atlas well™

Data Processing Agreement

This document is based in its entirety on the DPA (SE: **PUB-Avtal**) template provided by SKR (The Swedish Association of Local Authorities and Regions). Alterations made by Atlas Well AB is limited to contact details and descriptions in Appendix 1 and 2, as well as the addition of Appendix 3. All alterations are marked with grey.

Updated: 2023-11-01

Table of contents

1. PARTIES, POSITIONS OF THE PARTIES, CONTACT DETAILS AND CONTACT 2
2. DEFINITIONS 2
3. BACKGROUND AND AIM 4
4. PROCESSING OF PERSONAL DATA AND SPECIFICATION 4
5. OBLIGATIONS OF THE CONTROLLER 4
6. OBLIGATIONS OF THE PROCESSOR 5
7. SECURITY MEASURES 5
8. SECRECY/DUTY OF CONFIDENTIALITY 6
9. INSPECTION, SUPERVISION AND AUDITING 6
10. HANDLING OF CORRECTIONS AND DELETIONS ETC 7
11. PERSONAL DATA BREACHES 7
12. SUBPROCESSOR 8
13. LOCALISATION AND TRANSFER OF PERSONAL DATA TO A THIRD COUNTRY 9
14. LIABILITY FOR DAMAGE IN CONNECTION WITH THE PROCESSING 9
15. CONCLUSION, TERM AND TERMINATION OF THIS AGREEMENT 9
16. AMENDMENTS AND TERMINATION WITH IMMEDIATE EFFECT, ETC. 9
17. MEASURES IN THE EVENT OF TERMINATION OF THE AGREEMENT 10
18. NOTIFICATIONS WITHIN THE PURVIEW OF THIS AGREEMENT AND THE INSTRUCTIONS 10
19. CONTACT PERSONS 11
20. RESPONSIBILITY FOR INFORMATION REGARDING PARTIES, CONTACT PERSONS AND CONTACT INFORMATION 11
21. CHOICE OF LAW AND DISPUTES 11
22. THE PARTIES' SIGNATURES ON THE AGREEMENT 11

DATA PROCESSING AGREEMENT

Agreement pursuant to Article 28.3 of the General Data Protection Regulation EU 2016/679[1]

1. PARTIES, POSITIONS OF THE PARTIES, CONTACT DETAILS AND CONTACT

Data Controller	**Data Processor**
[Full name of the organisation]	Atlas Well AB
Corporate ID no.	**Corporate ID no.**
[Corporate ID no. of the organisation]	559442-3567
Mailing address	**Mailing address**
[Mailing address of the organisation]	info@atlaswell.co
Contact person for administration of this Data Processing Agreement	**Contact person for administration of this Data Processing Agreement**
Name: [Contact person's Name(s) and Surname(s)] Email: [Contact person's email address] Phone: [Contact person's telephone number]	Name: Philip Cabreus Email: philip@atlaswell.co Phone:+46706107175
Contact person for cooperation between the Parties about data protection	**Contact person for cooperation between the Parties about data protection**
Name: [Contact person's Name(s) and Surname(s)] Email: [Contact person's email address] Phone: [Contact person's telephone number]	Name: Philip Cabreus Email: philip@atlaswell.co Phone: +46706107175

2. DEFINITIONS

2.1. In addition to the concepts defined in the text for the Data Processing Agreement, these definitions shall, regardless of whether they are used in the plural or singular, in definite or indefinite form, have the following meaning when entered with capital letters as the initial letter.

[1] The General Data Protection Regulation EU 2016/679 stipulates that there must be a written agreement on the processing of personal data by the Processor on behalf of the Controller.

Processing

Any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction..

Data protection legislation

Refers to all privacy and personal data legislation, along with any other legislation (including regulations and directives) applicable to the Processing carried out in accordance with this Agreement, including national legislation and EU legislation.

Controller

A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

Instruction

The written instructions that more specifically define the object, duration, type and purpose of Personal Data, as well as the categories of Data Subjects and special requirements that apply to the Processing.

