 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.

[8] 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.

[9] 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.

Example 9: 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 through an app store, the wearable and the application together constitute a single product with digital elements, because they are designed and intended to operate together to deliver the functionality of the product with digital elements.

2.5 Data connection

26. 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 scope of the CRA is therefore anchored not in the mere presence of electronics, but in the capacity of a product with digital elements to exchange digital information.

27. 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 with digital elements that merely use electrical signals from those that participate in digital communication and are therefore exposed to cybersecurity risks.

28. 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 and therefore the product with digital elements does not fall within the scope of Article 2(1).

2.6 Complex systems

29. Products with digital elements within the scope 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 with digital elements, it constitutes a product with digital elements within the meaning of the CRA.

30. 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, to be placed on the market after the CRA enters into application, 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.

31. 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 characteristics and constraints of the product with digital elements, in accordance with Article 13(3) of the CRA. Those characteristics form part of its intended purpose and operating context and are therefore relevant when assessing compliance with the essential cybersecurity requirements (the 'essential requirements'). In particular, recital 55 explicitly recognises that certain essential requirements may not be fully compatible with the nature of a product with digital elements. For example, this may be the case where compliance would undermine mandatory interoperability requirements or the system's proper functioning.

32. 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 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 with digital elements 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 security of the product with digital elements. 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 constraints can be lifted or reduced over time, manufacturers should update the product with digital elements accordingly so that it can move towards an appropriate level of cybersecurity[10].

Example 10: A manufacturer places on the market a product with digital elements that communicates with external systems using a network protocol. As part of the application of the essential requirements, the manufacturer determines, on the basis

[10] It should be noted that the considerations laid down in this paragraph may be applicable, as appropriate, to all products with digital elements in scope of the CRA, and not just 'complex systems'.

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 with digital elements.
However, its 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 with digital elements 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.

Example 11: A manufacturer of an industrial automation system purchases some microcontrollers before the CRA enters into application. The manufacturer undertakes the cybersecurity risk assessment for its industrial automation system to be placed on the market after the CRA enters into application. On the basis of that cybersecurity risk assessment, the manufacturer does not identify specific cybersecurity risks associated with using one of those microcontrollers. The manufacturer integrates it into its industrial automation system and ensures that the product with digital elements as a whole (the industrial automation system) meets the essential requirements.

2.7 Products with digital elements designed before the CRA entered into application

33. In some cases, a manufacturer will place on the market, after the CRA enters into application on 11 December 2027, units of a product with digital elements 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 those units of the product with digital elements 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, on the basis of the intended purpose and reasonably foreseeable use of the product with digital elements, which of the essential requirements set out in Part I of Annex I are applicable to that product with digital elements, and how those requirements are implemented.

34. Where the outcome of that risk assessment demonstrates that the product with digital elements 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 with digital elements where this is not necessary to address the identified risks.

35. Nevertheless, the manufacturer remains subject to the obligations laid down in the CRA. These include making sure, before the product with digital elements 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 design of the product with digital elements required modification as a result of the risk assessment. For products with digital elements designed before the date of application of the CRA, but placed on the market after that date, 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 with digital elements, 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 with digital elements 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.

36. Accordingly, products with digital elements 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 with digital elements achieves an appropriate level of cybersecurity in light of its intended purpose and reasonably foreseeable use and complies with the cybersecurity essential requirements.

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

38. However, the application of such requirements needs to be interpreted in light of the cybersecurity risk assessment and the cybersecurity risk profile of the product with digital elements. Particularly in the case of products with digital elements designed before the date of application of the CRA (but placed on the market after that date) and subject to the conformity assessment procedures of Article 32(1), where the risk assessment demonstrates that the product with digital elements 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 with digital elements. This would not be necessary as it would not be contributing to increasing the security of the product with digital elements 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 families of products with digital elements, as further discussed in Section *7.4 Reuse of risk assessments and conformity documentation for families of products with digital elements*.

39. 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 12: 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 with digital elements, including products with digital elements 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 with digital elements meets the relevant essential 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 with digital elements. Where several variants of the microcontroller are based on the same design and share the same cybersecurity 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 requirements.

3 Free and open-source software

40. As recalled in Section *2.1 Placing on the market*, the CRA applies to products with digital elements that are made available on the EU market in the course of a commercial activity for the first time (i.e. 'placed on the market'), as well as to any subsequent instance that constitutes making that same product with digital elements 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 characteristics of the product, the intentions of the supplier, etc.

41. 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)[11].

42. 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 with digital elements 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'.

43. 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-

[11] It should also be recalled that, while often products with digital elements 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.

source software steward' (henceforth, 'steward') under Article 3(14). In that case, it is subject only to the obligations laid down in Article 24.

44. 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.

45. 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.

46. However, Article 3(48) goes beyond referring only to the licence terms, as it expressly requires that the source code 'is openly shared'. The notion of 'openly shared' indicates that the source code must be made publicly available (either 'upstream' or 'downstream'), 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.

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

47. The CRA places key responsibilities on economic operators that supply products with digital elements in the EU market. It defines the manufacturer as the natural or legal person that supplies a product with digital elements 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 with digital elements 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[12], but does not place it on the market within the meaning of the CRA.

48. 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 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.

49. 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 that the FOSS is under that person's responsibility; responsibility lies with those who publish and control the FOSS.

Example 13: An individual developer or an employee of a company submits a 'pull' or 'merge' request containing a security patch or a new feature to a FOSS project. The project's maintainers review, accept and merge the code into the main repository, subsequently including it in a new release. In this scenario, the person who submitted the pull request is a 'contributor' and is not subject to the CRA. Although that person contributed source code, they do not exercise primary control over the development, releases or distribution decisions.

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

50. Once it is established 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

51. Where the natural or legal person that supplies a FOSS charges a price for the software itself (e.g. by charging a price for the pre-compiled binaries), that person is placing a product with digital elements on the market. The person that places a FOSS on the market is therefore a manufacturer under the CRA.

[12] 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.

52. 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 with digital elements, 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 manufacturer's obligations. The version provided for free (or community version) is not monetised and therefore is not considered to be placed on the market for the purposes of the CRA. This is also the case where the paid version is an 'enhanced' commercial version, which extends the codebase of the version provided for free, or incorporates that version into a broader product with digital elements (e.g. as in the case of the 'open-core' model).

53. 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

54. 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 with digital elements 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 14: A natural or legal person publishes a free and open-source marketplace application. The application is available free of charge and enables users to purchase goods or services through it. The app allows the person that published it to monetise other products with digital elements and services offered through it (e.g. through advertisements, commission fees or subscription fees). Therefore, the application is considered placed on the market in the course of a commercial activity.

Example 15: 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 16: 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

55. The mere fact that a natural or legal person publishing a FOSS also offers paid support services related to it does not, as such, mean that the product with digital elements is supplied in the course of a commercial activity. Support services may include activities such as consultancy, training or professional services related to the use, documentation, configuration and deployment of the software by a customer.

56. The decisive factor is whether access to the FOSS itself (i.e. the provision of the product with digital elements), including its maintenance, is conditioned on remuneration, rather than the mere offering of professional services around a freely available product with digital elements, 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 professional services separately, that FOSS is not considered to be placed on the market.

57. By contrast, in some cases access to a specific version of the product with digital elements 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 with digital elements 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 17: 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 paid version of the operating system is considered placed on the market in the course of a commercial activity.

Example 18: 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 professional services, such as 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.

58. Particularly in the case of natural persons publishing FOSS, offering technical assistance directly bundled with access to the product with digital elements 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 assistance 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.

59. A natural or legal person offering technical assistance related to a FOSS not under its responsibility is not considered 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 assistance.

Example 19: 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 considered to be placing the FOSS on the market.

3.2.4 Donations

60. 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.

61. 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 with digital elements. 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 considered to be placed on the market. A FOSS supported only through donations is therefore unlikely to be considered to be placed on the market within the meaning of the CRA.

Example 20: 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 considered to be supplied in the course of a commercial activity and is not considered to be placed on the market within the meaning of the CRA.

62. Nonetheless, there are instances where a FOSS supported through donations may be considered 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 with digital elements or certain of its functionalities. This may be the case, in particular, where access to the FOSS, to essential functionalities or to updates is conditioned in practice on making a donation, or where donations are associated with contractual benefits or exclusive advantages that go beyond community perks.

Example 21: A natural or legal person publishes a software product with digital elements 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 with digital elements and therefore amount to charging a price. That FOSS is therefore considered to be placed on the market within the meaning of the CRA.

Example 22: 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 with digital elements and constitute remuneration for that product's supply. That FOSS is therefore considered to be placed on the market in the course of a commercial activity.

3.2.5 Financing of free and open-source software

63. 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.

64. As already recalled, recital 18 of the CRA, clarifies that 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 nature of that activity.

65. 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 with digital elements, that company is to exercise due diligence in accordance with Article 13(5) of the CRA.

Example 23: 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 codebase, openly sharing it and making it freely available for all to access, use, modify and redistribute. The individual developer is not considered to have placed that FOSS on the market. If the manufacturer integrates the FOSS into its product with digital elements, it needs to exercise due diligence in accordance with Article 13(5).

3.2.6 Not-for-profit entities set up to achieve not-for-profit objectives

66. 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 24: 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 considered to be placed on the market within the meaning of the CRA. The legal person publishing it is subject to the obligations applicable to stewards.

3.2.7 Integration by other manufacturers

67. 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.

68. 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 25: A legal person publishes a FOSS library for building user interfaces. It does not monetise the supply of that library, but integrates it into one of its products with digital elements (which is in turn placed on the market). The library is not considered placed on the market within the meaning of the CRA, but it is intended for integration into products with digital elements. The legal person that publishes it is its steward.

Example 26: 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, which are intended for integration into other products with digital elements. The legal person that publishes them is a steward to those FOSS libraries.

3.3 Open-source software stewards

69. 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).

70. 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.

71. 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 with digital elements 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[13]) 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.

72. 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*.

73. 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.

74. 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 considered to be 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[14].

3.3.1 Sustained support and ensuring viability of FOSS

75. Recital 19 explains that the provision of sustained support to the development of a product with digital elements may include (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 with digital elements qualifying as FOSS; and (iv) steering the development of such products with digital elements.

76. This may be the case, for example, for a legal entity that develops FOSS for integration into its own products with digital elements 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.

[13] 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.

[14] 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.

77. 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 placed 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.

78. 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.

79. 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).

80. For example, a steward that only provides non-technical support is, by definition, not involved in development of the product with digital elements, 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 with digital elements, 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 maintainers of the product with digital elements, in accordance with its cybersecurity policy. The maintainers of the products with digital elements and/or the stewards should also consider reporting the vulnerability on a voluntary basis, in accordance with Article 15.

81. On the other hand, where a steward provides the underlying IT infrastructure for certain products with digital elements, it is required to notify ENISA and the CSIRTs, in accordance with Article 14(3) of any severe incidents related to that infrastructure

that have an impact on the security of products with digital elements. 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.

82. Finally, where a steward also provides engineering resources to specific products with digital elements, 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).

