NOVEMBER 2024 Gökçe ISSUE: 132

THE FINE PRINT

Answers. Not theories.

FIRST OF ITS KIND: CYBER RESILIENCE ACT

- 2025 Presidential Annual Program Published: New Steps in Digital Transformation and Health Data
- Regulation on Market Surveillance and Inspection of Products Introduced to the Market via Remote Communication Tools

LATEST LEGAL NEWS

- Standard Contract Notification Module and Guide Published
- European Union Commission Fines Meta: 798 million Euros

First of its Kind: Cyber Resilience Act

The Cyber Resilience Act **(CRA)**, which aims to harmonize the cybersecurity requirements of digital products between the member states of the European Union and ensure that these products comply with cybersecurity standards, was published in the EU Official Journal on 20 November 2024.

In a world where cyber-attacks are on the rise, with reports predicting that **an attack will occur every 2 seconds by 2031 and that this may cause an annual cost of more than € 251 billion**[1] , this law will make a big name for itself.

Surely, cyber security-oriented regulations in the EU, such as the Cyber Security Law, Directive Network and Information Security Directive **(NIS2)** should not be disregarded.

Although the law will generally come into effect on 11 December 2027, certain provisions will apply earlier.

Definition and Scope of the EU Cyber Resilience Act

The first EU-wide CRA aims to establish a single set of rules for the whole EU, covering all software and hardware products, including data processing systems and components for sale separately.

The CRA aims to ensure that products with digital components are safe throughout their lifecycle, covering manufacturers, software developers, importers, distributors and resellers. It would be appropriate to say that the CRA focuses primarily on companies that develop and market non-embedded software.

All products that are directly or indirectly connected to the network, such as Internet of Things (IoT) devices, operating systems and high-risk artificial intelligence systems, are covered by the law. However, there are of course some exceptions to the scope:

- Devices already covered by other EU rules (**NIS2 Directive, AI Act**, etc.)
- Software as a service **(SaaS)** that is not a core component of the product. Some products are excluded, such as free open-source software, which is used for research and innovation and is not for profit.

However, it should be emphasized that open-source software from which developers derive some form of commercial activity is included.

The CRA divides products into two main categories according to their level of importance as important and critical:

- **Important products:** Products are considered "important" if they provide critical functions for cybersecurity or can adversely affect user and product security through manipulation. Examples include products that contain digital elements and provide critical functions for cyber security such as identity management, VPN, operating systems.
- **Critical products:** Critical products are defined according to the risk that vulnerabilities could cause serious disruptions in the supply chain. Examples include hardware devices with security boxes, smart meter gateways and smart cards.

[1] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

We have compiled the prominent regulations in the CRA for you below:

Basic Requirements: CRA sets out the basic requirements to ensure the cyber security of digital products. Products must be designed, developed and manufactured to address risks. These basic requirements include eliminating security vulnerabilities, offering default security configurations, providing timely security updates, and protecting data confidentiality, integrity, and availability.

Key Requirements Imposed on Manufacturers: Manufacturers must provide a control mechanism against unauthorized access, limit data collection to only what is necessary, and ensure resilience against potential attacks. In addition, manufacturers are required to test product security on a regular basis and immediately identify and fix security vulnerabilities.

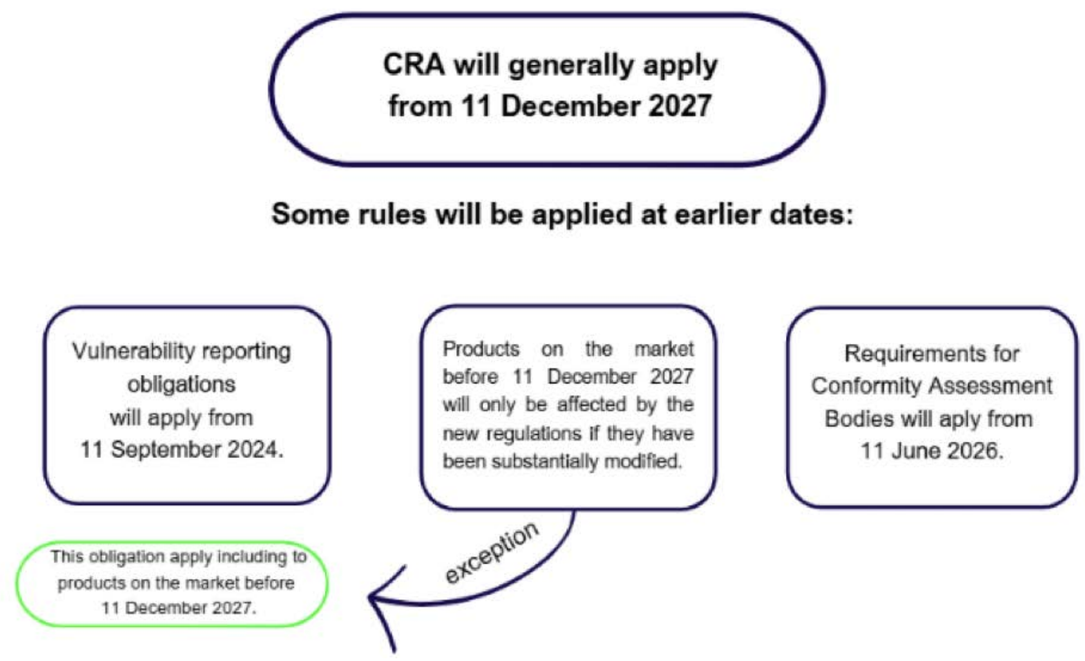
- **Product lifecycle security:** Manufacturers should ensure cybersecurity at all stages of the product (design, production, updates), remediate vulnerabilities and offer default security settings.
- **Product conformity assessments:** All products must undergo security checks before they can be sold on the EU market, and products that pass the checks must be CE marked, which is required before they can be sold in the EU.
- **Vulnerability reporting:** Manufacturers are required to provide a method for reporting vulnerabilities or receiving such reports. Manufacturers must report actively exploited vulnerabilities within 24 hours and provide a more detailed report after 72 hours.
- **Third-party component integration:** If manufacturers use components or software produced by others, including open-source components, they must secure them, document vulnerabilities, and report the person or organisation that produced or maintains the vulnerable component.

