atriis

ATRIIS Information Security Factsheet

Document Name:	ATRIIS Information Security Factsheet
Version:	1.0
Date of Version:	01.04.2021
Created by:	Tzach Mordechai
Approved by:	Omri Amsalem
Confidentiality Level	Confidential

Change History:

Date	Version	Updated by	Approved by	Description of Change
12.1.2022	8.0	Tzach Mordechai, CISO	Omri Amsalem	Review and reapproved the document
29.3.2023	8.1	Yair Levy, CISO		Review and reapproved the document, update broken links, update certificates
29.3.2023	8.2	Yair Levy, CISO		
01.05.2024	8.3	Yair Levy, CISO		Security controls update, certifications update

atriis

Contents

1. Introduction

Information security is a fundamental part of the Atriis' business. Atriis understands that the confidentiality, integrity and availability of its customer's data are paramount to their business success which is why Atriis' Global Travel Platform (ATRIIS), through a combination of audited processes and controls, delivers a level of security that is second to none..

2. Effective Date of this Factsheet

April 1, 2021

3. Changes to Policy

Atriis may change this Policy by posting an updated version of the Policy at its support site https://atriis.zendesk.com and such updates will be effective upon posting.

4. Purpose

This is a technical security summary description of ATRIIS product and corporate security.

5. Corporate Security

5.1. Security program

Our security program is designed with consideration for both local and international laws, standards, and regulations applicable to Atriis. It outlines the measures and controls implemented to safeguard the Atriis service and its customers' data. Anchored in ISO 27001 standards, the program encompasses the entire Atriis organization, including its employees, contractors, subcontractors, partners, and any party involved in creating, maintaining, storing, accessing, processing, or transmitting Atriis's or its users' information in relation to the service provided by Atriis.

5.2. Security and privacy regulations and standards

Atriis comply with the following certifications, reports and compliance programs:

ISO 27001, PCI-DSS, GDPR

Appendix A – Security Certifications

6. High-Level Architecture

Atriis GTP is a distributed, multi-tenant, multi-devices and multi-technologies based system. Atriis uses Microsoft Azure (located at West Europe) for its ATRIIS GTP application and Databases.

Atriis uses Microsoft Azure 'Platform as a Service' (PaaS), applying VM and APP (Standard) Scale Set architecture.

Azure PaaS provides following services:

(a) Storage

(b) Queues

(c) Service Bus

(d) BI & Reporting Services

(e) Local & Distributed Cache

(f) Load Balancing

(g) High Availability, Fault and Update Domain

(h) Staging environment

(i) Service Management

(j) Elasticity

(k) Content Delivery Network

(l) Securing Multi-Tenant Application and VPN services

(m) Identity and Authorization include Active Directory Services

(n) Automatic scaling, traffic management, data geo-replication

7. ATRIIS High-Level Network Diagram

Atriis uses the following network components:

(a) Full SSL connection. Secured connection between the user and CloudFlare, secured and authenticated connection between CloudFlare and ATRIIS .