83. Where an entity ceases to provide systematic support on a sustained basis for a specific FOSS, it may no longer meet the definition of steward and may therefore no longer be subject to the corresponding obligations. In such cases, that entity is encouraged to communicate clearly the change in its status for that specific FOSS.

84. In certain situations, an entity that was a steward to a specific project may decide to monetise that project directly, thereby placing the product with digital elements on the market and triggering the manufacturer's obligations under the CRA. In such circumstances, that entity qualifies as the manufacturer of the product with digital elements from the date on which it places it on the market (but not in respect of earlier versions for which it acted as a steward).

3.4 Contributors and downstream uses

85. 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).

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

87. Similarly, the mere fact that manufacturers integrate FOSS components into their own (monetised) products with digital elements has no impact on the status of that FOSS component under the CRA. Maintainers of FOSS components that are not placed on the market do not bear obligations in relation to other entities that may integrate such components into their products with digital elements. Whether the CRA applies to a given FOSS component depends solely on whether the natural or legal person that publishes it places it on the market.

88. 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 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

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

Example 27: 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 with digital elements. 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 within the meaning of the CRA. 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 28: Not-for-profit foundation F publishes a FOSS component for integration into other commercial products with digital elements. 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 considered to be placed on the market within the meaning of the CRA. 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 with digital elements.

Example 29: 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 considered to be placed on the market within the meaning of the CRA. 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 with digital elements.

Example 30: 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 considered a manufacturer to that FOSS[15]. 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).

Example 31: 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 with digital elements, 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 32: 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 with digital elements. Such features are incorporated into the FOSS's codebase.
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 33: 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 with digital elements.
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 with digital elements, they need to exercise due diligence in accordance with Article 13(5).

[15] 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 34: 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).

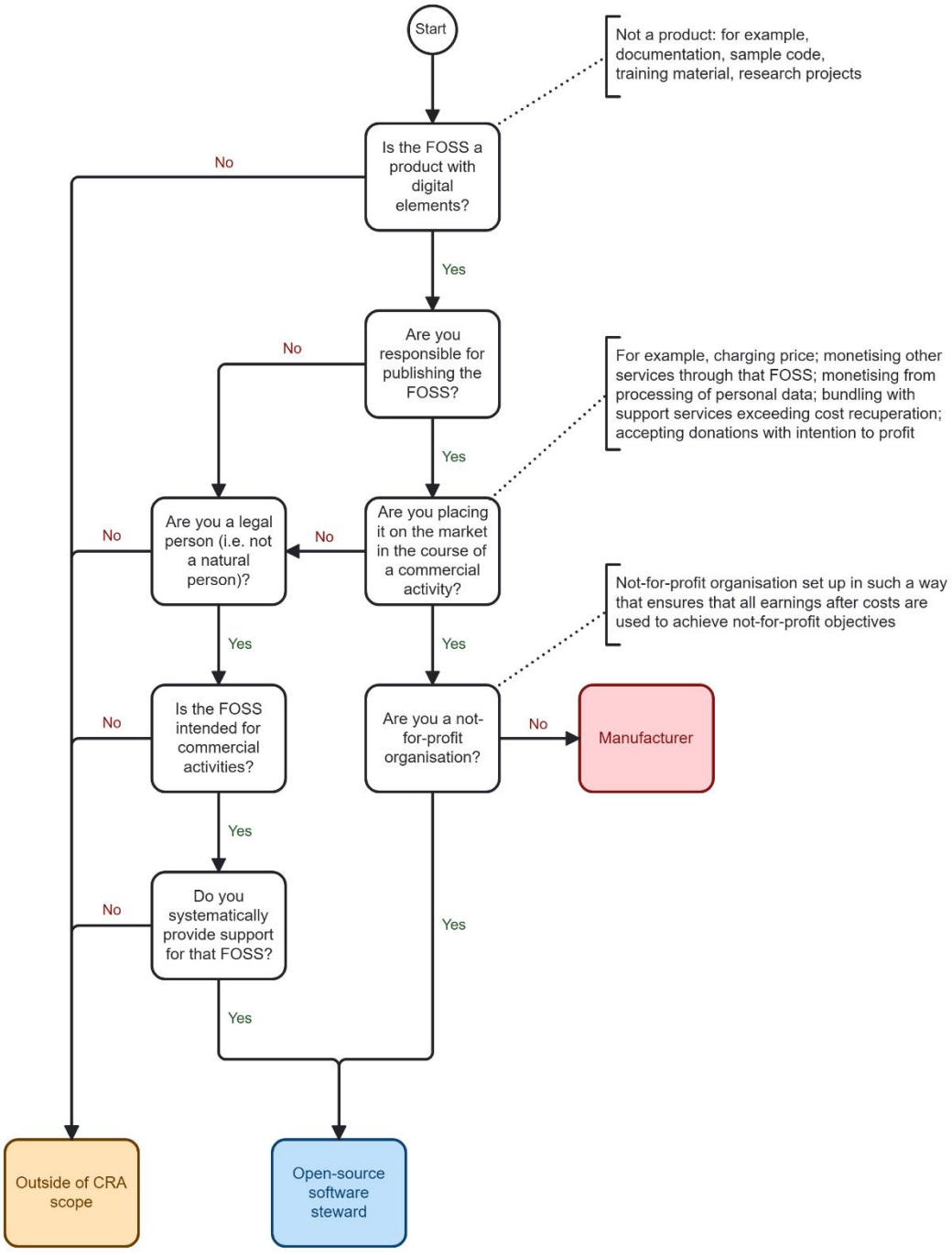

Figure 1: Stylised flowchart for CRA coverage of free and open-source software

4 Substantial modifications and spare parts

90. 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 compliance of the product with digital elements with the essential requirements set out in Part I of Annex I; or (ii) results in a modification to the intended purpose for which the product with digital elements has been assessed.

91. 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 with digital elements 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 with digital elements 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 with digital elements 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 with digital elements placed on the market after 11 December 2027, in order to determine whether a product with digital elements 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.

92. 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

93. 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'.

94. Operations of refurbishment, maintenance or repair which result in physical modifications of products with digital elements 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 compliance of the product with digital elements 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.

95. 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 with digital elements. It only does so if the performance change or the way the repaired product with digital elements operates (i) affects its compliance with the essential requirements or (ii) results in a change to the intended purpose that was not covered by the risk assessment.

Example 35: 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.

4.2 Spare parts

96. 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 with digital elements 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.

97. The exemption in Article 2(6) of the CRA should be understood as applying only where the spare part is specifically supplied to repair or extend the durability of a product with digital elements already placed on the market (before or after 11 December 2027). Where a product with digital elements is supplied as a standalone product, without any connection to the maintenance or repair of a pre-existing product with digital elements, it is placed on the market within the meaning of the CRA and should not be considered a spare part falling within the scope of Article 2(6). The maintenance or repair purpose should be apparent from the context of the supply, for example through identification of the product with digital elements or product family in the order or commercial offer, or through supply via after-sales or service channels. Supporting evidence to that effect should also be kept available to market

surveillance authorities. The fact that a product with digital elements could technically be used to replace a component is not, in itself, sufficient to bring it within the scope of the exemption in the absence of such elements.

98. Accordingly, where a spare part is identical to a component already included in a product with digital elements 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.

99. The assessment of whether a spare part should be considered identical to a component should focus on its functional role in the product with digital elements and the characteristics that may be relevant to cybersecurity. While a case-by-case assessment is always needed, differences that do not affect the security characteristics or the cybersecurity risk profile of the component do not, in themselves, prevent that spare part from falling within the scope of Article 2(6) of the CRA.

100. By contrast, differences in characteristics relevant to the cybersecurity of the component, such as algorithms, protocols, cryptographic mechanisms, access control features or other security-relevant characteristics, may mean that the new part cannot be considered identical to the component it is intended to replace.

101. Where a spare part is not identical to the original component, that spare part constitutes a product with digital elements in its own right and is therefore subject to the CRA. In such cases, compliance with the essential requirements must be assessed in light of the replacement component's intended purpose. Of particular relevance is the replacement component's function of ensuring compatibility or interoperability with an existing product with digital elements, including where that product is a product with digital elements 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 security of the product with digital elements. As also discussed in Section *2.6 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. 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 with digital elements.

Example 36: A manufacturer has placed connected controllers on the EU market. In one case, the controller was placed on the market in 2026, before the date of application of the CRA. In another case, the controller was placed on the market in 2028, in compliance with the CRA. In 2028, a digital communication module in both types of controllers fails. The manufacturer supplies as a spare part a replacement module that is identical and manufactured according to the same specifications as the original.

In both cases, 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 with digital elements. The repair does not constitute a substantial modification of the product with digital elements.

Example 37: 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 as a spare part a newer chip with equivalent functionality, but with a different cryptographic implementation and updated secure boot mechanism, in order to maintain compatibility and continued operation.
In this case, the replacement chip cannot be considered identical, as the differences in the cryptographic implementation and secure boot mechanism affect the chip's cybersecurity properties. It therefore does not benefit from the exemption in Article 2(6) and 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 product with digital elements placed on the market before the CRA entered into application.

Example 38: 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 as a spare part a new module that performs the same function using the same communication protocols and security mechanisms, but is based on a different chipset and has updated firmware that does not alter characteristics that may be relevant to cybersecurity.
In this case, the replacement module can be considered identical. The module therefore benefits from the exemption in Article 2(6) and is not subject to the CRA.

102. The exemption for spare parts applies regardless of whether the spare part replaces a component within a product with digital elements or whether it replaces a complete product with digital elements that itself forms part of a larger product, including where that larger product with digital elements is composed of several integrated components, provided that the replacement part is specifically supplied as a spare part, as explained in the preceding paragraphs.

Example 39: In 2027, a manufacturer places on the market an industrial automation system that incorporates a programmable logic controller (PLC) as one of its components. In 2031, the PLC's central processing unit (CPU) fails. The manufacturer offers two repair options: (i) the supply of a replacement CPU unit, which can be considered identical to the CPU originally installed; or (ii) the supply of a complete replacement PLC, which can be considered identical to the PLC originally installed. In each case, the replacement is supplied through the manufacturer's after-sales service channel as a spare part, and the industrial automation system for which the replacement is intended is clearly identified. In both cases, the replacement falls within the scope of the exemption in Article 2(6), whether the replacement concerns a component within the PLC, or the PLC as a whole.

4.3 Software updates as substantial modifications

103. Software development is iterative in nature, with software products with digital elements 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 with digital elements who make changes to their own products determine whether those changes amount to a substantial modification.

104. Recital 39 indicates that a product with digital elements 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 risk assessment.

105. Where a manufacturer introduces new functionalities in a product with digital elements 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 risk assessment. In such circumstances, the change would generally qualify as a substantial modification.

Example 40: 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 risk assessment, shifting from a situational awareness tool to a product with digital elements intended to exercise operational control over other devices. The dashboard has therefore been substantially modified.

Example 41: 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 risk assessment. The application has therefore been substantially modified.