What will be the Enforcement Sanctions?

In case of non-fulfilment of the CRA rules, the highest of the following amounts will be imposed as a fine:

- **Cyber security breaches:** up to €15,000,000 or 2.5 per cent of annual sales
- **Other infringements:** Up to €10,000,000 or 2% of annual sales
- **Providing incorrect information:** Up to €5,000,000 or 1% of annual sales

Table on the Application Date of the CRA:



The full text of the CRA is available here *(only available in EU languages)*.

2025 Presidential Annual Program Published: New Steps in Digital Transformation and Health Data

The 2025 Presidential Annual Program was published in the Official Gazette on 30 October 2024.

Several topics stand out in the plan. In this context, it is critical to re-emphasize the GDPR compliance targets, which were among the targets in previous years, in order to support the export of goods and services to global trade. Again, several measures included in to increase the use of digital public services with a user-oriented, integrated and participatory approach are also quite significant. To this end, emphasis is placed on strengthening cyber security in digital transformation in line with EU legislation and international standards, updating critical infrastructure sectors, establishing cyber security standards and preparing legislation in line with the EU Cyber Resilience Act. In particular, the implementation of the National Data Strategy and Action Plan and the establishment of a national open data portal through legislation on "open data" are also crucial.

In addition to these, another key issue that stands out is the target of establishing an infrastructure for the anonymization of health data for secondary use, especially for R&D and economic value creation.

This plan can be considered as the "initial steps" of the European Health Data Space **(EHDS)** in the EU. As a matter of fact, the EHDS aims for the primary and secondary use of health data within the EU. The relevant "space" is based on GDPR, the Data Governance Act, the Data Act and the NIS2 Directive. Although the transition is not yet complete, EU member states are expected to complete their participation in MyHealth@EU by 2025.

The EHDS was mainly created to increase digital access of individuals to digital health data, to create a single market for electronic health records and related systems, and to ensure the secure use of health data in research, innovation and policy-making processes.

The critical secondary use is similar to that in the plan. In this context, pursuant to the EHDS; if the necessary conditions are met,

- For secondary use, health data will be accessible in closed and secure environments that comply with cybersecurity standards and only anonymized or pseudonymised data can be used.
- Relevant health data can be used in areas such as research, innovation, public health and personalized medicine.
- Access to these data will be provided through the "HealthData@EU" digital infrastructure with the participation of member states.

It is a matter of curiosity in the sector how the plan will be reflected in our legislation and what kind of a systematic will be established particularly for the secondary use of health data.

You can reach the full text of 2025 Presidential Annual Programme here (*Only available in Turkish)*. You can find more detailed information on EHDS here.

Regulation on Market Surveillance and Inspection of Products Introduced to the Market via Remote Communication Tools

The Regulation on Market Surveillance and Inspection of Goods Introduced to the Market through Remote Communication Tools **(Regulation)** was published in the Official Gazette on 30 October 2024. The Regulation regulates the principles, safety standards and rules to be complied with by the market subjects regarding the products placed on the market and kept on the market through remote communication tools, especially internet channels.

Pursuant to the Regulation, a product must comply with the relevant technical regulations or the General Product Safety Regulation in order to be placed on the market or kept on the market through remote communication tools.

The products of economic operators selling through remote communication tools will be deemed to be "placed on the market" if they target end-users residing in Turkey, and compliance with this legislation will be required. Economic operators may be deemed to target end-users in Turkey if the following conditions are met:

- Turkish language, warning and safety information in the sale advertisements,
- Indication of the price in Turkish liras,
- Providing shipping to Turkey or address option,
- The domain name is registered in the regions where shipments can be made to Turkey.