Log

A Log is the result of Logging

Logging

Logging is a continuous collection of information about the Processing of Personal Data that is performed according to this Agreement and which can be associated with an individual natural person.

Processor

A natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

Personal Data

Any information relating to an identified or identifiable natural person, where an identifiable natural person is a person who directly or indirectly can be identified in particular by reference to an identifier such as name, social security number, location data or online identifiers or one or more factors which are specific to the natural person's physical, physiological, genetic, psychological, economic, cultural or social identity.

Personal Data Breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

Data Subject

Natural person whose Personal Data are Processed.

Third Country

A state that is not a member of the European Union (EU) or the European Economic Area (EEA).

Subprocessor

A natural or legal person, public authority, agency or other body which, in the capacity of subcontractor to the Processor, Processes Personal Data on behalf of the Controller.

3. BACKGROUND AND AIM

3.1. Through this Agreement, the Instructions and a list of possible Subprocessors (hereafter jointly referred to as "the Agreement"), the Controller regulates Processor'sProcessing of Personal Data on behalf of the Controller. The aim of the Agreement is to safeguard the freedoms and rights of the Data Subject during Processing, in accordance with what is stipulated in Article 28(3) of the General Data Protection Regulation (EU) 2016/679 ("GDPR").

3.2. When this Agreement forms one of several contractual documents within the framework of another agreement, the second agreement is referred to as the "Main Agreement" in this Agreement.

3.3. If anything stipulated in item 1, paragraph 3.2, item 165 or 16, paragraph 18.6, items 19–20 or 23 in this Agreement is otherwise regulated in the Main Agreement, the regulation of the Main Agreement shall have precedence.

3.4. References in this Agreement to national or EU legislation refer to applicable regulations at any given time.

4. PROCESSING OF PERSONAL DATA AND SPECIFICATION

4.1. The Controller hereby appoints the Processor to carry out the Processing on behalf of the Controller in accordance with this Agreement.

4.2. The Controller shall give written instructions to the Processor on how the Processing should be carried out.

4.3. The Processor may only carry out the Processing pertaining to this Agreement and the instructions in force at any given time.

5. OBLIGATIONS OF THE CONTROLLER

5.1. The Controller undertakes to ensure that there is a legal basis for the Processing at all times and for compiling correct Instructions with regard to the nature of the Processing so that the Processor and any Subprocessor can fulfil their tasks according to this Agreement and Main Agreement, where applicable.

5.2. The Controller shall, without unnecessary delay, inform the Processor of changes in the Processing which affect the Processor's obligations pursuant to Data Protection Legislation.

5.3. The Controller is responsible for informing Data Subjects about the Processing and protecting the rights of Data Subjects according to Data Protection Legislation as well as taking any other action incumbent on the Controller according to Data Protection Legislation.

6. OBLIGATIONS OF THE PROCESSOR

6.1. The Processor undertakes to only perform the Processing in accordance with this Agreement and for the specific purposes stipulated in the Instructions, as well as to comply with Data Protection Legislation. The Processor also undertakes to continuously remain informed about applicable law in this area.

6.2. The Processor shall take measures to protect the Personal Data against all types of Processing which are incompatible with this Agreement, Instructions and Data Protection Legislation.

6.3. The Processor undertakes to ensure that all natural persons working under its management follow this Agreement and Instructions and that such natural persons are informed of relevant legislation.

6.4. The Processor shall, at the request of the Controller, assist in ensuring that the obligations pertaining to Articles 32-36 in the GDPR are fulfilled and respond to requests for the exercise of a Data Subject's rights pertaining to the GDPR, Chapter III, taking into account the type of Processing and the information which the Processor has access to.

6.5. In the event that the Processor finds the Instructions to be unclear, in violation of the Data Protection Legislation or non-existent, and the Processor is of the opinion that new or supplementary Instructions are necessary in order to fulfil its undertakings, the Processor shall inform the Controller of this without delay, temporarily suspend the Processing and await new Instructions, if the Parties have not agreed otherwise.