106. At the same time, however, it is possible that a manufacturer progressively introduces new functionalities already included in its risk assessment or that do not, in themselves, alter the cybersecurity risk profile of the product with digital elements. This may be the case, for example, where 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. This may also be the case where the new functionalities do not implement changes that introduce new or increased risks. Updates of this nature should therefore not be regarded as substantial modifications, as they do not increase the cybersecurity risk and consequently do not change the implementation of the essential requirements.

Example 42: A messaging application is initially released with functionality limited to one-to-one messaging. The manufacturer's 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 43: 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 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.

107. Conversely, even limited or seemingly minor new functionalities may introduce significant cybersecurity risks that 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 adverse impact on the cybersecurity risk profile of the product with digital elements and consequently the implementation of the essential requirements.

Example 44: 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 risk assessment. The update therefore affects compliance with the essential requirements. The software application has been substantially modified.

Example 45: A manufacturer adds a new logging and diagnostics feature to an existing software product with digital elements, 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 cybersecurity risk profile of the

product with digital elements. The software product with digital elements has been substantially modified.

108. 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 with digital elements. A security update that does not modify that product's intended purpose and does not introduce new cybersecurity risks should therefore not be considered a substantial modification, even where that update may introduce significant technical changes. 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 46: A manufacturer deploys a security update to address a vulnerability in the codebase of a product with digital elements 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 that 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 47: 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 with digital elements, it does not alter its intended purpose and serves solely to enhance its security posture. The security update should not be considered a substantial modification.

Example 48: A manufacturer places on the market a software product with digital elements that secures communications using a configurable encryption framework supporting multiple cryptographic algorithms and key sizes, as described in the product's technical documentation and risk assessment. The risk assessment covers all the cryptographic options provided in the product with digital elements 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 introduce new cybersecurity risks, the security update should not be considered a substantial modification.

109. By contrast, a security update may qualify as a substantial modification where, notwithstanding its security objective, the update results in the intended purpose of the product with digital elements being modified beyond what was originally foreseen or introduces new or increased cybersecurity risks. This may be the case, for

example, where an update materially changes that product's boundaries or dependency structure in a way not foreseen in the risk assessment, e.g. by materially altering data flows, or adding new externally reachable interfaces.

Example 49: A manufacturer places on the market a software product with digital elements 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 with digital elements 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 that product's intended purpose in a manner not foreseen in the risk assessment and therefore qualifies as a substantial modification.

Example 50: A manufacturer places on the market a software product with digital elements that relies on an established encryption protocol and an internally managed key lifecycle to secure communications between components of the product with digital elements. 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 dependencies and data flows of the product with digital elements are materially altered, introducing new external interfaces and reliance on third-party services not considered in the risk assessment. Although the update is security-driven, it introduces new cybersecurity risks, and therefore qualifies as a substantial modification.

110. As stated in point 104 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 with digital elements, 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.

111. 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 risk assessment remain valid and effective. It is therefore likely that the update does not qualify as a substantial modification.

112. 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 cybersecurity risks of the product with digital elements and determine whether the essential requirements continue to be met, including whether the update introduces new or increased risks not foreseen in the risk assessment.

113. 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 91. 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 Part II of Annex I to 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

114. The consequences of a substantial modification carried out by an actor other than the original manufacturer of a product with digital elements already placed on the market are addressed in Articles 21 and 22 of the CRA. Article 21 concerns importers and distributors, while Article 22 concerns any natural or legal person other than the manufacturer, importer or distributor.

115. Where the substantial modification is carried out by the original manufacturer of the product with digital elements, the consequences derive from the generally established concept of substantial modification referred to in recital 41 of the CRA and are further elaborated in Section 2.1 of the Blue Guide. That section states that a product that has been subject to significant changes or an overhaul after being placed on the market is to be considered a new product where its original performance, purpose or type has been modified, the nature of the hazard has changed or the level of risk has increased, and the product with digital elements is made available on the market.

116. The generally established consequence is therefore that, where a modification of a product with digital elements qualifies as a substantial modification and the modified product with digital elements is made available on the market, it is to be treated as a new product with digital elements 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. This applies whether the substantial modification is carried

out by the original manufacturer or by another person. In order to ensure that the CRA is applied in a uniform and proportionate manner across the different categories of actor that may carry out a substantial modification, the following subsections address the resulting obligations of the person carrying out the substantial modification when the substantially modified product with digital elements is placed on the market. The consequences for the support period of the product with digital elements are addressed in Section *5 Support period*.

4.4.1 Substantial modifications carried out by a person other than the original manufacturer

117. In accordance with Articles 21 and 22, where a substantial modification of a product with digital elements already placed on the market is carried out by a natural or legal person other than the manufacturer of the product with digital elements, the person who carries out the substantial modification and makes the modified product with digital elements available on the market is to be regarded as the manufacturer of the modified product with digital elements, irrespective of whether that person was involved in the original design or placing on the market of that product.

118. Article 22 further clarifies that the person carrying out the modification is subject to the obligations laid down in Articles 13 and 14 only in respect of the part of the product with digital elements affected by the substantial modification, where that modification does not have an impact on the cybersecurity of the product with digital elements as a whole.

119. Where a substantial modification affects compliance with the essential requirements but does not negatively affect the cybersecurity of the product with digital elements as a whole, the person carrying out the modification is subject to Articles 13 (including the obligation to ensure compliance with the essential requirements and to carry out a conformity assessment procedure) and 14 (reporting obligations) only in relation to the part of the product with digital elements that has been substantially modified[16] . Furthermore, the original manufacturer's obligations under the CRA continue to apply to the original product with digital elements placed on the market, ensuring continuity in vulnerability handling and compliance for the unchanged parts.

120. A case of substantial modification should not be confused with cases of integration, in which a person assembles components (including, where appropriate, by modifying them) into a new product with digital elements that they themselves place on the market. In such cases, the integrator is not modifying a product with digital elements already placed on the market by another manufacturer; rather, it is placing

[16] In line with Section 2.1 of the Blue Guide, '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'.

a new product with digital elements of its own on the market. The integrator is the manufacturer of that new product with digital elements for the purposes of the CRA and is required to comply with the Regulation in its entirety in respect of the product with digital elements as a whole. Where the manufacturer integrates components that are subject to the CRA, it may rely on the compliance activities of the components' manufacturers to facilitate its own compliance with the CRA.

Example 51: A company purchases off-the-shelf microcontroller modules and connectivity components from third-party suppliers, develops proprietary firmware and a sensor package, and assembles them into a connected agricultural monitoring product with digital elements that it places on the market under its own name. Although the company has modified the underlying microcontroller modules and combined them with other components, it is not substantially modifying a product with digital elements already placed on the market; rather, it is placing a new product with digital elements on the market. The company is the manufacturer of the agricultural monitor for the purposes of the CRA and is required to comply with the Regulation in respect of the agricultural monitor as a whole.

121. Where a substantial modification carried out by a person other than the original manufacturer negatively affects the cybersecurity of the product with digital elements as a whole, for example because the modification is no longer targeted or limited to a specific component or subsystem, the modified product with digital elements made available on the market should be treated as a new product with digital elements subject to the CRA in its entirety. In such cases, that product's overall cybersecurity risk profile has changed, and the modification cannot be assessed without considering the product with digital elements as a whole. The person carrying out the modification is subject to the obligations of a manufacturer laid down in Articles 13 and 14 in respect of the modified product with digital elements as a whole.

4.4.2 Substantial modifications carried out by the original manufacturer

122. Where the substantial modification is carried out by the original manufacturer, including in the context of iterative development of software products with digital elements, that manufacturer remains the manufacturer for the purposes of the CRA. However, the substantially modified product with digital elements is to be considered as newly placed on the market.

123. In accordance with Section 2.1 of the Blue Guide, the original manufacturer placing the substantially modified product with digital elements on the market may reuse existing documentation and tests for aspects of the product with digital elements that are not impacted by the substantial modification. Particularly where the manufacturer places substantially modified versions of the same product with digital elements 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 with digital elements, it may reuse existing documentation and test results.

124. The proportionality considerations set out in the previous subsection apply equally to substantial modifications carried out by the original manufacturer of a product with digital elements placed on the market before 11 December 2027. Such a substantial modification carried out by the original manufacturer does not, in itself, require the manufacturer to bring the entire product with digital elements placed on the market before that date into full compliance with the CRA, unless the modification negatively affects the cybersecurity of the product with digital elements as a whole. Where the modification does not affect the cybersecurity of the product with digital elements as a whole, the original manufacturer's obligations in respect of the modification should be limited to the substantially modified parts.

5 Support period

125. Article 13(8) of the CRA requires manufacturers to determine the support period during which the vulnerabilities of the product with digital elements, including its components, are handled effectively and in accordance with the essential requirements set out in Part II of Annex I. The support period reflects the period of time during which the product with digital elements is expected to be in use (the expected use time), and should be determined in light of the criteria set out in Article 13(8), in particular reasonable user expectations, the nature of the product with digital elements, including its intended purpose, as well as relevant Union law determining the lifetime of products with digital elements[17]. Overall, such criteria are to be taken into account in a manner that ensures proportionality in determining the support period.

126. Article 13(8) further requires that the support period be at least five years, unless the product with digital elements 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 digital elements with genuinely shorter expected use times. Recital 60 provides more guidance in this respect, clarifying that products with digital elements 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 with digital elements. Instead, the manufacturer should determine the appropriate support period in light of the criteria referred to in Article 13(8).

127. 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 with digital elements. This obligation is intended to provide transparency to users as regards the duration for which security support can be expected.

128. In the case of software products with digital elements, 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 substantially modified version of a software product with digital elements 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

[17] Additional criteria that may be taken into account, in accordance with Article 13(8), include the support periods of products with digital elements offering a similar functionality placed on the market by other manufacturers, the availability of the operating environment, the support periods of integrated components that provide core functions and are sourced from third parties as well as relevant guidance provided by the CRA administrative cooperation group (ADCO) and the Commission.

clarified in recital 60. Section *5.1 Substantial modifications and the support period* further clarifies that, where the substantial modification does not lead to changes in the factors that originally determined the expected use time of the product with digital elements, the original support period is unaffected (i.e. including in cases where the remaining support period is less than five years).

129. Article 13(10) provides flexibility for software products with digital elements by allowing manufacturers, under certain conditions, to ensure compliance with the vulnerability handling requirement set out in point (2) of Part II of Annex I (addressing and remediating vulnerabilities) only for the version of the software product with digital elements 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.

130. 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 to 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.

131. For continuously evolving software products with digital elements, 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[18]. The manufacturer remains subject to the other vulnerability-handling requirements of Part II of Annex I, as well as to the reporting obligations of Article 14. As also explained in recital 40, these requirements include, among others, for all subsequent substantially modified versions of the software product with digital elements placed

[18] It should be recalled that Article 13(19) requires manufacturers, where technically feasible in light of the nature of the product with digital elements, to display a notification to users informing them that their product with digital elements 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, if technically feasible.

on the market: (i) maintaining a policy on coordinated vulnerability disclosure; and (ii) measures to facilitate the sharing of information about potential vulnerabilities[19].

