Accredible's Data Security

An in-depth look at the measures Accredible takes to protect your data.

July 7, 2017

Accredible

Introduction

This document is intended to provide a high-level overview of Accredible security and how we help manage compliance with data protection laws. It addresses the most common concerns customers may have about security and data privacy, particularly within the European Union. It outlines the organizational and technical measures in place at Accredible which relate to data processing and protection.

This document aims to help customers understand:

- The measures Accredible takes to protect the privacy and security of our customers' data.
- How Accredible uses the data customers send to us in order to provide credentials.
- The responsibilities of Accredible and our customers in managing and securing data sent to and processed by Accredible.

We'll answer the following commonly asked questions:

- How will Accredible secure data that is sent to us?
- Who can Accredible share data with in order to provide our service?
- Where and how long will data be stored for?
- Who has access to data?

The Data Protection Directive - Directive 95/64/EC

The Data Protection Directive (officially Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data) is a European Union directive adopted in 1995 which regulates the processing of personal data within the European Union.

The directive sets forth a number of data protection requirements which apply when “personal data” about an identified or identifiable individual is being “processed” as such terms are defined in the Directive.

In the context of Accredible’s services, the customer determines the purpose and means of processing of personal data and is therefore the “data controller” under the Directive. Accredible, as the entity which processes personal data on behalf of and at the direction of the data controller, is the “data processor.”

To provide our services, Accredible typically requires personal data such as a name or email address.

Accredible and Compliance with The Data Protection Directive

Please note that this document is merely intended to provide informational guidance on Accredible's services in the context of the Directive. Customers should bear in mind that the Directive may not apply to organizations established in certain EU Member States where differing national laws may be applicable. Further, this document does not address all privacy and data protection laws and regulations which may be applicable to individual customers, as this may depend on different factors, including, but not limited to, where and how a customer conducts its business and chooses to use the services, the industry in which the customer operates, and the type of data a customer may choose to process.

Upon request, Accredible is able to enter into a specific agreement with customers that is based upon the EU model clauses aligning with the directive and German law.

What data does Accredible Process?

The services provided by Accredible allow a customer to design, issue, administer and monitor certificates, badges and blockchain credentials using Accredible's online platform. In addition, Accredible may use personal data to reach out for the purpose of notifying a person of changes/updates of their certificates including password management and technical support.

To provide service Accredible typically need the data controller to provide names, email addresses, locations and information on individual performance for which a certificate/accreditation shall be granted.

Sub-processors

Accredible works with a small number of organizations to provide service to customers. These sub-processors:

- Provide communication tools enabling Accredible to email our customers or respond to our customers' support requests or the requests of our customers recipients.
- Provide hosting and backup solutions as part of Accredible's services.

Accredible maintains contractual safeguards to ensure that relevant industry standard data protection mechanisms are maintained for these subcontractors.

Data Storage

Data is stored at a location hosted by AWS, which is a secure tier 3 SOC 2-certified data center. All data is hosted within the US.

Access Control

Accredible employes a role-based access control framework that ensures access to data is only provided to employees where their job responsibilities necessitate such access. We conduct annual audits to ensure compliance with our access control policies. Any breaches or inconsistencies are documented, investigated and remediated according to a standard procedure.

Data Retention

Upon termination of the Accredible services, data is expired out of Accredible's systems within a commercially reasonable period of time, but no more than 90 days.

Compliance and Audit

Accredible's security and data privacy controls, software, infrastructure and systems are audited both internally and independently (externally) on an annual basis.

We regularly undergo penetration tests and enforce a framework and set of policies which help ensure that we're compliant with security and privacy standards.

Conclusion

Maintaining the security of our services and managing the privacy concerns of our customers are our top priorities. We understand that the data we process for you is important and needs to be protected.

To further understand how we address security and privacy, customers are encouraged to read the materials, best practices, and other guidance that is made available on the Accredible website. This material can be found at https://www.accredible.com. If you require further information, please contact our support team at https://help.accredible.com.