6.6. If the Controller provides the Processor with new or revised Instructions, the Processor shall without unnecessary delay from receipt, communicate to the Controller whether the implementation of the new Instructions causes changed costs for the Processor.

7. SECURITY MEASURES

7.1. The Processor shall take all appropriate technical and organisational security measures required pertaining to Data Protection Legislation to prevent Personal Data Breaches, by ensuring that the procedure of Processing meets the requirements of the GDPR and that the rights of the Data Subjects are protected.

7.2. The Processor shall continuously ensure that the technical and organisational security in connection with Processing is executed with an appropriate level of confidentiality, integrity, accessibility and resilience.

7.3. Any added or revised requirements for protective measures from the Data Controller, after the Parties have signed this Agreement, will be considered as new Instructions pertaining to this Agreement.

7.4. The Processor shall, through its control systems for authority, only grant access to the Personal Data for such natural persons working under the Processor's management and who need access to be able to perform their duties.

7.5. The Processor undertakes to continuously log access to the Personal Data in accordance with this Agreement to the extent required according to the Instructions. Logs may be erased only five (5) years after the logging event, unless otherwise stated in the Instructions. Logs will be subject to the required protection measures pertaining to Data Protection Legislation.

7.6. The Processor shall systematically test, investigate and evaluate the effectiveness of the technical and organisational measures which will ensure the security of the Processing.

8. SECRECY/DUTY OF CONFIDENTIALITY

8.1. The Processor and all natural persons working under its management shall observe both confidentiality and professional secrecy during the Processing. The Personal Data may not be used or disseminated for other purposes, either directly or indirectly, unless otherwise agreed.

8.2. The Processor shall ensure that all natural persons working under its management, participating in the Processing, are bound by a confidentiality agreement pertaining to the Processing. However, this is not a requirement if they are already covered by a legally sanctioned duty of confidentiality. The Processor also undertakes to ensure that there is a nondisclosure agreement with its Subprocessor and confidentiality agreement between the Subprocessor and all natural persons working under its management, participating in the Processing.

8.3. The Processor shall promptly inform the Controller of any contacts with supervisory authorities pertaining to the Processing. The Processor does not have the right to represent the Controller or act on behalf of the Controller towards supervisory authorities in matters relating to the Processing.

8.4. If the Data Subject, supervisory authority or third Party requests information from the Processor pertaining to the Processing, the Processor shall inform the Controller about the matter. Information about the Processing may not be submitted to the Data Subject, supervisory authority or third parties without written consent from the Controller, unless mandatory law so stipulates that such information must be provided. The Processor shall assist with the communication of the information covered by a consent or legal requirement.

9. INSPECTION, SUPERVISION AND AUDITING

9.1. The Processor shall, without unnecessary delay, as part of its guarantees, pursuant to Article 28.1 of the GDPR, be able to report, at the request of the Controller, which technical and organisational security measures are being used for the processing to meet the requirements according to the DPA and Article 28.3.h of the GDPR.

9.2. The Processor shall review the security of the Processing at least once a year by performing a checks to ensure that the Processing complies with this Agreement. Upon request, the results of such checks shall be shared with the Controller.

9.3. The Controller or a third party it appoints (who cannot be a competitor of the Processor) is entitled to check that the Processor meets the requirements of this Agreement, Instructions and Data Protection Legislation. During such a check, the Controller shall assist the Controller, or the person carrying out the review on behalf of the Controller, with documentation, access to premises, IT systems and other assets needed to be able to check the compliance of the Controller with this Agreement, Instructions and Data Protection Legislation. The Controller shall ensure that staff who carry out the check are subject to confidentiality or non-disclosure obligations pertaining to law or agreement.

9.4. As an alternative to the stipulations of items 9.2–9.3, the Processor is entitled to offer other means of checking the Processing, such as checks carried out by

independent third parties. In such a case, the Controller shall have the right, but not the obligation, to apply such alternative means. In the event of such a check, the Processor shall provide the Controller or third party with the assistance needed for performing the check.

