REQUEST FOR COMMENT RESPONSE

Regulation of International Transfers of Personal Data and the Model of Standard Contractual Clauses

Brazil's General Data Protection Law (LGPD)

September 14, 2023

I. INTRODUCTION

In response to Brazil's National Data Protection Authority's ("ANPD") request for feedback on the Regulation of International Transfers of Personal Data and the model of Standard Contractual Clauses ("Regulation"), CrowdStrike offers the following views.

We approach these questions from the standpoint of a leading international, US-headquartered, 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 ANPD's effort to create a mechanism for international transfers of personal data, as well as a model of Standard Contractual Clauses (SCCs). The global digital ecosystem is reliant upon onward transfers of personal data, which must be done according to certain transfer mechanisms, one of which is SCCs. CrowdStrike provided comments to the ANPD on this mechanism last year, in response to ANDP's Request for Comment on "International Transfers of Personal Data".[1] In this comment, we offer ideas to further improve the regulation of international transfers of personal data, as well as re-iterating some of our previous points.

[1] For a copy of our comment, please email policy@crowdstrike.com.

Chapter III. International Data Transfer

Article 9 of the proposed Regulation states that the international data transfer shall only be carried out for legitimate, specific and explicit purposes communicated to the data subject. Regarding this issue, we suggest considering the importance of cybersecurity, which is not mentioned in any of the chapters of the proposed regulation.

Supporting contractual agreements and SCCs can be done with a strong policy on cybersecurity. Cross-border data flows are necessary for cybersecurity. In fact, many of the most innovative technologies for protecting personal data against data breaches leverage endpoint telemetry data, cloud-native Software-as-a-Service (SaaS) delivery, 24/7 global threat hunting, and cross correlation of indicators of attack. Moreover, modern IT infrastructure in general often invariably involves cross-border data transfers.

Some of the biggest risks to personal data come from cyber threat actors associated with nation states, hacktivists and eCriminals. In addition to encrypting enterprise networks to disrupt or halt operations, such threat actors increasingly threaten to publicly leak stolen data, from sensitive business information and intellectual property to internal communications and customer data, including financial or health data.

Therefore, to better preserve personal data, it is critical to promote policies that ensure access to security data for global operating 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 perhaps 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.

Furthermore, research has shown that limiting data transfers can have an adverse impact to cybersecurity and restricts the ability of defenders to follow best practices.[2] Data sharing limitations reduce the ability of countries to identify, protect, detect, respond, and recover in the face of cyberattacks. Ultimately, it is important to

[2] *Risks to Cybersecurity from Data Localization, Organized by Techniques, Tactics, and Procedures*, 2023. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4466479

incentivize strong technical mechanisms for data protection, rather than focusing on data transfer limitations, which cyber threat actors ignore.

Chapter IV. Adequacy Decision

Chapter IV, Article 10 and Article 12 provide that the ANPD will determine which jurisdictions have an adequate level of protection to allow the free flow of personal data between Brazil and such countries. The Articles also provide that the ANPD will prioritize the review of jurisdictions that offer reciprocal protections. We find this approach difficult and caution against it.

The European Union's "allow list approach" has shown it is difficult to rely on a small number of countries or jurisdictions designated as providing parity data laws. The difficulty with this approach is two-fold. First, instead of relying upon a single international standard, such approaches create competing standards for adequacy that may or may not take into account a holistic approach to data protection in another jurisdiction nor other risk-mitigation measures related to data flows. Second, current experience has demonstrated that approval processes can be burdensome for both the applicant country and the host data protection authority. Brazil's economy is dependent upon global data flows, and relying upon an allow list approach can take years of administrative time, as it involves review and complex analysis of legal regimes that are often not static. The allow list approach creates obstacles that can inhibit Brazilian companies, organizations and public sector bodies from engaging in cross border data flows and even accessing key technologies.

Chapter V and Annex II. Standard Contractual Clauses (SCCs)

Annex II, Section 1, Clause 4, Option A and B

Under Annex II, Section 1, Clause 4, Option A and Option B, ANPD notes that regardless of whether the exporter or importer (as the Designated Party) is listed as the responsible party for certain measures, the controller is ultimately responsible for (i) compliance with the obligations under the law and the agreement, (ii) responding to the ANPD, (iii) guaranteeing the data subject's rights and (iv) the reparation of damage they may suffer. Furthermore, under Annex II, Section I, Clause 4, Option B, the ANPD notes that when exporter and importer are processors, the third party controller, which instructs the processor that exports the personal data to the importer outside Brazil, must co-sign the SCCs and be responsible under the SCCs.

Experience has shown that well-drafted, technology-neutral SCCs can be a reliable, easy to use and manageable means to flow down legal protections. As the ANPD considers developing and implementing SCCs, we emphasize that SCCs should be written with flexibility and harmonization[3] in mind as an international transfer mechanism. When parties have the flexibility to negotiate contractual terms, they may be customized to specific use cases and technological designs. Accordingly, SCCs written with narrow specifications and rigid obligations risk being impractical with the realities of the data flows they seek to protect.

