REQUEST FOR COMMENT RESPONSE

European Data Protection Board: Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (adopted 10 November 2020)

21 December 2020

I. INTRODUCTION

In response to the European Data Protection Board's (EDPB) request for public consultation, on Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data ("Recommendations"), to gather the views and concerns of all interested stakeholders and citizens, CrowdStrike offers the following views.

We approach this public consultation from the standpoint of a leading international, US-headquartered cloud-native cybersecurity provider, with various establishments in the EU, that defends globally-distributed enterprises from globally-distributed threats such as intellectual property theft, financially-motivated crime, destructive attacks, and data breaches. CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is shaped by CrowdStrike's role in protecting organizations from data breaches and a variety of other cyber threats.

Consistent with our engagement in the GAIA-X project for the development of an efficient, competitive, secure and trustworthy data ecosystem for Europe, we believe today's economy depends on more cross-border data flows than ever before. This trend will continue, especially in light of the digital transformation accelerated by Covid-19 and the "work from anywhere" movement. The importance of cross-border data flows is far-reaching, from data subjects who benefit from offerings or contribute to the digital workforce all the way to the organizations that manage data flows. Consequently, it is important for EDPB guidance to recognize the dependency of EU innovation, EU workforce jobs, and effective cybersecurity on cross-border data flows. This means that it is critical to provide organizations with deference to make their own context-informed decisions about cross-border data by adhering to the Court of Justice of the European

Union's ("ECJ") Schrems II principle of focusing on the circumstances of specific transfers and weigh risks accordingly.

II. COMMENTS

The ECJ's Schrems II decision,[1] which invalidated the EU-U.S. Privacy Shield on the basis of an adequacy decision adopted by the European Commision, revolves around the question of how "appropriate safeguards" and "adequate levels of protection" can be met when transferring personal data from the EU to a third country without any level of adequate protection in terms of Art. 45(I) of the GDPR ("Third Country"), and further, how the protection afforded is "essentially equivalent" to the protections guaranteed in the GDPR as read in light of the EU Charter of Fundamental Rights. We commend the EDPB for its goal of helping personal data exporters navigate the process of identifying adequate supplementary measures to protect international data transfers from the European Economic Area (EEA) to any third country.

In its ruling, the ECJ focused on the importance of assessing the totality of the circumstances of any particular transfer, recognizing that not all transfers or data types pose the same risk to data subjects. Even though the EDPB supports the idea of reviewing supplemental transfer tools on a case-by-case basis, the EDPB's current draft six-step test fails to appropriately ascribe value to the actual circumstances of the transfer in line with ECJ's ruling and practical implications for data subjects. We believe that it would be beneficial for data subjects and data exporters alike for the EDPB to align the characterization of international data transfers with the European Commission's future vision for new standard contractual clauses,[2] artificial intelligence innovation,[3] and cybersecurity priorities.[4]

CrowdStrike has previously noted in the public consultation of the European Commission on the latest draft SCCs the "Chain of Contractual Accountability," imposed by GDPR Art. 28, and the "Chain of Independent Obligations" imposed directly by GDPR writ large, provide substantial protections for EU personal data regardless of where it is transferred.[5] Accordingly, the EDPB is in a unique position to provide guidance on circumstances that may be novel to specific types of transfers under certain conditions that may materially affect pre-existing contractual and direct regulatory obligations. Simply put, data protection is best achieved where intentional international transfers of personal data are permitted with practical safeguards while unintentional transfers of

[1] C-311/18 - Facebook Ireland and Schrems.
[2] Draft implementing decision - Ares(2020)6654686, Annex - Ares(2020)6654686; Draft implementing decision - Ares(2020)6654429, Annex - Ares(2020)6654429.
[3] See https://ec.europa.eu/digital-single-market/en/artificial-intelligence.
[4] See https://ec.europa.eu/digital-single-market/en/cybersecurity-strategy.
[5] *See* https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Data-protection-standard-contractual-clauses-for-transferring-personal-data-to-non-EU-countries-implementing-act-/F1305866.

personal data via data breaches are thwarted by protecting against ever-evolving cybersecurity threats with innovative technologies.

A. Step 2: Identify the transfer tools

Consistent with our public comment to the Report from the Commission on the application of the General Data Protection Regulation, European Commission, DG JUST.C3 and C4, of 29 April 2020,[6] we applaud the EDPB for clearly articulating the hierarchy of adequacy mechanisms, whereby alternative mechanisms like standard contractual clauses ("SCCs") are only necessary where a country-specific adequacy decision does not exist.

