CROWDSTRIKE RESPONSE TO THE EUROPEAN COMMISSION CALL FOR EVIDENCE ON THE DIGITAL OMNIBUS (DIGITAL PACKAGE ON SIMPLIFICATION)

14 October 2025

I. INTRODUCTION

In response to the European Commission's ("Commission") Call for Evidence on the Digital Omnibus, CrowdStrike offers the following views.

We approach these questions from the standpoint of a leading international, AI-native, cloud-native cybersecurity provider that defends globally distributed enterprises from globally distributed threats. CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive hunting, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is informed by CrowdStrike's role in protecting organizations from data breaches and a variety of other cyber threats.

II. COMMENTS

The Commission's proposal for a Digital Omnibus rightly identifies the urgent need to reduce complexity in the EU's digital regulatory environment. Stakeholders across industries face significant burdens from overlapping obligations, fragmented implementation, and legal uncertainty. These issues are particularly acute in the provision of **state-of-the-art cybersecurity services**, which are critical not only for the digital economy but also for the protection of fundamental rights and the resilience of European society.

A central tension in the current acquis is that measures designed to protect data and users sometimes **inadvertently constrain defenders**. Obligations arising from the GDPR, the Data Act, and sector-specific rules often conflict or overlap in ways that undermine rapid, effective cybersecurity operations. For example, restrictions on cross-border data flows or ambiguous definitions of "data processing services" can delay incident detection and response. In practice, such rules risk leaving defenders with **less visibility and agility than attackers**, a situation that is both paradoxical and dangerous.

Equally, the **multiplicity of incident reporting obligations** under GDPR, NIS2, and DORA illustrates the unintended administrative load placed on organisations during active crises. The Commission is correct to acknowledge that divergent timelines and formats for breach notifications create unnecessary burdens. Importantly, these obligations fall most heavily on small and mid-cap enterprises, which often lack the resources to dedicate staff solely to regulatory reporting during emergencies. The result is a compliance-driven environment where precious time and expertise are diverted away from containing threats.

The Commission is also right to stress that regulatory simplification must not compromise protection standards. Indeed, the **effectiveness of cybersecurity safeguards is directly tied to their ability to be deployed quickly, consistently, and at scale**. Fragmented obligations and unclear definitions weaken that effectiveness, leading to gaps in coverage and hesitancy in adopting advanced technologies. For AI-driven cybersecurity in particular, ambiguity around risk classification under the AI Act threatens to slow adoption of tools that are already indispensable to detecting zero-day attacks and stopping malware-free intrusions.

More broadly, the Digital Omnibus represents an important opportunity to reaffirm that **data protection and cybersecurity are mutually reinforcing objectives**. High levels of data protection cannot be achieved without strong, agile cybersecurity; conversely, effective cybersecurity enables the safeguarding of personal data and the trustworthiness of digital services. Simplifying the legal environment is therefore not merely an administrative exercise: it is a prerequisite for enabling Europe to deploy world-class security capabilities across all sectors, from critical infrastructure to small- and medium-sized enterprises (SMEs).

The Commission's initiative to launch a Digital Fitness Check is a welcome step in this direction. However, the urgency of current threats makes it essential that immediate simplification under the Digital Omnibus focus on those areas where complexity most directly undermines defenders. Without such adjustments, organisations may be forced to operate under compliance regimes that consume resources at the expense of genuine resilience — ultimately leaving Europe less secure and less competitive.

III. RECOMMENDATIONS

To achieve the objectives of the Digital Omnibus and deliver meaningful simplification, we recommend the Commission adopt the following measures:

A. Artificial Intelligence Act – Clarification of Recital 55

The Commission should provide binding clarification that AI systems developed exclusively for cybersecurity purposes do not fall within the scope of "safety components" under Article 6(1). Recital 55 makes clear that such systems should not be treated as high-risk unless they are directly tied to physical safety outcomes. Operationalising this principle will prevent the misclassification of cybersecurity AI tools—such as intrusion detection, anomaly monitoring, or access control—and avoid regulatory disincentives that could otherwise discourage deployment of state-of-the-art defensive technologies.

