## Discourse Transfer Impact Assessment Whitepaper for Enterprise Customers

This whitepaper is intended to provide support to our customers in their performance of transfer impact assessments ("TIAs") for use of Discourse products and services. We track the recommendations published by the European Data Protection Board ("EDPB Recommendations") following the Court of Justice of the European Union's decision in *Schrems II*.

Please note that the information below is intended to help Discourse customers conduct their own independent assessments in consultation with their legal counsel and compliance teams. It is provided "as is," for informational purposes only, and does not constitute legal advice.

### 1. What is the purpose of a TIA?

A TIA is meant to determine whether personal data transferred outside the European Union ("EU") or countries deemed by the European Commission to provide "adequate protection" for personal data will be subject to a level of protection that is "essentially equivalent" to that guaranteed within the EU.

In conducting TIAs, data exporters must evaluate, among other things, the transfer tool used, the circumstances of the transfer, the laws and practices in the receiving jurisdiction that might allow government authorities to access or obtain the transferred personal data, the likelihood that transferred personal data would be subject to governmental requests or direct access, and any "supplementary measures" that the parties have implemented to ensure an essentially equivalent level of protection.

### 2. What is a transfer tool?

Under the EU's General Data Protection Regulation ("GDPR"), personal data cannot be transferred outside of the EU unless an appropriate transfer tool is in place. Under GDPR, these transfer tools include:

1. A decision by the European Commission under Article 45 of GDPR that the importing country ensures an "adequate level of protection" for personal data.
2. The implementation by the data exporter of "appropriate safeguards" described in Article 46 of GDPR, such as Standard Contractual Clauses ("SCCs") or binding corporate rules, that serve to provide an adequate level of data protection in the importing country.
3. Derogations under Article 49 of the GDPR, which can be used in limited circumstances when other transfer tools do not apply.

### 4. Why is reliance on a transfer tool identified in GDPR Article 46 (such as the SCCs) not sufficient, and why is a TIA needed?

In its recommendations, the EDPB explained that SCCs and other transfer tools described in Article 46 of GDPR "do not operate in a vacuum," and that under the decision in *Schrems II*, data exporters relying on those tools to transfer personal data to a third country must still verify, on a case-by-case basis, if the law or practices in that third country "impinge on the effectiveness of the appropriate safeguards contained in the . . . transfer tools."

As a result, even when a data exporter relies on a transfer tool described in Article 46 of GDPR (such as the SCCs), the data exporter must still assess whether the law and practices in the third country—especially with respect to public authorities' ability to request and obtain personal data—could

undermine the protections offered by that transfer tool, and if so whether supplementary measures can be implemented to address any gaps.

In addition, the updated SCCs issued by the EU Commission pursuant to Article 46 of GDPR in June 2021 impose a separate and independent obligation to conduct a TIA on exporters that rely on that tool for transfers of personal data to third countries.

## 5. What are the EDPB's recommendations for conducting a TIA?

The EDPB recommendations outline six steps for data exporters to take when conducting a TIA:

1. Know your transfers by mapping all transfers of personal data across borders to identify where personal data may be located or processed.
2. Identify transfer tool(s) that will be used, such as an adequacy decision, SCCs, or other tools as discussed under item 2 above.
3. If relying on a transfer tool listed in Article 46 of GDPR, such as the SCCs, assess whether the tool is effective, considering all circumstances of the transfer and taking into account the laws or practices of the importing country.
4. If necessary in light of the assessment under the above step, identify and adopt supplementary measures to bring the level of protection for the data transferred up to the standard of "essential equivalence."
5. Take any formal procedural steps that the adoption of the supplementary measures may require.
6. Reevaluate, when appropriate, the level of protection for personal data transferred to third countries and monitor any developments that may affect the transfers.

## 7. What information does Discourse provide to help customers carry out their TIAs?

To help our customers conduct the required TIA when they act as data exporters in transferring EU personal data to Discourse, we are providing the information below with respect to each of the EDPB-recommended steps.

### Step 1: Know your transfers

The first step is to understand if personal data is transferred outside the EU (including remote access when data stays physically in the EU) in order to apply a level of protection to that data which complies with EU law. In addition, data exporters need to assess whether the transferred data is limited only to what is necessary.

You control the extent of personal data collection, use, disclosure, and retention with respect to forums that Discourse hosts. This control includes content moderation, authorizing and administering access rights for forum members, the extent to which forums are publicly available or restricted to controlled audiences, administering the type of data collected, and determining data retention. You may use your control and available tools to identify personal data that may be transferred out of the EU.

Discourse also offers an option of hosting using data servers in the EU for data at rest as of the date. This feature provides you with the ability to limit personal data storage outside of the EU without your express permission.

### Step 2: Identify the transfer tool you are relying on

Step 2 requires that data exporters identify the transfer tool supporting transfers of personal data to third countries.

For its processing of EU personal data on behalf of customers, Discourse relies on the standard contractual clauses annexed to Commission Implementing Decision (EU) (2021/914) of 4 June 2021 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 (the "EU SCCs").

