SIMPPLR

Simpplr Government Data Request Policy

Summary

At Simpplr, we take the privacy and security of our customers and their data very seriously. We understand that the data our customers entrust to us is confidential, and we are committed to protecting it from unauthorized access or disclosure.

Therefore, we have taken precautions designed to ensure that we are safeguarding the information entrusted to us by our users from any unlawful access or intrusions. This policy was created to provide greater transparency regarding the guidelines we use to determine how and when we will process demands received from law enforcement, national security, and other regulatory bodies (“government”) for information about our customers, their employees, and/or their users (“customer data”).

In addition, it is important to note that while this policy is not specifically intended to address requests for customer data arising from private or commercial disputes, Simpplr will, to the extent applicable, take the same precautions specified herein for such requests.

Purpose

This Government Data Request Policy sets out the Simpplr procedure for responding to a request received from a law enforcement or other government authority (together the “Requesting Authority“) to disclose personal data processed by Simpplr (hereafter “Data Disclosure Request“).

The Policy also sets out the Simpplr notification procedure for instances where we became aware of a direct access (i.e., access to personal data without prior request and/or approval/collaboration by Simpplr) by law enforcement or other government authority to personal data processed by Simpplr (hereafter “Direct Access”).

SIMPPLR

Safeguarding Customer Information

Upon receipt of a government request for customer data, Simpplr takes the following steps into consideration in order to safeguard customer information before responding:

- **Subject**. Wherever possible, Simpplr believes that a government should first seek to obtain the information that they are seeking directly from the customer or end user who is the subject of the investigation before requesting such Information from Simpplr.

- **Authority**. Simpplr will only provide customer data if a government has appropriate authority under applicable law to request such information. Absent a valid warrant, subpoena, court order, equivalent legal process, or emergency situation, it is Simpplr's position not to provide customer data to the government.

- **Scope**. Wherever possible, Simpplr will seek to ensure that any request for customer data is limited to a clear and reasonable scope about a specific customer account, request additional context if the nature of the investigation is not clear, and may push back on the request for other reasons. In the event Simpplr does provide information, it will be the minimum amount of information required to comply with the demand.

- **Notice**. Except in circumstances where Simpplr has been advised by a government not to notify, is prohibited from doing so, or there is a clear indication of illegal conduct or risk of harm, Simpplr will notify the customer of a request before disclosing any customer data so that the customer may seek available legal remedies.

Simpplr will only disclose customer data in response to a lawful request from a government agency in accordance with applicable law, our terms of service, and any applicable Data Protection Agreement (DPA). Each and every request received will be carefully reviewed for legal sufficiency. If a request does not comply with applicable laws, we will seek clarification or take steps to challenge the request. We will reject or require greater specificity on requests that appear overly broad or vague.

Whenever possible, Simpplr will provide notice to customers when their data is being requested by a government. This notice will be provided in a timely manner and will include information about the nature of the request, the specific data being requested, and the agency making the request. We will also provide customers with the opportunity to object to the disclosure of their data.

SIMPPLR

General Principle

As a general principle, Simpplr does not disclose personal data in response to a Data Disclosure Request unless either:

- Simpplr is under a legal obligation to make such disclosure; or
- taking into account the nature, context, purposes, scope and urgency of the Data Disclosure Request and the privacy rights and freedoms of any affected individuals, there is an imminent risk of serious harm that merits compliance with the Data Disclosure Requests in any event.

For that reason, unless it is legally prohibited from doing so or there is an imminent risk of serious harm, Simpplr will notify and consult with the customer and the competent data protection authorities to address the Data Disclosure Request.

Handling

If Simpplr receives a Data Disclosure Request, the recipient of the request within Simpplr must pass it to the Simpplr Legal Team immediately upon receipt, indicating the date on which it was received together with any other information that may assist the Legal Team to respond to the request. Similarly, if Simpplr becomes aware of Direct Access, it shall communicate this to the Legal Team immediately, indicating the date on which it occurred together with any other information that may assist the Legal Team to respond in line with this Policy.

We examine the legitimacy of every Data Disclosure Request document we receive and if we determine that a document is forged, we will not comply. We do not honor requests that have not been made through the appropriate channels.

We evaluate the completeness of every government request. In order for us to evaluate a request, it must be in writing, as specific as possible about the data to be shared, and clear in its explanation of the legal basis for the request. If we receive a verbal request, we ask for it in writing. Any Data Disclosure Request, however made, must be notified to the Legal Team for review.

Simpplr's Legal Team will carefully review each and every Data Disclosure Request and Direct Access on a case-by-case basis. The Legal Team will consult with the Privacy Team and outside counsel as appropriate to determine the nature, context, purposes, scope and urgency of the Data Disclosure Request/Direct Access, and its validity under applicable laws and principles of international comity, to identify whether action may be needed to challenge the Data Disclosure Request/Direct Access, including by means of an appeal to the Requesting Authority, and/or by

seeking interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits or otherwise requiring the disclosure under the applicable procedural law, as appropriate, and/or to notify the customer and/or competent data protection authorities.

Notification

A) Notification to the Customer

If a request concerns personal data for which a customer is the controller, Simpplr will ordinarily ask the Requesting Authority to make the Data Disclosure Request directly to the relevant customer. If the Requesting Authority agrees, Simpplr will support the customer in accordance with the terms of its contract to respond to the Data Disclosure Request.

If this is not possible (for example, because the Requesting Authority declines to make the Data Disclosure Request directly to the customer), Simpplr will notify and provide the customer with the details of the Data Disclosure Request prior to disclosing any personal data, unless legally prohibited from doing so or where an imminent risk of serious harm exists that prohibits prior notification.

If Simpplr becomes aware of a Direct Access concerning personal data for which a customer is the controller, Simpplr will notify and provide the customer with the details of such Direct Access, unless legally prohibited from doing so or where an imminent risk of serious harm exists that prohibits such notification.

B) Notification to Data Protection Authorities

If the Requesting Authority is in a country that does not provide an adequate level of protection for the personal data in relation to such request, in accordance with applicable data protection laws, then Simpplr will also put the request on hold to notify and consult with the competent data protection authorities, unless legally prohibited or where an imminent risk of serious harm exists that prohibits prior notification.

If the law enforcement or other government authority which carried out a Direct Access is in a country that does not provide an adequate level of protection for the personal data in relation to such request, in accordance with applicable data protection laws, then Simpplr will also notify and consult with the competent data protection authorities, unless legally prohibited or where an imminent risk of serious harm exists that prohibits prior notification.

Where Simpplr is prohibited from notifying the competent data protection authorities and/or suspending the request, Simpplr will use its best efforts (taking into account the nature, context, purposes, scope, and urgency of the request) to inform the Requesting Authority that carried out the Direct Access about its obligations under applicable data protection law and to obtain the right to waive this prohibition. Such efforts may include asking the Requesting Authority that carried out the Direct Access to put the request on hold, so that Simpplr can consult with the competent data protection authorities, or to allow disclosure to specified personnel at Simpplr's customer, and may also, in appropriate circumstances, include seeking a court order to this effect.

Simpplr will maintain, and upon reasonable request provide, to its customers and competent data protection authorities, a written record of the efforts it takes, in line with its established business record maintenance practices, unless legally prohibited from doing so.

Bulk Transfers Prohibited

In no event will Simpplr transfer personal data to a Requesting Authority in a massive, disproportionate, and indiscriminate manner that goes beyond what is necessary in a democratic society.