Trust Center

Enterprise Level Security and Privacy

Privacy Shield List

Collective[i]'s first priority is keeping your data private and secure. We recognize the importance of maintaining the confidentiality, integrity, and availability of business information existing in a network with the world's leading companies. This is vital to the business operations of our clients and to our own success. To that end, we have designed our application from inception with a multi-layered approach to securing key information and have established an industry-leading security and privacy program dedicated to ensuring clients have the highest confidence in our protection of their data.

Our Privacy Philosophy: Data Minimization and Client Control of Data

The two core philosophies of Data Minimization and Client Control consistently inform how our team--from engineering to client success--builds our product and handles client data. Unlike many other AI/ML companies we only collect data that is required for us to provide our services to our clients and no more. Additionally, we ensure that our clients always have complete transparency around and control over their data. This means that you choose which CRM fields and which email inboxes to provide via secure API access, and you can turn off API access to any data source at any time. For more information on our privacy program, please see our Privacy Policy.

Our Security Philosophy: Confidentiality, Integrity and Availability

We recognize the importance of maintaining the confidentiality, integrity and availability of business information while existing in a network with our clients, many of whom are large, multinational corporations operating in highly regulated industries. Our security program is SOC 2 Type 2 compliant and aligned to the ISO 27000 standards. In addition to maintaining industry-leading, multilayered administrative, physical and technical safeguards to protect client data, we constantly monitor and improve our application, systems, and processes to meet the growing demands and challenges of an ever-evolving security landscape. For more information on our security program and policies, please see our Security Overview.

collective[i]™

SOC 2 Type II Certified

We have achieved SOC 1, 2 & 3 accreditation, which is reserved for organizations that have demonstrated standard operating procedures for organizational oversight, vendor management, risk management and regulatory oversight. The American Institute of Certified Public Accountants (AICPA) and Service Organization Controls (SOC) reports give assurance over control environments as they relate to data retrieval, storage, processing, transfer, privacy and more. Specifically, the SOC 2 reports evidence our achievement of key controls around the security, availability and confidentiality of client data.

Additional information can be found here.

Privacy Shield List

Privacy Shield Certified

We are proudly registered with EU-U.S. and EU-Swiss Privacy Shield. The EU-U.S. and Swiss-U.S Privacy Shield Frameworks were designed by the U.S. Department of Commerce and the European Commission and Swiss Administration to provide companies in Europe and the United States with a mechanism to comply with data protection requirements when transferring data from the European Union and Switzerland to the United States. Our Privacy Shield certificate can be found here.

Additional information can be found here.

Third Party Audits

We are frequently audited and assessed by third parties and clients. For the past few years, we have partnered with TRUSTe/TrustArc, the leader in privacy compliance and data protection for over two decades, to ensure that our client's data is safe and secure. Our controls are also annually audited by A-LIGN, a nationally recognized cybersecurity and compliance firm, to confirm our SOC 1&2 accreditation.

Penetration Testing

We perform regular vulnerability and automated network and application penetration scans and engage qualified external entities to perform independent application-level and infrastructure-level penetration tests. Finally, we work closely with clients who have strict security requirements welcoming additional testing and verification to ensure we are committed to the protection of your data.

collective[i]™

Physical Data Centers

Client data is hosted in physical data centers in two locations within the United States. We use multi-vendor diversity to ensure that a single failure does not negatively impact our clients. Access to these physical data centers is strictly controlled and monitored by security staff. Our data center partners are ISO, SOC, PCI, FIPS and HIPPA certified. Additionally, our data centers operate in environmentally friendly LEED and Energy STAR certified facilities.

Robust Data Encryption

We encrypt your data, including emails, contacts and calendar events, using AES-256-bit data-at-rest encryption and TLS 1.2 SHA-256 data-in-transit protection. The keys for these systems are frequently rotated to comply with industry standard KMS practices and are secured by KMS protections.

GDPR and CCPA Compliance

We maintain full compliance with GDPR, CCPA and other applicable privacy regulations. We have built and continue to build our products with the principles of data minimization and client control and privacy in mind. In a continually changing privacy landscape, we continue to seek up-to-date guidance from outside legal counsel and consultants.

For more information, please see our Privacy Policy.

GDPR Representative

We have engaged a EDPO as our GDPR Representative. We partner with EDPO, based in Brussels, Belgium, to ensure full compliance with an EU data subject's various individual rights under GDPR, including the right "to be forgotten".

For more information, please see our Privacy Policy.

collective[i]™