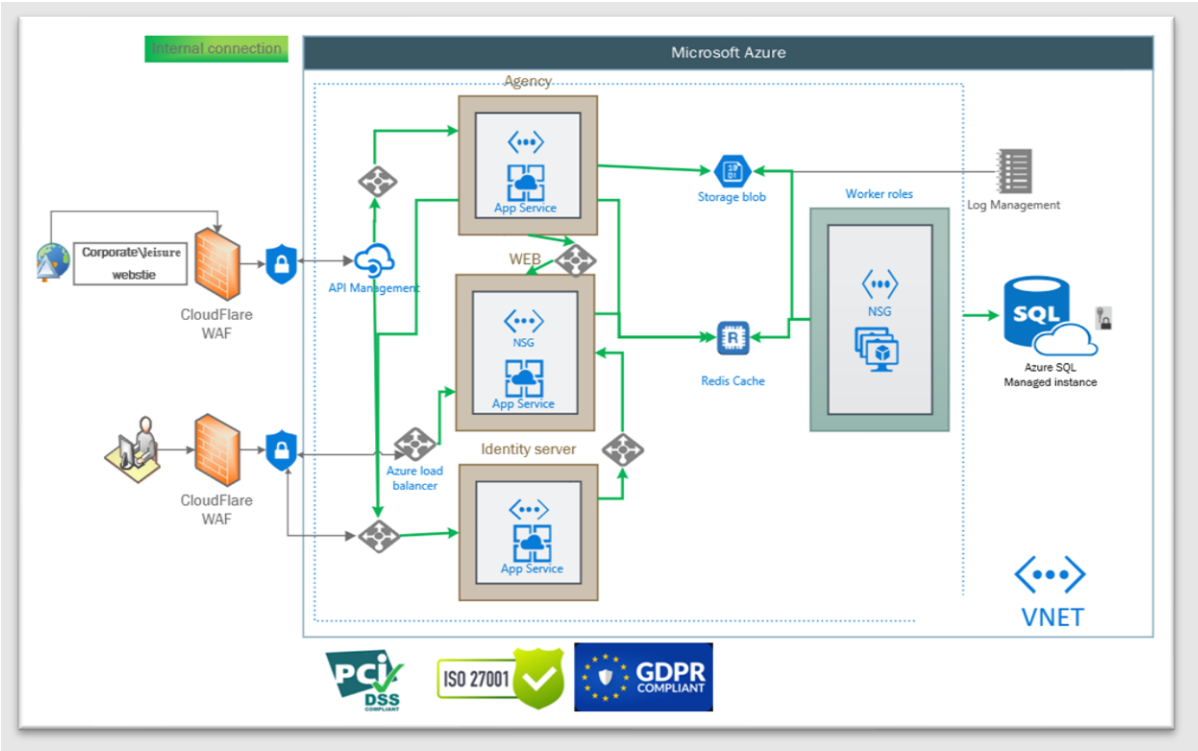
(b) CloudFlare Web Application Firewall (WAF).

(c) Azure Infrastructure protection and customer protection (Network isolations, DDoS/DOS/IDS and Host firewalls).

(d) Azure Firewall.

(f) User data is encrypted with AES128.

(g) Mobile and private websites (which uses ATRIIS backend services) access is controlled and monitored by Azure API Management.



8. ATRIIS Security Envelope through Microsoft Azure

8.1. Infrastructure Protection

Windows Azure infrastructure includes hardware, software, administrative and operations staff, and physical data centers. Windows Azure addresses security risks across its infrastructure with continuous intrusion detection and prevention systems, denial of service attack prevention, regular penetration testing, and forensic tools that help identify and mitigate threats. With Windows Azure, customers can reduce the need to invest in these capabilities on their own and benefit from economies of scale in Microsoft datacenter infrastructure.
Employes devices' protection: Microsoft Intune is a cloud-based service that focuses on organizational device management and mobile application management.

IT policies control how our organization's devices are used, including mobile phones, tablets, and laptops. We can also configure specific policies to control applications.
Make sure operating system and Antivirus are up to date and all employees devices are encrypted, secure with real time protection and no unauthorized software is installed.

8.2. 24-hour monitored physical security

Microsoft datacenters are physically constructed, managed, and monitored 24 hours a day to shelter data and services from unauthorized access as well as environmental threats.

8.3. Monitoring and logging

Centralized monitoring, correlation, and analysis systems manage the large amount of information generated by devices within the Windows Azure environment, providing continuous visibility and timely alerts to the teams that manage the service. Additional monitoring, logging, and reporting capabilities provide visibility to customers.

8.4. Microsoft Azure Network Security

Microsoft Azure networking provides the infrastructure necessary to securely connect Virtual Machines (VMs) to one another and be the bridge between the cloud and remote datacentres, content suppliers and ATRIIS 's users. Azure's network services maximize flexibility, availability, resiliency, security, and integrity by design. Azure Virtual Networks use a combination of logical isolation, firewalls, access controls, authentication, and encryption to protect customer data in-transit. Microsoft's Azure data center operations implement comprehensive information security policies and processes using standardized industry control frameworks such as ISO 27001, SOC 1, and SOC 2. Third-party auditors regularly certify Microsoft's adherence to these standards for both the physical and virtual aspects of Azure infrastructure.

8.5. Vulnerability Management

ATRIIS uses Azure services to protect from potentially harmful vulnerability.