B. Step 3: Assess efficacy

An assessment of whether the Article 46 GDPR transfer tool is effective in light of all circumstances of the transfer should not only focus on a third country's legislation and practices applicable to the transfer, but on other details as well, such as the actual risk inherent in the data itself as framed by those articulated in Recitals 75 and 76 of the GDPR. The GDPR itself recognizes in these recitals, and the EDPB has previously recognized in data breach impact guidance,[7] that potential risks posed by various data processing activities vary greatly and depend heavily upon the type of personal data in question.

As a practical matter, the narrow approach taken by the EDPB to focus its Recommendations on the mere existence of certain legislation and practices of third countries: i) is not in line with the ECJ's emphasis on a case-by-case analysis for transfers, and ii) ignores other factors that may be more indicative of the true adequacy of a particular transfer. Assessing whether the Article 46 GDPR transfer tool is effective on a case-by-case basis should take into account the overall circumstances of a transfer including, but not limited to, the categories of personal data involved, processed and transferred.

As a matter of principle, the distinction between EU member state laws and those of any particular third country are not necessarily indicative of whether or not an international transfer of personal data will affect the rights and liberties of data subjects. In fact, cross border transfers amongst EU member states sometimes trigger more onerous national security authorities than those posed by third countries.[8] In other words, an EU citizen in one member state may be afforded more protections under their domestic laws than those in another EU member state. Nonetheless, this

[6] *See* https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12322-/F514249.
[7] Art. 29 Working Group, Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01).
[8] *See generally*, Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU, FRA (2017), https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf.

legal phenomenon is absent from the analysis applied in the current draft EDPB guidance.

The mere existence of a legal authority is often not indicative in and of itself about how such authority is actually used in practice, nor the probability that it would actually affect data in a given transfer. In fact, judicial recourse and institutional safeguards may drastically reduce the likelihood of a given law's applicability[9] or, alternatively, provide robust safeguards against abuse. For example, the EDPB guidance notes that the U.S. surveillance authority 50 U.S.C. § 1881a ("FISA 702") may be applicable in the case of cross-border transfers, but does not consider the fact that there are safeguards in place such as targeting restrictions and minimization procedures subject to judicial review. Moreover, the same legal framework enables electronic communications service providers the ability to challenge in court a government request to turn over data.[10] Many observers have argued that such judicial recourse goes further than those available today in some EU member states and provides safeguards similar in purpose and substance to the safeguards proposed in the EU E-Evidence Regulation.[11] Consequently, the mere existence of a legal authority, on its own, is not necessarily indicative of whether or not a transfer to a third country will violate the rights of EU data subjects. Conversely, similar or "adequate" laws in third countries do not automatically guarantee data protection.

As a cybersecurity provider that defends globally distributed enterprises from globally distributed threats, we find that threats to personal data often come by extra-judicial means and disregard the rule of law. While responsible data controllers and processors adhere to robust compliance programs, cyber adversaries do not play by the rules.

Finally, it is critical to focus on internationally-accepted principles-based concepts rather than prescriptive technical requirements to enhance privacy while fostering technologies that secure personal data. Endorsing a risk-based approach whereby factors such as the sensitivity of data in question, the impact posed by a potential breach, and mitigation actions that would be available to affected individuals best meets data projection objectives and reflects the realities of a world where technological innovation advances at a faster pace than law. This means that the nature of personal information and context of data processing activities should be central to the applicability of requirements.

---

[9] *See* https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF (U.S. government noting that FISA is more likely to be applicable in the context of certain communications rather than all data processing activities).

[10] 50 U.S.C. § 1881a(d) - (e), (i).

[11] *See* https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en.

C. Step 4: Adopt supplementary measures

Regarding the adoption of supplementary measures, we agree with the EDPB that the identification of supplementary measures should be done on a case-by-case basis.[12] Further, we commend the EDPB for its non-exhaustive list of factors for identifying which supplementary measures may be the most effective in protecting transferred data.[13] Here, we highlight the most important supplementary measure, cybersecurity. Cross-border data flows are necessary for cybersecurity in the private sector, not much unlike how national security depends upon cross-border data flows in the public sector.[14]

We recommend thinking about the importance of cybersecurity as a supplemental measure by looking at threats, predominantly in terms of threat actors. Malware, malicious infrastructure, and adversary tactics, techniques, and procedures (TTPs) change over time, but often the groups behind malicious activities are more durable. This means that considering threat actor motivations helps defenders understand everything from their incentives to the risks posed by failing to prevent them from breaching your environment. Threat actors generally fall into the categories of: criminal groups, which largely seek profit; nation state entities, which pursue a variety of geopolitical ends; and 'hacktivists,' which have ideological motives. When crafting guidance, entities like the EDPB must be concerned with each, particularly during a time of unprecedented attacks from specific nation states along with the general trend of increased e-crime.

