25 JULY 2025

Towards clear guidance for remote data processing solutions under the CRA

Executive summary

The Cyber Resilience Act (CRA) presents a critical step towards a high level of cybersecurity across the Union.[1] Its success, however, depends on effective implementation. Uncertainty remains amongst manufacturers – those that must comply with, and implement, the CRA – regarding the extent to which cloud solutions will fall within its scope. The forthcoming CRA guidance must urgently provide clarity on this long-debated question.

To ensure the CRA imposes manageable obligations, the following boundaries should be considered:

- Cloud solutions should be in scope of the CRA only if they qualify as a remote data processing solution integrated into a product with digital elements. To be considered as such, the cloud solution must be: 1) essential for the functions of the product; and 2) designed, developed and applied by (or on behalf of) the manufacturer.

- The scope of remote data processing solutions should be limited to bidirectional data exchanges directly enhancing product functions with a remote processing capability. It would, thereby, exclude services solely receiving or transmitting data, or not interacting directly with a product to enable one or more of its functions.

- General-purpose cloud services that are not specifically designed and developed on behalf of a manufacturer of products with digital elements should be explicitly excluded from the scope of the CRA. Such services do not meet the criteria of remote data processing solutions, and are typically subject to the NIS2 Directive,[2] obliging a high level of cybersecurity.

---

[1] Regulation (EU) 2024/2847.

[2] Directive (EU) 2022/2555.

Table of contents

The need for legal clarity

As product regulation, the CRA's recitals purport to exclude services such as cloud-based solutions like software-as-a-service (SaaS), platform-as-a-service (PaaS) or infrastructure-as-a-service (IaaS). However, the CRA's text includes ambiguous language that could be read as capturing all three cloud service models. This conflicting language contributes to the current confusion in the industry regarding the circumstances under which cloud-based services might still fall within its scope.

To provide clarity, we recommend that the guidelines elaborate further on the concept of remote data processing. Firstly, it should be explicitly stated that cloud services provided as SaaS, PaaS or IaaS, do not, by themselves, qualify as products with digital elements. To ensure consistency across different EU regulations, we recommend using the definition of 'cloud computing services' under the NIS2 Directive in description of these services excluded from the scope.

Secondly, we recommend the guidelines bring further clarity on when cloud solutions would be considered as 'remote data processing.' Recital 12 references cloud solutions, stating they could be categorised as 'remote data processing' solutions if they meet the definition outlined in the CRA.[3] To avoid any confusion and bring further clarity on the meaning of this recital, it should be explicitly stated that cloud services that are not specifically designed and developed by (or on behalf of) their manufacturer for a specific product with digital elements are excluded from the CRA's scope. Such services do not meet the CRA's definition of remote data processing.

Furthermore, cloud services are already governed under the NIS2 Directive's security requirements, which introduces obligations to ensure a high level of cybersecurity in provision of such services. This would avoid confusion regarding the regulatory obligations for cloud services versus products with digital elements. Provision of cloud services alone should not cause the providers of such services to be classified as manufacturers under the CRA, nor as providers of remote data processing solutions, solely because customers using their services are manufacturers of products with digital elements.

Further difficulties could arise where the CRA and sector-specific legislation, such as DORA,[4] meet. Where the European Commission acknowledges overlaps, the scope of the remote data processing solutions should exclude back-end data and infrastructure otherwise captured by sector-specific legislation. In certain sectors, such as the banking sector, a mobile application provides its users with access to multiple services comprising the core purpose of the manufacturer. In such case, the majority of the network and information system is directly or indirectly designed or developed to provide functionality for the mobile application.

Included data processing

Based on Recitals 11-12 and Arts 3(1) and (2), the guidelines should clarify that 'remote data processing' refers to data stored, collected or generated by a product with digital elements, where that processing occurs outside the product and at a distance (i.e. remotely). This remote processing can be considered part

[3] The CRA defines '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;'

[4] Regulation (EU) 2022/2554

of the product with digital elements itself, and therefore in scope of the CRA, if the following three specific conditions are fulfilled:

1) It must be necessary for the product with digital elements to perform its functions;

2) It must be explicitly linked to the operation of the product with digital element's functions;

3) The remote data processing must be designed and developed by or on behalf of the manufacturer of the product. This excludes general purpose cloud services that are not specifically developed by the cloud service provider for a product with digital elements.

