Response to EDPB Recommendations on Supplementary Measures for Data Transfers

Introduction

Salesforce welcomes the opportunity to provide comments on the European Data Protection Board's ("**EDPB**") draft recommendations on measures to supplement transfer tools ensuring compliance with the EU level of protection of personal data (the "**draft Recommendations**").

Salesforce acknowledges that the draft Recommendations are long-awaited and provide helpful guidance for businesses. When final, they can help businesses address their obligations to identify and implement appropriate supplementary measures to ensure an essentially equivalent level of protection for data transfers, following the *Schrems II* decision. Salesforce is particularly appreciative of the acknowledgement by the EDPB that there are no quick fixes, nor a 'one-size-fits-all' solution for all transfers. Salesforce welcomes the flexibility granted to organisations to implement effective measures (where needed), taking into account the many different types of processing operations and the transfers in question.

At Salesforce, trust is our number one value. The protection of our customers' data is paramount, and we safeguard that data with a robust and comprehensive privacy and security program. To that end, we continuously undertake significant efforts towards developing a data protection program that accounts for the ever-evolving landscape of global data protection laws. For example, Salesforce was among the first software companies to achieve approval for our Processor Binding Corporate Rules, in November 2015. In addition, we are continuously adding to the numerous best in class security certifications, such as ISO 27001, 27017 and 27018, among many others specific to individual jurisdictions. Beyond compliance, Salesforce supports the development of strong and effective privacy laws that build customer confidence in the digital economy, and we engage in external advocacy, such as to promote consistent high standard privacy protections in the United States.

Given this commitment and our ongoing collaboration with policy makers and regulators, we respectfully provide the EDPB with our comments on two key areas of the draft Recommendations. Although Salesforce appreciates the flexible approach of the draft Recommendations, we recommend that they could be strengthened, so as to optimize enabling businesses to put effective, proportionate and realistic measures in place to facilitate data transfers, while also continuing to uphold fundamental privacy rights.

1. The 'likelihood' of government access requests should be considered a relevant factor

The EDPB describes in 'step 3' of the draft Recommendations the assessment that organisations should carry out to ensure that the proposed transfer mechanism is effective in light of all circumstances of the transfer. As part of this assessment, organisations must consider the legislation applicable to non-EEA data recipients that may impinge on the effectiveness of that transfer mechanism, taking into account the nature, scope and circumstances of the transfer in question.

In paragraph 42 of the draft Recommendations, the EDPB recommends that such assessments should be **primarily focused on third country legislation** governing the circumstances in which

public authorities may access the personal data transferred. In the absence of such legislation and where an organisation may still wish to proceed with the transfer, the EDPB recommends that organisations should instead **consider 'other relevant and objective factors' but <u>should not</u> consider factors such as the likelihood of public authorities' access** to data in a manner not in line with EU standards.

This would impose a disproportionate and unnecessary restriction on data transfers. Excluding the assessment of the <u>likelihood</u> of public authorities' access to data does not represent a risk-based, proportionate approach to safeguarding data transfers. For example, the EDPB can examine objective results in published transparency reports over a series of years to know that there is a far lower probability for law enforcement authorities to request access to business enterprise data as compared to mass market consumer data, for purposes of law enforcement or national security investigations. Critically, it is also inconsistent with the approach of the CJEU in the *Schrems II* decision, the requirements of the GDPR and the newly proposed draft standard contractual clauses. Accordingly, Salesforce urges the EDPB to revisit this position and consider how previous experience based on the conduct of public authorities should be regarded as an objective factor for the purposes of the assessment. This is supported by a number of factors as set out below.

<u>Schrems II</u>

In *Schrems II,* the CJEU considered that it is for the controller or processor to verify on a '**case-by-case basis**' whether the law of the destination country ensures adequate protection, under EU law, of the personal data transferred pursuant to the standard contractual clauses, by providing, where necessary, additional safeguards to those offered by those clauses[1].

The CJEU notes that where the controller or processor is not able to take '**adequate additional measures**' to guarantee such protection, the controller or processor should suspend or end the transfer of personal data to the third country concerned[2].

We consider that the CJEU's emphasis on a case-by-case analysis and the need to implement "*appropriate safeguards*" and "*adequate additional measures*" confirms that an individual assessment of all relevant elements, including the likelihood of access, should be undertaken.

<u>GDPR</u>

The GDPR introduces and embraces a risk-based approach to data protection compliance.

For example, controllers are required to "*ensure a level of security appropriate to the risk*"[3] and can comply with this requirement by implementing "*appropriate technical and organisational measures*"[4]. In carrying out this risk assessment, controllers are encouraged to consider the "*risk of varying likelihood and severity for the rights and freedoms of natural persons*"[5]. In assessing data security risk, the GDPR encourages controllers to consider the risks that are presented by the particular personal data processing activities[6]. It follows that the GDPR encourages controllers to implement security measures based on a risk assessment which considers the actual likely risks to the relevant data subjects.

Similarly, Article 33 GDPR specifies that controllers must notify supervisory authorities of a personal data breach "*unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons*". On this basis, controllers are required to carry out a risk assessment following a personal data breach including assessing the impact of the personal data breach on the relevant individual.

