Official Journal
of the European Union

EN
L series

2024/2847

20.11.2024

2024/2847 20.11.2024

REGULATION (EU) 2024/2847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

欧洲议会和欧盟理事会第（EU）2024/2847 号条例

of 23 October 2024

2024 年 10 月 23 日

on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)

关于具有数字元素产品的横向网络安全要求，并修订第（EU）168/2013 号和第（EU）2019/1020 号条例及第（EU）2020/1828 号指令（《网络弹性法案》）

(Text with EEA relevance)

（与欧洲经济区有关的文本）

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

欧洲议会和欧盟理事会，

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

鉴于《欧洲联盟运行条约》，特别是其第 114 条，

Having regard to the proposal from the European Commission,

鉴于欧盟委员会的提案，

After transmission of the draft legislative act to the national parliaments,

在将立法草案送交各国议会之后，

Having regard to the opinion of the European Economic and Social Committee [1],

鉴于欧洲经济和社会委员会的意见（1），

After consulting the Committee of the Regions,

在征询地区委员会意见之后，

Acting in accordance with the ordinary legislative procedure [2],

按照普通立法程序（2），

Whereas:

鉴于以下理由：

(1) Cybersecurity is one of the key challenges for the Union. The number and variety of connected devices will rise exponentially in the coming years. Cyberattacks represent a matter of public interest as they have a critical impact not only on the Union's economy, but also on democracy as well as consumer safety and health. It is therefore necessary to strengthen the Union's approach to cybersecurity, address cyber resilience at Union 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 Union market. Two major problems adding costs for users and society should be addressed: a low level of cybersecurity of products with digital elements, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them, and an insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner.

（1）网络安全是欧盟面临的主要挑战之一。未来几年，联网设备的数量和种类将呈指数级增长。网络攻击事关公共利益，因为其不仅严重影响欧盟经济，也影响民主制度以及消费者的安全和健康。因此，有必要加强欧盟应对网络安全问题的方式，在欧盟层面解决网络弹性问题，并通过制定统一的法律框架，对进入欧盟市场的具有数字元素的产品规定基本网络安全要求，以改善内部市场的运行。应当解决两个增加用户和社会成本的主要问题：一是具有数字元素产品的网络安全水平较低，表现为漏洞普遍存在，以及用于修复这些漏洞的安全更新提供不足且不一致；二是用户理解不足、获取信息不充分，因而无法选择具备适当网络安全特性的产品，或无法安全地使用产品。

(2) This Regulation aims to set the boundary conditions for the development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and that manufacturers take security seriously throughout a product's lifecycle. It also aims to create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements, for example by improving transparency with regard to the support period for products with digital elements made available on the market.

（2）本条例旨在设定开发安全的具有数字元素产品的基本条件，确保投放市场的硬件及软件产品漏洞更少，并确保制造商在产品的整个生命周期内认真对待安全问题。本条例还旨在创造条件，使用户在选择和使用具有数字元素的产品时能够考虑网络安全因素，例如提高此类上市产品支持期限的透明度。

(3) Relevant Union law in force comprises several sets of horizontal rules that address certain aspects linked to cybersecurity from different angles, including measures to improve the security of the digital supply chain. However, existing Union law related to cybersecurity, including Regulation (EU) 2019/881 of the European Parliament and of the Council ([3]) and Directive (EU) 2022/2555 of the European Parliament and of the Council ([4]), does not directly cover mandatory requirements for the security of products with digital elements.

（3）现行相关欧盟法律包含多套从不同角度处理网络安全相关事项的横向规则，其中包括改善数字供应链安全的措施。然而，现行欧盟网络安全法律，包括欧洲议会和理事会第（EU）2019/881 号条例（3）及第（EU）2022/2555 号指令（4），并未直接涵盖针对具有数字元素产品安全性的强制性要求。

([1]) OJ C 100, 16.3.2023, p. 101.
([2]) Position of the European Parliament of 12 March 2024 (not yet published in the Official Journal) and decision of the Council of 10 October 2024.
([3]) Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).
([4]) 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).

（1）《欧盟官方公报》C 100，2023 年 3 月 16 日，第 101 页。（2）欧洲议会 2024 年 3 月 12 日的立场（尚未刊登于《官方公报》）及理事会 2024 年 10 月 10 日的决定。（3）欧洲议会和理事会 2019 年 4 月 17 日关于欧洲联盟网络安全局（ENISA）和信息通信技术网络安全认证、并废止第（EU）526/2013 号条例的第（EU）2019/881 号条例（《网络安全法》）（《欧盟官方公报》L 151，2019 年 6 月 7 日，第 15 页）。（4）欧洲议会和理事会 2022 年 12 月 14 日关于在整个欧盟实现共同的高水平网络安全、修订第（EU）910/2014 号条例和第（EU）2018/1972 号指令并废止第（EU）2016/1148 号指令的第（EU）2022/2555 号指令（NIS 2 指令）（《欧盟官方公报》L 333，2022 年 12 月 27 日，第 80 页）。

