Data Transfer Impact Assessment

Below is a reference copy of Zapier's previous Data Transfer Impact Assessment from March 9, 2023. Please note that this information is now outdated; it was replaced by Zapier's current Data Transfer Impact Assessment which may be accessed at: https://zapier.com/legal/data-transfer-impact-assessment

Zapier takes the protection of our customers' information seriously. We have taken steps to comply with applicable EU and UK law regarding international data transfers.

For our customers who are data exporters from the European Economic Area/European Union ("EU") or the United Kingdom ("UK" and collectively, "Europe"), this page is designed to provide information about key issues for transfers made to Zapier in the US, and support our customers as they complete data transfer impact assessments pursuant to the Schrems II decision and EU standard contractual clauses.

For more details about Zapier's data privacy compliance program, including with respect to GDPR and UK GDPR, please visit our Data Privacy Overview page.

1. What products and services does Zapier provide?

Zapier provides subscriptions to our "software as a service" (SaaS) platform to automate workflows, transfer data, and provide other functionalities available to our customers as part of the Zapier platform ("Zapier Services").

2. What types of personal data does Zapier process?

Our customers control the types of personal data they provide to us in connection with their use of Zapier Services. Accordingly, the types of personal data we process include any personal data that a customer uploads to Zapier Services, and may relate to that customer's end-users (including their employees, customers, or suppliers). Customers are responsible for compliance requirements that may apply to such uploaded data, including ensuring a lawful basis for processing. The exact nature of the processed data varies per Zapier Service and each customer's own use cases. Zapier processes personal data governed by European data protection laws as a data processor (on behalf of our customers), in accordance with our obligations under the Zapier Data Processing Addendum, including our Standard Contractual Clauses (SCCs).

You may find further information about Zapier's data processing activities in connection with our customers' use of Zapier Services in Schedule 1 of our Data Processing Addendum,

including the type and categories of personal data, nature and scope of data processing, purpose of processing, and categories of personal data transferred.

3. Where do we store and otherwise process data?

We store and otherwise process personal data in the US. We also store data with our subprocessors. Information about our subprocessors and their locations is available here.

4. How do we protect data that is transferred?

Zapier is based in the US, where neither the EU nor the UK has issued an adequacy decision to permit transfers of, respectively, EU or UK personal data to. Therefore, Zapier has adopted standard contractual clauses, as approved by the relevant supervisory authority or applicable law, to be the transfer safeguard instead.

> For transfers from the EU, we have implemented the standard contractual clauses from the European Commission's Decision of 2021/914 of 4 June 2021 ("EU SCCs"), with the appropriate module(s) selected (e.g. controller-to-processor, or processor-to-processor.
>
> For transfers from the UK, we have implemented the UK International Data Transfer Addendum issued by the ICO and laid before the UK Parliament in accordance with s119A of the Data Protection Act 2018 of the UK on 2 February 2022.

Where applicable data protection requirements change, we may update these transfer mechanisms to comply with applicable law.

Data processed by Zapier in connection with our customers' use of Zapier Services is both transferred to and stored in the US.

5. What controls do we have in place with subprocessors?

We also make onward transfers to subprocessors and take steps to agree to appropriate transfer safeguards, such as relevant standard contractual clauses, with each subprocessor. We take measures to evaluate the privacy and security practices of our subprocessors, including:

> Each subprocessor is required to agree to a data processing agreement with us.

We evaluate the data privacy and security practices of each subprocessor prior to engaging and onboarding such subprocessor.

We conduct periodic audits of key subprocessors throughout the terms of our respective agreements with them.

Information about Zapier's subprocessors and their locations is available here.

6. How long is data retained?

Information regarding data retention and deletion on Zapier Services is available here.

7. How do we manage requests from data subjects to exercise their GDPR rights?

We have processes to receive, analyze, and respond to data subject requests from our employees, customers, and marketing prospects. Additionally, our customers may delete and export data from their Zapier Services account as described here.