Example: If an e-reader uses a third-party cloud storage service that is made available to the public generally for any use case, to store electronic books purchased by their customers and allowing them to access their book, this underlying cloud storage service would not qualify as remote data processing as it is not 'software designed and developed by the manufacturer of the e-reader.' If, however, the e-reader manufacturer develops its own data processing solution to use with the products it manufactures, or requests a third-party provider to build such solution on its behalf, in order to enable its customers to synchronise their reading progress, manage their device settings, and receive personalised reading recommendations based on their usage patterns, the product with digital elements-specific parts of such service would qualify as a remote data processing solution of the e-reader.

Example: If a smart home security system uses a general-purpose database service to store and instantly retrieve device states, configuration settings, and event logs with millisecond latency, this underlying database service would not qualify as remote data processing, as it is not 'software designed and developed by the manufacturer of the security system.' If, however, the security system manufacturer develops its own data processing solution to use with the products it manufactures, or requests a third-party provider to build such solution on its behalf, in order to enable real-time alert processing, automated threat detection, and device state management (such as arming/disarming commands or camera configuration updates), the product with digital elements-specific parts of such service would qualify as a remote data processing solution of the security system, as it is specifically designed to enable core security system functions and affects the device's core functionality.

Given the diverse and evolving architectures in cloud computing, manufacturers need clear guidance. When it comes to cloud services specifically, in contrast to the conditions outlined above for remote data processing solutions generally, we strongly recommend limiting the scope of remote data processing under CRA to meet all the following conditions:

1) The software performing the processing must be designed, developed and applied by or on behalf the manufacturer of the product. This is to indicate that the remote data processing service is specifically designed and integrated into the product with digital elements by its manufacturer to ensure its functionality;

2) The service software performing the remote data processing directly interacts with the product;

3) The service involves both remote processing and a bidirectional exchange of data. This means data stored or processed by the product is sent from the product to a remote data processing service, and then the processed results are sent back to the product to enable one or more of its functions;

4) The service has been exclusively designed, developed and deployed for the remote data processing and/or storage of data for the product with digital elements.

Specifically, it should state that general-purpose cloud services that are not specifically developed for a product with digital elements are explicitly excluded from the CRA's scope.

Example: Systems controlling an industrial robot, where a camera feed from the robot is sent to a remote service developed by (or on behalf of) the manufacturer (e.g., not generally made available for sale by a third party service provider) that calculates the position of a part based on the camera feed and sends control commands back to the robot to pick it up.

Here, the robot, including the camera, is the product with digital elements. The remote data processing service is part of that product and has been designed, developed and applied specifically for such product. The part of this remote data processing service specifically developed for the robot is in scope of the CRA. The robot and its driver software will need to meet the essential requirements of Annex I.I.2e. This also concerns the data flow to, and from, the remote service which needs to be encrypted.

To make the abovementioned points more actionable, in the Annex to this paper, we provide a condensed step-by-step guide on how to assess whether the remote data processing solution is in scope of the CRA.

Excluded data processing

Remote services that solely receive data from a product, or that solely transmit data to a product, without any bilateral exchange and impact on the product's core functionality should not fall within the scope the CRA. Examples include services that receive and log information from products for storage. Likewise, general-purpose cloud services that are not specifically developed by a cloud service provider for a product with digital elements are explicitly excluded from the CRA's scope.

Similarly, any remote services not directly interacting with the product – even if the remote data processing solution interacts with them on the backend after receiving data – should be excluded from the CRA's scope. Remote services that store or process data in a manner that is incidental to another function should likewise not fall within the scope of CRA's remote data processing.

Example: If a smart thermostat sends usage data to the manufacturer's analytics service to improve its products and services generally, this data processing would be incidental to the thermostat's core temperature control function and would not qualify as remote data processing under the CRA.