9.5. The Processor shall provide the supervisory authority, or other authority which has the legal right to do so, the means to carry out supervision according to the authority's request pertaining to the legislation in force at any time, even if such supervision would otherwise be in conflict with the provisions of this Agreement.

9.6. The Processor shall assure the Controller rights towards any Subprocessor corresponding to all of the rights of the Controller towards the Processor according to section 9 of this Agreement.

10. HANDLING OF CORRECTIONS AND DELETIONS ETC

10.1. In the case of the Controller requesting correction or deletion due to incorrect processing by the Processor, the Controller shall take appropriate action without unnecessary delay, within thirty (30) days at the latest, from the time the Processor has received the required information from the Controller. When the Controller requests deletion, the Processor may only carry out Processing of the Personal Data in question as part of the process for correction or deletion.

10.2. If technical and organisational measures (e.g., upgrades or troubleshooting) are taken by the Processor in the Processing, which can have an effect on the Processing, the Processor shall inform the Controller in writing pursuant to what is stipulated about notifications in item 19 of this Agreement. The information shall be submitted in good time prior to the measures being taken.

11. PERSONAL DATA BREACHES

11.1. The Processor shall have the capability to restore accessibility and access to Personal Data within a reasonable time in the event of a physical or technical incident pertaining to Article 32.1.c of the GDPR.

11.2. If technical and organisational measures (e.g. upgrades or troubleshooting) are taken by the Processor with regard to the Processing, and these can be expected to affect the Processing, the Processor shall inform the Controller in writing in accordance with the provisions on notifications set out in Section 18 of the Agreement. This information shall be communicated well in advance of the measures being taken.

11.3. In the event of a Personal Data Breach, which the Processor has been made aware of, the Processor shall notify the Controller of the Breach in writing without unnecessary delay. The Processor shall, taking into account the type of Processing and the information available to the Processor, provide the Controller with a written description of the Personal Data Breach.

11.4. The description shall give an account of:

a. The nature of the Personal Data Breach and, if possible, the categories and number of Data Subjects affected and the categories and number of Personal Data records affected,

b. the likely impact of the Personal Data Breach, and

c. measures taken or proposed and measures to mitigate the potential negative effects of the Personal Data Breach.

11.5. If it is not possible for the Processor to provide the full description at the same time, according to item 11.3 of this Agreement, the description may be provided in instalments without unnecessary further delay.

12. SUBPROCESSOR

12.1. The Processor is entitled to hire the Subprocessor(s) listed in the Subprocessor appendix. 2.

12.2. The Processor undertakes to enter a written agreement with the Subprocessor to regulate the Processing that the Subprocessor carries out on behalf of the Controller and to only hire Subprocessors who provide adequate guarantees. The Subprocessor shall carry out appropriate technical and organisational measures to ensure that the Processing fulfils the requirements of GDPR. When it comes to data protection, such an agreement shall entail the same obligations for the Subprocessor as are set out for the Processor in this Agreement.

12.3. The Processor shall ensure in its agreement with the Subprocessor that the Controller is entitled to terminate the Subprocessor and instruct the Subprocessor to, for instance, erase or return the Personal Data if the Processor has ceased to exist in the actual or legal sense, or has entered into insolvency.

12.4. The Processor shall be fully responsible for the Subprocessor's Processing on behalf of the Controller. The Processor shall promptly inform the Controller if the Subprocessor fails to fulfil its undertakings under the Agreement.

12.5. The Processor is entitled to hire new subprocessors and to replace existing subprocessors unless otherwise stated in the Instructions.

12.6. When the Processor intends to hire a new subprocessor or replace an existing one, the Processor shall verify the Subprocessor's capacity and ability to meet their obligations in accordance with the Data Protection Legislation. The Processor shall notify the Controller in writing of

a. the Subprocessor's name, corporate identity number and head office (address and country),

b. which type of data and categories of Data Subjects are being processed, and

c. where the Personal Data will be processed.

