CONVERCENT DATA PRIVACY

Frequently Asked Questions

1. How does Convercent encrypt data?
Data is encrypted at rest using AES 256 and in transit using TLS 1.2.

2. What are Convercent's security certifications?
Convercent completes four independent third-party audits annually to meet standard cyber security frameworks including SOC 2, ISO 27001, HITRUST, and NIST.

3. How does Convercent test the security of the application?
We test our security using methods that include system/network scans, dynamic application system tests on the application, static application system tests to test our code, and annual third-party penetration tests to manually verify our application is safe from a hacker's perspective.

4. Where do you host data?
Our data is hosted in two European locations and two US locations, depending on customer need. Within the EU, data is hosted primarily in Dublin, Republic of Ireland, with Failover in Amsterdam, Netherlands. Within the US, data is hosted primarily in Seattle, Washington, with Failover in Cheyenne, Wyoming.

5. What subprocessors do you use, and can they access data?
Microsoft Azure, Amazon Web Services, and Google Cloud Platform in Europe. Our cloud service providers do not have access to our data due to hardened security controls and encryption.

6. Do call centre agents have access to data?
Computer Generated Solutions (CGS) call centres provide our whistleblowing phone intake; data is received by a call centre agent and entered as remote hands into the system. Once the report has been completed and confirmed, it is submitted to the data hosting environment chosen by the customer at the call centre location of choice. Organisations can opt for the CGS locations in Romania or in the United States (Must have dedicated lines and programming) or global organisations may choose multiple locations across the continents. Call centre agents do NOT have access to the underlying database. The data will NEVER leave the EU for customers who opt for the Romanian call centre operation.

7. How are you responding to the invalidation of the EU-US Privacy Shield?
On July 16, 2020 the Court of Justice of the European Union invalidated EU-US Privacy Shield as a data transfer mechanism between the EU and US. Since then, additional guidance on supplementary measures for international data transfers has been released by the European Data Protection Board, and updated draft Standard Contractual Clauses by the European Commission. Our Data Processing Agreements incorporate the updated Standard Contractual Clauses (SCCs) from the European Commission, as well as European Data Protection Board (EDPB) recommendations on supplementary measures to ensure compliance with the EU level of protection of personal data.