Table of content

Introduction

At Atlas Well we are committed to offering advanced, personalized, high quality health and well-being solutions - Available from anywhere, at any time.

As pioneers in the healthtech industry, we prioritize information security, legal compliance and data privacy in every tier of our organization. Data security is hence a fundamental aspect of both our development process and everyday operations. Atlas Well's system architecture is, in addition, carefully designed to meet the strict requirements of both private and municipal health institutions.

This document outlines our dedicated efforts and the features of our platform designed to address security, compliance, and privacy. It's our way of assuring users that their personal data is in safe hands with Atlas Well.

How Atlas Well works

Atlas Well is a system and service for obtaining and sharing of BAC-values. The system consists of a device for measurement, a mobile app for registration and a web platform for management. With Atlas Well, it is possible to retrieve an individual's BAC value from anywhere, at any time. This can in turn build motivation, improve safety and strengthen important relationships.

How we partner with sub-processors

We thoroughly assess suppliers throughout the procurement process, engaging them exclusively for specific and essential purposes to enhance Atlas Well for our end-users. We hold our suppliers to the same high standards of technical competence and security that we maintain ourselves.

For our most critical sub-processors, we insist on ISO 27001 certification, as well as GDPR compliance. All contracts entered into with selected suppliers detail our expectations concerning their IT environment and information security measures. Every supplier is required to provide documentation regarding their technology, practices, processes, as well as their IT and information security policies.

We also regularly monitor and assess the access rights and other aspects of our agreements with suppliers to ensure compliance and security.

How we ensure continuity

Data backup is one of the cornerstones of our continuity plan. Trained personnel oversee and monitor the execution of backups to guarantee the security, confidentiality, and accuracy of the stored data.

The second key element of our continuity plan involves our IT and management procedures and routines for handling serious incidents. We maintain a continuous effort to keep these processes up-to-date, and the plan is periodically tested, guided by regular risk assessments.

Our third foundation lies in our substantial digitization efforts; all our services and tools are accessible digitally. This means that, in the event of office closures due to extreme circumstances, most employees can continue their work from alternative safe location.

How we control access to our system and processes

We maintain stringent measures to prevent unauthorized access to our systems and processes. This includes adhering to the principle of least privilege and implementing role-based permissions for system access. For highly confidential data, we require multi-factor authentication.

To secure physical access to our core systems, we partner with top-tier data center and cloud infrastructure providers. These providers employ continuous 24/7 surveillance and biometric access control within their data centers. Additionally, they hold certifications such as ISO27001, ISO27017, ISO27018, SOC2 Type II, PCI DSS, and CSA STAR.

We meticulously control access to Atlas Well's data, ensuring that authorized individuals only access data relevant to their permissions. Our security measures include leading password validation and recovery techniques, password hashing. We proactively scan for vulnerabilities and malicious activities.

We make certain that personal data remains secure during electronic transmission and storage. Our approach to IT security incorporates regular risk assessments and annual penetration tests to identify and address vulnerabilities.

We guarantee the ability to promptly review and identify any access, modifications, or deletions of personal data within our system through continuous event monitoring and logging. Crucial logs are securely stored for a minimum of 2 months.

To safeguard personal data from accidental loss or destruction, we employ several protective measures. These include daily full backup copies of production data, a robust patch management process, and logical separation of development, testing, staging, and production environments. These practices work in tandem to ensure the resilience and integrity of personal data throughout its lifecycle.

How we manage risk

We implement effective risk management and security controls, including regular reviews and assessments of potential risks. We continually monitor adherence to our policies and procedures and maintain an up-to-date risk map that is approved by senior management. These measures are in place to ensure the ongoing security and integrity of our operations.

How we secure operations

We take comprehensive measures to protect our IT infrastructure against malicious code. This includes employing various systems and methods designed to safeguard operations. Our proactive approach

includes monitoring to ensure that antivirus scanners and spam filters remain active and up to date. We also prioritize the installation of the latest security updates and patches.

To bolster our security, we require all employees to undergo security training at least once a year. This collective effort helps us maintain a robust defense against potential security threats and ensures the safety of our IT environment.

How we uphold security with our staff

Our most valuable asset is our workforce, and we are committed to recruiting top talent from around the world. To ensure that our team members adhere to legal requirements, regulations, and the terms outlined in supplier and customer agreements, we have a clear expectation that Atlassins conduct themselves in a manner consistent with our guidelines regarding business ethics, confidentiality and professional standards. In addition to our standards, we mandate that our personnel enter into confidentiality agreements. They are also required to acknowledge receipt of, and compliance with, Atlas Well's confidentiality and privacy policies. This reinforces our commitment to ensuring the utmost protection of sensitive information and data privacy.

Roles and responsibilities of the staff

The Data Protection Officer (DPO)

The DPO has the responsibility to ensure that our organisation and its staff processes personal data in compliance with GDPR and other applicable legal security requirements. The role of the DPO is to advice on GDPR compliance and to ensure that data subjects are informed of data processing and their rights, as well as to handle complaints and data breaches within the organisation.

Other personell

Other than the DPO, personal data can be processed by various staff within functions such as sales, marketing, software development, customer care and similar. Each staff member is obliged to and responsible for being informed of and compliant with Atlas Well's confidentiality and security policies.