12.7. The Controller is entitled within thirty (30) days of the notice pursuant to item 12.6 to object to the Processor's hiring of a new subprocessor and, due to such an objection, to cancel this Agreement to be terminated in accordance with the provisions of item 164 of this Agreement.

12.8. The data processor shall at all times keep a correct and updated list of the Subprocessors hired for tte Processing of Personal Data on behalf of the Controller and make the list accessible to the Controller. The list shall specifically state in which country the Subprocessor Processes Personal Data and types of Processing the Subprocessor carries out.

12.9. When the Processor ends its collaboration with a Subprocessor, the Processor shall notify the Controller in writing. When an agreement terminates, the Processor shall ensure that the Subprocessor erases or returns the Personal Data.

12.10. At the Controller's request, the Processor shall send a copy of the agreement regulating the Subprocessor's Processing of Personal Data in accordance with item 12.1.

13. LOCALISATION AND TRANSFER OF PERSONAL DATA TO A THIRD COUNTRY

13.1 The Processor shall ensure that the Personal Data shall be handled and stored within the EU/EEA by a natural or legal person who is established in the EU/EEA, unless the parties to this Agreement agree otherwise.

13.2 The Processor is only entitled to transfer Personal Data to a Third Country for Processing (e.g. for service, support, maintenance, development, operations or other similar handling) if the Controller has given advance written approval of such transfer and has issued Instructions to this end.

13.3 Transfer to a Third Country for Processing in accordance with item 13.2 of the Agreement may be carried out only if it complies with the Data Protection Legislation and fulfils the requirements for the Processing set out in this Agreement and the Instructions

14. LIABILITY FOR DAMAGE IN CONNECTION WITH THE PROCESSING

14.1. In the event of a compensation for damage in connection with Processing, through a judgment given or settlement, to be paid to a Data Subject due to an infringement of a provision in the Agreement, Instructions and/or applicable provision in Data Protection Legislation, Article 82 of the GDPR shall apply.

14.2. Fines pursuant to Article 83 of the GDPR, or Chapter 6, Section 2 of the Data Protection Act (2018:218) with supplementary provisions to the EU's data protection regulation shall be borne by the Party to the Agreement named as recipient of such sanctions.

14.3. If either party becomes aware of circumstances that could be detrimental to the other party, the first party shall immediately inform the other party of this and work actively with the other party to prevent and minimise the damage or loss.

14.4. Regardless of the content of the Main Agreement, items 15.1 and 15.2 of this Agreement take precedence to other rules on the distribution between the Parties of claims among themselves as far as the processing is concerned.

15. CONCLUSION, TERM AND TERMINATION OF THIS AGREEMENT

15.1. This Agreement shall enter into force from the time the Agreement is signed by both Parties and until further notice. Either party has the right to terminate the Agreement with thirty (30) days' notice.

16. AMENDMENTS AND TERMINATION WITH IMMEDIATE EFFECT, ETC.

16.1. Each party to the Agreement shall be entitled to invoke a renegotiation of the Agreement if there is a major change of the ownership of the other party or if applicable legislation or interpretation thereof changes in a way that significantly affects the Processing. The invoking of a renegotiation pursuant to the first sentence does not mean that any part of the Agreement will cease to be in effect, but only means that a renegotiation of the Agreement will commence.

16.2. Additions and amendments to the Agreement must be made in writing and signed by both parties.

16.3. If either party becomes aware that the other party is acting in violation of the Agreement and/or Instructions, the first party shall inform the other party without delay of the actions in question. The party is then entitled to suspend the performance of its obligations pursuant to the Agreement until such time as the other party has declared that the actions have ceased, and the explanation has been accepted by the party that made the complaint.

16.4. If the Controller objects to the Processor using a new Subprocessor, pursuant to item 12.6 of this Agreement, the Controller is entitled to terminate the Agreement with immediate effect.

