CONVERCENT DATA PRIVACY

Transparency Report

Convercent is committed to being as transparent as possible about its privacy practices. Here, we describe our policy for managing government and law enforcement requests for customers' personal data and provide our Transparency Report that documents relevant information about the requests received.

Convercent's Transparency Report shows requests received globally:

- The identities of the requesting authorities
- The number of accounts related to each request
- The types of personal data requested
- The number of requests we have challenged
- The number of times we disclosed personal data in response to the requests

Year	2013	2014	2015	2016	2017	2018	2019	2020	2021 to date
Number of Requests	0	0	0	0	0	0	0	0	0
Identity of Authorities	-	-	-	-	-	-	-	-	-
Accounts Requested	0	0	0	0	0	0	0	0	0
Types of Personal Data	-	-	-	-	-	-	-	-	-
Requests Challenged	0	0	0	0	0	0	0	0	0
Disclosures	0	0	0	0	0	0	0	0	0

Government & Law Enforcement Request Policy

Convercent does not voluntarily disclose any personal data of customers to government authorities or otherwise grant them access to such data. In addition, Convercent has not built, and will not purposefully build, backdoors to enable government actors to access its data or information systems, and has not changed, and will not purposefully change, its processes in a manner that facilitates government access to data.

However, Convercent may receive a legally binding subpoena, writ, warrant, or other court order from a government authority requesting that it disclose a customer's personal data. Convercent will only provide the requested customer data in response to formal and valid legal process. Where Convercent receives such a request, Convercent's legal team reviews the request to ensure that it satisfies applicable legal requirements. If the legal assessment reveals legitimate and lawful grounds for challenging the request, Convercent will do so where appropriate. Convercent's policy is to construe such requests narrowly to limit the scope of the personal data provided.

For Convercent to disclose any customer data, the request must also satisfy the following policies:

- be made in writing and on official letterhead,
- identify and be signed by an authorized official of the requesting party and provide official contact information,
- including a valid email address,
- indicate the reason for, and nature of, the request,
- identify the customer or customer account that is the target of the request,
- describe with specificity the data/information sought and its relationship to the investigation, and
- be issued and served in compliance with applicable law.

Where Convercent receives a legally binding request for a customer's personal data, Convercent's policy is to notify the customer via email before disclosing any information. To the extent permissible under the request and/or applicable law, the notice will describe the personal data requested, the authority making the request, the legal basis of the request, and any response already provided. This notice gives the customer an opportunity to pursue a legal remedy, such as filing an objection with a court or the requesting authority.

Exceptions to Convercent's policy for personal data requests by government authorities:

- A statute, court order, or other law may prohibit Convercent from notifying the customer about the request, but Convercent will make reasonable efforts to obtain a waiver of the prohibition or provide notice once the prohibition requirement ends.
- Convercent might not give notice to the customer in exceptional circumstances involving imminent danger of death or serious physical injury to any person or to prevent harm to Convercent's services.
- Convercent might not give notice to the customer when it has reason to believe that the notice would not go to the actual customer account holder, for instance, if an account has been hijacked.
- Where Convercent identifies unlawful or harmful activity, or suspects any such activity, related to a customer's account, it might notify appropriate authorities, such as in the cases of hacking.