ELI: http://data.europa.eu/eli/reg/2024/2847/oj 1/81

EN OJ L, 20.11.2024

(4) While existing Union law applies to certain products with digital elements, there is no horizontal Union regulatory framework establishing comprehensive cybersecurity requirements for all products with digital elements. The various acts and initiatives taken thus far at Union and national levels only partially address the identified cybersecurity-related problems and risks, creating a legislative patchwork within the internal market, increasing legal uncertainty for both manufacturers and users of those products and adding an unnecessary burden on businesses and organisations to comply with a number of requirements and obligations for similar types of products. The cybersecurity of those products has a particularly strong cross-border dimension, as products with digital elements manufactured in one Member State or third country are often used by organisations and consumers across the entire internal market. This makes it necessary to regulate the field at Union level to ensure a harmonised regulatory framework and legal certainty for users, organisations and businesses, including microenterprises and small and medium-sized enterprises as defined in the Annex to Commission Recommendation 2003/361/EC ([5]). The Union regulatory landscape should be harmonised by introducing horizontal cybersecurity requirements for products with digital elements. In addition, legal certainty for economic operators and users, as well as a better harmonisation of the internal market and proportionality for microenterprises and small and medium-sized enterprises, creating more viable conditions for economic operators aiming to enter that market, should be ensured across the Union.

（4）尽管现行欧盟法律适用于某些具有数字元素的产品，但尚无欧盟层面的横向监管框架，为所有具有数字元素的产品规定全面的网络安全要求。迄今为止在欧盟和成员国层面采取的各项法令及举措，仅部分解决了已识别的网络安全问题及风险，导致内部市场法律规则碎片化，增加了制造商与用户的法律不确定性，并使企业和组织因需对类似产品遵守多套要求及义务而承担不必要的负担。此类产品的网络安全具有特别明显的跨境性质，因为在一个成员国或第三国制造的具有数字元素的产品，往往被整个内部市场的组织及消费者使用。因此，有必要在欧盟层面监管这一领域，以确保统一的监管框架，并为用户、组织及企业（包括委员会建议 2003/361/EC 附件所定义的微型企业以及中小型企业（5））提供法律确定性。应通过引入针对具有数字元素产品的横向网络安全要求，协调欧盟监管环境。此外，应在整个欧盟保障经济经营者和用户的法律确定性、改善内部市场的协调程度，并兼顾对微型企业及中小型企业的比例原则，从而为拟进入该市场的经济经营者创造更可行的条件。

(5) As regards microenterprises and small and medium-sized enterprises, when determining the category an enterprise falls into, the provisions of the Annex to Recommendation 2003/361/EC should be applied in their entirety. Therefore, when calculating the staff headcount and financial ceilings determining the enterprise categories, the provisions of Article 6 of the Annex to Recommendation 2003/361/EC on establishing the data of an enterprise in consideration of specific types of enterprises, such as partner enterprises or linked enterprises, should also be applied.

（5）对于微型企业及中小型企业，在确定企业所属类别时，应完整适用建议 2003/361/EC 附件的规定。因此，在计算决定企业类别的员工人数及财务限额时，也应适用该附件第 6 条关于确定企业数据的规定，并考虑合伙企业或关联企业等特定类型企业。

(6) The Commission should provide guidance to assist economic operators, in particular microenterprises and small and medium-sized enterprises, in the application of this Regulation. Such guidance should cover, inter alia, the scope of this Regulation, in particular remote data processing and its implications for free and open-source software developers, the application of the criteria used to determine support periods for products with digital elements, the interplay between this Regulation and other Union law and the concept of substantial modification.

（6）欧盟委员会应提供指导，以协助经济经营者，特别是微型企业及中小型企业适用本条例。该指导除其他事项外，应涵盖本条例的适用范围，尤其是远程数据处理及其对自由开源软件开发者的影响；确定具有数字元素产品支持期限所采用标准的适用；本条例与其他欧盟法律之间的相互关系；以及实质性修改的概念。

(7) At Union level, various programmatic and political documents, such as the Joint communication of the Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 16 December 2020, entitled 'The EU's Cybersecurity Strategy for the Digital Decade', the Council Conclusions of 2 December 2020 on the cybersecurity of connected devices and of 23 May 2022 on the development of the European Union's cyber posture and the European Parliament resolution of 10 June 2021 on the EU's Cybersecurity Strategy for the Digital Decade ([6]), have called for specific Union cybersecurity requirements for digital or connected products, with several third countries introducing measures to address this issue on their own initiative. In the final report of the Conference on the Future of Europe, citizens called for 'a stronger role for the EU in countering cybersecurity threats'. In order for the Union to play a leading international role in the field of cybersecurity, it is important to establish an ambitious regulatory framework.

（7）在欧盟层面，多项计划性及政策性文件——例如委员会与欧盟外交和安全政策高级代表 2020 年 12 月 16 日发布的题为《欧盟数字十年网络安全战略》的联合通报、理事会 2020 年 12 月 2 日关于联网设备网络安全的结论和 2022 年 5 月 23 日关于发展欧盟网络态势的结论，以及欧洲议会 2021 年 6 月 10 日关于欧盟数字十年网络安全战略的决议（6）——均呼吁针对数字产品或联网产品提出专门的欧盟网络安全要求；若干第三国亦已主动采取措施解决这一问题。在欧洲未来会议的最终报告中，公民呼吁"欧盟在应对网络安全威胁方面发挥更强作用"。为使欧盟在网络安全领域发挥国际领导作用，建立雄心勃勃的监管框架十分重要。

(8) To increase the overall level of cybersecurity of all products with digital elements placed on the internal market, it is necessary to introduce objective-oriented and technology-neutral essential cybersecurity requirements for those products that apply horizontally.

