13 July 2026

Van Bael & Bellis

Commission presents Action Plan on Cybersecurity and Artificial Intelligence

On 7 July 2026, the European Commission (the ***Commission***) published its Action Plan on Cybersecurity and Artificial Intelligence (COM(2026) 577 final) (the ***Action Plan***). The Action Plan provides a targeted response to support Member States and organisations in the Union in addressing the new realities that Artificial Intelligence (***AI***) brings to the cybersecurity landscape. Rather than introducing new legislative obligations, the Action Plan builds on the EU's existing legal and regulatory framework and sets out concrete actions structured around three pillars. In this client alert, we provide an overview of the Action Plan's scope, the entities it affects, and the main actions and timelines set out by the Commission.

1. BACKGROUND

AI is transforming the cybersecurity landscape in two fundamental ways. AI can help detect vulnerabilities, prevent cyberattacks and strengthen the protection of critical infrastructure. At the same time, it can also be exploited by malicious actors to automate attacks, identify weaknesses and carry out cyber operations at unprecedented speed and scale. The EU enters this new reality with a solid legal foundation already in place, including the AI Act, the Cyber Resilience Act (***CRA***), the NIS2 Directive, the Digital Operational Resilience Act (***DORA***), and the Cyber Solidarity Act. Building on these foundations, the Action Plan structures its response around three pillars, each with specific key actions and delivery timelines.

PILLAR 1: PROMOTING THE SAFE AND RESPONSIBLE USE OF ADVANCED AI

The first pillar addresses the need to secure early awareness of advanced AI-enabled cyber capabilities so as to evaluate them *before* they are released, at the development stage, rather than discovering them after deployment, when they may already be accessible to malicious actors. In coordination with the European Union Agency for Cybersecurity (***ENISA***), the Commission will also develop a European Blueprint, as a guidance document, to spell out how providers of AI with advanced cyber capabilities can grant access to European organisations, including companies, and thereby support their mitigation of cyber risks. It will also enable the safe testing of AI tools through a secure European testing platform. The Commission will also exercise its supervisory and enforcement powers under the AI Act to ensure effective oversight of general-purpose AI models, including those presenting systemic cybersecurity risks.

PILLAR 2: REINFORCING THE EU'S CYBERSECURITY AND RESILIENCE

The second pillar focuses on preparedness, vulnerability management, and the practical application of AI tools across the EU's cyber ecosystem. ENISA is due to issue guidance, recommendations, and best practices on protection against AI-powered threats and the secure integration of AI in cybersecurity operations, with tailored guidance for SMEs. The Commission and the Member States will cooperate with ENISA and the industry to upgrade existing vulnerability management practices and tools for the AI age. ENISA will also launch a Critical Open Source Resilience Campaign to accelerate patching of open source components relevant to critical infrastructure, leveraging AI to support open source maintainers responsible for the ongoing upkeep and security patching of those components.

PILLAR 3: SCALING UP EUROPE'S AI CAPABILITIES FOR CYBERSECURITY

The third pillar aims to ensure that the Union can develop, deploy and scale its own AI-powered cybersecurity solutions, rather than remaining strategically dependent on capabilities developed elsewhere. For that purpose, the Commission has committed significant investment under Horizon and Digital Europe (EUR 200 million by the end of the current Multiannual Financial Framework, i.e. 2027) and through the European Innovation Council (EUR 100 million for strategic defence tech start-ups and scale-ups). Key initiatives also include launching a dedicated Grand Challenge on AI-assisted vulnerability remediation and addressing the need to build sovereign European frontier AI capabilities, including for defence. In addition, the Commission plans to develop training modules for cybersecurity professionals on the use of AI tools under the Cybersecurity Skills Academy.

ENTITIES AFFECTED

The Action Plan is relevant to a broad range of entities. Providers of general-purpose AI models with systemic risk will be subject to supervisory and enforcement action by the Commission under the AI Act as of 2 August 2026, including cybersecurity risk assessment and mitigation obligations. Operators of critical infrastructure and financial entities, subject to the NIS2 Directive and DORA respectively, are called upon to adjust their risk management frameworks for AI-powered threats. Product manufacturers will need to comply with the CRA's secure-by-design and vulnerability management requirements, fully applicable as of 11 December 2027, while SMEs and cybersecurity professionals are also specifically targeted by the Action Plan's guidance and skills initiatives.

2.CONCLUSION

The Action Plan marks the continuation of a sustained and coordinated European effort to address the cybersecurity implications of advanced AI. With the majority of key actions targeted for delivery by Q4 2026, organisations operating in critical infrastructure sectors, the financial sector, and the AI supply chain should begin assessing their existing cybersecurity and AI risk management frameworks without delay. For further information or assistance, please do not hesitate to reach out to us.

The full text of the Action Plan on Cybersecurity and Artificial Intelligence can be downloaded on the Action Plan press release page here.

Van Bael & Bellis regularly advises clients across industry sectors on EU cybersecurity and AI regulatory matters, including compliance with the AI Act, the NIS2 Directive and DORA. Our team can assist with assessing the implications of the Action Plan for your organisation, reviewing and updating cybersecurity risk management frameworks, advising on obligations vis-à-vis ENISA and national authorities, and engaging with public consultation and standard-setting processes as they develop. Please do not hesitate to contact us if you have any questions.

Key contacts

Tanguy Van Overstraeten
Partner
tvanoverstraeten@vbb.com

Gert-Jan Fraeyman
Counsel
gfraeyman@vbb.com

Sarah Muzembo
Associate
smuzembo@vbb.com

Brussels
Glaverbel Building
Chaussée de La Hulpe 166
B-1170 Brussels
Belgium
+32 (0)2 647 73 50

Geneva
2 Chemin des Mines
CH-1202
Geneva
Switzerland
+41 (0)22 320 90 20

London
Holborn Gate
330 High Holborn
London, WC1V 7QH
United Kingdom
+44 (0)20 7406 1471

www.vbb.com