Each of the parties in the SSCs – controllers, processors, and sub processors – are contractually bound to those with whom there is privity of contract, and the resulting legal protections create a "Chain of Contractual Accountability."

Moreover, each party must abide by its own General Data Protection Law (LGPD) requirements in a "Chain of Independent Obligations." In other words, data subject rights remain protected by (i) enforceable contractual obligations between respective parties, and (ii) direct application of Brazil's General Data Protection Law (LGPD) to any party processing personal data within the scope of LGPD.

Where both the Chain of Contractual Accountability and the Chain of Independent Obligations exist, the legal position of the data subject is adequately protected. For example, a controller that is party to a Data Processing Agreement with a processor will afford protections to its own data subjects because the processor is also obligated to obtain commitments from its own processors that process the controllers' data.

Acting in concert with these contractual protections, the parties' independent obligations under LGPD, including the requirements to establish a compliant LGPD program and deploy state-of-the-art and risk appropriate security safeguards in line with LGPD Article 6 and Article 46, act to further strengthen the protection of personal data and the legal rights of data subjects. Ultimately, existing, well-established concepts of privity of contract coupled with LGPD's direct application to global processing activities provide sufficient protections for data subjects.

Annex II, Section II, Clause 14

[3] Mutual recognition of equivalent terms and SCCs are a scalable and practical way to protect data flows

Annex II, Section II, Clause 14 requires that upon request, the parties must make a copy of the SCCs available free of charge to data subjects, subject to commercial and industrial secrets and that all information made available to holders, under the terms of these Clauses, must be written in Portuguese.

CrowdStrike's view on this is that it is impractical to provide a copy of the Clauses to data subjects. Although parties may redact parts of the Clauses or limit disclosure based on commercial/industrial secrets, the requirement to disclose SCCs provides a potential cyber security vulnerability roadmap to adversaries and for the public to learn about the requirements for customers of any given company. Thus creating a new risk for data security – the very thing the ANPD aims to mitigate.

Annex II, Clause 16. Security Incident Reporting

Clause 16 of Annex II states that in the event of a security incident which may entail significant risk or damage to data subjects, the designated party shall notify both the ANPD and the data subject as soon as reasonably feasible. This notification is required to include certain information about the incident. In some situations, revealing information about a cyber incident – to both regulators and data subjects – actually makes data less secure because it discloses information about an ongoing cyber investigation.

Mass security incident notifications would adversely affect the cybersecurity and privacy interests that the ANDP seeks to protect. They also risk publicly revealing the digital supply chain of affected parties. Revealing such information to a broad group of data subjects makes it likely that a bad actor or adversary can leverage such information to engage in further cybercrime or threatening cyber behavior, such as supply chain attacks and targeted phishing schemes. It also alerts the adversary that the cyberattack has been discovered, meaning any ongoing cyber forensic investigations might be thwarted.

Separately, the proposed regulation, as written, would require covered entities to give the ANPD written notice of a security incident "as soon as reasonably feasible". This timeline does not allow for organizations to understand any component of the incident or even validate that an incident has occurred. Due to the nature of cybersecurity incidents, organizations often do not know the full extent of impacts at the immediate point of detection. For example, an incident where a threat actor gains access to a single resource but is not able to move laterally due to strong security practices likely

would have a minor impact on the covered entity. Whereas, another incident in which a threat actor gains access, successfully moves laterally, establishes persistence, and is able to compromise a broader set of systems may have a severe impact. While these are important distinctions, the two incidents could look similar in the early investigation stage.

Consideration of the impact and severity of an incident is important not only when initially assessing evidence of an intrusion but also in discerning the efficacy of mitigation measures. Consequently, it is extremely difficult, if not impossible, for an organization to make a report with any meaningful information "as soon as reasonably feasible."

The United States is also taking action in regards to incident reporting. As the ANPD reviews this regulation, and drafts other pieces of regulation, CrowdStrike urges alignment where possible with existing international rules and regulations. New regulations will not be issued in a vacuum but instead amongst a Venn diagram of cybersecurity regulations across the globe. We recommend the ANPD review the U.S.'s Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA") and the forthcoming implementing regulation, and where appropriate, make efforts for alignment.

III. CONCLUSION

The ANPD's proposed regulation provides a thoughtful analysis of a complex legal and policy area. In order to remain future-flexible, it is important to prioritize the goal of protecting data regardless of where it is, rather than equating data protection with restrictions on cross-border data transfers and data portability. Consequently, providing as many means as possible to lawfully transfer data abroad will continue to afford Brazil-based organizations the ability to create and use innovative technologies, including data security and privacy technologies, on a global scale.

As updates to the Regulation move forward, we recommend continued engagement with stakeholders. Finally, because the underlying technologies evolve faster than law and policy, we recommend and emphasize that any legislative updates and proposed rulemaking focus on principles rather than prescriptive requirements and include a mechanism for periodic revisions.

IV. ABOUT CROWDSTRIKE

CrowdStrike®, 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 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/.

CONTACT

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

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

Rob Sheldon
Director, Public Policy and Strategy

Email: policy@crowdstrike.com

***