Palo Alto Networks comments on
the European Data Protection Board (EDPB)'s "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data"
21 December 2020

Palo Alto Networks is pleased to provide our input to the EDPB's "Recommendations 01/2020 on measures that supplement transfer tools to ensure with the EU level of protection of personal data" compliance("Recommendations"). Palo Alto Networks strongly supports the protection of personal information, and we believe that privacy is important for our customers' and employees' trust and for the protection of individual rights. Our privacy practices are informed by key principles of Accountability, Transparency and Control, Trustworthy Third Parties, Privacy by Design, Data Integrity and Proportionality, Customer Benefit, and Security. [1]

We appreciate the EDPB's efforts in drafting the document under consultation, but we are concerned that the Recommendations propose a rather prescriptive approach that in our opinion goes beyond the requirements set by the Court of Justice of the European Union (CJEU)'s *Schrems II* decision. We worry that this may impair flows of data that do not pose risks to individual rights and freedom of individuals, but which are instead necessary for the protection of individuals and for a secure digital life. The Recommendations eschew the risk-based approach to protecting personal data enshrined in the GDPR and also in the *Schrems II* ruling, which recognizes that exporters must make "case-by-case" assessments, and that "all the circumstances of the transfer" must be considered when determining whether a transfer can proceed (e.g., *Schrems II* decision paragraphs 121, 126, 134).

It is important that data exporters are allowed to perform an assessment that is truly risk-based and takes into accounts all elements that can expose data to risk. We fear that the Recommendations as currently written do not allow this and this would have an unintended negative impact on the EU's cybersecurity, as detailed below. We urge the EDBP to encourage data exporters to assess the magnitude but also the likelihood of government access to the data exported, based on the nature of the data and the purpose of data processing. We are concerned that entities will feel they cannot take into account the applicability, but also the actual application of the law, and we hope the EDPB will invite them to perform a balancing act of risks and benefits for data subjects and society, in alignment with GDPR principles, as is required for instance for cybersecurity. The Recommendations consider a factor "such as the likelihood of public authorities' access to your data in a manner not in line with EU standards" as subjective, while instead this is a factual and measurable event. Data exporters must be able to perform assessments that are truly risk-based and take into accounts all elements that can expose data to risk, including the likelihood of something happening. Depending on its business model, a particular data importer may very likely not be the target of public authorities' demands for data. It should be possible to consider if a U.S. company has previously been requested to provide data to U.S. authorities under a given law, when determining the risks to individual rights.

Overemphasis on technical measures

The Recommendations overly emphasize technical measures such as encryption as additional safeguards. Such measures are not always compatible with many purposes of data processing. Therefore, we

[1] https://www.paloaltonetworks.com/legal-notices/trust-center/privacy

encourage the EDPB to adopt technology-neutral recommendations in line with GDPR that allow companies of all sizes to assess their security requirements in line with the risks and to adopt contractual measures as safeguards.

Considerations related to cybersecurity

Palo Alto Networks understands and is committed to support the EU's objectives to achieve a high level of data protection. The EU is equally committed to cybersecurity. In fact, just on 16 December the European Commission released a package of new cybersecurity proposals[2] that keeps the EU on a trajectory begun in 2013 to improve the level of security across the Union. The EU understands that cybersecurity is essential to economic activity and growth as well as to the user confidence in online activities that underpins it. Furthermore, individuals' freedom and rights depend also on the protection of the security of their data. European entities must ensure they are resilient to cyberattacks— particularly as they undergo the accelerated digital transformation brought about by the Covid-19 pandemic where many Europeans now are working, shopping, and going to school remotely.

Cybersecurity enables privacy in that it serves to protect personal information. The GDPR acknowledges this, requiring security measures for the protection of personal information, and actually acknowledges the purpose of cybersecurity as a legitimate basis of data processing. The fact that cybersecurity requires some degree of personal data processing is why processing personal data for security purposes is broadly recognized as a "legitimate interest" in the GDPR (Recital 49).

Because cybersecurity threats are global, the flow of data is critical to develop effective threat intelligence and threat prevention. Restricting global flow of cybersecurity data just because of a limited amount of personal data it may contain (such as IP addresses and user IDs) can have a serious impact on worldwide ability to counter global cyberthreats, at a time when threats are becoming more frequent and more sophisticated. To best secure all entities and individuals —including those located in the EU-- cybersecurity companies like Palo Alto Networks must understand threats (such as malware, viruses, remote code execution, command-and control (C2)) on a global scale, to be able to detect and prevent cybersecurity attacks in real time. This requires transferring and analyzing threat data regularly across geographies, entities, and users. Segregating data about security events/incidents and localizing it will greatly diminish the effectiveness of threat intelligence and threat prevention, and ultimately the protection of individuals.

Conclusion

Cross-border data transfers and meaningful privacy protection are not mutually exclusive goals. Securing customers and the broader digital infrastructure against global threats is essential to protecting personal data. To best meet the EU's dual goals of privacy and cybersecurity, Palo Alto Networks cautions against overly rigid approaches on international data transfers set forth in the Recommendations and asks the EDPB to consider adopting a risk-based balanced and practical approach.

[2] This packaged included a new cybersecurity strategy, a proposed revision of the Directive on the security of network and information systems (NIS), and a proposal on critical infrastructure security.