Example: If a smart speaker sends usage statistics to the manufacturer's cloud service for general product improvement and troubleshooting purposes, this data processing would be incidental to the speaker's core voice assistant function and would not qualify as remote data processing under the CRA.

Furthermore, the implementation of essential security requirements in Annex I Part 1 require elucidation. It should be made to explicitly exclude classifying the implementation of essential security requirements as remote data processing solutions, such as distributing automatic updates[5] and recording and monitoring internal activity[6] even though those implementations are likely to include bi-directional information transfer.

Cloud services may be consumed via mobile applications accessing APIs or databases as part of their IaaS/PaaS/SaaS offerings. Consistent with Recital 12 CRA, the guidelines should clarify that such mobile apps that have the main purpose of connecting to a website or to consumption of cloud services do not qualify as products with digital elements in scope of the CRA, nor should cloud providers be considered manufacturers for providing such mobile applications.

Example: If a cloud-based video conferencing service provides a downloadable client application that enables users to connect to the service, establish audio/video streams, and manage basic settings, this client software should not qualify as a product with digital elements. The client application primarily serves to facilitate access to the cloud service, where the core functionality (such as managing meeting rooms, participant controls, real-time communication protocols, and video processing) actually resides. Treating such components as PDEs would create overlapping obligations under CRA and NIS2, as the cloud service provider is already subject to comprehensive security requirements for these components under the NIS2 Directive.

Besides, offline and online activities performed by a manufacturer, such as compiling software updates for a product, do not constitute remote data processing according to Art. 3(2). While automated updates can be important for product cybersecurity, it should be taken in the context of DIGITALEUROPE's long-standing view that security updates alone should not automatically be considered substantial modifications.[7]

To make the abovementioned points more actionable, we provide a condensed step by step guide how to assess if the RDP service is out of scope of the CRA in the Annex to this paper.

Conformity assessment of remote data processing

Product manufacturers will be required to consider remote data processing in their conformity assessments (when in scope of the CRA). Further consultations with cloud computing experts will be needed to ensure future conformity assessments are manageable. In general, we suggest more in-depth discussions with concerned stakeholders for further clarifications, as the Commission is already conducting on Annex III definitions.

The guidelines should provide additional clarity as to how manufacturers should incorporate the security of remote processing into their products' conformity assessments. Like the due diligence requirements imposed on manufacturers, remote data processing services shall be included in the risk assessments and demonstrate how risks are adequately mitigated. It's important to acknowledge that achieving 100% security for every line of code involved in remote data processing is impossible. To avoid bureaucratic burden for

[5] Annex I, Part 1, 2(c) CRA.

[6] Annex I, Part 1, 2(i) CRA.

[7] See DIGITALEUROPE, Developing guidelines for the Cyber Resilience Act, p. 13, available at https://cdn.digitaleurope.org/uploads/2024/09/Developing-guidelines-for-the-Cyber-Resilience-Act_DE.pdf.

the manufacturers it should be assumed that the necessary security requirements for the RDP are met if its manufacturer is a managed service provider under the NIS2.

Lastly, it is also important to distinguish between risk assessment and the security of the remote data processing solutions and the generic technical, operational or organisational measures aiming to manage the risks posed to the security of a manufacturer's network and information systems, as indicated in Recital 11 CRA. It would be recommended to include in the guidelines' further clarification on this topic.

Annex: Step-by-step assessment for remote data processing solutions

Included data processing

The following set of guidelines shall be fulfilled by the remote data processing service (RDPS) for it to be considered part of a product with digital elements, and therefore in scope of the CRA:

- I1: The RDPS must be designed, developed and applied by or on behalf of the manufacturer of the product with digital elements, specifically for the product. This to stress that the product with digital elements is offered by the manufacturer as a vertically integrated product to ensure its functionality.
- I2: Data stored, collected or generated by the product with digital elements, is processed by the RDPS outside the product and at a distance (i.e. remotely, see Recitals 11-12 and Arts 3(1)-(2)).
- I3: The processing or storage offered at a distance by the RDPS must be necessary for the product with digital elements to perform its functions.
- I4: The RDPS has, as its main function, the remote processing/storage of data for the respective product with digital elements.
- I5: The service performing the remote data processing directly interacts with the product with digital elements.
- I6: Besides remote data processing, the service involves a bidirectional exchange of data to the product with digital elements. This means data stored or processed by the product with digital elements is sent to a RDPS, and then the processed results are sent back from the RDPS to the product with digital elements to enable one or more of its functions.