8.6. Physical and Environmental Security

https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security

9. Access Control Management

9.1. Identity (SSO) & Security

Authentication and Authorization in ATRIIS are based on OAuth2. More detailed information could be found in

https://azure.microsoft.com/en-us/services/security-center/ .

https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/auth-oauth2

9.2. Access Management

Atriis utilizes Azure Role-Based Access Control (RBAC) and Single Sign-On (SSO) to regulate access to all Global Travel Platform (GTP) components, infrastructure and applications.

The principles of least privilege and need-to-know are implemented across all systems and processes.

9.3. Password Policy

Passwords must adhere to the following guidelines:

- At least one lowercase letter;
- At least one uppercase letter;
- At least one number;
- One special character (e.g !@#$);
- Eight characters minimum;
- History: 3 months;
- Max age: 90 days;

9.4. Access Rights & Permissions Review

Atriis has established a structured and periodic review process to meticulously assess user access rights, aligning with our commitment to robust information security practices. Our approach includes:

Regular Users/Applications:

A comprehensive review of access rights for regular users and applications is conducted annually.

This systematic examination ensures that access permissions remain aligned with business needs and individual responsibilities, promoting the principle of least privilege.

Privileged Users/Sensitive Applications:

A heightened frequency characterizes the review process for privileged users and sensitive applications, occurring on a quarterly basis.

This more frequent assessment recognizes the elevated risk associated with privileged access and sensitive applications, allowing for swift identification and mitigation of potential security vulnerabilities.

10. Web Application Firewall (WAF) protection

In addition to security means provided by Microsoft Azure, ATRIIS is protected by CloudFlare web application firewall against SQL injection, cross-site scripting (XSS) and zero-day attacks, including OWASP-identified vulnerabilities and threats targeting the application layer and DDoS protection. In addition, CloudFlare accelerates and optimizes the delivery of ATRIIS data. More information could be found at

https://developers.cloudflare.com/waf/

11. Personal Information

Atriis strives to comply with applicable laws and regulations related to Personal Data protection in countries where it operates. Atriis' security policy sets forth the basic principles by which Atriis processes personal data of its customers and suppliers.

Atriis is compliance with GDPR and PCI-DSS (see Appendix A).

12. Data Security

12.1. Handling and store of sensitive data

Data, whether at rest or in transit, is secured through robust encryption methods, safeguarding its confidentiality and integrity against unauthorized access. Atriis enforce the data encryption controls:

- Employing Azure SQL Database Transparent Data Encryption (TDE) to secure data at rest. TDE encrypts the database files, encompassing both data and log files, through the use of a symmetric key.
- PII data filed is encrypted using AES 128-bit encryption.
- Credit card data is encrypted using RSA 2048-bit encryption.
- All data transfer in secured channels (HTTPS and TLS 1.2 or higher).
- PII fields are encrypted.
- Decryption key is stored on Azure Key vault.

12.2. Data Classification

Our classification labelling system is rigorously enforced through policy enforcement mechanisms and the utilization of Azure's advanced data classification feature, which offers robust capabilities for managing and categorizing data according to its sensitivity and importance.

Our classifications encompass three main categories:

Public: This category includes information that has been intentionally made available to the public and does not contain any restricted or classified information. It encompasses data that poses no risk to the company's objectives, business, reputation, or liability.

Restricted: Information falling under this classification is subject to legal restrictions and regulations. It comprises data that is legally protected and requires special handling to ensure compliance with relevant laws and regulations.

Classified: This category encompasses information that, if exposed, could potentially harm the company's objectives, business operations, reputation, or legal liability. It includes sensitive data that is not necessarily legally restricted but requires stringent protection measures to mitigate risks.

12.3. Data Retirement

Atriis diligently adheres to a comprehensive data handling process to ensure the utmost security and compliance. Our practiced approach encompasses the following key steps:

Removal from Production Database:

When data is no longer required in the production database, it is promptly removed to minimize exposure.

This proactive measure mitigates any potential risks associated with unnecessary data retention.

Encrypted Trip Data Storage:

Trip data, considered sensitive, is encrypted before being transferred to a separate database.

This dedicated storage facility ensures the confidentiality and integrity of trip-related information for a period of three years, aligning with our commitment to secure data retention practices.

