Transfers of Personal Data to Suppliers

Subject to the General Data Protection Regulation

Defined Terms. As used below, "you" or "your" means Kyndryl Supplier and "Third Country" means a country (1) where you process personal data that Kyndryl provided or made accessible to you and (2) that the EU Commission does not consider as offering adequate data protection.

Notice. Where Kyndryl asks you below to notify Kyndryl (e.g., if you believe that certain statements below do not accurately reflect your experience regarding government access requests to personal data), please make such notification to datagovernance@kyndryl.com.

Purpose. By entering into the European Union standard contractual clauses, as approved by the EU Commission (Decision 2021/914 EU) ("EU SCC"), with Kyndryl Inc. or one of its affiliates ("Kyndryl"), you:

(a) warrant that you have no reason to believe that the laws and practices in a Third Country, including any requirements to disclose personal data or measures authorizing access by public authorities, prevent you from fulfilling your obligations under the EU SCC;

(b) also warrant that you used your best efforts to provide Kyndryl with relevant information to support your warranty referenced in (a) above, including with respect to the laws and practices of the Third Country (including those requiring the disclosure of data to public authorities or authorizing access by such authorities), and any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under the EU SCC; and

(c) agree to notify Kyndryl promptly if, after having entered into the EU SCC and for the duration of the EU SCC, you have reason to believe that you are or have become subject to laws or practices that prevent you from fulfilling your warranty obligations referenced in (a) above.

Kyndryl has prepared this document to:

(1) help you understand how Kyndryl, as a data exporter, performed its own assessment (set forth below) that the laws and practices of the Third Country do not prevent you from fulfilling your obligations under the EU SCC;

(2) afford you the opportunity to confirm that you have provided Kyndryl with all relevant information necessary for Kyndryl to perform its assessment of those laws and practices, consistent with your warranty obligations, as referenced above;

(3) afford you the opportunity to identify and provide any information that you believe might be missing from or incorrect within Kyndryl's assessment; and

(4) provide you with a template for conducting similar assessments of authorized onward transfers to your affiliates or third parties in Third Countries.

EDPB's Recommendations. Kyndryl completed its assessment below in accordance with the judgment of the Court of Justice of the European Union ("**CJEU"**) in Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems ("**Schrems II**") and the associated recommendations by the European Data Protection Board ("**EDPB**"). [1]

The EDPB adopted recommendations to help assess whether personal data transferred from the European Union would receive protections from Third Countries that are sufficient to fulfil the standards of the General Data Protection Regulation ("**GDPR**"). See, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Version 2.0, Adopted on

[1] Because Schrems II also applies to the United Kingdom ("**UK**"), KYNDRYL's assessment is also relevant for the associated UK requirements.

18 June 2021). The EDPB's recommendations are intended to help implement the Schrems II judgment and provide a guide for EU SCC implementation.

The EDPB identified the following six steps to take in completing those assessments.

Step 1: Map transfers of personal data to Third Countries and verify the data transferred are adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

Step 2: Verify the relevant "transfer tool", such as whether the European Commission has already declared a country as adequate through one of its adequacy decisions under Article 45 of the GDPR. The EU SCC are an appropriate transfer tool.

Step 3: Assess whether the laws and/or practices of a Third Country impinge on the effectiveness of the appropriate safeguards of the transfer tool, in the context of a specific transfer.

Step 4: Identify and adopt supplementary measures that are necessary to bring the level of protection of the data transferred to the standard of essential equivalence with the GDPR. This step is only necessary if an assessment reveals that the Third Country legislation and/or practices impinge on the effectiveness of the relevant transfer tool.

Step 5: Take any formal procedural steps that the adoption of supplementary measures may require.

Step 6: Re-evaluate at appropriate intervals the level of protection afforded to the personal data transferred to Third Countries and monitor if there have been or there will be any developments that may affect it.

Kyndryl's Assessment

Map Transfers of Personal Data to the Third Country. This section describes how Kyndryl has addressed Step 1 of the EDPB recommendations.

For the processing of personal data, you have entered into the Kyndryl Privacy and Security Terms (the Terms) with a processing details exhibit (current version of the Terms can be found here). The processing details exhibit lists, among other things, the categories of personal data processed, processing activities, business purposes, intended onward transfers, and subprocessors' names, location of processing, and processing activities. More precisely, with respect to Step 1, the processing details exhibit identifies transfers of personal data to Third Countries.

If you are unable to find the above processing information in your contracts with Kyndryl, please contact your Kyndryl Buyer for assistance. In addition, please remember to notify Kyndryl promptly if any of your processing information changes.

Verify the Relevant Transfer Tool. This section describes how Kyndryl has addressed Step 2 of the EDPB recommendations.

The EU SCC remain an acceptable means for transferring GDPR personal data under Schrems II and the EDPB recommendations. Accordingly, the EU SCC are the relevant transfer tool.

Assess the Laws and Practices of the Third Countries. This section describes how Kyndryl has addressed Step 3 of the EDPB recommendations.

Schrems II requires that data exporters and data importers assess whether the laws and/or practices of a Third Country impinge on the effectiveness of the appropriate safeguards of the transfer tool, in the context of a specific data transfer. Kyndryl relied on EDPD guidelines, and in particular the Recommendations 02/2020 on the Essential Guarantees for Surveillance Measures, to assess whether a Third Country's surveillance laws permitting access by governments prejudice the fundamental rights and freedoms of data subjects. Based on Kyndryl's assessment, the supplementary measures described below are, in KYNDRYL's view, appropriate.