8. What US laws apply to Zapier with respect to data transferred from the EU or the UK?

Zapier's customers, as data exporters, should assess whether anything in the law or practices of the third country (i.e. the US) may impact the effectiveness of relying on the standard contractual clauses as a transfer tool. Exporters should assess whether the level of protection in the recipient country (i.e. the US) is essentially equivalent to what is guaranteed under the UK and/or EU GDPR, as applicable – or, if not, what supplementary measures will be required.

The US Constitution, Executive Order 12333 ("E.O. 12333"), Presidential Policy Directive 28 (PPD-28"), s.702 Foreign Intelligence Surveillance Act ("FISA") may be relevant. We have provided a summary of key considerations below; however, this information does not constitute legal advice, and we recommend that you consult with your counsel regarding any intended data transfer.

FISA Section 702: authorizes the US government to acquire information about non-US persons located outside of the US through compelled assistance of electronic communications service providers. We do not believe that Zapier Services processes personal data of interest to US authorities and if that were to be the case, the data in question would be held by other entities, and US authorities would likely approach those

other entities directly. As detailed in the US Department of Commerce White Paper on this subject, for most companies, concerns about US government access to company data are “unlikely to arise because the data they handle is of no interest to the US intelligence community.” Companies handling “ordinary commercial information like employee, customer, or sales records, would have no basis to believe US intelligence agencies would seek to collect that data.”

> Additionally, FISA Section 702 requires an independent court to authorize a specific type of foreign intelligence data acquisition that is generally unrelated to commercial information.
>
> To date, Zapier has never received any requests under FISA Section 702.

EO 12333: authorizes US intelligence agencies to conduct surveillance outside of the US. In particular, it provides authority for US intelligence agencies to collect foreign "signals intelligence" information - information collected from communications and other data passed or accessible by radio, wire, and other electromagnetic means. However, bulk data collection, the type of data collection at issue in Schrems II, is expressly prohibited under EO 12333, and EO 12333 contains no authorization to compel private companies (such as Zapier) to disclose personal data to US authorities. As such, Zapier has not provided assistance to, or cooperation with, the US government under EO 12333.

> We are not aware that the US government has collected any signals intelligence from Zapier’s communications or other data. Moreover, we do not believe that Zapier Services processes personal data of interest to US authorities. We do not voluntarily disclose any customers’ personal data to US authorities without the consent of such customer.

9. How do we respond to government requests to access personal data of our customers?

As of the “last updated” date at the top of this page, Zapier has never received a FISA Section 702 or EO 12333 data access request from the US government in connection with Zapier Services.

If we were to receive a request from a governmental authority for personal data that we process on behalf of a customer, we will promptly notify the customer, unless prohibited by law from doing so. In any such notice, we’d include information about the personal data requested, the requesting authority, the legal basis for the request, and the response provided. Where legally permissible, we would also notify the customer if we became aware

of any direct access by public authorities to personal data that we process on behalf of such customer.

If we were to be prohibited by law from doing so, we would use reasonable efforts to obtain a waiver of the prohibition with a view to communicating as much information as possible to our customer in an expeditious manner.

10. What measures does Zapier take to protect personal data?

Zapier undertakes technical and organizational measures to secure customer data as described in Schedule 1 of Zapier's Data Processing Addendum, as well as security measures, including encryption, which are further described here.

Zapier's contractual measures are set out in our Data Processing Addendum which incorporates the SCCs. These include:

> Technical measures: Zapier is contractually obligated to have in place appropriate technical and organizational measures to safeguard personal data.
>
> Transparency: Zapier is obligated under our SCCs to notify our customers in the event we are made subject to a request for government access to customer personal data from a government authority. In the event Zapier is legally prohibited from making such a disclosure, we will use reasonable efforts to obtain the right to waive the prohibition to communicate as much information to you as possible.
>
> Actions to challenge access: Under our SCCs, Zapier is obligated to review the legality of government authority access requests and challenge such requests where they are considered to be unlawful.

Zapier will review and, if necessary, reconsider the risks involved and the measures it has implemented to address changing data privacy regulations and risk environments associated with transfers of personal data outside of Europe.