If at least one of these conditions is not fulfilled, then the RDPS shall be excluded from the CRA's scope.

Excluded data processing

Complementing the guidance provided in the previous section, the following specific conditions are meant to explicitly exclude a remote service from the scope of the CRA:

- E1: General purpose cloud services that are not specifically developed by the cloud service provider for a product with digital elements.
- E2: General-purpose cloud services compliant with NIS2 requirements.
- E3: Remote services that solely receive data from a product with digital elements, or that solely transmit data to a product with digital elements.
- E4: Remote services that do not directly interact with the product with digital elements, even when the RDPS integrated with the product with digital elements interacts with those remote services on the backend after receiving PDE data. In this case, only the product-integrated RDPS is in scope of the CRA, not the backend remote services.

- E5: Remote services that store or process data in a manner that is incidental to another core functionality of the product with digital elements.

- E6: Remote services implementing the essential security requirements for the product with digital elements.

- E7: Cloud services that are consumed via mobile applications and accessed through APIs or databases that are part of the cloud service provider's IaaS/PaaS/SaaS offerings. In this case, such mobile apps connecting to websites or cloud services do not qualify as products with digital elements in scope of the CRA, nor should cloud service providers be considered manufacturers for providing such mobile applications.

- E8: Cloud services that include downloadable software or hardware components as part of their IaaS/PaaS/SaaS offerings. These cloud services neither qualify as RDPS nor as products with digital elements. Typically, these software and hardware components are used merely to facilitate a connection or transmission of data to the cloud service, which is the component of the SaaS offering that provides most of the functionality.

- E9: Offline and online activities performed by the manufacturer of the product with digital elements, such as compiling software updates.

If any of these conditions is fulfilled, the remote data processing service shall be excluded from the CRA's scope.

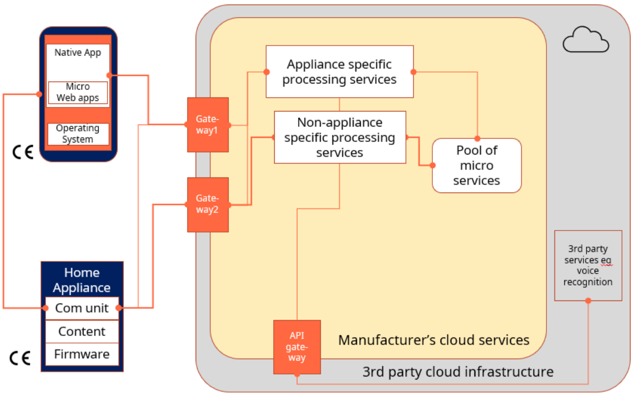
The guidance related to included (I1–I6) and excluded (E1–E9) RDPS seek to reduce the overlapping obligations that manufacturers are likely to face under CRA and NIS2. We refer to general purpose cloud services, which are already governed under NIS2 security requirements, where they exceed the respective threshold criteria.

Specific examples of RDP services

Example	Remote data processing service in-scope of the CRA? [Yes/No]	Rationale
An e-reader device uses a third-party cloud storage service that is made available generally to store electronic books purchased by customers, allowing them to access their book.	No	This general-purpose cloud storage service would not qualify as remote data processing in-scope of CRA, as it is not 'software designed and developed by the manufacturer of the e-reader'. See E1.
An e-reader manufacturer develops its own cloud storage service to use with the products it	Yes	The product with digital elements-specific parts of the