（8）为了提高投放内部市场的所有具有数字元素产品的整体网络安全水平，有必要针对这些产品引入目标导向、技术中立且普遍适用的基本网络安全要求。

(9) Under certain conditions, all products with digital elements integrated in or connected to a larger electronic information system can serve as an attack vector for malicious actors. As a result, even hardware and software considered to be less critical can facilitate the initial compromise of a device or network, enabling malicious actors to gain privileged access to a system or to move laterally across systems. Manufacturers should therefore ensure that all products with digital elements are designed and developed in accordance with the essential cybersecurity requirements laid down in this Regulation. That obligation relates to both products that can be connected physically via hardware interfaces and products that are connected logically, such as via network sockets, pipes, files, application programming interfaces or any other types of software interface. As cyber threats can propagate through various products with digital elements before reaching a certain target, for example by chaining together multiple vulnerability exploits, manufacturers should also ensure the cybersecurity of products with digital elements that are only indirectly connected to other devices or networks.

（9）在特定条件下，所有集成于更大型电子信息系统或与之连接的具有数字元素产品，都可能成为恶意行为者的攻击途径。因此，即便是被认为不那么关键的硬件和软件，也可能促使设备或网络最初遭受入侵，使恶意行为者获得系统的特权访问权限，或在系统之间横向移动。因此，制造商应确保所有具有数字元素的产品均按照本条例规定的基本网络安全要求进行设计和开发。此项义务既涉及通过硬件接口进行物理连接的产品，也涉及通过网络套接字、管道、文件、应用程序编程接口或其他软件接口进行逻辑连接的产品。由于网络威胁可能通过多个具有数字元素的产品传播才到达特定目标，例如通过串联利用多个漏洞，制造商也应确保仅与其他设备或网络间接连接的具有数字元素产品的网络安全。

(5) Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).
(6) OJ C 67, 8.2.2022, p. 81.

（5）委员会 2003 年 5 月 6 日关于微型、小型和中型企业定义的建议 2003/361/EC（《欧盟官方公报》L 124，2003 年 5 月 20 日，第 36 页）。（6）《欧盟官方公报》C 67，2022 年 2 月 8 日，第 81 页。

(10) By laying down cybersecurity requirements for placing on the market products with digital elements, it is intended that the cybersecurity of those products for consumers and businesses alike be enhanced. Those requirements will also ensure that cybersecurity is taken into account throughout supply chains, making final products with digital elements and their components more secure. This also includes requirements for placing on the market consumer products with digital elements intended for vulnerable consumers, such as toys and baby monitoring systems. Consumer products with digital elements categorised in this Regulation as important products with digital elements present a higher cybersecurity risk by performing a function which carries a significant risk of adverse effects in terms of its intensity and ability to damage the health, security or safety of users of such products, and should undergo a stricter conformity assessment procedure. This applies to such products as smart home products with security functionalities, including smart door locks, baby monitoring systems and alarm systems, connected toys and personal wearable health technology. Furthermore, the stricter conformity assessment procedures that other products with digital elements categorised in this Regulation as important or critical products with digital elements are required to undergo, will contribute to preventing potential negative impacts on consumers of the exploitation of vulnerabilities.

（10）通过规定具有数字元素的产品投放市场时应符合的网络安全要求，旨在同时提高消费者和企业使用此类产品时的网络安全水平。这些要求还将确保在整个供应链中考虑网络安全，从而使最终产品及其组件更加安全。这也包括针对玩具、婴儿监护系统等面向弱势消费者的具有数字元素的消费产品的上市要求。本条例归类为重要的具有数字元素的消费产品，因其功能可能造成程度严重、足以损害用户健康、安保或安全的不利影响而具有较高网络安全风险，因此应接受更严格的符合性评估程序。这适用于具有安全功能的智能家居产品，包括智能门锁、婴儿监护系统和报警系统、联网玩具以及个人可穿戴健康技术。此外，本条例归类为重要或关键的其他具有数字元素的产品须遵循更严格的符合性评估程序，也有助于防止利用漏洞给消费者造成潜在不利影响。

(11) The purpose of this Regulation is to ensure a high level of cybersecurity of products with digital elements and their integrated remote data processing solutions. Such remote data processing solutions should be defined as data processing at a distance for which the software is designed and developed by or on behalf of the manufacturer of the product with digital elements concerned, the absence of which would prevent the product with digital elements from performing one of its functions. That approach ensures that such 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. At the same time, processing or storage at a distance falls within the scope of this Regulation only in so far as it is necessary for a product with digital elements to perform its functions. Such processing or storage at a distance includes the situation where a mobile application requires access to an application programming interface or to a database provided by means of a service developed by the manufacturer. In such a case, the service falls within the scope of this Regulation as a remote data processing solution. The 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.