***Kyndryl's Business, Approach to Government Access to Data, and Transparency*.** The nature of Kyndryl's business, Kyndryl's approach to government access requests to data, and Kyndryl's transparency regarding those requests, reduces any risk that a government would successfully obtain GDPR personal data from Kyndryl:

• Kyndryl is fundamentally an enterprise client company. Our business model sets us apart from many of the companies associated with the surveillance laws highlighted in the Schrems II decision.

• Kyndryl's business does not involve providing traditional telephone or Internet-based communications services to the general public, which sets us apart from providers that regularly receive law enforcement access requests, such as consumer digital services. Instead, we deal primarily with corporate data that would provide little utility for national security intelligence purposes and generally is not the target of such requests.

• Nor does Kyndryl typically process sensitive personal or consumer data. In the limited areas where Kyndryl does such processing, many of the relevant offerings are either not subject to the EU SCC data transfer requirements or do not handle GDPR personal data. For example, business to consumer offerings where Kyndryl is a controller are not necessarily subject to EU SCC data transfer requirements, as derogations under Art. 49 of the GDPR may apply.

In addition, Kyndryl does not voluntarily share data with governments requesting access to Kyndryl client data:

- Kyndryl has a strict process to safeguard client personal data in the event of a government request. At the heart of this policy is the core principle that if Kyndryl receives a request from a government, we ask the government to directly approach our client.
- In light of the CJEU ruling in Schrems II and the subsequent EDPB recommendations, Kyndryl has gone further by incorporating our existing policy on government access to client data directly into our client contracts.
- Furthermore, Kyndryl has not provided client data to a government agency under any surveillance program involving the bulk collection of content or metadata.
- Further, Kyndryl publishes regular Law Enforcement Request Transparency Reports ("Transparency Reports") with metrics on law enforcement requests. Our Transparency Reports reflect the minimal interest that governments and law enforcement have in Kyndryl client data.
- We share these transparency practices with you in the hope that you will implement similar transparency mechanisms for your business, if you have not already done so.

Your Business and Experience with Government Access Requests. As a Supplier to Kyndryl, we expect that the nature of your business and your experience regarding government access requests to data, would similarly reduce the limited risk that a government would successfully obtain GDPR personal data from you:

- Kyndryl Suppliers provide services and deliverables to Kyndryl or Kyndryl's corporate clients and are rarely engaged by Kyndryl to provide services directly to individuals or to process consumer data.
- By entering into the Kyndryl Privacy and Security Terms, you likely agreed that if a government, including any regulator, demands access to personal data (e.g., if the U.S. government serves a national security order on you to obtain personal data), or if a disclosure of personal data is otherwise required by law, you will notify Kyndryl in writing of such demand or requirement and afford Kyndryl a reasonable opportunity to challenge any disclosure (and where law prohibits notification, you agree to take the steps that you reasonably believe are appropriate to challenge the prohibition and disclosure of personal data through judicial action or other means and you commit to providing the minimum amount of information permissible when responding, based on a reasonable interpretation of the demand or requirement).
- As you have not notified Kyndryl of any disclosures to governments in accordance with your contractual commitments to Kyndryl, we assume that you have not shared personal data that Kyndryl provided or made accessible to you to a government agency under any circumstance, including surveillance programs involving the bulk collection of content or metadata.

In short, we trust that your separate experience with government requests for access to personal data reflects the same minimal interest that Kyndryl has experienced.

Requests to You. Please address the following requests:

1. If any of the statements above do not accurately reflect the nature of your business, your contractual commitments to Kyndryl, or your experience regarding government access requests to the data that Kyndryl has provided or made accessible to you, please promptly notify Kyndryl with sufficient details to explain the nature of the inaccuracy.

2. If you were prohibited by law from notifying Kyndryl of any government demand for access to personal data or any disclosure of personal data that was otherwise required by law, please take this opportunity to now notify Kyndryl, in writing, of general information relative to any such demand or requirement during the preceding twelve months.

3. If you have any reason to believe that the laws and practices of a Third Country prevent you from fulfilling your obligations under the EU SCC, please notify Kyndryl immediately.

Conclusion on Step 3. For all the reasons set forth above, in the context of your services to Kyndryl, Third Country laws and practices regarding governmental access to GDPR personal data are unlikely, in Kyndryl's view, to prevent the fulfilment of your and Kyndryl's obligations under the EU SCC.

Supplementary Measures. This section describes how Kyndryl has addressed Steps 4, 5 and 6 of the EDPB recommendations.

Kyndryl requires its Suppliers to implement supplementary measures to help attain the essential equivalency referenced in Step 4 above, including, in particular, through the contractual commitment of Suppliers to notify Kyndryl of government requests to access personal data as described in the **Your Business and Experience with Government Access Requests** section above and the security requirements in Article 4 of Kyndryl Privacy and Security Terms that Kyndryl Suppliers accept when working with Kyndryl.

Please notify Kyndryl immediately if you believe that the security terms in your contract with Kyndryl are not sufficient to bring the level of protection of the data transferred to the standard of essential equivalence with the GDPR.

Conclusion

We trust this document is helpful in explaining how Kyndryl has addressed important issues relating to Schrems II, the EDPB recommendations and the new EU SCC. This document does not constitute Kyndryl legal advice, and we urge you to conduct your own evaluations of applicable Third Country laws and practices, as you believe appropriate and necessary.