Example 52: A manufacturer places a smartphone model on the EU market and declares a support period of X years from the date of placement on the market, during which it will provide security updates addressing vulnerabilities. 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 53: A manufacturer places an enterprise software product with digital elements 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 upgrades 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.

5.1 Substantial modifications and the support period

132. As set out in Section *4.4 Consequences of a substantial modification,* where a modification of a product with digital elements qualifies as a substantial modification and the modified product with digital elements is made available on the market, it is to be treated as a new product for the purposes of the CRA, and the act of making the substantially modified product with digital elements available on the market constitutes a new placing on the market. It is therefore useful to clarify the effect that this new placing on the market has on the support period of the substantially modified product with digital elements.

133. The support period of a substantially modified product with digital elements should be determined by reference to that product's expected use time, in light of the criteria set out in Article 13(8) of the CRA. A substantial modification should therefore require a reassessment against those criteria, but does not automatically result in the

[19] It should be noted that, where users can upgrade to the latest version of the software without additional costs, manufacturers may nevertheless choose to continue addressing and remediating vulnerabilities in earlier versions of that software, including on a paid basis or under other commercial arrangements. The CRA does not require manufacturers to provide security updates for such earlier versions free of charge.

support period being reset, or even extended. The relevant question is whether the substantial modification affects the factors that originally determined that product's expected use time and, therefore, the original support period.

134. Where the substantial modification does not affect those factors, the criteria set out in Article 13(8) continue to indicate the same expected use time as originally determined, and the support period of the modified product with digital elements should align with the remaining expected use time of the product as originally placed on the market. This will typically be the case where the expected use time was determined primarily by factors that the modification does not alter, such as the physical durability of hardware components, where the substantial modification concerns only software functionality or back-end services.

Example *54: A manufacturer places on the market a robot vacuum cleaner with an expected use time of X years, determined on the basis of the nature of the product with digital elements, including the physical durability and wear characteristics of the hardware components, and taking into account reasonable user expectations as to that product's lifetime. The manufacturer sets a support period of X years. After Y years, the manufacturer releases a software update that qualifies as a substantial modification, adding new cleaning modes and navigation features. The software update does not affect the physical durability of the hardware and does not alter reasonable user expectations as to that product's lifetime. The Article 13(8) criteria therefore continue to indicate the same expected use time. The support period of the modified product with digital elements aligns with the remaining expected use time as originally determined.*

Example 55: A manufacturer places on the market a complex industrial machinery product with digital elements, with a cloud back-end that constitutes a remote data processing solution. The expected use time is X years, determined in light of reasonable user expectations and the nature of the product with digital elements, such as the physical durability of the machinery hardware and expected wear and tear. The support period is set to align with that expected use time at X years. After Y years, the manufacturer rearchitects the cloud back-end (the remote data processing solution), introducing new APIs and data flows, in a manner that qualifies as a substantial modification of the product with digital elements but does not alter the nature of that product or affect user expectations. The Article 13(8) criteria therefore continue to indicate the same expected use time. The support period of the modified product with digital elements aligns with the remaining expected use time as originally determined.

135. Where the substantial modification affects the factors that originally determined the expected use time of the product with digital elements, the manufacturer should recalculate the support period to reflect the new expected use time, applying the Article 13(8) criteria accordingly. This may be the case, for example, of revitalising hardware modifications that extend that product's operational life, or of a substantial

reprogramming or rewrite of that product's core software that materially changes its expected use time[20].

Example 56: A manufacturer places on the market a programmable logic controller (PLC) with an expected use time of X years, determined primarily on the basis of the nature of the product with digital elements and the durability of the underlying hardware. The support period is set accordingly. Several years after the initial placing on the market, the manufacturer carries out a substantial modification consisting of the replacement of the PLC's embedded computing platform, including the processor, memory and runtime environment, with a new generation of components designed for a significantly longer operational lifetime. As a result of the modification, reasonable user expectations and the nature of the product with digital elements change: the PLC's user may now reasonably expect the PLC to remain in productive use beyond its originally declared expected use time, supported by the new computing platform. The Article 13(8) criteria therefore indicate a longer expected use time, and the manufacturer recalculates the support period for that specific PLC accordingly.

[20] It should be recalled that, as indicated in Section *4.1 Physical repairs,* operations of refurbishment, maintenance or repair are generally not considered to amount to substantial modifications.

6 Important and critical products with digital elements

136. Article 7(1) of the CRA establishes that products with digital elements that have the core functionality of a product category set out in Annex III to the Regulation are considered to be 'important products with digital elements'. Annex III further divides important products with digital elements into class I and class II. Similarly, Article 8(1) establishes that products with digital elements that have the core functionality of a product category set out in Annex IV to the CRA are considered to be 'critical products with digital elements'[21].

137. The classification of a product with digital elements as important or critical or, conversely, as belonging to the 'default' category[22], 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 with digital elements on the market. Notably, products with digital elements in the default category can always rely on the internal control procedure based on module A ('self-assessment') [23]. Important products with digital elements of class I or II and critical products with digital elements are subject to more stringent conformity assessment procedures. This does not include important products with digital elements of class I or II qualifying as free and open-source software that are placed on the market, for which, in accordance with Article 32(5), manufacturers are allowed to follow the procedures of the default category.

138. 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 with digital elements can perform a range of functions, some of which may be ancillary to that 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

139. The core functionality of a product with digital elements refers to that product's main features and technical capabilities, without which it would not be able to meet its intended purpose. It can be assessed in light of that product's specific context and conditions of use, taking into account, among others, the information the

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

[22] The term 'default' category is not a term defined in the CRA. The use of the term in this document refers to products with digital elements 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).

[23] The manufacturer can nonetheless always choose to apply a more stringent conformity assessment procedure, as set out in Article 32(1).

manufacturer supplies in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation.

Example 57: A software product with digital elements provides an abstraction layer over the underlying hardware and manages the execution of software components. Its main features include hardware and peripheral initialisation, 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 the device's hardware and software resources. The technical documentation indicates that the product with digital elements orchestrates 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 with digital elements has the core functionality of an operating system, as described in Annex I, point 11, to Implementing Regulation (EU) 2025/2392.

140. The functionality of a product with digital elements is rarely restricted exclusively to its core functionality, as products with digital elements 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 with digital elements. However, the fact that a product with digital elements performs functions other than or additional to those detailed in the technical descriptions of important or critical products with digital elements does not in itself prevent the product from having one such core functionality.

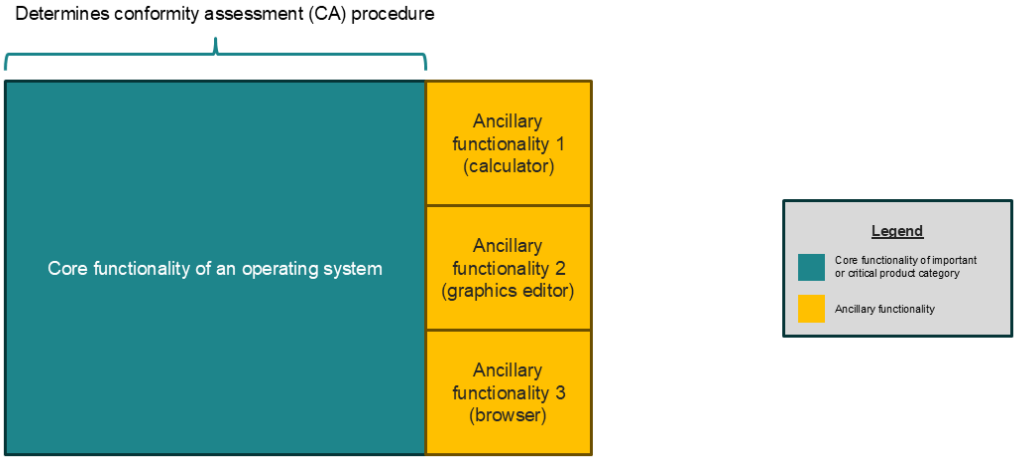

Figure 2: Illustration of how core functionality, and not ancillary functionalities, determine the applicable conformity assessment procedure

141. A product with digital elements 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 with digital elements would not qualify as an important or critical product with digital elements. As stated explicitly in Article 7(1) of the CRA for important products with

digital elements (and applying the same logic for critical products with digital elements), the mere integration of an important or critical product with digital elements does not in itself render the product with digital elements an important or critical product with digital elements.

Example 58: 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 and access information and services). The mere integration of an operating system does not mean that the smartphone has the core functionality of an operating system.

142. Some products with digital elements may be similar to an important or critical product category, or belong to the same general product family, yet their core functionality may substantially exceed or fall substantially short of the core functionality of that category. This is not the case where a product with digital elements includes additional functionalities that merely complement or enhance the core functionality, which itself corresponds to that of an important or critical product category; in such cases, the product with digital elements retains the core functionality of that category and is classified accordingly. This assessment should be based on that product's main features and technical capabilities, considered objectively in light of its intended purpose, and not on the way in which the product with digital elements is described or marketed, where that description does not reflect the product's actual technical characteristics.

Example 59: 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 as core elements of its technical capabilities. Therefore, SOAR software is generally not considered to have the core functionality of SIEM systems.

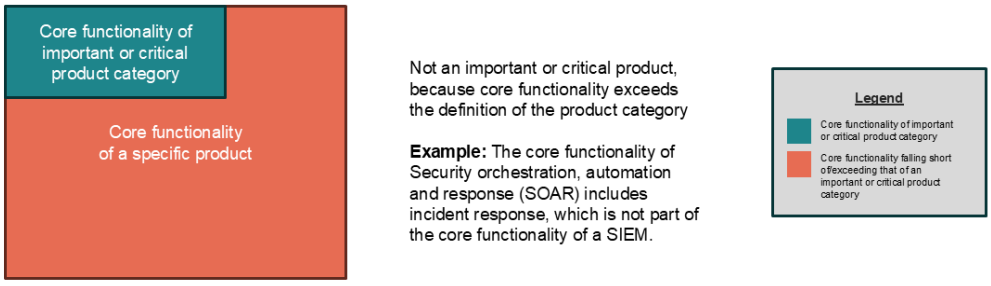

Figure 3: Illustration of the core functionality of a product with digital elements substantially exceeding the definition of an important or critical product category

Example 60: 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.

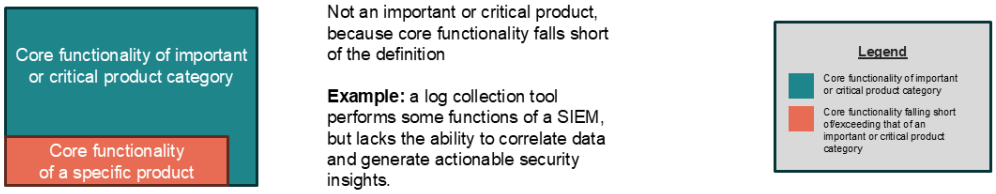

Figure 4: Illustration of the core functionality of a product with digital elements substantially falling short of the definition of an important or critical product category

143. A manufacturer may not misrepresent the core functionality of its product with digital elements in such a way as to escape the conformity assessment regime applicable to important or critical products with digital elements, e.g. by overly emphasising or downplaying the role of certain functionalities, so that the product substantially 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.