PII Data Purge (Right to Be Forgotten - GDPR):

Personal Identifiable Information (PII) undergoes a rigorous purging process in strict accordance with the "Right to Be Forgotten" principle mandated by the General Data Protection Regulation (GDPR).

This commitment to data privacy empowers individuals with control over their personal information, reflecting our dedication to compliance with global data protection standards.

Encrypted Invoice Information Storage:

Relevant invoice information is subjected to encryption protocols before storage.

This encryption aligns with both legal and fiscal requirements, ensuring that sensitive financial data is safeguarded in compliance with regulatory standards.

13. Secure Development Live Cycle

Atriis system development methodology is deeply rooted in the principles of security by design and resilience, ensuring that required information security functionalities are embedded from the earliest stages of development. We adhere to a structured and industry-approved system development methodology that incorporates the following key strategies:

Security by Design: From the initial design phase, security is a primary consideration. We adopt a proactive approach to security, identifying and incorporating security functionalities such as authentication, authorization, encryption, and logging into the system architecture.

Risk Assessment and Mitigation: Early in the development process, we conduct thorough risk assessments to identify potential security vulnerabilities and threats. This allows us to build mitigation strategies directly into the system design, ensuring resilience against known and emerging threats.

Secure Development Practices: Our development teams adhere to secure coding practices informed by the latest industry standards, such as OWASP Secure Coding Practices. We utilize both static and dynamic analysis tools throughout the development process to identify and address security vulnerabilities, ensuring that the codebase is robust and secure.

Agile Project Management: Azure DevOps Boards are used for project management, supporting our Agile workflow with features for backlog management, sprint planning, and issue tracking. These tools enhance visibility and coordination among development, QA, and product teams.

Testing: Security testing is an integral part of our quality assurance process. We employ a variety of testing methodologies, including penetration testing, vulnerability scanning, and security audits, to validate the security and functionality of information security controls within our systems. This thorough testing regime ensures that systems are resilient and can withstand both current and future security challenges.

Training: We provide ongoing training for our development teams on secure coding practices and emerging security threats, ensuring that our personnel remain aware of the latest developments in cybersecurity.

atriis

Appendix A – Security Certifications

atriis

ISO270001 & PCI-DSS certifications

CERTIFIED ISMS SI ISO 27001 2013
THE STANDARDS INSTITUTION OF ISRAEL
IQNET
ANAB ANSI National Accreditation Board ACCREDITED ISO/IEC 17021-1 MANAGEMENT SYSTEMS CERTIFICATION BODY
MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT IAF

The standards Institution of Israel
42 Chaim Levanon St,
Tel-Aviv 6997701

CERTIFICATE

This is to certify that the Information Security Management System of

ATRIIS TECHNOLOGIES LTD.

14, Ha'lamish St., Caesarea, Israel

Has been assessed and complies with the requirements of :

ISO/IEC 27001:2013

This Certificate is Applicable to

The Information Security Management System is Applicable to IT Operations Department Related to: Development and marketing of travel management systems.

According to Statement of Applicability: 5.1.2020

Initial Approval:	15/06/2020		
Valid From:	22/11/2023		
End of previous certification cycle:	15/06/2023	Recertification audit:	18/07/2023
Valid Until:	31/10/2025	Certificate No.:	108218

SII-QCD assumes no liability to any party other than the client, and then only in accordance with the agreed upon Certification Agreement.
This certificate's validity is subject to the organization maintaining their system in accordance with SII-QCD requirements for system certification. The continued validity may be verified via scanning the code with a smartphone, or via website www.sii.org.il. This certificate remains the property of SII-QCD.

Dr. Gilad Golub
CEO

R.N 513790048

Avital Weinberg
Director, Quality & Certification Division

Page 1 of 1

The Standards Institution of Israel -Your Preferred Choice

atriis

IQNET

Building trust together.

CERTIFICATE

THE STANDARDS INSTITUTION OF ISRAEL

has issued an IQNET recognized certificate that the organization:

ATRIIS TECHNOLOGIES LTD.