（11）本条例旨在确保具有数字元素的产品及其集成的远程数据处理解决方案具有较高水平的网络安全。此类远程数据处理解决方案应定义为：由相关具有数字元素的产品的制造商或代表其设计开发的软件所实现的远程数据处理，若缺少该处理，该产品便无法执行其某项功能。此种做法确保无论数据在用户设备本地还是由制造商远程处理或存储，制造商均对产品整体提供充分保护。同时，只有远程处理或存储是产品实现其功能所必需时，才属于本条例范围。例如，移动应用程序需要访问应用程序编程接口或由制造商开发的服务提供的数据库时，该服务即属于远程数据处理解决方案。因此，本条例对该类解决方案的要求不涉及旨在管理制造商整个网络和信息系统安全风险的技术、运营或组织措施。

(12) Cloud solutions constitute remote data processing solutions within the meaning of this Regulation only if they meet the definition laid down in this Regulation. For example, cloud enabled functionalities provided by a manufacturer of smart home devices that enable users to control the device at a distance fall within the scope of this Regulation. On the other hand, websites that do not support the functionality of a product with digital elements, or cloud services designed and developed outside the responsibility of a manufacturer of a product with digital elements do not fall within the scope of this Regulation. Directive (EU) 2022/2555 applies to cloud computing services and cloud service models, such as Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS). Entities providing cloud computing services in the Union which qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC, or exceed the ceilings for medium-sized enterprises provided for in paragraph 1 of that Article, fall within the scope of that Directive.

（12）云解决方案仅在符合本条例定义时才构成远程数据处理解决方案。例如，智能家居设备制造商提供的云端功能，使用户能够远程控制设备，属于本条例的适用范围。相反，不支持具有数字元素的产品功能的网站，或者不在此类产品制造商责任范围内设计开发的云服务，不属于其适用范围。指令（EU）2022/2555 适用于云计算服务及云服务模式，例如软件即服务（SaaS）、平台即服务（PaaS）和基础设施即服务（IaaS）。在欧盟提供云计算服务、根据建议 2003/361/EC 附件第 2 条属于中型企业或超过该条第 1 款所规定中型企业上限的实体，受该指令约束。

(13) In line with the objective of this Regulation to remove obstacles to the free movement of products with digital elements, Member States should not impede, for the matters covered by this Regulation, the making available on the market of products with digital elements which comply with this Regulation. Therefore, for matters harmonised by this Regulation, Member States cannot impose additional cybersecurity requirements for the making available on the market of products with digital elements. Any entity, public or private, can however establish additional requirements to those laid down in this Regulation for the procurement or use of products with digital elements for its specific purposes, and can therefore choose to use products with digital elements that meet stricter or more specific cybersecurity requirements than those applicable for the making available on the market under this Regulation. Without prejudice to Directives 2014/24/EU ([7]) and 2014/25/EU ([8]) of the European Parliament and of the Council, when procuring products with digital elements, which must comply with the essential cybersecurity requirements laid down in this Regulation, including those relating to vulnerability handling, Member States should

（13）本条例旨在消除具有数字元素的产品自由流通的障碍。因此，对于本条例涵盖的事项，成员国不得阻碍符合本条例的产品在市场上提供。对于本条例已协调的事项，成员国不得就该类产品的市场提供设置额外的网络安全要求。然而，公私实体可以为其特定目的采购或使用具有数字元素的产品设定超出本条例的要求，因而可以选择满足比市场提供适用要求更严格或更具体网络安全要求的产品。在不影响欧洲议会和理事会指令 2014/24/EU（7）及 2014/25/EU（8）的前提下，成员国在采购必须符合本条例网络安全基本要求（包括漏洞处理要求）的具有数字元素的产品时，应当

([7]) Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94, 28.3.2014, p. 65).
([8]) Directive 2014/25/EU of the European Parliament and of the Council of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC (OJ L 94, 28.3.2014, p. 243).

（7）欧洲议会和理事会 2014 年 2 月 26 日关于公共采购并废止指令 2004/18/EC 的指令 2014/24/EU（《欧盟官方公报》L 94，2014 年 3 月 28 日，第 65 页）。（8）欧洲议会和理事会 2014 年 2 月 26 日关于水务、能源、运输和邮政服务领域实体采购并废止指令 2004/17/EC 的指令 2014/25/EU（《欧盟官方公报》L 94，2014 年 3 月 28 日，第 243 页）。

ELI: http://data.europa.eu/eli/reg/2024/2847/oj 3/81

EN OJ L, 20.11.2024

ensure that such requirements are taken into consideration in the procurement process and that the manufacturers' ability to effectively apply cybersecurity measures and manage cyber threats are also taken into consideration. Furthermore, Directive (EU) 2022/2555 sets out cybersecurity risk-management measures for essential and important entities as referred to in Article 3 of that Directive that could entail supply chain security measures that require the use by such entities of products with digital elements meeting stricter cybersecurity requirements than those laid down in this Regulation. In accordance with Directive (EU) 2022/2555 and in line with its minimum harmonisation principle, Member States can therefore impose additional cybersecurity requirements for the use of information and communications technology (ICT) products by essential or important entities pursuant to that Directive in order to ensure a higher level of cybersecurity, provided that such requirements are consistent with Member States' obligations laid down in Union law. Matters not covered by this Regulation can include non-technical factors relating to products with digital elements and the manufacturers thereof. Member States can therefore lay down national measures, including restrictions on products with digital elements or suppliers of such products that take account of non-technical factors. National measures relating to such factors are required to comply with Union law.