144. A product with digital elements 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 the intended purpose of their product with digital elements 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.

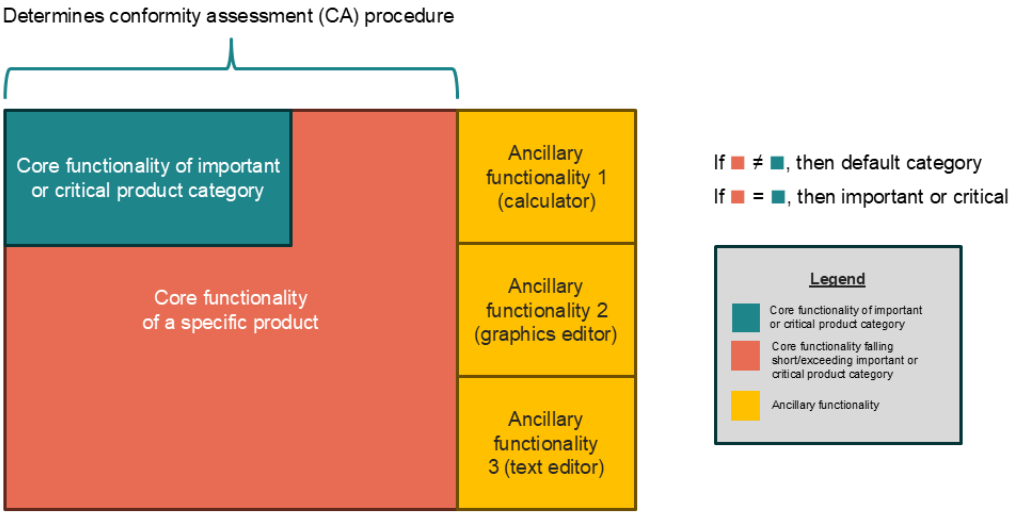

Figure 5: Illustration of how the core functionality a specific product with digital elements determines the product class and therefore the applicable conformity assessment procedure

145. Some products with digital elements are placed on the market as single products with digital elements but are composed of distinct modules with separate functionalities. Where a manufacturer also makes those modules available on the market separately, such as in the case where they are offered for separate purchase, licensing or subscription, those modules constitute standalone products with digital elements in their own right. As such, they are to be classified on the basis of their respective core functionalities (and therefore subject to the appropriate conformity assessment regime on the basis of each module's core functionality). This is without prejudice to modules supplied solely as components of an integrated product with digital elements and not made available separately; in such cases, the core functionality is determined at the level of the integrated product with digital elements.

Example 61: a manufacturer places on the market a unified security suite combining multiple modules, including a SIEM, an intrusion detection system, and an analytics module. The manufacturer also offers those modules for separate subscriptions. In this scenario, each module is a distinct product with digital elements and is classified on the basis of its own core functionality. The SIEM module is subject to the conformity assessment regime for important products with digital elements of class I, as its core functionality is that of 'Security information and event management (SIEM) systems'. The intrusion detection system is subject to the conformity assessment regime for important products with digital elements of class II, as its core functionality is that of 'Firewalls, intrusion detection and prevention systems'. The analytics module is subject to the conformity assessment regime for 'default' products with digital elements, as its core functionality is not that of an important or critical product category.

146. 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 with digital elements

147. Once the manufacturer has determined the core functionality of its product with digital elements, it needs to perform one of the applicable conformity assessment procedures. The manufacturer needs to ensure that the product with digital elements as a whole meets the essential requirements, considering, as appropriate, the security of the components or functionalities integrated into it.

148. A more stringent conformity assessment procedure, with the involvement of a thirdparty (based on module B+C, module H or cybersecurity certification schemes) is mandatory for important products with digital elements 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 with digital elements[24]. By contrast, important products with digital elements 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 procedure 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' [25].

149. Therefore, for an important product with digital elements of class I 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 cybersecurity risks associated to that product's core functionality.

150. The scope of the product with digital elements may be broader than the scope foreseen by the relevant harmonised standard, and such additional functions may present different or additional cybersecurity risks. The manufacturer is always required to carry out a risk assessment pursuant to Article 13(2) and should consequently check whether implementing a harmonised standard covers all risks associated with the product with digital elements. Where implementing the standard does not cover all risks, the manufacturer should ensure via other means that its product with digital elements is in compliance with the essential requirements.

151. Therefore, if the manufacturer of an important product with digital elements of class I has applied a relevant harmonised standard that covers the risks associated to that 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

[24] 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.

[25] For brevity's sake, the remainder of this section only refers to harmonised standards the references of which have been published in the Official Journal of the European Union. However, the same guidance also applies to common specifications adopted in accordance with Article 27(2) and to European cybersecurity certification schemes where specified by the Commission via delegated acts in accordance with Article 27(9).

assessment activities, the manufacturer will still be required to demonstrate that all risks applicable to its product with digital elements are addressed. Hence, where there is a gap between the coverage of the harmonised standard and the scope of the product with digital elements as a whole, the manufacturer still needs to document which additional measures it has put in place to treat those risks.

Example 62: 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 with digital elements 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 with digital elements in its entirety, including the antivirus's core functionality, the disk-cleaning and the anti-tracking functions. It applies a harmonised standard covering the risks associated with 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 with digital elements as a whole, including the disk-cleaning and the anti-tracking functions.

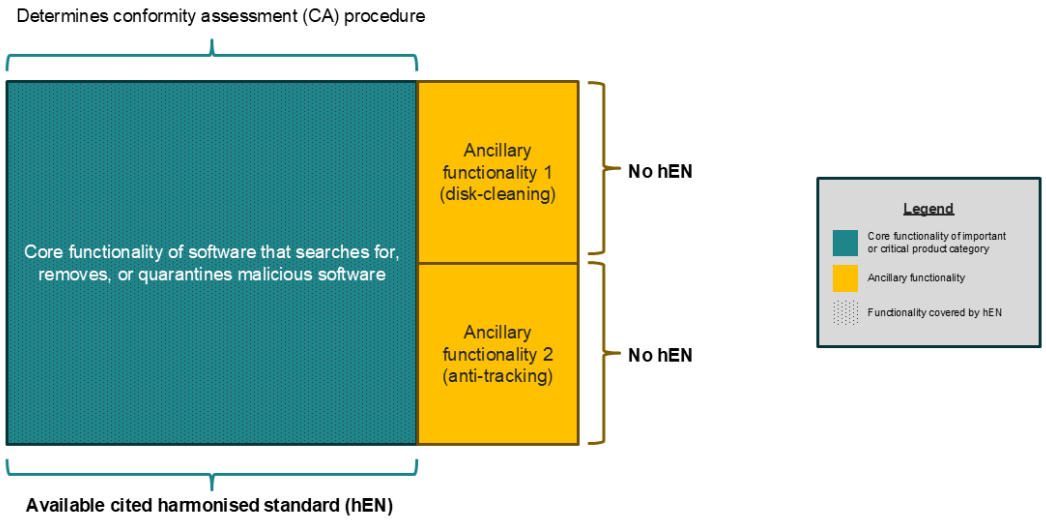

Figure 6: Illustration of how the use of a cited harmonised standard covering only core functionality determines the applicable conformity assessment procedure

152. This is also the case where the product with digital elements integrates an additional function that is itself that of another important or critical product with digital elements. In fact, it is the core functionality of the product with digital elements as a whole, and not the functionality of the integrated components taken in isolation, that determines whether the product with digital elements belongs to the important or critical product category (and therefore the applicable conformity assessment regime). For example, if a product with digital elements has the core functionality of an important product with digital elements of class I, that product as a whole is subject to the conformity assessment regime applicable to important products with digital elements of class I, even though it integrates a component that is itself a critical product with digital elements. In these cases, where the manufacturer applies

a harmonised standard covering the risks associated to that product's core functionality, it is allowed to make use of the internal control procedure.

Example 63: A hardware product with digital elements has the core functionality of a router, as described in Annex I, point 12, to Implementing Regulation (EU) 2025/2392. That product with digital elements also includes additional functionalities, including firewalling capabilities, as it integrates a firewall component. The manufacturer carries out a risk assessment covering the product with digital elements in its entirety, including the router's core functionality and the firewall functionality. It applies a harmonised standard covering the risks associated with the router's core functionality, and additional measures to deal with risks stemming from additional functions. For instance, the manufacturer may apply the harmonised standard for firewalls to cover the risks associated with the firewall functionality. The manufacturer is allowed to make use of the internal control procedure for its conformity assessment, covering the product with digital elements as a whole, including the firewall functionality.

6.3 Implications for presumption of conformity

153. Article 27(1) of the CRA establishes that products with digital elements 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 requirements of the CRA covered by those standards or parts thereof[26]. Article 27(5) extends the same presumption of conformity to products with digital elements 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 with digital elements 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)[27].

154. Therefore, where the manufacturer has applied a harmonised standard whose references have been published in the OJEU, it benefits from a presumption of conformity for the risks covered by that standard. This could be the case, for example, where the referenced harmonised standard addresses all the risks associated with the core functionality of a product with digital elements and there are no additional functionalities that present cybersecurity risks. For instance, it is expected that the

[26] 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 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'.

[27] As above, for brevity's sake, the remainder of this section only refers to harmonised standards the references of which have been published in the OJEU. However, the same guidance also applies to common specifications and to European cybersecurity certification schemes.

harmonised standard for routers will address at least the risks associated with the core functionality of these products with digital elements. If such a product does not contain any additional functionalities or if these additional functionalities do not present risks unaddressed by the standard, the product with digital elements can benefit from presumption of conformity.

155. In the cases discussed in points 151 and 152, the manufacturer is allowed to use the internal control procedure because the harmonised standard covers the risks associated with the core functionality of the product with digital elements. However, the products with digital elements 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. Those products with digital elements may therefore not benefit from presumption of conformity for those additional functionalities.

Example 64: An antivirus software has the core functionality of software that searches for, removes, or quarantines malicious software, and risks associated with that core functionality are covered by the harmonised standard. That product with digital elements also includes additional functionalities, namely a disk-cleaning function and an anti-tracking functionality protecting the user when navigating on the web, whose risks 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 presumption of conformity for the risks associated with that product's core functionality, but not for the risks associated with additional functionalities.