14, Ha'lamish St., Caesarea, Israel

Has implemented and maintains a Information Security Management System
that is Applicable For The Following scope of IT Operations Department Related to

Development and marketing of travel management systems.

which fulfils the requirement of the following standard:

ISO/IEC 27001:2013

Issued on:	**22/11/2023**
First issued on:	**15/06/2020**
Expires on:	**31/10/2025**

Registration Number: IL - 108218

IQNET

Alex Stoichitoiu
President of IQNET

Avital Weinberg
Director, Quality & Certification Division

מתי

This attestation is directly linked to the IQNET Members original certificate and shall not be used as a stand-alone document

IQNET Members*:
AENOR *Spain* **AFNOR Certification** *France* **APCER** *Portugal* **CCC** *Cyprus* **CISQ** *Italy* **COC** *China* **COM** *China* **CQS** *Czech Republic* **Cro Cert** *Croatia* **DQS Holding GmbH** *Germany* ***EAGLE Certification Group*** *USA* **FCAV** *Brazil* **FONDONORMA** *Venezuela* **ICONTEC** *Colombia* **ICS** *Bosnia and Herzegovina* **Inspecta Sertifiointi Oy** *Finland* **INTECO** *Costa Rica* **IRAM** *Argentina* **JQA** *Japan* **KFQ** *Korea* **LSQA** *Uruguay* **MIRTEC** *Greece* **MSZT** *Hungary* **Nemko AS** *Norway* **NSAI** *Ireland* ***NYCE-SIGE*** *México* **PCBC** *Poland* **Quality Austria** *Austria* **SII** *Israel* **SIQ** *Slovenia* **SIRIM QAS International** *Malaysia* **SQS** *Switzerland* **SRAC** *Romania* **TEST St** Petersburg *Russia* **TSE** *Turkey* **YUQS** *Serbia*

* The list of IQNET Members is valid at the time of issue of this certificate. Updated information is available under www.iqnet-certification.com

www.sii.org.il

COMSEC GLOBAL

CERTIFICATE OF COMPLIANCE

PCI DSS CERTIFIED ★★★ COMSEC ★★★ PCI DSS CERTIFIED

AWARDED TO: atriis

THIS IS TO CERTIFY THAT: **Atriis Technologies Ltd.** has successfully completed an assessment by COMSEC Ltd. against the Payment Card Industry Data Security Standard v4 (PCI:DSS) as a Service Provider level 2

VALID: January 08, 2024 – January 07,2025

January 08, 2024	Omer Sonder	Omer Sonder
DATE	QUALIFIED SECURITY ASSESSOR	SIGNATURE

Conditions:

i. The certificate offers no guarantee or warranty to any third party that the company is invulnerable to security attacks or breaches. Accordingly, Comsec accepts no liability of any third party in the event of loss or damage of any description caused by any failure in or breach of customers' security.
ii. This certificate is issued in conjunction with a Compliance Report that is a material and inseparable part of this certification, and is only valid as long as the terms and conditions stipulated by the PCI:DSSand in the report are upheld.
iii. It is the validated entity's responsibility to maintain compliance with PCI security requirements throughout the certification period.

atriis

Appendix B – Privacy Policy

Atriis Privacy Policy

Subscriber's User and Business End-User Privacy Policy

This User/Business End-User Privacy Policy is offered by Atriis as a template for the Subscriber to consider using to create a suitable document regarding privacy. As such, defined terms highlighted in yellow and terms the Subscriber will need to change to be consistent with the Subscriber's defined terms in its relationship with its customers. Terms highlighted in green and sections to be considered by the Subscriber and assessed in terms of their applicability and relevance to the Subscriber's circumstances, and modified accordingly.

[ADD SUBSCRIBER NAME] AND/OR ITS SUBSIDIARIES (DOING SUBSCRIBER UNDER THE BRAND NAME: "[ADD SUBSCRIBER' BRAND NAME]") ("**SUBSCRIBER**", "**WE**", "**US**", "**OUR**"), RESPECTS YOUR PRIVACY.

This privacy policy (the "Policy") explains our privacy practices for our services ("Services").

We are the data controller, as described below in this Policy. We work with data processors to whom we have instructed to collect, store and process personal information on our behalf for the purposes of providing our services.

This Policy describes the ways your personal information and data is collected, used and shared and the rights and options available to you with respect to your information.

To the maximum extent permitted by law, you hereby agree to the use of: (a) electronic means to provide you with any notices given pursuant to this Policy and, if so necessary and permissible, to consent to this Policy; and (b) electronic records to store information related to this Policy and your use of the Service.