### Step 3: Assess the laws or practices of the recipient country and their impact on the effectiveness of the transfer tool.

The EDPB Recommendations provide that data exporters relying on a transfer tool under Article 46 of GDPR must consider whether the "practices in force in the third country" could undermine the protections offered by that transfer tool.

Discourse has assessed publicly available information related to the laws and practices of the United States ("US") and other countries outside the EU to which personal data may be transferred in connection with its customers' use of the Discourse. Based on this assessment, Discourse has concluded that these laws and practices do not prevent it from fulfilling its obligations under the EU SCCs regarding transfers of personal data outside of the EU and are compatible with commitments made by Discourse in the EU SCCs.

Given the focus of the *Schrems II* judgement on US law and our status as a US company, US law is particularly relevant. To that end, Discourse has conducted a review of the potential impact of the laws at issue in *Schrems II*—Section 702 of FISA and Executive Order 12333—on Discourse, taking into account the circumstances of the transfers that occur between Discourse and its customers. Based on that review and our practical experience (including that Discourse has never received any order or request for personal data under FISA Section 702 or any similar national security or surveillance law of any other country), we concluded that the risks posed by those provisions either do not apply to Discourse's processing of personal data on its customers' behalf and/or can be sufficiently mitigated by supplemental contractual, technical, and organizational measures that Discourse offers.

For example, the EDPB has indicated in an Information Note that "safeguards that have been put in place . . . in the area of [U.S.] national security (including the redress mechanism [implemented by Executive Order 12333])" to respond to *Schrems II* and facilitate the EU-U.S. Data Privacy Framework also "apply to all data transferred to the US, regardless of the transfer tool used." We adopt the EDPB's finding to conclude that the laws and practices of the US provide an adequate level of protection for EU personal data.

### Step 4: Identify and implement supplementary measures

Step 4 of the EDPB Recommendations requires data exporters to identify supplementary measures that may be used to bring the level of protection of personal data transferred up to the required standard of "essential equivalence." Data exporters need to take this step only if their assessment in Step 3 reveals that the laws or practices of the destination country could negatively impact the effectiveness of the transfer tool. As discussed above, the EDPB concluded that the laws and practices of the US provide an

adequate level of protection for EU personal data, such that no supplementary measures would be necessary for transfers of EU personal data to the US.

If needed, this section summarizes various contractual, technical, and organizational measures that Discourse makes available to our customers to ensure that an equivalent level of protection exists for EU personal data that you process through your use of Discourse.

### Contractual measures

Discourse's Data Processing Addendum includes several contractual measures suggested by the EDPB Recommendations, including:

- A commitment by Discourse to implement specific technical and organizational security measures with respect to personal data processed through Discourse to protect that personal data against unauthorized access;
- A commitment by Discourse, pursuant to the EU SCCs, to provide the customer with information on requests received from public authorities for the disclosure of personal data transferred to Discourse by the customer;
- A commitment by Discourse, pursuant to the EU SCCs, to take steps to resist any binding order for compelled disclosure of personal data transferred to Discourse by the customer, and to only disclose the minimum amount of personal data necessary to satisfy the order when Discourse remains compelled to disclose personal data; and
- A commitment by Discourse, pursuant to the EU SCCs, to promptly inform the customer of any changes to the legislation applicable to Discourse that could undermine the protections provided for personal data in the Data Processing Addendum.

### Technical Measures

Discourse relies on several technical measures to ensure the protection of personal data transferred to it by Discourse Cloud customers which are described below. We maintain various security certifications and audit reports, including ISO 27001 and SOC 2 Type II, and share results from our penetration tests. You can also learn more about the security measures we apply to customer personal data, including access controls and encryption, by reviewing our Security Brief.

### Organizational measures

Discourse has implemented organizational measures to protect transferred personal data, including policies made available here. Our organizational measures are audited by third parties, including in connection with Discourse's ISO 27001 certification and SOC 2 Type II audit.

### Step 5: Formal procedural steps needed to adopt the supplementary measures

Step 5 under the EDPB Recommendations is to take any formal procedural steps required to effectively implement any supplementary measures adopted under Step 4.

As indicated above, many of the supplementary measures that Discourse has implemented are incorporated into Discourse's Data Processing Addendum, and thus are legally binding on Discourse by virtue of the customer's agreement with Discourse.

### Step 6: Re-evaluate the level of protection at appropriate intervals

Step 6 under the EDPB Recommendations requires the data exporter to reassess, at appropriate intervals, the protection afforded to personal data in third countries to which the data exporter transfers personal data, and to monitor any developments that may affect the initial assessment of the level of protection in those countries.

Discourse monitors developments in the laws and practices of the US and other countries in which it processes personal data, and updates our agreements, policies, and procedures as necessary to address those developments.

To help customers carry out this step, we also commit, in our Data Processing Addendum, to promptly notify customers of any change in legislation applicable to Discourse that could have a substantial adverse effect on our Data Processing Addendum commitments with respect to the protection of personal data.

## 8. WHAT IF I STILL HAVE OTHER QUESTIONS?

Please contact privacy@discourse.org with any questions or comments.