Specific threats vary across these different types of actors, but a few are especially notable. Criminal groups increasingly target public sector entities with ransomware, which disrupts victim IT environments in order to extort funds. Nation state groups have also used ransomware-like tools and TTPs to cause disruptions for other ends. Additionally, nation states have been observed to hack and leak sensitive communications for political ends, or steal intellectual property or sensitive business information to strengthen domestic commercial actors. Across all types of threat groups, adversaries are leveraging TTPs that enable them to avoid using malware, which complicates detection and prevention for entities using unsophisticated or legacy security solutions.

---

[12] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Nov. 10, 2020), at para. 46.

[13] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Nov. 10, 2020), at para. 49.

[14] https://www.wsj.com/articles/eu-leans-heavily-on-u-s-program-tracking-terror-financing-11605794404; https://documents.pclob.gov/prod/Documents/EventsAndPress/b8ce341a-71d5-4cdd-a101-219454bfa459/TFTP%20Chairman%20Statement%2011_19_20.pdf.

Further, we advocate the "1-10-60 Rule."[15] This concept holds that organizational leaders should measure each of these performance indicators over time, and improve them until security teams can reliably detect malicious events within one minute; investigate them within ten minutes; and isolate or remediate affected hosts or resources within one hour. Some third countries are associated with nation-state sponsored data breaches against EU citizens, but organizations that can defend themselves at this velocity will outpace the vast majority of threat actors,[16] and prevent minor security events from becoming costly, complex, and sometimes devastating incidents.

To summarize, cyber attacks from advanced nation-state actors, hacktivists, and more, pose a substantial threat to the safety of personal data and thus, we emphasize the importance of cybersecurity as a supplemental measure in future EDPB guidance.

D. Annex 2 - Examples of Supplementary Measures

In addition to the steps outlined by the EDPB, we find it important to comment on Annex 2's examples of supplementary measures and, in particular, the scenarios for which effective measures could be found. Although these scenarios are helpful, they lack consideration of cross border transfers between EU member states and assume that the public authorities of a third country may be the only entity responsible for inadequate protections. Thus, we reiterate the commentary made above regarding Step 3.

III. CONCLUSION

The EDPB's recommendations are a thoughtful response to the complex legal and policy issue of supplementary measures and transfer tools regarding the transfer of personal data to third countries. CrowdStrike is in the business of data protection and presents its feedback in the context of understanding the diversity of its own customers IT management and security organizations, as well as technologies dependent upon cross-border data flows. As the EDPB considers appropriate revisions to the supplementary measures to transfer tools, we reiterate the importance of reviewing with an eye towards protecting personal data in a holistic manner that incentivizes the adoption of strong cybersecurity safeguards. Adversaries innovate at a record-pace, and it is important to empower defenders to leverage global data flows, big data analytics, and machine learning to protect against ever-evolving threats. Ultimately, there is an indisputable distinction between trusted, intentional cross-border data flows and unintentional, adversary-initiated exfiltration of data. Consequently, guidance should

[15] A more in-depth explanation of this concept is available here: https://www.crowdstrike.com/resources/crowdcasts/the-1-10-60-minute-challenge-a-framework-for-stopping-breaches-faster/.

[16] The EDPB's draft guidance does not currently reference any of the nation states associated with persistent and major data breaches against EU citizens. *See* CrowdStrike's 2020 Global Threat Report: https://www.crowdstrike.com/resources/reports/2020-crowdstrike-global-threat-report/.

defer to parties to make their own data flow decisions while incentivizing the adoption of sophisticated security safeguards to protect against breaches.

IV. ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale AI and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events 4 per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches. Learn more: https://www.crowdstrike.com/.

V. CONTACT

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

Drew Bagley CIPP/E
VP & Counsel, Privacy and Cyber Policy

Dr. Christoph Bausewein CIPP/E
Director & Counsel, Data Protection & Policy

Email: Privacy@crowdstrike.com

***