Privacy Policy Summary

1	Summary – for the full text please review the respective Section of this Policy
2	Personal information that you voluntarily provide. We collect personal information you voluntarily provide, mainly through a Registration Form customized by us, which you fill in and submit while you register to the Services. If you choose not to provide information determined by us as mandatory, you will not become a Registered Member, and only Basic Functionalities, as determined by us, will be available to you.
3	Information collected from all Users \ Business End-Users. We collect information in regard of (a) your mobile device identifier and/or account identifier, the Internet protocol (IP) address of the device used to access the Internet, geo-location (if enabled), device type and its operating system version; and (b) your usage of the Service, including, without limitation, interactions you make with the Service's features and functionalities, websites and content you have accessed, clicked or interacted with through/via the Service.

4	Other Information collected from Registered Members. We collect information regarding messages you receive through the Service, your participation in, or use of, certain features available to Registered Members only, and purchases you make.
5	Collection of your location. We collect your geolocation (if made available to us by you) and other information which can identify your assumed location.
6	Additional Information collected. We collect information regarding your activity with us and when you interact with us, as further described below.
7	Process of Sensitive Information. We do not require you to provide sensitive information and do not intentionally collect or process otherwise sensitive information.
8	Children's Privacy. If you are under age of 13 years, or other minimum age which applies in your country (e.g. 16 in most EU countries) you are not permitted to register to any Members Features, or use any aspect of the Service.
9, 10	Use of information. The information collected will be used for several purposes, such as: (a) providing you with the Service's functionalities, features and services, which includes specific and/or personalized activities, promotions, advertisements, features and/or services (including location-based services); (b) developing new services and/or improving the Service; or (c) enforcing this Policy or complying with applicable laws. Further information is provided in Section 9 below. Legal basis (GDPR only). The GDPR legal basis applicable to each purpose is identified next to each purpose in Section 9 below.
11	Anonymized or aggregated information that does not include personal data may be used in any way without restrictions or limitations.
12	Automated decision making. We use automated decision-making, based on the information you provide us and your usage of the Service, including number of transactions, frequency and volume. As a result, you will receive different offerings that we pre-customize for you.
13	Third parties services. You may provide information through certain areas, features, frames or sections of the Service such as when a link directs you to a third party (such as a social media channel). Please note that these are operated by third parties and, to the maximum extent permitted by law, we are not responsible for their own data-collection practices.
14	Information regarding transfers (GDPR only): we store your personal information in connection with the Service either in the European Economic Area, in the US, in the country where we are located, or in countries deemed as providing an *adequate level of data protection*. Your data will be accessible in the country where we or our service providers are

	located, the UK, the US, and countries deemed as providing an *adequate level of data protection*. If you wish to receive further information, please contact us.
15	Your rights. You are entitled to exercise any of the rights set forth in privacy laws or regulations applicable to you. We handle these requests in accordance with applicable law. Please note that these rights may be subject to certain derogations, exceptions or limitations.
16	Data retention. We retain your data for as long as we have a legitimate need, reason or purpose to use it. For example, we retain your data while you are a registered user to the Service. If you want to be deleted, you can contact us or exercise your rights and we will process your request in accordance with applicable law and this Policy.
18	Changes to this policy. We may change this Policy from time to time. Updated versions will be made available in an electronic or equivalent manner.

Personal information that you voluntarily provide

1) You are requested to submit a registration form (or otherwise provide personal information about you in an equivalent form or manner) in order to become a registered (or logged in) member of our Service ("Registered Member" and the "Registration Form" respectively). The Registration Form includes personal details such as: name, phone number, email and home address. It is customized by us and may include fields which are explicitly indicated as mandatory (i.e.: fields determined by us, which must be completed in order to submit the registration form and to join the Service; "Mandatory Fields").
2) You may choose not to share your personal information with us. There are many activities, functionalities, features of the Service (as will be determined by us; such as, opening hours, locations list, menus, catalogues or promotions), which will be available to you if you choose not to fill in all Mandatory Fields and not become a Registered Member thereof ("Basic Functionalities").
3) If you specifically opt-in to permit access and collection of information from your social network account(s), then your basic personal information in your social network account will be collected (such as your name, photo and email address) as well as your social network user ID (but not your password). Please refer to the social network's privacy policy for more details on how you can set the privacy preferences of your account to control the information that may be accessed and retrieved. We collect this information for the purpose of enabling your registration to the Service.
4) In order to enjoy the benefits of the Service, you will be requested to identify yourself upon usage of Third Parties Services. We will use the information you provide through the Registration Form to verify your identification (including enabling the Third Parties Services) and to attribute your purchases or actions (made online or offline) to you (including those made through the Third Parties Services) and for redemption purposes.
5) Depending on the context, we may ask you to provide additional information or your information may be provided in several occasions or phases and/or in separate submissions. Please note that refusal to provide any additional information or to accept further terms or offers shall not derogate from our right to store former information provided or submitted to the Service or to us.