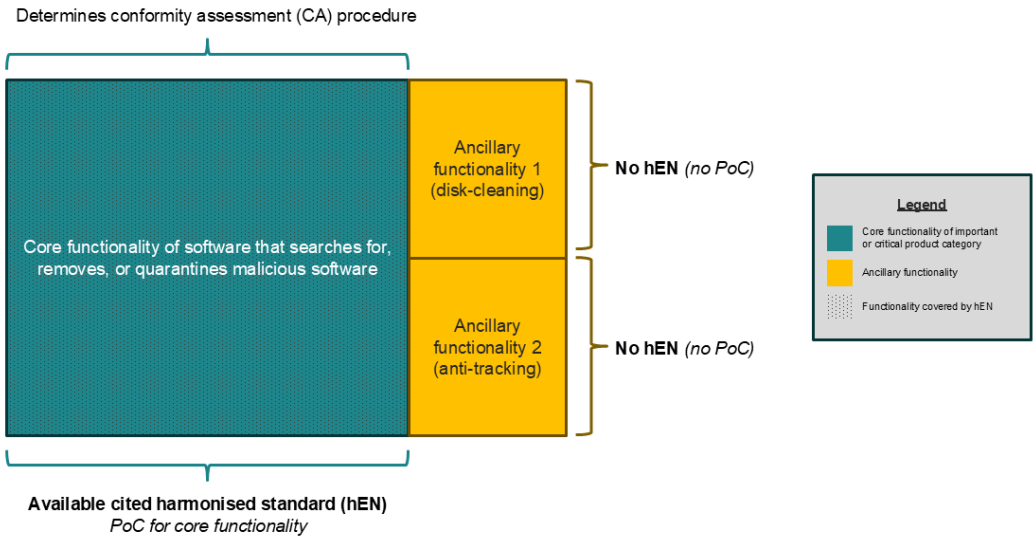

Figure 7: Harmonised standard grants presumption of conformity (PoC) for core functionality, as it addresses all risks associated with that core functionality, but not for ancillary functionalities

Example 65: In the same scenario as the previous example, the harmonised standard has now been updated to also cover risks associated with 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 risks associated with that product's core functionality and for the disk-cleaning functionality, but not for the risks related to the anti-tracking functionality.

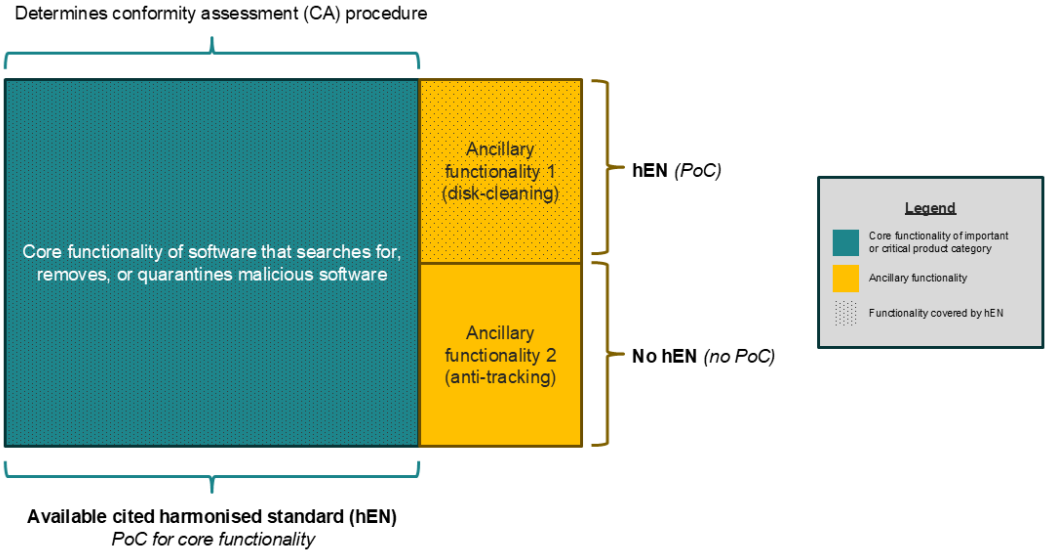

Figure 8: Harmonised standard grants PoC for core functionality and ancillary functionality 1, as it addresses all risks associated with those two functionalities, but not for ancillary functionality 2

7 Cybersecurity risk assessment and integration of products with digital elements and components

7.1 On the evaluation and treatment of cybersecurity risks

156. 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 with digital elements. Manufacturers also need to implement appropriate measures to address those risks, in accordance with the essential requirements of Annex I.

157. 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 should be assessed in light of the requirement that the product with digital elements placed on the market ensures an appropriate level of cybersecurity based on the risks, taking into account its intended purpose and reasonably foreseeable use.

158. Accordingly, the manufacturer's internal risk tolerance, commercial strategy or mere cost considerations are not relevant in determining whether risks have been addressed. 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 through the implementation of the essential requirements of Part I of Annex I, in light of the intended purpose, reasonably foreseeable use and conditions of use, including, where relevant, the operational environment (for example the intended users of the product with digital elements) and the assets to be protected, taking into account the length of time the product with digital elements is expected to be in use.

159. 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 with digital elements may only be placed on the market where the residual risks, once appropriate measures have been taken, have been sufficiently addressed through the implementation of the essential requirements, taking into account the intended purpose and reasonably foreseeable use of the product with digital elements.

160. In accordance with Article 13(3), where cybersecurity risks are identified, manufacturers are required to address them through appropriate measures, including 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 intended purpose of the product with digital elements more precisely. Manufacturers may also take steps to shape the reasonably foreseeable use of the product with digital elements, for instance through risk communication, user guidance, or user interface design, in order to steer user behaviour toward secure use patterns.

161. The CRA does not provide for the transfer of cybersecurity risk or responsibility to users or third parties to compensate for shortcomings in product design or to justify leaving cybersecurity risks unaddressed. The obligation to place a secure product with digital elements on the market and to demonstrate conformity with the essential requirements remains with the manufacturer.

162. Information and instructions provided to users may be used to support the secure deployment and operation of the product with digital elements, including where the manufacturer has chosen to restrict the intended purpose of that product to trusted environments, and to inform users of residual risks, in a manner that is appropriate to the nature of the product with digital elements and its intended users.

Example 66: A manufacturer develops an industrial sensor for use in trusted environments. For the sensor to perform its functionality correctly, the manufacturer does not implement measures to protect against physical attacks on the sensor itself. To mitigate the associated risks identified in the risk assessment, the manufacturer limits the sensor's intended purpose to use only in trusted environments where unauthorised physical access to the product with digital elements is prevented. Information and instructions to the users provide clear information on these limitations on the sensor's use, in a manner that is appropriate to the nature of the product with digital elements and its intended users.

Example 67: A manufacturer develops a software application for professional use on managed desktop and mobile devices. The application processes locally stored sensitive data and user-generated content. During the risk assessment, the manufacturer identifies the risk of unauthorised access to such data if they are stored in clear text on the device. Rather than designing and implementing a proprietary encryption mechanism within the application itself, the manufacturer chooses to rely on the encryption and key management functions provided natively by the operating system on which the application is intended to run, as the operating system's built-in cryptographic services are mature and regularly maintained.

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

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

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

165. This essential requirement is aimed at addressing all cybersecurity risks that have been identified as part of the cybersecurity risk assessment. Particularly, this

includes cybersecurity risks 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). This essential requirement is different from the legal obligation to carry out a cybersecurity risk assessment, which is to be carried out pursuant to Article 13(2).

166. Where all relevant cybersecurity risks related to a product with digital elements 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 with digital elements 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

167. 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 with digital elements 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 with digital elements remains secure, including where it relies on remote data processing solutions, remote services, or third-party software or hardware components.

168. The cybersecurity risk assessment concerns the identification and management of relevant risks that may affect the product with digital elements, including risks that originate outside the product itself, such as external networks, environmental factors, or other external aspects which might affect the product with digital elements 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 with digital elements itself. This will involve implementing the appropriate essential requirements set out in Part I of Annex I and, where necessary, providing information and instructions to users on integration or deployment risks.

169. For example, a manufacturer may identify a risk that unauthorised persons may gain access to back-end systems that are not part of the product with digital elements itself while the product is in operation, and attempt to send malicious commands to the product with digital elements. Such back-end systems, where they are not designed and developed by the manufacturer or under its responsibility, or where they do not support one of the functions of the product with digital elements, do not constitute remote data processing solutions and therefore fall outside the scope of

the product with digital elements for the purposes of the CRA. Nonetheless, the CRA requires the manufacturer to address the risk they may pose 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 resulting from such an external service becoming unavailable, for example due to power outages or failures of the infrastructure, the CRA may require product-level mitigation measures against such cybersecurity risks, e.g. ensuring that the outage does not cause the product with digital elements to enter into insecure states. In such cases, the CRA regulates how the product with digital elements responds to those external risks; it does not impose obligations on how the back-end infrastructure is organised, staffed or operated, nor does it treat that infrastructure as part of the product with digital elements.

170. Due diligence relates to elements that form part of the product with digital elements 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 compliance of the product with digital elements with the essential requirements. This can only be achieved by determining what the product with digital elements 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.

171. In alignment with its cybersecurity risk assessment, the manufacturer has to identify the requirements that the integrated component should satisfy. For example, if the product with digital elements 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 tests to verify that those components adequately perform the relevant functions. While due diligence is a separate legal obligation, it supports and underpins the manufacturer's ability to demonstrate compliance with the essential requirements for the product with digital elements as a whole.

172. When assessing the risks to the product with digital elements 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 through product-level measures to ensure compliance of the product with digital elements with the essential requirements. Components that are physically or logically integrated into the product with digital elements but sourced from a third party must also be considered as part of the risk assessment. However, for compliance purposes, the manufacturer should treat those as externally supplied components whose properties are verified through due

diligence upon integration, as the manufacturer may not have redesigned or redeveloped them.

173. The same logic applies during the development and integration of components. Where the manufacturer develops functionalities itself, it must directly implement the essential 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 with digital elements as a whole to comply. In both cases, the objective remains the same: that the product with digital elements, as placed on the market, achieves an appropriate level of cybersecurity as required by the CRA, taking into account the risks identified in the cybersecurity risk assessment.

7.4 Reuse of risk assessments and conformity documentation for families of products with digital elements

174. Manufacturers may place on the market products with digital elements that are similar, for example different variants, models or configurations of the same product family. Where such products with digital elements 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 with digital elements for the purposes of risk assessment and conformity assessment.

175. 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 with digital elements, as long as it clearly identifies the product variants to which it applies.

176. The decisive factor is whether the differences between the variants are relevant to cybersecurity. Variations that do not affect the cybersecurity properties of the product with digital elements, such as differences in 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 the implementation of essential requirements, for example through different communication interfaces, software stacks, update mechanisms or remote connectivity. In such cases, those differences must be reflected in the risk assessment and, where necessary, in the conformity assessment and technical documentation.

177. Manufacturers remain responsible for ensuring that the risk assessment and the related documentation accurately reflect the products with digital elements 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 with digital elements do not present differences with regards to their cybersecurity properties.

8 Remote data processing

178. 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'. In this light, the manufacturer must consider the product with digital elements as a whole, including its remote data processing solutions (RDPS). For instance, when demonstrating that the product with digital elements 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).

179. The purpose of this guidance is to provide further support to manufacturers in determining whether their product with digital elements 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 with digital elements 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*).

180. 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 with digital elements, the hardware that remote data processing may rely upon.

181. 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.'

182. 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 with digital elements 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 with digital elements is an essential requirement laid down in point (3) of Part II of Annex I to the CRA, this does not mean that such activities are to be considered RDPS for the product with digital elements.

183. 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)[28], which establishes cybersecurity risk-management requirements for cloud computing service providers. Those requirements are further specified by Commission Implementing Regulation (EU) 2024/2690[29].