This issue is of critical importance for many platforms that sell from abroad to Turkey.

The economic operator will reflect the necessary information regarding the product that it introduces on the market or keeps on the market through remote communication tools in the sale advert. The details of this information are set out in the Regulation and in the relevant legislation for the products themselves.

The intermediary service provider will determine an electronic contact point for end-users to communicate quickly and directly on product safety, so that consumers can make complaints and notifications about the safety and suitability of the products at the contact points.

The intermediary service provider will provide easy access to information on products on its online platforms and will fulfil content-removing requests from authorized institutions within 24 hours at the latest.

The Regulation also regulates in detail the obligations of authorized representatives, performance service providers and intermediary service providers, and the duties, powers and responsibilities of authorized institutions responsible for product safety inspection and supervision.

Those who violate the Regulation will face administrative sanctions under the Law and other relevant legislation.

You can reach the full version of the Regulation here.

Standard Contract Notification Module and Guide Published

Turkish Data Protection Authority **(Authority)** announced through a public statement dated 25 October 2024, published on its website, that notifications of standard contracts would be made via the Standard Agreement Module.

As known, according to Article 9/5 of the Law on the Protection of Personal Data **(Law)**, the Authority must be notified in terms of the standard contracts, within 5 (five) business days after signing. Pursuant to Article 14 of the Regulation on the Procedures and Principles Regarding the Transfer of Personal Data Abroad, it is also stated that this notification can be made physically or via registered electronic mail **(KEP)** address or other methods to be determined by the Turkish Data Protection Board **(Board)**.

Due to the operational difficulties of physical transmission and the lack of widespread use of KEP, the announcement of facilitating methods has been expected for some time. The Standard Contract Notification Guideline **(Guideline)**, which explains the methods for the realization of standard contract notifications, has also been published. In summary, the Guideline explains the steps to be followed in terms of the processes of using the standard contract module. The steps to be followed for the use of the module are briefly as follows:

- Registering to the system as a data controller/data processor via https://standartsozlesme.kvkk.gov.tr.
- Adding an authorized person.
- Authorized persons add the parties to be included in the contract.
- Authorized person adds the contract: As an important note regarding this step, the authorized person must be logged in and the data controller/data processor selection process must be completed.
- On the contract editing page, it is necessary to select the transferor-recipient in terms of the parties, add information such as the party role, file description and the date that the signatures were completed.

It is also possible to send the contract to the Authority from the contract adding page. To proceed, an authorized person account must be used for login, following the same general logic as the module.

You can access the related Authority announcement here, the standard contract module here and the Guidelines here *(only available in Turkish)*.

European Union Commission Fines Meta: 798 million Euros

The European Commission (Commission) has fined Meta approximately €798 million for abusive practices that benefit Facebook Marketplace. The Commission's decision regarding the fine was published in a press release on 14 November 2024.

The basis for the Commission's decision is EU antitrust rules, which Meta used to link its online classified ad service Facebook Marketplace to the personal social network Facebook and imposed unfair trading conditions on other online classified ad providers.

The press release on the fine stated that Meta, by abusing its dominant position, breached Article 102 of the Treaty on the Functioning of the European Union, which prohibits the abuse of a dominant position in the internal market or in a substantial part of it. The Commission stated that Meta's infringement stemmed from two main issues:

- **Tying its online classified ads service Facebook Marketplace to its personal social network Facebook:** It was underlined that this would cause all Facebook users to be exposed to the Facebook Marketplace against their will and that this could hinder competitors in terms of competition. The Commission considered it anticompetitive for Facebook Marketplace to provide an advantage in terms of distribution that its competitors could not achieve through such a connection.
- **Meta's unilateral imposition of unfair commercial terms on its platforms on other online classified ad service providers who advertise:** In this case, the Commission's finding, in particular, that Meta will use data on other advertisers' ads exclusively for the benefit of its own platform, Facebook Marketplace, again points to a restriction of competition.

With the fine that was determined according to the Commission's 2006 Guideline on Fines, the issue that Meta should stop these anti-competitive activities was once again emphasized by the Deputy Executive Vice President for Competition Policy Margrethe Vestager.

You can access the press release regarding the decision from here.

Editors

Görkem Gökçe
gorkem.gokce@gokce.av.tr

Dr. Mehmet Bedii Kaya
bedii.kaya@gokce.av.tr

Elif Aksöz
elif.aksoz@gokce.av.tr

Yağmur Yollu
yagmur.yollu@gokce.av.tr

About us

Gokce Attorney Partnership is an Istanbul-based law firm offering legal services across a broad range of practice areas including mergers and acquisitions, joint ventures, private equity and venture capital transactions, banking and finance, capital markets, insurance, technology, media, telecoms and internet, e-commerce, data protection, intellectual property, regulatory, debt recovery, real property, and commercial litigation. Please visit our web site at www.gokce.av.tr for further information on our legal staff and expertise.

Please contact us at
info@gokce.av.tr
0 212 352 88 33