---

1 Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, para 134
2 Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, para 135
3 Article 32(1) GDPR
4 Article 32(1) GDPR, Art. 24(1) GDPR
5 Article 32(1) GDPR, Art. 24(1) GDPR
6 Recital 83 GDPR

These examples expressly highlight that where the concept of risk appears in the GDPR, it is defined by reference to the likelihood and severity of a negative impact on data subject rights. This guiding precedent reinforces that it is appropriate to apply the same approach to the data transfers assessment set out in the draft Recommendations, by considering the actual likelihood for government access to personal data and the practical risk of the conduct of public authorities.

We respectfully recommend that the EDPB revise this draft recommendation, and consistent with GDPR and CJEU guidance, to permit parties to make a risk-based assessment of the likelihood of public authorities' access.

European Commission's draft standard contractual clauses

In its implementing decision on the draft standard contractual clauses, the European Commission notes that in considering whether the laws of the destination country provide an adequate level of protection, the data exporter and data importer should in particular take into account the **specific circumstances** of the transfer[7]. To that end, the European Commission provides that data exporters and data importers should take into account, amongst other factors, "*any relevant practical experience indicating the existence or absence of prior instances of requests for disclosure from public authorities received by the data importer for the type of data transferred*"[8].

A similar approach is adopted under the draft new standard contractual clauses themselves. Under Section II, clause 2 of the draft standard contractual clauses, the data exporter and the data importer warrant that they have no reason to believe that the laws of the destination country prevent the data importer from fulfilling its obligations under the standard contractual clauses. In providing this warranty, the parties declare that they have taken due account of a number of elements, most notably, the specific circumstances of the transfer.

In assessing these circumstances, the parties are required to consider a number of factors including "*any relevant experience with prior instances, or the absence of requests for disclosure from public authorities received by the data importer for the type of data transferred*"[9]. It follows that the European Commission has made clear its view that it is appropriate for those involved in data transfers to consider the absence of requests for disclosure from public authorities (or prior experiences) in assessing whether the laws of the destination country are adequate.

Taking all of the above into account, there is compelling precedent demonstrating the intention of the CJEU, the European Parliament, the Council of the European Union (through the implementation of the GDPR) and the European Commission (under the draft standard contractual clauses), that organisations should be able to take a risk-based approach to ensuring compliance with European data protection laws.

Consistent with this long-standing and uniform support for a risk-based approach, an assessment of the likelihood of government access can be objectively measured based on observable, objective metrics, such as the frequency of requests in previous years. Accordingly, when assessing whether a third country offers an adequate level of protection for personal data, companies should be able to continue taking into account highly relevant risk-based factors, such as the likelihood of public authorities' access to data.

2. Remain 'technologically neutral' to ensuring consistency with the requirements of the GDPR

---

7 Draft Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, Recital 20

8 Draft Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, Recital 20

9 Draft Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, Annex, Section II, Clause 2(b)

In the draft Recommendations, the EDPB describes in 'step 4' the requirement to adopt "supplementary measures" to ensure that data transferred is afforded a level of protection essentially equivalent to that guaranteed within the EU. The draft Recommendations consider three types of supplementary measures: contractual, technical and organisational. Salesforce would like to highlight to the EDPB that the emphasis on technical safeguards over contractual and organisational safeguards is not consistent with the technology-neutral approach of both the GDPR and also the *Schrems II* decision. For consistency, we respectfully recommend that this position technology specification be revisited by the EDPB.

In particular, the technical safeguards appear to be given more weight than the contractual and organisational safeguards. For example, we note that the draft Recommendations provide that "*contractual and organisational measures alone will generally not overcome access to personal data by public authorities of third country"* and "*there will be situations where only technical measures might impede or render ineffective access by public authorities…"*[10]*.*

The draft Recommendations go on to provide examples of technical measures that could potentially be effective to ensure essentially equivalent protection. The draft Recommendations go into a considerable amount of detail regarding what appropriate technical safeguards would look like, including in which circumstances encryption and pseudonymisation would be effective.

We are of the opinion that the emphasis on technical safeguards and the in-depth-analysis of certain technical safeguards is not consistent with the GDPR, which is intended to be technologically neutral. Recital 15 GDPR expressly provides that the protection of natural persons should be technologically neutral and should not depend on the techniques used. It follows that the GDPR avoids dictating the technical requirements that must be implemented to protect personal data and affords companies a degree of flexibility to adopt a risk-based approach with respect to these appropriate technical and organisational measures.

Conclusion

Salesforce is committed to our collaboration with the government in developing effective data protection laws that build and sustain confidence in the digital economy. We are encouraged by the flexible approach taken by the EDPB in preparing the draft Recommendations. To further improve the draft Recommendations, we recommend that they be revisited in order to ensure consistency with the GDPR, and to ensure a risk-based assessment of the likelihood for government access requests can continue to be applied. Thank you for the opportunity to provide comments to this important process. We remain respectfully at your disposal, should you require further information.

[10] Draft Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Adopted on 10 November 2020, para 48