Keeping Up with EU Digital Policy 2022: Cybersecurity Edition

Written by Florina Pop and Laura Grant

Part four of the series: Digital Round-up 2022

Read part one here, read part two here, and read part three here

Welcome back to our blog series on EU digital policy developments of 2022! Moving on from the healthcare sector in our last instalment, we are ready to share our final segment where we will highlight some of the most important EU legislative developments of 2022 when it comes to cybersecurity, in addition to EIPA's courses in this area.

Cybersecurity

- **Cyber Resilience Act**

Background: With the number of cyberattacks continuously on the rise causing devastating impacts and the global cost of cybercrime at €5.5 trillion in 2021, the EU proposed the Cyber Resilience Act as a means of ensuring all products with digital elements meet rigorous cybersecurity standards before they are placed on the EU market. It is the first ever EU-wide legislation of its kind, which will help to ensure sufficient security and place the onus on manufacturers to remain responsible for cybersecurity throughout the product lifecycle.

Key Aims of the Cyber Resilience Act:

- Improve the security of products with digital elements, ensuring they're placed on the market with fewer vulnerabilities
- Ensure manufacturers remain actively responsible and accountable for cybersecurity throughout the lifecycle of the product
- Improve transparency for consumers on the security of products with digital elements
- Allow businesses and consumers to benefit from better cybersecurity protection and be well-informed about the security of the products they purchase and use

Key obligations of the Cyber Resilience Act:

- Manufacturers must take cybersecurity into account during the planning, design, development, production, delivery and maintenance phases
- Manufacturers must document all cybersecurity risks
- Manufacturers must report actively exploited vulnerabilities and incidents
- Manufacturers must ensure that vulnerabilities are handled effectively for the product lifetime or 5 years (whichever is shorter) once the product is on the market

Impact of the Cyber Resilience Act:

- Ensure products which meet cybersecurity standards will be placed on the market with the CE marking
- Harmonise the rules across Member States for placing products with digital elements on the market
- Harmonise the rules across Member States for the duty of care of the whole lifecycle of the product
- Consumers will be properly informed of the cybersecurity standards of the products they buy and use

Progress: The Act was proposed on 15 September 2022. The European Parliament and the Council will then examine the proposal. Once adopted, economic operators and Member States will have two years to adapt to the new requirements. The obligation to report actively exploited vulnerabilities and incidents will apply after one year.

- **NIS2 Directive**

Background: The NIS Directive aimed to create a common level of cybersecurity across the EU, and the NIS2 Directive will build on that, strengthening cybersecurity requirements, increase reporting requirements, and extending the scope of the original Directive across sectors.

Key Aims of the NIS2 Directive:

- Expand the scope of the NIS Directive to include a broader scope of entities and actors
- Harmonise cybersecurity requirements by setting out minimum rules for regulatory frameworks and incident reporting
- Create mechanisms for effective cooperation amongst Member States, including a national security strategy
- Implement fines for non-compliance

Impact of the NIS2 Directive:

- Strengthens cybersecurity risk and incident management across the EU
- Extends supervision and enforcement
- Creates accountability for non-compliance

Progress: The NIS2 Directive was adopted in November 2022 and entered into force on the 16 January 2023. EU Member States will have until 17 October 2024 to implement new requirements into national law.

Check out our topic-related courses

If you are interested in the EU's approach to cybersecurity and how it can impact your business or working environment, keep up to date with our website for updates on our our upcoming courses and seminars on data protection, artificial intelligence and cybersecurity.

The views expressed in this blog are those of the authors and not necessarily those of EIPA.