CROWDSTRIKE

CROWDSTRIKE RESPONSE TO THE EUROPEAN COMMISSION CALL FOR EVIDENCE ON THE DATA UNION STRATEGY

18 July 2025

I. INTRODUCTION

In response to the European Commission's ("Commission") Call for Evidence on the *Data Union Strategy* ("Strategy") 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

CrowdStrike applauds the Commission's efforts to streamline existing data rules, potentially creating a simplified, clearer, and more coherent legal framework for businesses and administrations to share data more seamlessly and at scale, while still upholding high privacy and security standards. Additionally, we appreciate the opportunity to provide input on examining ways to use data to reduce administrative burden, and address the external aspects of data flows. In this comment, we offer ideas to further improve the regulation of international transfers of data, as well as cooperation and measures necessary to ensure the security of data.

Currently, we have observed the following themes in international data strategies as it relates to cybersecurity.

A. *Data Protection Requires Global Threat Visibility*

Effective cybersecurity depends on access to large volumes of diverse, real-time telemetry across regions. Leading cybersecurity vendors, such as CrowdStrike, rely on cloud-scale analytics and global threat hunting to detect and stop breaches. Limiting data flows undermines the very protections that EU data protection law seeks to ensure under Article 32 of the GDPR and Recital 49, which call for "state of the art" cybersecurity.

Hard data localization—which could restrict the transmission of security-relevant telemetry—risks creating gaps in visibility. At a minimum, this could increase the time to detect attacks, and potentially it could cause failure to detect attacks at all.[1]

B. The Current Legal Framework Creates Friction and Risk

The interplay between the GDPR, the Data Act, and proposals like the EUCS certification creates legal ambiguity and conflicting obligations. Cybersecurity service providers, for example, must comply with data minimization principles under the GDPR while simultaneously enabling detailed telemetry analysis required under the Data Act's data access obligations. Moreover, the GDPR's strict transfer rules (e.g., the Schrems II ruling) have led to enforcement actions that threaten critical services, including lawful red teaming and penetration testing.

The result is an environment where defenders know less than attackers—one where defensive practices like incident response, threat hunting, and vulnerability testing are inhibited due to legal uncertainties surrounding international data transfers.

Therefore, to better preserve personal data, it is critical to promote policies that ensure access to security data for globally-distributed cybersecurity teams. Data protection is best achieved where intentional transfers of personal data are permitted with practical safeguards, while unintentional transfers of personal data via data breaches are thwarted by protecting against ever-evolving cybersecurity threats with innovative technologies. As a leading cybersecurity provider, it is our view that the most significant threat to personal data comes from threat actors operating unlawfully. While responsible data controllers and processors adhere to robust compliance programs, cyber adversaries do not play by the rules.

C. Fragmentation Undermines Cybersecurity and Digital Sovereignty

The current patchwork of national data policies, combined with extraterritorial application of GDPR and sector-specific rules, makes it difficult for defenders to maintain coherent security strategies across borders. This fragmentation inhibits incident response collaboration, weakens supply chain security, and disproportionately affects small- and medium-enterprises. Instead of enhancing digital sovereignty, such approaches create blind spots in security visibility and delay response capabilities.

[1] Swire, P., Kennedy-Mayo, D., Bagley, D., Krasser, S., Modak, A., & Bausewein, C. (2024). Risks to cybersecurity from data localization, organized by techniques, tactics and procedures. Journal of Cyber Policy, 9(1), 20–51. https://doi.org/10.1080/23738871.2024.2384724.

III. RECOMMENDATIONS

CrowdStrike recommends the Commission leverage the following principles while drafting the Strategy. We view these as best practices to protect, and encourage the use of best-in-class cybersecurity practices.

1. Adopt a Cybersecurity Exception for Cross-Border Data Transfers

The Data Union Strategy should include a cybersecurity exception under GDPR Chapter V to permit the transfer of personal data strictly for essential security purposes such as threat detection, incident response, red teaming, or penetration testing. These functions are necessary to uphold GDPR Article 32's mandate for "state of the art" security safeguards and Recital 49's recognition that cybersecurity is intrinsic to data protection. The EU should take note of international models that allow for international data transfers for legitimate purposes such as enabling security operations.[2]

2. Align EU Data Localization Rules with State-of-the-Art Cybersecurity

ENISA guidelines define “state of the art” cybersecurity as including practices like global threat intelligence and cloud-based detection. Any certification scheme (e.g., EUCS) or data localization proposal should explicitly assess its impact on cybersecurity capabilities and provide flexibility to maintain cross-border operational integrity

3. Promote International Data Flows Anchored in Trust and Transparency

CrowdStrike supports the Data Free Flow with Trust (DFFT) initiative and the OECD Trusted Government Access Declaration. The EU should lead efforts to develop global frameworks that protect privacy while enabling responsible data sharing for cybersecurity and innovation.

4. Streamline and Harmonize Regulatory Requirements

The Commission should initiate regulatory simplification across the digital acquis—spanning the GDPR, Data Act, DGA, and sectoral laws—to avoid overlapping

[2] Saudi Arabia’s Personal Data Protection Law and Cloud Cybersecurity Controls (https://nca.gov.sa/ccc-en.pdf) recognize that cybersecurity is both a necessary justification for data transfer and a compliance obligation, explicitly requiring implementation of state-of-the-art safeguards and technologies such as Endpoint Detection and Response (EDR) for effective data breach prevention and threat management.

obligations. A “report once, comply many” principle, common definitions of personal vs. non-personal data, and coordinated guidance from data protection and cybersecurity authorities would significantly reduce compliance friction.

IV. CONCLUSION

CrowdStrike appreciates the opportunity to contribute to the shaping of the EU Data Union Strategy. A balanced, innovation-friendly, and security-conscious approach to data governance is essential to achieving Europe’s ambitions for AI, competitiveness, and digital sovereignty.

Data protection and cybersecurity are not competing objectives—they are mutually reinforcing. CrowdStrike looks forward to continuing our engagement with the Commission and EU stakeholders to support a strong, agile, and secure European data ecosystem.

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