

Security and Integrity

The essence of every company's revenue growth plan is based on how well they attract, nurture, hire, grow and challenge the best employees they can find. Often relying on manual techniques and systems decades old, companies are struggling to find the right employees to help them grow. Anyone who has hired and managed people can appreciate the upside potential of talent management today.

✓ **GDPR-Ready**

✓ **SOC2 Compliant**

✓ **Never Breached**

How does Eightfold protect your data?

1. **Data segregation.** Every customers' data is stored separately and encrypted at rest.
2. **Secure API.** Eightfold uses secure protocols to connect with your ATS's API using Transport Layer Security 1.2 for HTTPS encryption, which is authenticated by AES-256 bit encryption.
3. **Secure web application.** Entire Eightfold site uses HTTPS by default and all data is encrypted in transit.
4. **Internal data encryption.** In addition to encrypting API traffic Eightfold encrypts all internal traffic. All data at rest, from databases to file systems to caches, is encrypted using AES-256, managed through AWS Key Management Service.
5. **Account Passwords.** All passwords are encrypted with bcrypt, a strong cryptographic hashing algorithm with built-in randomly-generated salts.

Who can access to your data?

Access to customer data is only provided to select employees to troubleshoot in the event of a customer issue that needs to be resolved Arbitrary access is prohibited. Every access is logged for audit trail.

Is Eightfold backed up?

Eightfold uses database replication and periodic snapshots to avoid data loss. In case of a data loss, we use replicas to quickly recover to a known previous state.

What physical security measures are in place to protect your data?

Eightfold does not store any data on-premise We currently uses AWS for all data storage and processing, which is compliant with some of the most stringent security requirements:

<https://aws.amazon.com/security/>

What is Eightfold's data breach response plan?

Eightfold has procedures in place to disallow external access to data at short notice. We also have strict logging for all access in order to identify breaches.

Is Eightfold compliant with GDPR, EEO, OFCCP?

Eightfold does process and store, but does not collect Personally Identifiable Information including Equal Employment Opportunity (EEO data. For customers that require it, Eightfold can meet recordkeeping standards established by the Office of Federal Contract Compliance Programs (OFCCP).

Eightfold is a data processor that is fully compliant with the GDPR. No Eightfold customers have required additional internal compliance work.

Does Eightfold support access control and provisioning?

Yes—Eightfold supports SAML-based provisioning systems, and has an internal permissions-based account system.