Ascend by Assessio
Security and Privacy Overview

Assessio Psychometrics has a security first culture and is dedicated to providing a secure, stable and reliable platform to our customers and users. We continually strive to keep the Ascend platform and our internal processes up-to-date and at the forefront with regards to all aspects of data security, privacy and compliance.

We understand that many of our customers have business and legal requirements regarding the security of the systems they use and the data they collect. One of our primary goals is to ensure that the Ascend platform and supporting services provide our customers with the confidence they require to use our services and know that their data is secured and stored in line with industry best-practices. What follows is a general overview of some of the core aspects around security and privacy regarding the Ascend platform.

Infrastructure and Hosting

The Ascend platform is hosted and managed within the Amazon Web Services (AWS) cloud. We leverage extensive security features provided by AWS, including: identity and access management defining fine-grained access controls to cloud resources; multi-factor authentication for all cloud administrators; fully encrypted communications to, from, and between cloud resources; network firewalls and web application firewalls for protecting cloud resources; comprehensive monitoring and logging of cloud resource access and usage.

The AWS cloud allows us to provide high availability and scalability of the Ascend platform. Our production servers are located within Europe, in the eu-west-1 AWS region (Ireland), with disaster recovery infrastructure, including data backups, located within the eu-central-1 AWS region (Frankfurt). Within the production region, the application resources can scale according to demand, and are load-balanced across multiple availability zones, ensuring that a failure in any single availability zone will not result in any loss to application availability. In the event of a complete region failure, the Ascend platform has disaster recovery infrastructure and procedures in place to bring up new resources within an alternative region, minimizing the impact to data, customers and users.

The AWS cloud is trusted by some of the largest solution providers in the world, have strict and comprehensive security infrastructure and procedures in place, and an array of security related certifications, including ISO 27001, as well as certifications relating to specific industries such as government, healthcare and finance. For more information on cloud security for the AWS cloud, please see https://aws.amazon.com/security/. For additional information on compliance and certifications for the AWS cloud, please refer to http://aws.amazon.com/compliance/.

Application Security

Security within the application itself is managed using standards based frameworks and follows current best practices.

The Ascend platform uses Transport Layer Security (TLS) encryption for all transmitted data, meaning that all communication with the Ascend system requires secure HTTPS connections.

Authentication and authorization mechanisms use industry standard mechanisms, and we try to follow web application security best-practices by actively following the OWASP recommendations, implementing preventive measures to many of the well-known web vulnerabilities, including: SQL Injection protection; Cross Site Scripting (XSS) protection; Cross Site Request Forgery (CSRF) protection; Strong Session Management. More information on these issues can be found on the OWASP website here: https://www.owasp.org/

In a multi-tenant cloud platform, it is paramount that data is only available to the data owners, and we employ fine grained access control and authorization checks at multiple layers in the application to ensure that data is only accessible to the owners of that data. Additional measures include secure storage of account passwords using strong encryption, and short-lived token-based access to the user interface and API.

Privacy

Assessio Psychometrics understands the importance of ensuring the privacy of our customers and users personally identifiable information. Please read below for more information, including how the Ascend platform adheres to a number of key data protection regulations.

Swedish Personal Data Act (PUL)

Ascend complies with the Swedish Personal Data Act (PUL). The legislation is intended to protect individuals from having their personal integrity violated through the processing of personal data. As part of this law, persons who are the subject of the personal information processed should be informed about any actions taken. According to PUL, personal information refers to any information that directly or indirectly is related to a physical person that is living.

According to PUL whoever makes use of a cloud service for processing of personal data is the controller of personal data, even if the processing is carried out by a cloud service provider or its subcontractors. The provider of the cloud service, and all of its sub-contractors hired for the processing, is the controller's data processors. The data processor must not process personal data for purposes other than those for which the processor has been appointed. As a data processor Ascend is obliged to take appropriate security measures in accordance with the PUL legislation.

More information on the Personal Data Act: http://www.datainspektionen.se/in-english/legislation/the-personal-data-act/

EU General Data Protection Regulation (GDPR)

Ascend will also comply with the European Union General Data Protection Regulation (GDPR), which goes into effect on May 25, 2018. The law introduces measures to ensure security of personal data, specifying how organisations should manage data from their employees, customers and partners. Personal data is considered any information that can directly or indirectly identify an individual, whether it relates to their private, professional or public life.

The GDPR requires data processors to develop and implement a number of internal procedures and practices to protect personal data. Most of those procedures and practices are related to information security management. The GDPR also extends specific rights to individuals regarding the use of their personal data. These include processes around the transfer of data and when to erase data.

More information on the General Data Protection Regulation: http://www.eugdpr.org/