确保采购过程中考虑上述要求，并考虑制造商有效实施网络安全措施和管理网络威胁的能力。此外，指令（EU）2022/2555 规定了该指令第 3 条所称基本实体和重要实体的网络安全风险管理措施，这可能包括供应链安全措施，要求这些实体使用满足比本条例更严格网络安全要求的具有数字元素的产品。因此，根据指令（EU）2022/2555 及其最低限度协调原则，成员国可以依照该指令对基本或重要实体使用信息与通信技术（ICT）产品施加额外网络安全要求，以确保更高的网络安全水平，但这些要求必须符合欧盟法所规定的成员国义务。本条例未涵盖的事项可以包括与具有数字元素的产品及其制造商相关的非技术因素。因此，成员国可以制定考虑非技术因素的国内措施，包括限制具有数字元素的产品或其供应商。涉及这些因素的国家措施须符合欧盟法律。

(14) This Regulation should be without prejudice to the Member States' responsibility for safeguarding national security, in compliance with Union law. Member States should be able to subject products with digital elements that are procured or used for national security or defence purposes to additional measures, provided that such measures are consistent with Member States' obligations laid down in Union law.

（14）本条例不应影响成员国依照欧盟法律维护国家安全的责任。成员国可对为国家安全或国防目的采购或使用的具有数字元素的产品采取附加措施，但须符合欧盟法规定的成员国义务。

(15) This Regulation applies to economic operators only in relation to products with digital elements made available on the market, hence supplied for distribution or use on the Union market in the course of a commercial activity. Supply in the course of a commercial activity might be characterised not only by charging a price for a product with digital elements, but also by 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. Accepting donations without the intention of making a profit should not be considered to be a commercial activity.

（15）本条例对经济运营者的适用仅限于在市场上提供的具有数字元素的产品，即在商业活动中为在欧盟市场分销或使用而供应的产品。商业活动中的供应不仅可以表现为对产品收费，还包括收取超出实际成本回收范围的技术支持服务费用、意图通过例如提供软件平台将其他服务变现、将出于提高软件安全性、兼容性或互操作性以外的目的处理个人数据作为使用条件，或接受超过产品设计、开发和提供成本的捐赠。无盈利意图地接受捐赠不应视为商业活动。

(16) Products with digital elements provided as part of the delivery of a service for which a fee is charged solely to recover the actual costs directly related to the operation of that service, such as may be the case with certain products with digital elements provided by public administration entities, should not be considered on those grounds alone to be a commercial activity for the purposes of this Regulation. Furthermore, products with digital elements which are developed or modified by a public administration entity exclusively for its own use should not be considered to be made available on the market within the meaning of this Regulation.

（16）作为服务提供的一部分而提供的具有数字元素的产品，若收取的费用仅用于收回与服务运营直接相关的实际成本，例如某些公共行政实体提供的产品，不应仅据此被视为本条例所称商业活动。此外，公共行政实体专为自身使用而开发或修改的具有数字元素的产品，不应被视为本条例所称的在市场上提供。

(17) Software and data that are openly shared and where users can freely access, use, modify and redistribute them or modified versions thereof, can contribute to research and innovation in the market. To foster the development and deployment of free and open-source software, in particular by microenterprises and small and medium-sized enterprises, including start-ups, individuals, not-for-profit organisations, and academic research organisations, the application of this Regulation to products with digital elements qualifying as free and open-source software supplied for distribution or use in the course of a commercial activity should take into account the nature of the different development models of software distributed and developed under free and open-source software licences.

（17）公开共享并允许用户自由访问、使用、修改和再分发的或其修改版本的软件及数据，有助于市场研究与创新。为促进自由及开源软件的开发和部署，特别是微型、小型和中型企业、初创企业、个人、非营利组织及学术研究机构的活动，本条例适用于在商业活动中供应分销或使用的自由及开源软件类具有数字元素的产品时，应考虑在自由及开源软件许可下分发和开发软件的不同开发模式的性质。

(18) Free and open-source software is understood as software the source code of which is openly shared and the licensing of which provides for all rights to make it freely accessible, usable, modifiable and redistributable. Free and open-source software is developed, maintained and distributed openly, including via online platforms. In relation to economic operators that fall within the scope of this Regulation, only free and open-source software made available on the market, and therefore supplied for distribution or use in the course of a commercial activity, should fall within the scope of this Regulation. The mere circumstances under which the product with digital elements has been developed, or how the development has been financed, should therefore not be taken into account when determining the commercial or non-commercial nature of that activity. More specifically, for the purposes of this Regulation and in relation to the economic operators that fall within its scope, 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. Furthermore, the supply of products with digital elements qualifying as free and open-source software components intended for integration by other manufacturers into their own products with digital elements should be considered to be making available on the market only if the component is monetised by its original manufacturer. For instance, the mere fact that an open-source software product with digital elements receives financial support from manufacturers or that manufacturers contribute to the development of such a product should not in itself determine that the activity is of commercial nature. In addition, the mere presence of regular releases should not in itself lead to the conclusion that a product with digital elements is supplied in the course of a commercial activity. Finally, for the purposes of this Regulation, the development of products with digital elements qualifying as free and open-source software by not-for-profit organisations should not be considered to be a commercial activity provided that the organisation is set up in such a way that ensures that all earnings after costs are used to achieve not-for-profit objectives. This Regulation 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.