17. MEASURES IN THE EVENT OF TERMINATION OF THE AGREEMENT

17.1. Upon termination of the Agreement, the Processor shall, without unnecessary delay, depending on what the Controller chooses, either delete and certify to the Controller that it has been carried out, or return

a. all Personal Data Processed on behalf of the Controller and

b. all associated information such as Logs, Instructions, system solutions, descriptions and other documents which the Processor has obtained through information exchange in pursuance of the Agreement.

17.2. In connection with the return of data, the Processor shall also delete existing copies of Personal Data and associated information.

17.3. The obligation to delete or return Personal Data or/and associated information does not apply if storage of the Personal Data or information is required under EU law or relevant national law where Processing may be carried out pursuant to the Agreement.

17.4. If Personal Data or associated information is returned, it must be in a commonly used and standardised format, unless the Parties have agreed to another format.

17.5. Until the data is deleted or returned, the Processor shall ensure compliance with the Agreement.

17.6. Return or deletion pertaining to the Agreement shall be carried out no later than thirty (30) calendar days counting from the time of termination of the Agreement, unless otherwise stated in the Instructions. Processing of Personal Data which the Processor subsequently carried out shall be regarded as unauthorised Processing.

17.7. Confidentiality/professional secrecy in item 8 shall continue to apply even if the Agreement otherwise ceases to apply.

18. NOTIFICATIONS WITHIN THE PURVIEW OF THIS AGREEMENT AND THE INSTRUCTIONS

18.1. Notifications about the Agreement and its administration, including termination, shall be submitted via email or in any other manner agreed by the Parties to each Party's contact person for the Agreement.

18.2. Notifications about the collaboration of the Parties regarding the data protection shall be submitted via email or in any other manner agreed by the Parties to each Party's contact for the Parties' cooperation on data protection.

18.3. A notification shall be deemed to have reached the recipient no later than one (1) business day after the notification has been sent.

19. CONTACT PERSONS

19.1. Each Party shall appoint their contact person for the Agreement.

19.2. Each Party shall appoint their contact person for the Parties' cooperation on data protection.

20. RESPONSIBILITY FOR INFORMATION REGARDING PARTIES, CONTACT PERSONS AND CONTACT INFORMATION

20.1. Each Party is responsible for the information entered in item 1 of the Agreement always being current and correct.

20.2. Change of information in item 1 shall be communicated to the other Party pursuant to item 19.1 of the Agreement.

21. CHOICE OF LAW AND DISPUTES

21.1. When interpreting and applying the Agreement, Swedish law shall apply with the exception of the choice of law rules. Disputes regarding the Agreement shall be settled by a competent Swedish court.

22. THE PARTIES' SIGNATURES ON THE AGREEMENT

22.1. The Agreement can be produced either in digital format for electronic signature or in paper format for manual signature. In the latter case, the Agreement is drawn up in two identical copies, whereof each Party receives one.

22.2. If the Agreement is signed electronically, the page with signature shall be ignored.

[Rest of the page has intentionally been left blank. Signature page follows.]

Controller

[Full name of the organisation]

Place and date: [Enter place and date of signature]

_____

Name in print

_____

Signature

Processor

Atlas Well AB

Place and date:

Philip Cabreus

Name in print

_____

Signature

Appendix 1 - The Controller's instruction for the processing of Personal Data

In addition to what is already mentioned in the Data Processing Agreement, the Processor shall also follow the following Instructions:

1. The purpose, object and nature
1 a. The object of the Processing of Personal Data by the Processor for the Controller is to: The purpose is to enable the data controller's ability to obtain and share a person's BAC-value, from anywhere at any time. 1 b. The objective of the Processing of Personal Data by the Processor for the Controller is to: The objective is to benefit both the Data Controller and end user by providing means to share specific data (especially BAC-values) between the parties. This is in turn ment to increase safety and strengthen relations. 1 c. The Processing of Personal Data by the Processor on behalf of the Controller refers mainly to the following measure of Processing (type or nature of the Processing): The data Processor collects data from a mobile application and a web based portal - The data is then stored on secure EU-based servers. Upon the request of the Data Controller, the data can be viewed and managed through the Atlas Well system.
2. The Processing includes the following types of Personal Data
The Processor has the right to Process the following types of Personal Data on behalf of the Controller: **Normal Data:** Name, e-mail, phone number. **Special data**: BAC value, photo, self-registered mood.

