



DocuSign, Inc.
221 Main Street, Suite 1550
San Francisco, CA 94105

Dr. Andrea Jelenik
Chair, European Data Protection Board
Rue Wiertz 60
B-1047 Brussels
Belgium

Re: EDPB Recommendations on Supplemental Measures for Data Transfers

Dear Dr. Jelenik:

Thank you for the opportunity to provide comments to the European Data Protection Board (EDPB) regarding its recent recommendations on supplemental measures for data transfers. While we appreciate the EDPB's efforts to provide guidance on continued use of the Standard Contractual Clauses (SCCs) following the European Court of Justice's ruling in the *Schrems II* decision, the recommendations pose both procedural and substantive concerns.

DocuSign is a global public corporation that helps organizations connect and automate how they prepare, sign, act on and manage agreements. As part of the DocuSign Agreement Cloud software as a service (SaaS), we offer eSignature, the world's #1 way to sign electronically on practically any device, from almost anywhere, at any time. Today, more than 750,000 customers and hundreds of millions of private and public sector users in over 180 countries use our agreement cloud services to accelerate the process of doing business and providing essential services to their constituents, to simplify their lives. As a global SaaS provider, our customers look to us to support their critical worldwide uses of our services by balancing seamless cross-border data transfers while reasonably safeguarding their data.

With respect to process, even before consideration of any comments received during the consultation period, we are concerned that the EDPB has taken the unusual step of issuing the recommendations and declaring them applicable immediately. The EDPB originally proposed an extremely short consultation period of nineteen (19) days and, after feedback from U.S. and European stakeholders, has extended the deadline to December 21. With consultations in some cases having lasted up to twelve (12) weeks, the timeframe for consideration remains rushed considering the unprecedented disruption of the COVID-19 pandemic. In addition, given the complex subject matter of the consultation and potentially significant economic implications, it is important that the EDPB meaningfully evaluates input from impacted parties that have both operational and technical expertise to share, especially if that input differs from the recommendations as drafted.

With respect to the substance of the recommendations, we are concerned that they are overly prescriptive considering the *Schrems II* decision. In *Schrems II*, the Court held that the SCCs remain valid and that supplementary measures need to be assessed on a "case-by-case" basis considering the data transferred. Yet, the EDPB recommendations essentially treat all transfers to a given country the same, without accounting for the nature of the data transferred or the likelihood of government access. The

decision asks to ensure an “*essentially equivalent*” level of data protection. This approach does not mean that EU data protection laws apply throughout the world, but rather that the separate laws and practices in third countries must be reviewed and checked for equivalence with the EU’s laws, with some room to assess individual situations on a case-by-case basis.

Moreover, the recommendations appear to require technical measures that make government access nearly impossible, without any consideration of the effectiveness of contractual protections. We urge the EDPB to adopt a *risk-based* approach, consistent with the General Data Protection Regulation (GDPR), that recognizes that certain categories of data—such as employee data, sales data, and health data—are highly unlikely to be of interest to government authorities and thus subject to access.

It is not clear why the EDPB is categorically ruling out a risk-based approach regarding the supplementary measures to be taken to secure international data transfers to third countries. In many data transfer situations, the likelihood of risk for the rights and freedoms of natural persons can indeed be very low because of the type of data, a company's technical and organisational measures, business model, customers, or other sector specific regulatory specifications that it is bound by.

Determining measures according to the underlying risk for natural persons is a cornerstone of EU data protection law. The law imposes on the controller the task of conducting risk assessments on several occasions. According to Article 24 of the GDPR “(...) *the risks of varying likelihood and severity for the rights and freedoms of natural persons (...)*” must be considered by the controller. Article 32 of the GDPR, the essential provision on the security of processing, also explicitly states that the controller shall consider “*the risk of varying likelihood and severity for the rights and freedoms of natural persons*” and that the controller (or processor) “*shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (...)*”. In addition, other crucial provisions of the GDPR, such as Articles 33 and 34 regarding the notification of security breaches, oblige the controller to assess the risk for the data subjects. All these provisions have in common that they provide for the possibility to determine a low risk (e.g., if the likelihood of risk would be (almost) zero), then even the potential high severity of impact would still mean a low risk. Furthermore, the new draft SCCs provided by the EU Commission also allow taking measures according to the individual risk, such as in Module 1, Clause 1.6. on the “Security of processing”, where it states that the “*data importer (...)* shall take due account of the risks involved in the processing (...)”.

Data protection is a fundamental right, but as with any right the required protections must be evaluated against the realistic risks. Other civil liberties, such as the Freedom to conduct business as well as the Right to property, are essential not only to companies conducting business, but also to EU citizens. However, these principles would be severely limited if one were to restrict international data transfer generally – without considering the individual processing activity and associated risk. This dynamic is particularly true given the economic importance of trans-Atlantic data flows, which according to a recent CSIS paper are worth approximate \$7.1 trillion annually. We believe an effective, pragmatic approach is required to ensure the continued success of Europe’s digital transformation.

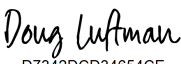


DocuSign, Inc.
221 Main Street, Suite 1550
San Francisco, CA 94105

For the foregoing reasons, we respectfully request and urge the EDPB to adopt a *risk-based* approach, consistent with the GDPR, that recognizes that certain categories of data are highly unlikely to be of interest to government authorities and thus subject to access.

Thank you for your time and consideration.

Best regards,

DocuSigned by:

D7342DCD34654CE...

Douglas Luftman
Vice President, Deputy General Counsel & Chief Privacy Officer
DocuSign, Inc.

Cc: Mr. Bruno Gencarelli, Head, International Data Flows and Protection Unit
European Commission