（18）自由及开源软件是指源代码公开共享，且许可授予公众自由访问、使用、修改和再分发全部权利的软件。此类软件以公开方式开发、维护和分发，包括通过在线平台。就本条例适用的经济运营者而言，只有在市场上提供，即在商业活动中供应以供分销或使用的自由及开源软件，才属于其适用范围。因此，不能仅根据具有数字元素的产品的开发环境或开发资金来源，判断有关活动的商业或非商业性质。具体而言，为本条例之目的，并针对其适用范围内的经济运营者，为明确区分开发和供应阶段，提供符合自由及开源软件条件的具有数字元素的产品，若其制造商未将其商业化，不应视为商业活动。此外，供应旨在由其他制造商集成至其具有数字元素的产品中的自由及开源软件组件，只有原制造商将该组件商业化时，才应视为在市场上提供。例如，自由及开源软件产品获得制造商资金支持，或制造商参与其开发这一事实，本身不应决定活动具有商业性质。同样，定期发布新版本也不足以表明产品是在商业活动中供应。最后，就本条例而言，非营利组织开发符合自由及开源软件条件的具有数字元素的产品，只要其组织结构确保扣除成本后的全部收益用于实现非营利目标，即不应视为商业活动。本条例不适用于向不由其负责的自由及开源软件类具有数字元素的产品贡献源代码的自然人或法人。

(19) Taking into account 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 this Regulation, legal persons who provide support on a sustained basis for the development of such products which are intended for commercial activities, and who play a main role in ensuring the viability of those products (open-source software stewards), should be subject to a light-touch and tailor-made regulatory regime. Open-source software stewards include certain foundations as well as entities that develop and publish free and open-source software in a business context, including not-for-profit entities. The regulatory regime should take account of their specific nature and compatibility with the type of obligations imposed. It should only cover products with digital elements qualifying as free and open-source software that are ultimately intended for commercial activities, such as for integration into commercial services or into monetised products with digital elements. For the purposes of that regulatory regime, an intention for integration into monetised products with digital elements includes cases where manufacturers that integrate a component into their own products with digital elements either contribute to the development of that component in a regular manner or provide regular financial assistance to ensure the continuity of a software product. The provision of sustained support to the development of a product with digital elements includes but is not limited to the hosting and managing of software development collaboration platforms, the hosting of source code or software, the governing or managing of products with digital elements qualifying as free and open-source software as well as the steering of the development of such products. Given that the light-touch and tailor-made regulatory regime does not subject those acting as open-source software stewards to the same obligations as those acting as manufacturers under this Regulation, they should not be permitted to affix the CE marking to the products with digital elements whose development they support.

（19）鉴于许多已发布但未按本条例定义在市场上提供的自由及开源软件类具有数字元素的产品对网络安全的重要性，持续支持旨在用于商业活动的此类产品的开发，并在维持其可持续性方面发挥主要作用的法人（开源软件管理者），应受宽松且量身定制的监管制度约束。开源软件管理者包括某些基金会以及在商业环境中开发和发布自由及开源软件的实体，包括非营利实体。该监管制度应考虑其特性及所施加义务的适配性。它仅应涵盖最终拟用于商业活动的自由及开源软件类具有数字元素的产品，例如集成至商业服务或商业化产品中。就该制度而言，拟集成到商业化产品的情形包括：集成组件的制造商定期参与组件开发，或定期提供资金援助以确保软件产品延续。对开发提供持续支持包括但不限于托管和管理软件开发协作平台、托管源代码或软件、治理或管理自由及开源软件类具有数字元素的产品以及引导其开发。鉴于这种宽松且定制化的监管制度并不对开源软件管理者施加与制造商相同的义务，开源软件管理者不应被允许在其支持开发的产品上加贴 CE 标志。

(20) The sole act of hosting products with digital elements on open repositories, including through package managers or on collaboration platforms, does not in itself constitute the making available on the market of a product with digital elements. Providers of such services should be considered to be distributors only if they make such software available on the market and hence supply it for distribution or use on the Union market in the course of a commercial activity.

（20）仅仅将具有数字元素的产品托管在开放式代码仓库（包括通过软件包管理器或协作平台），本身不构成在市场上提供该产品。只有此类服务提供者将软件作为商业活动的一部分在欧盟市场供应、用于分销或使用时，才应将其视为分销商。

(21) In order to support and facilitate the due diligence of manufacturers that integrate free and open-source software components that are not subject to the essential cybersecurity requirements set out in this Regulation into their products with digital elements, the Commission should be able to establish voluntary security attestation programmes, either by a delegated act supplementing this Regulation or by requesting a European cybersecurity certification scheme pursuant to Article 48 of Regulation (EU) 2019/881 that takes into account the specificities of the free and open-source software development models. The security attestation programmes should be conceived in such a way that not only natural or legal persons developing or contributing to the development of a product with digital elements qualifying as free and open-source software can initiate or finance a security attestation but also third parties, such as manufacturers that integrate such products into their own products with digital elements, users, or Union and national public administrations.