3. Processing covers certain categories of Data Subject
The Processor has the right to process Personal Data regarding the following categories of Data Subjects: Staff, colleagues, customers, clients, patients, relatives.
4. Specify special requirements when it comes to Processing of Personal Data carried out by the Processor
The Processor must observe the following Processing requirements when Processing Personal Data on behalf of the Controller: Please view Appendix 3 - Security Whitepaper
5. Specify the special technical and organisational security measures which apply to the Processing of Personal Data by the Processor
The Processor shall take the following security measures when Processing Personal Data: Please view Appendix 3 - Security Whitepaper
6. Specify special requirements for logging with regard to the Processing of Personal Data and who should have access to them

The Processor shall observe the following requirements regarding the user activity and Processing of logs:

We log all access to personal data. The access log includes the date and time of access, the UserID and the type of access. Security logging are enabled on all network equipment, servers and on all applications including databases and on IT system administrators. A centralized system for collecting and reviewing security logs is in place. Logs of access to personal data and the use of personal data is monitored and available for review in order to detect unauthorized access to personal data. It is documented when and how often log files are reviewed and who has performed the control. Failed login attempts is logged and kept for 6 months in order to detect unauthorized access to personal data.

7. Location and transfer of Personal Data to Third Countries

The Processor shall observe the following requirements regarding the location of Personal Data:

The Processor is only entitled to Process the Personal Data at the following locations:

- Locations within the EU/EES area.

If the Controller has not given instructions on the transfer of Personal Data to a Third Country, the Processor shall not have the right to make such a transfer.

The Processor shall observe the following requirements for transferring Personal Data to a Third Country:

- N/A. If this becomes relevant, the Data processor will inform the Data Controller with 60 days notice.

8. Duration of Processing

The processing starts when the data controller registers a new client (end-user).
The processing ends when the data controller chooses (via the system) to end the subscription for the client (end-user). End-user photos are automatically deleted after 14 days.

9. Other Instructions regarding the Processing of Personal Data carried out by the Processor

-

Appendix 2 – List of approved Subprocessors

The Controller approves the hiring of the Subprocessors below by the Processor for the Processing of Personal Data.

Company/ organisation	Address and contact details	Location of Personal Data (address, country)	Types of Personal Data Processed by the Subprocessor	Purpose of processing by the Subprocessor	Processing time	Additional information about the Subprocessor's Processing of Personal Data
OVHcloud	2 Rue Kellerman, 59 100, Roubaix, France	Frankfurt, Germany	**Normal Data:** Name, e-mail, phone number. **Special data:** BAC value, photo, self-registered mood.	CSP, SMS provider, domain host. French entity. Servers located in France or Germany.	Same as the Data Processor.	https://us.ovhcloud.com/enterprise/certification-conformity/
Sarbacane Software (Tipimail)	Parc d'activité des 4 vents, 3 Avenue Antoine Pinay, 59 510 Hem, France	Hem, France	**Normal data:** E-mail. **Other:** OTP codes.	E-mail service provider. French entity.	Same as the Data Processor.	https://www.sarbacane.com/en/contracts-and-conditions
Ralabs	Harju maakond, Tallinn, Kesklinna linnaosa, Vesivärava tn 50-201, 101 52 Estonia	EU/EES-area.	**Normal Data:** Name, e-mail, phone number. **Special data:** BAC value, photo, self-registered mood.	Software development resource. Estonian entity.	Same as the Data Processor.	Provided upon request.

Appendix 3 - Security Whitepaper

Updated 2023-11-01

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.