B. Data Act – Definition of "Related Services" and "Data Processing Services"

Article 2(6) of the Data Act contains ambiguous wording around "related services" and "data processing services," creating a risk of divergent national interpretations. To ensure legal certainty, the Commission should explicitly clarify that processing activities undertaken strictly for cybersecurity purposes (e.g., incident response, threat detection, penetration testing) are distinct from commercial data or cloud services. Security-related processing should benefit from a recognised exception aligned with GDPR Article 32 and Recital 49, which establish "state of the art" security as integral to data protection.

C. Data Flows and Localization – Cybersecurity Exception

Hard data localisation impedes global threat visibility, delays detection of attacks, and undermines the ability of defenders to meet ENISA's "state of the art" cybersecurity expectations. To preserve Europe's cyber resilience, the Digital Omnibus should embed a universal **cybersecurity exception to localisation requirements to future legislation**, permitting the cross-border transfer of telemetry strictly for defensive purposes such as threat hunting, incident response, and penetration testing. This would prevent adversaries from exploiting regulatory blind spots while ensuring EU organisations can leverage the best available protections.

D. ePrivacy – Remove Duplication and Ensure Security Exceptions

The Commission should recognise that the ePrivacy Directive has become outdated and duplicative of GDPR. Its coexistence with GDPR creates unnecessary uncertainty for cybersecurity providers, particularly when processing security-relevant data such as telemetry, logs, and IP addresses. We recommend that ePrivacy provisions be repealed and fully integrated into GDPR, which already provides a robust framework for personal data processing in electronic communications. This would remove regulatory

overlap, provide legal certainty, and ensure that state-of-the-art cybersecurity services can be delivered without undue legal risk.

E. Cybersecurity – Towards a One-Stop-Shop for Incident Reporting

The current fragmentation of breach notification obligations under GDPR, NIS2, and DORA creates significant administrative burdens, particularly at the critical early stages of incident response. Divergent timelines are impractical when supervisory authorities themselves lack 24/7 capacity to process notifications. We strongly support the establishment of a **"report once, comply many"** one-stop-shop model, harmonising definitions, timelines, and formats across these frameworks. This approach would reduce duplication, improve efficiency, and allow security teams to prioritise containment and remediation. AI tools for ensuring the ease of reporting should be allowed in the process of ensuring improved compliance.

F. Simplification and Coherence Across the Digital Acquis

Finally, the Commission should ensure that the Digital Omnibus promotes consistency and avoids duplication across the entire EU digital rulebook. Applying a **"report once, comply many" principle** more broadly, not only for cybersecurity, and aligning requirements across overlapping legal instruments will significantly reduce unnecessary compliance costs, especially for SMEs and mid-caps, without lowering protection standards.

G. Cybersecurity Risk Management Practices

Finally, the following points outline key considerations to help ease the burden on businesses while strengthening Europe's overall cybersecurity posture. Policymakers should ensure that regulatory frameworks promote practical, risk-based approaches that encourage innovation, operational resilience, and cross-border cooperation. Effective cybersecurity risk management requires proactive security requirements and a comprehensive, risk-based strategy leveraging key technologies such as cloud security, Endpoint Detection and Response (EDR), next-generation SIEM solutions, machine learning-based prevention, and Identity Threat Detection and Response (ITDR). These capabilities enable organizations to defend against evolving threats across hybrid environments. Essential security practices include ensuring speed in incident response, conducting continuous threat hunting, adopting Zero Trust architectures to limit lateral movement and privilege escalation, maintaining robust logging practices for detection and investigation, and leveraging Managed Security Service Providers (MSSPs) to augment internal security capabilities. Together, these

measures enhance resilience, situational awareness, and protection against sophisticated cyber adversaries across Europe.

IV. CONCLUSION

CrowdStrike supports the Commission's simplification agenda. The Digital Omnibus offers a unique opportunity to cut unnecessary compliance costs, align overlapping requirements, and strengthen both competitiveness and resilience. A streamlined EU digital rulebook—anchored in legal clarity, proportionality, and cybersecurity best practice—will better protect citizens, empower SMEs, and enable Europe to lead in innovation and digital security.

V. ABOUT CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/.

CONTACT

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

Drew Bagley
VP & Counsel, Privacy and Cyber Policy

Līga Rozentāle, CISM
Director, Public Policy EU/International

Email: policy@crowdstrike.com

###