（21）为支持和便利制造商在将不受本条例网络安全基本要求约束的自由及开源软件组件集成到其具有数字元素的产品时履行尽职调查，委员会应能够通过补充本条例的授权法案，或依据条例（EU）2019/881 第 48 条请求制定顾及自由及开源软件开发模式特殊性的欧洲网络安全认证方案，建立自愿安全证明计划。这些安全证明计划的设计应确保，不仅开发或参与开发符合自由及开源软件条件的具有数字元素的产品的自然人或法人可以发起或资助安全证明，制造商、用户及欧盟或成员国公共行政机构等第三方也可以这样做。

(22) In view of the public cybersecurity objectives of this Regulation and in order to improve the situational awareness of Member States as regards the Union's dependency on software components and in particular on potentially free and open-source software components, a dedicated administrative cooperation group (ADCO) established by this Regulation should be able to decide to jointly undertake a Union dependency assessment. Market surveillance authorities should be able to request manufacturers of categories of products with digital elements established by ADCO to submit the software bills of materials (SBOMs) that they have generated pursuant to this Regulation. In order to protect the confidentiality of SBOMs, market surveillance authorities should submit relevant information about dependencies to ADCO in an anonymised and aggregated manner.

（22）考虑到本条例的公共网络安全目标，并为提高成员国对欧盟依赖软件组件、特别是可能属于自由及开源软件的组件的态势认知，本条例设立的专门行政合作组（ADCO）应有权决定联合开展欧盟依赖性评估。市场监督机关可要求 ADCO 确定

的具有数字元素的产品类别的制造商提交依本条例生成的软件物料清单（SBOM）。为保护 SBOM 的保密性，市场监督机关应以匿名、汇总方式向 ADCO 提交有关依赖关系的信息。

(23) The effectiveness of the implementation of this Regulation will also depend on the availability of adequate cybersecurity skills. At Union level, various programmatic and political documents, including the Commission communication of 18 April 2023 on Closing the cybersecurity talent gap to boost the EU's competitiveness, growth and resilience and the Council Conclusions of 22 May 2023 on the EU Policy on Cyber Defence acknowledged the cybersecurity skills gap in the Union and the need to address such challenges as a matter of priority, in both the public and private sectors. With a view to ensuring an effective implementation of this Regulation, Member States should ensure that adequate resources are available for the appropriate staffing of the market surveillance authorities and conformity assessment bodies to perform their tasks as laid down in this Regulation. Those measures should enhance workforce mobility in the cybersecurity field and their associated career pathways. They should also contribute to making the cybersecurity workforce more resilient and inclusive, also in terms of gender. Member States should therefore take measures to ensure that those tasks are carried out by adequately trained professionals, with the necessary cybersecurity skills. Similarly, manufacturers should ensure that their staff has the necessary skills to comply with their obligations as laid down in this Regulation. Member States and the Commission, in line with their prerogatives and competences and the specific tasks conferred upon them by this Regulation, should take measures to support manufacturers and in particular microenterprises and small and medium-sized enterprises, including start-ups, also in areas such as skill development, for the purposes of compliance with their obligations as laid down in this Regulation. Furthermore, as Directive (EU) 2022/2555 requires Member States to adopt policies promoting and developing training on cybersecurity and cybersecurity skills as part of their national cybersecurity strategies, Member States may also consider, when adopting such strategies, addressing the cybersecurity skills needs resulting from this Regulation, including those relating to re-skilling and up-skilling.

（23）本条例实施的有效性还取决于能否获得充分的网络安全技能。欧盟各项政策和规划文件，包括委员会 2023 年 4 月 18 日关于弥合网络安全人才缺口、促进欧盟竞争力、增长及韧性的通讯，以及理事会 2023 年 5 月 22 日关于欧盟网络防御政策的结论，均承认欧盟存在网络安全技能缺口，且公私部门均须优先应对这一挑战。为确保本条例得到有效实施，成员国应确保市场监督机关和符合性评估机构具有充足的人力和资源执行规定任务。有关措施应促进网络安全人才流动及职业发展，并提升该领域人员队伍的韧性与包容性，包括性别方面的包容性。因此，成员国应采取措施，确保由经过充分培训、具备必要网络安全技能的专业人员承担这些任务。同样，制造商应确保其员工拥有履行本条例义务所需技能。成员国与委员会应在各自职责、权限及本条例赋予的任务范围内，采取措施支持制造商，特别是微型、小型和中型企业及初创企业，例如通过技能培养协助其履行义务。此外，鉴于指令（EU）2022/2555 要求成员国将促进和发展网络安全培训及技能的政策纳入国家网络安全战略，成员国在制定相关战略时也可考虑本条例带来的网络安全技能需求，包括再培训和技能提升需求。

(24) A secure internet is indispensable for the functioning of critical infrastructures and for society as a whole. Directive (EU) 2022/2555 aims at ensuring a high level of cybersecurity of services provided by essential and important entities as referred to in Article 3 of that Directive, including digital infrastructure providers that support core functions of the open internet, ensure internet access and provide internet services. It is therefore important that the products with digital elements necessary for digital infrastructure providers to ensure the functioning of the internet are developed in a secure manner and that they comply with well-established internet security standards. This Regulation, which applies to all connectable hardware and software products, also aims at facilitating the compliance of digital infrastructure providers with the supply chain requirements under Directive (EU) 2022/2555 by ensuring that the products with digital elements that they use for the provision of their services are developed in a secure manner and that they have access to timely security updates for such products.