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

184. 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 with digital elements 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'

185. The notion of 'at a distance' referred to in Article 3(2) is relevant but not sufficient to determine whether a product with digital elements 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.

186. 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 user environment of a product with digital elements or an organisation's operational environment (for a professional user). This, however, does not prevent processing from also taking place

[28] 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.

[29] 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.

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.

187. 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.

188. 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 *8.2*. 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 with digital elements from performing one of its functions?

189. As laid down in the definition of 'remote data processing' included in Article 3(2), for data processing at a distance to qualify as an RDPS, its absence would need to prevent the product with digital elements from performing one of its functions. The notion of 'functions' included in this definition is not limited to the 'core functionality' or 'intended purpose' of the product with digital elements, 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 with digital elements as experienced by users and functions that support the product's overall performance.

190. Examples of functions where data processing at a distance may happen and that would prevent a product with digital elements 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 with digital elements); (v) automated distribution of updates, including feature update and security patching; (vi) identity and access management.

191. 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 with digital elements offers.

192. By contrast, where the absence of a certain data processing does not prevent the product with digital elements from performing one of its functions, such processing is not considered as an 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.

193. Nevertheless, even when data processing does not support a function of a product with digital elements, manufacturers may need to consider if those remote

components introduce risks to the product with digital elements as part of their cybersecurity risk assessment (e.g. in light of the product's operational environment), and mitigate such risks accordingly (e.g. through product-level mitigations).

194. Websites are a specific case that deserves further clarification, as also explained in *Section 2.1 Placing on the market*. Websites are not within the scope of RDPS if they do not support a function of a product with digital elements, as explained in recital 11 of the CRA. It is not sufficient for a website to contain information about a product with digital elements 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 an RDPS. By contrast, a website may be within the scope of RDPS if it enables or supports a function of a product with digital elements. For example, an authentication portal that issues credentials or tokens required for the product with digital elements 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?

195. 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 with digital elements 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 by or on behalf of the manufacturer, based on designs and specifications provided by it.

196. 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 with digital elements. 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 with digital elements that they place on the market.

197. 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).

198. 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).

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

200. 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 with digital elements. 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.

201. 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) but are integrated into the product with digital elements in a manner that affects its security, such solutions should be considered similar to third-party components. The manufacturer is required to identify and assess risks linked to the integration of those elements and to address them by implementing the essential requirements on the product with digital elements itself. This can, where relevant, be supported by the security functions made available by the cloud service provider through its shared responsibility model, where the manufacturer uses or configures those functions to address the identified risks. 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, in a manner that is proportionate to the risk that the remote solution poses to the security of the product with digital elements.

202. Therefore, it can be summarised that:

a. For data processing to qualify as RDPS, the answer to both questions posed in Sections *8.1.2 Would the absence of such data processing prevent the product with digital elements 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. If the answer to the question in Section *8.1.2 Would the absence of such data processing prevent the product with digital elements 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.

c. If the answer to the question in Section *8.1.2 Would the absence of such data processing prevent the product with digital elements 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, manufacturers should treat the third-party solution as a component. 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.

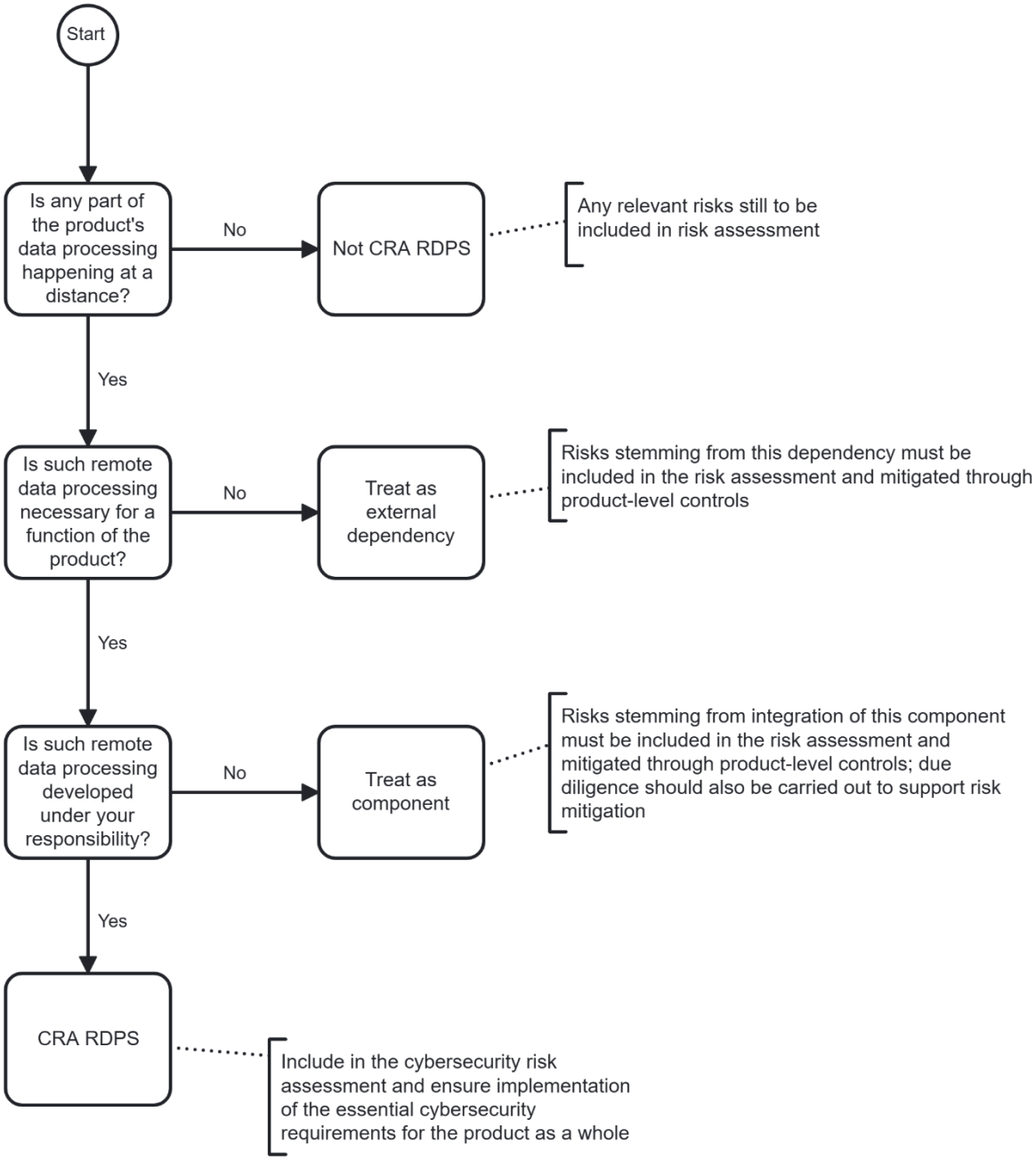

Figure 9: Stylised flowchart to determine if a product with digital elements contains RDPS

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

203. 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 with digital elements.

204. First, manufacturers should (i) indicate in the technical documentation that their product with digital elements has RDPS or relies on third-party remote solutions and (ii) describe such solutions. If the same RDPS supports several products with digital elements, the RDPS needs to be declared in each product's technical documentation. The documentation concerning RDPS serving several products with digital elements may be re-used from one product conformity assessment to another.

205. As indicated in recital 11, the RDPS that are part of the product with digital elements and therefore subject to the product's conformity assessment should be limited to those software modules that are responsible for the functionality of the product with digital elements, and to the interfaces those modules use with external services. Further back-end systems that carry out subsequent processing, and with which the product with digital elements does not directly interact, are not considered RDPS.

206. Nonetheless, those back-end systems remain external dependencies that must be assessed as part of the cybersecurity risk assessment and mitigated through product-level measures. In fact, the risk assessment performed by the manufacturer should consider: (i) risks related to RDPS; (ii) risks related to reliance on third-party remote solutions (similar to third-party components); and (iii) risks related to the product environment (e.g. underlying hardware). Manufacturers should implement security controls on the product with digital elements itself to mitigate those risks.

207. Furthermore, as part of the conformity assessment and/or the fulfilment of due diligence obligations related to third-party remote services, the following non-exhaustive list of assurance artefacts can be re-used in support of the manufacturer's assessment:

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

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

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

    d. evidence of conformity with ISO/IEC 27017:2015 or ISO/IEC 27001:2022.

208. Finally, in their interactions with third-party remote service providers, manufacturers need to implement the most appropriate security measures based on their risk assessment (and, where appropriate, supported by the provider's shared responsibility model). Those mitigation measures should include security controls for their products with digital elements 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 remote services providers should not qualify as a substantial modification of the product with digital elements, 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 cloud 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 controls are 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 with digital elements that rely on remote data processing and illustrating whether such processing qualifies as remote data processing solutions within the meaning of the CRA.

8.3.1 Mobile banking application

A financial entity places a mobile 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 remote solutions to support the app's functionalities. These include:

Self-hosted infrastructure developed by the financial entity:

- The customer opens the mobile banking application and is authenticated through the banking interface, a self-hosted solution developed by the financial entity that receives the app's requests and returns the corresponding responses. The banking interface verifies the customer's identity by querying the account management system and grants access to the application.
- The customer initiates a transfer via the app. The app transmits the instruction to the banking interface, which submits a corresponding request to the ledger system.
- The account-management system and ledger system, both self-hosted but logically segregated from the banking interface, record the transaction.
- The ledger system returns the transaction status to the banking interface, which presents the result to the customer.

Implications for RDPS:

- The banking interface is necessary for the app to perform its functions, namely authenticating the customer, submitting the customer's instructions, including payment and transfer instructions, and returning the resulting status. The banking interface is designed and developed under the responsibility of the manufacturer. As the answer to both questions presented in earlier sections is affirmative, the banking interface is to be considered an RDPS. It must therefore be included in the cybersecurity risk assessment and in the implementation of the essential requirements for the product with digital elements as a whole. The subsequent processing of an instruction once submitted, in

particular the recording of the transaction in the account-management and ledger systems, settlement and clearing, is carried out by systems with which the app does not interact directly and does not, on that basis, constitute an RDPS.

- The account-management system and the ledger system do not qualify as RDPS for the banking application. The app does not interact directly with them (interacting instead with the banking interface, which in turn relies upon them). Although their availability may be necessary for a function to be completed, the CRA covers only those parts of the system that interact directly with the product with digital elements. 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 with digital elements. 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 back-end interfaces, integrity protection of transaction data, secure communication channels and verification of responses received by the app.