Example	Remote data processing service in-scope of the CRA? [Yes/No]	Rationale
manufactures or requests a third-party provider to build such service on its behalf for usage in its e-readers (or other products with digital elements it manufactures).		cloud storage service would qualify as a remote data processing solution of the e-reader. See I1, I2, I3, I4, I5 Note: based on the provided example, I6 cannot be evaluated and is therefore omitted from the criteria.
A smart home device uses a general-purpose cloud storage service from a third-party provider to store user preferences and settings, allowing users to access their configurations remotely.	No	This storage service would not qualify as remote data processing since it was not designed and developed by the manufacturer of the smart home device, the product with digital elements. See E1.
Systems controlling an industrial robot, where a camera feed from the robot is sent to a remote service developed by or on behalf of the manufacturer (e.g., not generally made available for sale by a third party service provider) that calculates the position of a part based on the camera feed and sends control commands back to the robot to pick up a part.	Yes	The robot, including the camera, is the product with digital elements. The remote data processing service is part of that product and has been designed, developed and applied specifically for such product. This remote data processing service should not compromise the security of the robot. For example, the robot (and its driver software) needs to ensure essential requirements of Annex I.I.2e (confidentiality). This also concerns the data flow to and from the remote service which needs to be encrypted. The remote data processing controller was developed on behalf of the industrial robot manufacturer, which is the product with digital elements. The RDPS performs some sort of computation (i.e., position) based on data received directly from the product with digital elements, and this processing is needed by the robot's

Example	Remote data processing service in-scope of the CRA? [Yes/No]	Rationale
		functionality. Finally, processed data is sent back from the RDPS to the robot. See I1, I2, I3, I4, I5, I6.
Remote servers that receive requests from an app to detect whether the device on which it is running has internet connectivity.	No	In this case, the function of the remote service is to support internet connectivity rather than to store or process data received from the product. See E3, E5.
A smart thermostat sends usage data to the manufacturer's analytics service to improve its products and services.	No	Generally, this data processing would be incidental to the thermostat's core temperature control function and would not qualify as remote data processing under the CRA. See E5.
A smart speaker sends usage statistics to the manufacturer's cloud service for general product improvement and troubleshooting purposes.	No	This data processing would be incidental to the speaker's core voice assistant function and would not qualify as remote data processing under the CRA. See E5.
Distributing automatic updates (Annex I, Part 1, (2)(c)) and recording / monitoring internal activity (Annex I, Part 1, (2)(l), even though those implementations are likely to include bi-directional information transfer.	No	Despite the inclusion of bi-directional information transfer (see I6), the remote service implements part of the essential security requirements for its products with digital elements. See E6.
A remote service provides automated security updates to its PDEs, which can be important for a product's cybersecurity.	No	This example should be taken in the context of DIGITALEUROPE's previous position that security updates alone should not automatically be considered substantial modifications. Furthermore, the

Example	Remote data processing service in-scope of the CRA? [Yes/No]	Rationale
		remote service implements part of the essential security requirements for its products with digital elements. See E6.
	Yes, for product with digital elements-specific parts	This is a typical setup in the realm of home appliances. Connected home appliances often have functions that use cloud services. The cloud services used by these appliance functions are 'backend functions.' These are often developed by the product manufacturer themselves (the yellow area within the visual) but run on a cloud computing environment provided by a professional third party (the grey area within the visual). It should be noted, however, that in case the product manufacturer is a Managed Service Provider under the NIS2 Directive it should be assumed that the necessary security requirements for the yellow part are met.

FOR MORE INFORMATION, PLEASE CONTACT:

Sid Hollman

Policy Manager for Cybersecurity, Digital Infrastructure & Mobility

sid.hollman@digitaleurope.org / +32 491 37 28 73

Milda Basiulyte

Senior Executive Director for Digital Policy

milda.basiulyte@digitaleurope.org / +32 493 89 20 59

Alberto Di Felice

Policy and Legal Counsel

alberto.difelice@digitaleurope.org / +32 471 99 34 25

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies. Our membership represents over 45,000 businesses who operate and invest in Europe. It includes corporations which are global leaders in their field of activity, as well as national trade associations from across Europe.

DIGITALEUROPE
Rue de la Science, 37, B-1040 Brussels
+32 2 609 53 10 ▶ Info@digitaleurope.org
▶ www.digitaleurope.org
EU Transparency Register: 64270747023-20

@DIGITALEUROPE DIGITALEUROPE digitaleurope_org