（24）安全的互联网是关键基础设施乃至整个社会正常运转所不可或缺的。指令（EU）2022/2555 旨在确保其第 3 条所称基本实体和重要实体提供的服务具有较高网络安全水平，包括支持开放互联网核心功能、确保互联网接入并提供互联网服务的数字基础设施提供者。因此，数字基础设施提供者用以维持互联网运行的具有数字元素的产品必须安全开发，并遵守成熟的互联网安全标准。本条例适用于所有可连接的硬件和软件产品，还旨在通过确保数字基础设施提供者所用产品得到安全开发并可及时获得安全更新，便利其遵守指令（EU）2022/2555 规定的供应链要求。

(25) Regulation (EU) 2017/745 of the European Parliament and of the Council ([9]) lays down rules on medical devices and Regulation (EU) 2017/746 of the European Parliament and of the Council ([10]) lays down rules on in vitro diagnostic medical devices. Those Regulations address cybersecurity risks and follow particular approaches that are also addressed in this Regulation. More specifically, Regulations (EU) 2017/745 and (EU) No 2017/746 lay down essential requirements for medical devices that function through an electronic system or that are software themselves. Certain non-embedded software and the whole lifecycle approach are also covered by those Regulations. Those requirements mandate manufacturers to develop and build their products by applying risk management principles and by setting out requirements concerning IT security measures, as well as corresponding conformity assessment procedures. Furthermore, specific guidance on cybersecurity for medical devices is in place since December 2019, providing manufacturers of medical devices, including in vitro diagnostic devices, with guidance on how to fulfil all the relevant essential requirements set out in Annex I to those Regulations with regard to cybersecurity. Products with digital elements to which either of those Regulations apply should not therefore be subject to this Regulation.

（25）欧洲议会和理事会条例（EU）2017/745（9）规定医疗器械规则，条例（EU）2017/746（10）规定体外诊断医疗器械规则。这两项条例针对网络安全风险采取了与本条例相关的特定监管方式。具体而言，这些条例规定了通过电子系统运作的医疗器械或作为软件的医疗器械的基本要求，并涵盖某些非嵌入式软件及全生命周期方法。这些要求规定制造商须应用风险管理原则开发和制造产品，制定信息技术安全措施及相关符合性评估程序。此外，自 2019 年 12 月以来已有关于医疗器械（包括体外诊断器械）网络安全的专门指南，指导制造商满足上述条例附件 I 所列的全部相关网络安全基本要求。因此，适用上述任一条例的具有数字元素的产品，不应受本条例约束。

(26) Products with digital elements that are developed or modified exclusively for national security or defence purposes or products that are specifically designed to process classified information fall outside the scope of this Regulation. Member States are encouraged to ensure the same or a higher level of protection for those products as for those falling within the scope of this Regulation.

（26）仅为国家安全或国防目的而开发或修改的具有数字元素的产品，或者专门用于处理机密信息的产品，不属于本条例适用范围。鼓励成员国确保这些产品获得不低于本条例适用产品的保护水平。

([9]) Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1).

([10]) Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p. 176).

（9）欧洲议会和理事会 2017 年 4 月 5 日关于医疗器械、修订指令 2001/83/EC、条例（EC）178/2002 和条例（EC）1223/2009 并废止理事会指令 90/385/EEC 和 93/42/EEC 的条例（EU）2017/745（《欧盟官方公报》L 117，2017 年 5 月 5 日，第 1 页）。（10）欧洲议会和理事会 2017 年 4 月 5 日关于体外诊断医疗器械并废止指令 98/79/EC 和委员会决定 2010/227/EU 的条例（EU）2017/746（《欧盟官方公报》L 117，2017 年 5 月 5 日，第 176 页）。

(27) Regulation (EU) 2019/2144 of the European Parliament and of the Council ([11]) establishes requirements for the type-approval of vehicles, and of their systems and components, introducing certain cybersecurity requirements, including on the operation of a certified cybersecurity management system, on software updates, covering organisations' policies and processes for cybersecurity risks related to the entire lifecycle of vehicles, equipment and services in compliance with the applicable United Nations regulations on technical specifications and cybersecurity, in particular UN Regulation No 155 – Uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management system ([12]) and providing for specific conformity assessment procedures. In the area of aviation, the principal objective of Regulation (EU) 2018/1139 of the European Parliament and of the Council ([13]) is to establish and maintain a high uniform level of civil aviation safety in the Union. It creates a framework for essential requirements for airworthiness for aeronautical products, parts and equipment, including software, that includes obligations to protect against information security threats. The certification process under Regulation (EU) 2018/1139 ensures the level of assurance aimed for by this Regulation. Products with digital elements to which Regulation (EU) 2019/2144 applies and products certified in accordance with Regulation (EU) 2018/1139 should not therefore be subject to the essential cybersecurity requirements and conformity assessment procedures set out in this Regulation.