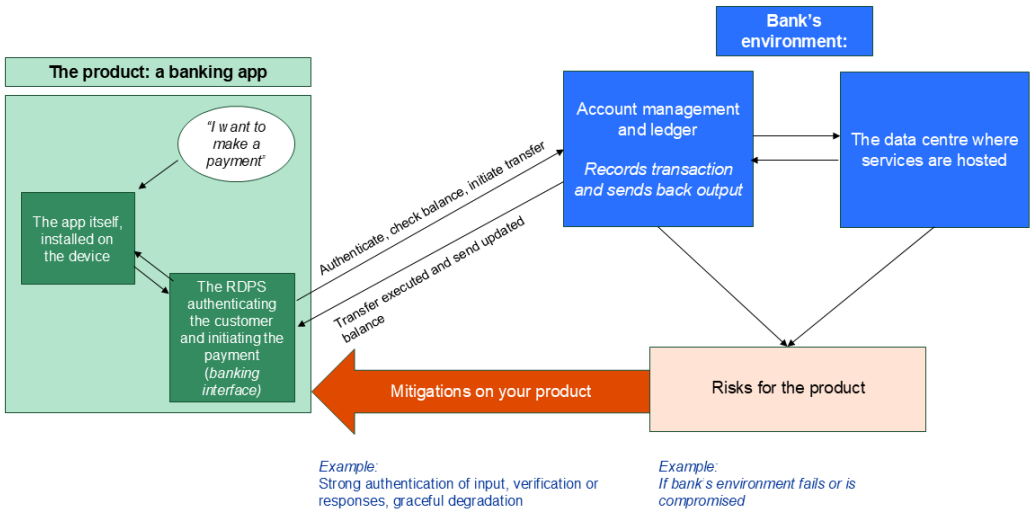

Figure 10: Stylised representation of a banking app relying on RDPS

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 with digital elements to perform one of its functions, but is not designed and developed by the financial entity, or under its responsibility; it therefore is not an 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.

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 be able to perform its smart functionalities without this remote data processing, its absence would prevent the product with digital elements from performing one or more 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 technical documentation of the product with digital elements, including details of the contracted service. The manufacturer needs to consider those elements in the risk assessment, which includes the intended purpose and reasonably foreseeable use of the product with digital elements. 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 with digital elements 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 with digital elements 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 with digital elements as a whole can comply with the essential 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 technical documentation of the product with digital elements (including details of the contracted service). The manufacturer also needs to consider those elements in the risk assessment, which includes the intended purpose and reasonably foreseeable use of the product with digital elements. The manufacturer implements the CRA's essential requirements on the product with digital elements, including its RDPS, on the basis of the risks. Due diligence when selecting the IaaS 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 with digital elements 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 with digital elements is working correctly. The network is only a communication channel and is not necessary for the product with digital elements 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 with digital elements from performing one of its functions, but rather an enabler of communication/connectivity.

Consequently, the cellular network does not meet the definition of RDPS. The network should not be considered like a third-party component, as there is no software integrated into the product with digital elements, 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 Reporting obligations

209. 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 with digital elements that it becomes aware of; and (ii) any severe incident having an impact on the security of the product with digital elements that it becomes aware of.

210. In accordance with Article 69(3) and 71(2), second sentence, the obligation to comply with Article 14 applies from 11 September 2026 to all products with digital elements that fall within the scope of the CRA, including products with digital elements placed on the market before 11 December 2027. Furthermore, unlike the vulnerability handling obligations, which continue only for the length of a product's support period, the reporting obligations continue to apply after a product with digital elements is no longer supported. Where a product with digital elements was placed on the market before 11 December 2027, or where its support period has ended, the manufacturer is not required to comply with the vulnerability handling obligations set out in Part II of Annex I.

211. It should be recalled that 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 with digital elements 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.

212. Manufacturers 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.

213. 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 with digital elements. 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 with digital elements is being actively exploited; or (ii) a severe incident has occurred and has led to the security of its product with digital elements being compromised.

214. 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 with digital elements 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 with digital elements. 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.

215. Furthermore, the structure of the reporting obligations requires manufacturers to update their notifications progressively, as their internal investigations advance 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.

216. As also recalled in Section *3.3.1 Sustained support and ensuring viability of FOSS,* open-source software stewards are also required to report actively exploited vulnerabilities in accordance with Article 24(3)[30]. That obligation applies upon becoming aware of an actively exploited vulnerability, and not merely where a vulnerability exists in the codebase of a FOSS for which that entity is a steward. In practice, because FOSS components are typically integrated downstream into other products with digital elements, a steward is likely to become aware of active exploitation via reports from third parties, which identify exploitation in FOSS components as integrated into other products with digital elements. This may be the case, for example, where a manufacturer of a product with digital elements detects active exploitation in a FOSS component integrated into its own product and reports it to that component's steward; or when a user or a security researcher finds evidence of exploitation of a FOSS component integrated in a product with digital elements and reports that active exploitation to the component's steward.

217. It should also be clarified that, because the obligation to report actively exploited vulnerabilities applies when the manufacturer becomes aware of active exploitation, the manufacturer is not required to report vulnerabilities of whose active exploitation it had already become aware before 11 September 2026 (the date on which the reporting obligation starts to apply). The CRA, therefore, does not require the

[30] To the extent that the steward is involved in the development of a product with digital elements.

retroactive reporting of such vulnerabilities. By contrast, the obligation does apply where the manufacturer was aware of a vulnerability before 11 September 2026 but was not, at that time, aware of any active exploitation of it (either because none had yet occurred or because the manufacturer had not become aware of it). If, after 11 September 2026, active exploitation subsequently occurs or the manufacturer becomes aware of it, the vulnerability is deemed an actively exploited one subject to the reporting obligation.

218. Similarly, a manufacturer is only required to report actively exploited vulnerabilities contained in their product with digital elements. Where a product with digital elements contains an actively exploited vulnerability originating from a third-party component, the manufacturer of the product with digital elements is required to notify that actively exploited vulnerability. However, if a manufacturer is aware that a third-party component contains a vulnerability, but that vulnerability either (i) cannot be exploited in its product with digital elements (e.g. because the vulnerable code is not reachable) or (ii) has not been exploited in its product with digital elements, that vulnerability does not qualify as an actively exploited vulnerability contained in its product with digital elements, and therefore it is not subject to mandatory reporting for that manufacturer. That manufacturer can still notify that vulnerability on a voluntary basis, in accordance with Article 15 of the CRA. It is also required to comply with the vulnerability handling requirements of Part II of Annex I to the CRA, as well as to report the vulnerability to the person or entity manufacturing or maintaining the component, in accordance with Article 13(6), and as further explained in Section *9.2.1 Reporting upstream and sharing security fixes*.

219. After becoming aware of an actively exploited vulnerability or a severe incident, manufacturers are also 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.

220. 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 nature of the product with digital elements, 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 with digital elements used in sensitive or essential environments, where public disclosure of technical details could itself increase cybersecurity risks or facilitate further exploitation.

221. 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 with digital elements 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 nature of the product with digital elements and the interests of the users concerned. Furthermore, point (4) of Part II of Annex I requires manufacturers to publicly disclose information about fixed vulnerabilities once a security update has been made available.

9.2 Vulnerability handling

9.2.1 Reporting upstream and sharing security fixes

222. 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').

223. Manufacturers are required to report upstream only in respect of the version of the component that they integrate. Where the person or entity manufacturing or maintaining the component has established security policies, coordinated vulnerability disclosure processes or designated channels for reporting vulnerabilities, manufacturers should report in accordance with them, particularly where premature disclosure of unpatched vulnerabilities could increase cybersecurity risks. Furthermore, in order to reduce the burden on upstream maintainers, particularly in open-source projects, manufacturers are not required to report upstream where they can confirm that the person or entity manufacturing or maintaining a component is aware of the existence of a vulnerability. Manufacturers are encouraged to take reasonable steps to avoid the submission of duplicate reports, for example by checking publicly accessible vulnerability databases, project-specific security advisories, or established issue trackers before reporting upstream.

224. Manufacturers are required to report upstream only those vulnerabilities that exist in the integrated component itself, and not vulnerabilities that exist as a 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 with digital elements 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.

225. Finally, manufacturers are also not required to report the vulnerability upstream where the component no longer has a maintainer, or when the manufacturer no longer relies on the original maintainer for new versions or security fixes. In such cases, the manufacturer is nonetheless encouraged to inform users of that component via reasonable alternative measures, e.g. through existing community

mechanisms (such as mailing lists or issue tickets) or through public vulnerability records.

226. 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').

227. Where manufacturers are required to share a security fix under Article 13(6), the fix should, where appropriate, be provided in a machine-readable format, 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. Where the maintainer of that component has guidelines on how security fixes should be shared, the manufacturer should follow those guidelines.

228. 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.

229. 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. The manufacturer is nonetheless encouraged to do so where this can support the person or entity maintaining the component.

9.2.2 Known exploitable vulnerabilities

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

231. 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 the operational environment of a product with digital elements.

232. 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.

233. A 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.

234. Additionally, a 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, including, for example, when making use of AI-powered services. Likewise, a vulnerability may be known when it has been publicly and prominently reported in reliable media outlets, including specialised cybersecurity publications or general mass media.

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

236. Furthermore, the obligation for manufacturers to comply with the essential 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 development lifecycle of the product with digital elements, including shortly before it enters the distribution chain (and is therefore placed on the market).

237. As the obligation to place products with digital elements 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 with digital elements 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 with digital elements 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 with digital elements itself once in use. They may also take into account the risks of postponing the product's release until the vulnerability is fixed, for example because the new release also addresses other exploitable vulnerabilities, or is necessary for the continued operation of critical systems. In any case, once a product with digital

elements 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.

9.2.3 Effective and regular tests and reviews

238. Point (3) of Part II of Annex I requires manufacturers to apply effective and regular tests and reviews of the product with digital elements throughout its support period. Applying regular tests does not require the mechanical repetition, at fixed intervals, of an unchanged test campaign. It means regularly reviewing whether new input, such as newly identified threats or newly discovered vulnerabilities, requires the existing tests to be updated, and executing tests accordingly.

239. The frequency, depth and content of the review should be proportionate to the cybersecurity risk profile of the product with digital elements, its evolution over time, and the state of the threat landscape. Where the review identifies relevant new input affecting the test set, new or modified tests should be devised and executed on the product, to ensure that no vulnerabilities remain unaddressed. This may include re-executing existing tests where a modification to the product with digital elements makes such types of testing appropriate, such as regression testing.

240. Where the review identifies no such input, additional tests need not be devised. Other vulnerability handling obligations, including that of addressing and remediating vulnerabilities in relation to the risks posed, continue to apply in parallel.

9.3 Interplay with other legislation

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

241. Point (c) of Article 2(2) of the CRA establishes that the Regulation does not apply to products with digital elements 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'.

242. 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)).

243. 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 with digital elements within the meaning of the CRA.

244. 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.

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

246. 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))

247. 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'.

248. 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 with digital elements they intend to place on the market on or after 11 December 2027 and until 11 June 2028[31]. This is the case for certificates and approval decisions issued where the applicable Union harmonisation legislation requires the manufacturer to perform the conformity

[31] Products with digital elements 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.

assessment procedure via a notified body, as well as where the manufacturer has voluntarily chosen to do so.

249. 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.

250. 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.

251. This can be illustrated by considering the case where a product with digital elements 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 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').

252. 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.

253. 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.

254. 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.

255. Similarly, where a product with digital elements 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.

256. 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.

257. 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.