21 December 2020

Standard Contractual Clause – Consultation

Vodafone is pleased to provide our response to the European Data Protection Board's (EDPB) consultation on Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (the "Recommendations").

Introduction

1. We welcome the opportunity to submit comments on the Recommendations.

2. In a data-driven economy, cross border data transfers underpin all industries. We all rely on data flows to enable enterprise and consumer services, supplier support, data centres and back-office/support functions.

3. Data localisation will sever European companies from the expertise and technology underlying the resilience, reliability and security of global supply chains with additional negative impacts to the global digital agenda across all European companies. This position would be an extremely bad outcome for European businesses and would undermine the EU's digital agenda. Moreover, the necessity of data transfers to third countries to the livelihoods and social lives of Europeans is acknowledged within GDPR itself.[1]

Coordination of Guidance

4. Vodafone would welcome confirmation that the EDPB, the Commission and Member States will coordinate the responses from national DPAs ensuring a harmonised approach and avoiding the risk of contradictory or divergent national guidance that would undermine the single market and put pan-European businesses in an intolerable position.

Risk-Based Assessment

5. Vodafone supports the Commission's approach for assessing data importers' compliance with the SCCs[2] on the basis that it fulfils the GDPR criteria that severity of risk to data subject's rights and freedoms must be assessed with reference to context and likelihood[3] whilst also protecting Europeans' data to the higher standard required by the Schrems judgement.

6. There is a perception that the Recommendations require every transfer to be assessed in the same way, and that "any" risk to the data being transferred could invalidate the transfer mechanism.[4] This puts an unrealistic assessment burden on companies that would lead to outcomes that are disruptive to existing, accepted business processes. For example, employee access to an employee directory containing publicly available information should not be prevented on the basis that the country in which they are located lacks redress for EU data subjects.

7. The Recommendations also outline that the nature and context of the transfer and the likelihood of such data being requested by a law enforcement authority must not be considered when transferring data to countries without data protection frameworks of

[1] See Recitals 6 and 101 of GDPR
[2] See Recital 20 of the SCC decision
[3] See Recital 76 of GDPR
[4] See Para 30 of the Recommendations

equivalent sophistication to GDPR.[5] The Recommendations confirm this position by stating that any companies subject to FISA may only receive data protected by supplementary measures, excluding the possibility of assessing the nature and context of the transfer or the likelihood of the data being requested.[6] In the case of FISA, for example, the confidentiality of employee performance data, health records etc. are not compromised by the legislation, but the EDPB guidance would rule out such a granular assessment.

8. GDPR is widely recognised as the global standard-bearer of data protection; restricting all data transfers to countries that match these standards is detrimental to Europeans who need to rely on technology and expertise unavailable in European countries. Furthermore, the EDPB's position excluding the assessment of "subjective" criteria when transferring to countries without EEA equivalent protections contradicts:

    a. the GDPR text linking severity of the risk with the likelihood of a breach of GDPR occurring;[7] and

    b. the standards set in the Recommendations themselves emphasising that the transfer tool must be effective in practice[8] and that assessments must be made considering "all circumstances of the transfer".[9]

9. Specifically we request that:

    c. Para 30 is aligned to the Commission standard for assessing data importer compliance with the SCCs.

    d. Para 40 is modified to ensure that severity of risk is always assessed with reference to context and likelihood of breach.

    e. The Executive Summary is updated to reflect (a) and (b) above in addition to reaffirming that the risk-based analysis envisaged by GDPR[10] applies to all processing, including all cross border transfers of personal data.

Assessment of Data Importer Laws

10. Vodafone would welcome the Recommendations being enhanced to include benchmarking of third countries' surveillance laws against EU adequacy criteria to identify high-risk data transfers to individual countries and steps that companies can take to mitigate against such risk. For example, the FISA assessment being updated to highlight that there is risk to communications data would enable companies to make better decisions about the supplementary measures needed to protect data transfers to the US. Vodafone would welcome the EDPB to perform this type of analysis for ***all third countries***.

11. The Recommendations require data exporters to assess how local laws applicable to data importers and subprocessors impact the privacy of EU data subjects.[11] For example, the resilience of supply chains is often based on data being accessed from or stored in a multitude

[5] See para 42 of the Recommendations
[6] See para 44 of the Recommendations
[7] See Recitals 75, 76, 77, 88 and 90 as well as Articles 24 (1), 25 (1), 32 (1) and 34 (4)
[8] See para 28 of the Recommendations
[9] Step 3 at page 12 of the Recommendations
[10] See GDPR Article 27 and Recital 76
[11] See para 35-38 of the Recommendations

of locations in which data exporters have no presence. Expecting data exporters, particularly SME companies, to perform a detailed assessment of the laws applicable to all data importers and subprocessors in a complex supply-chain is not only unrealistic but it also is very likely to lead to fundamental inconsistencies in data handling practices. Furthermore, any analysis needs to be replicated across the entire market for data to be effectively protected.

12. The Recommendations currently list a variety of sources to which data exporters may refer when assessing the laws applicable to data importers and subprocessors.[12] This approach is too general to be meaningful or practical and will almost certainly lead to inconsistencies in the protection afforded to EU data subjects' data.

13. Companies need certainty about the privacy risk of different legal regimes in order to make investment decisions. The EDPB is in the best position to provide the guidance that companies need to make such decisions by assessing the privacy risks arising from individual countries' legal regimes. Moreover, the EDPB would be fulfilling its mandate to issue practical guidance envisaged in GDPR[13] and also drive consistency of outcomes for EU data subjects by doing so. In the absence of such guidance, companies will still need objective, measurable criteria against which country laws can be assessed to drive decision-making, and our view is that the adequacy criteria provides the best "off-the-shelf" basis for conducting such assessments.

Application of the Recommendations

14. Companies subject to GDPR through extra-territorial application[14] should not be required to follow the Recommendations as a third country data importer. This is consistent with the SCC position that they apply to transfers where either a) the recipient is not subject to GDPR; or b) onward transfers.[15] Further, explicit clarification on this point would be desirable.

Derogations

15. Vodafone is strongly against any additional narrowing of the derogations available to companies permitting data transfers contained in GDPR. The Recommendations suggest that all data transfer derogations are only available where they are on an occasional basis. However, GDPR provides that transfers on the basis of legitimate interests may only be occasional. A narrowing of the derogations in guidance that sits under legislation is likely to cause confusion and undermine the trust in the rules more broadly.

[12] See Appendix 3 of the Recommendations

[13] See Recital 77 of GDPR

[14] Companies that are not located in the EEA but to which GDPR applies by virtue of their operational footprint as an "establishment" or targeting EU data subjects with good/services or monitoring tools. See Article 3 of GDPR.

[15] See Article 1 of the new SCCs