Information collected by Us from all Users \ Business End-Users

1) The following section applies to our data collection practices which apply to all User \ Business End-User, including User \ Business End-User which do not voluntarily share their personal information with us and use the Basic Functionalities of the Service.
2) We collect from all User \ Business End-User information about the mobile device, such as mobile device identifier and/or account identifier (Android UDID, iOS UUID; Advertising ID: IDFA for iOS devices and AAID for Android devices, or their equivalent), the Internet protocol (IP) address of the device used to access the Internet, geo-location (if enabled), device type and its operating system version.
3) We also collect information regarding the features, content, services or websites accessed, clicked or interacted with through the Service as well as information regarding the interactions made with the Service's interface and features such as logging info, the Service's tabs, banners, or pages that are clicked on or accessed, ads and/or promotions viewed through the Service and receipt of notifications sent through the Service.

Other Information collected by Us from Registered Members

1) In addition to the above, if you are a Registered member, we collect information regarding (i) receipt of SMS text messages or emails sent to you through the Service; (ii) your participation in, or use of, the Service features available to Registered Members only (such as: scratch card, point accumulation plans, punch card, coupons, gift card, cash back, "Pay with Budget" or their equivalent; collectively: "Members Features"); and (iii) details of purchases made online or offline by using the Service (e.g., time and date of your purchase, place where purchase was made, the amount paid and information about the items purchased).

Collection of your location

1) We process your geolocation information in order to provide you with offers and/or promotions which are based on your location ("Location Based Services"). These Location Based Services apply whenever your location is made available to us.
2) Your location will be available to us (i) via your mobile phone, if you provide permission to share it with us; and/or (ii) other sources integrated to the Service such as: (a) upon purchase at our premises – since we have the knowledge about these premises location; (b) external services integrated with the Service; and/or (c) through Beacons if used by us at our premises or nearby.
3) By disabling your geo-location (e.g. through the mobile device operating system), certain features which require your geo-location information may not function or may be interrupted. Please note that by such disabling, your location may still be assumed and/or collected by us from other available sources as described above.
4) A beacon is a device designed to attract attention to a specific location by using Bluetooth low energy signals ("Beacon"). We may place these Beacons in or nearby our premises in order to collect your approximate location. Once your mobile phone device identifies a signal from a specific Beacon, the Service will send that identification to our servers. By receiving such identification, we will assume that you are physically located in proximity of the location of that respective Beacon as registered in our database.

Additional information collected

1) We will collect information regarding purchases made online or at our premises. If you identify yourself at our premises, we will attribute the information in regard of your purchases to you. Purchase details may include: time and date of your purchase, place where purchase was made, the amount paid and information about the items purchased.

2) We may have collected or processed non-personal or personal information about you prior to joining the Service. Such information will be added to, or combined with, other information processed under this Policy, and shall be processed in accordance with this Policy.
3) Third parties which provide other services or Services to us, which are embedded in or integrated with the Service, such as ordering, payment, e-commerce or scheduling services ("Third Parties Services"), will share with us information regarding your interactions with their systems such as: (i) your name, email address and/or phone number (if provided by you); and (ii) purchase details (time and date of the purchase, place where purchase was made, the amount paid and information about the items purchased). Please note that we are not responsible for the data collection and processing practices of such Third Parties Services, which you are encouraged to review before interacting with them.

Processing of Sensitive Information

1) We do not require Users \ Business End-Users to provide sensitive information and do not intentionally collect or process otherwise sensitive information.
2) If by using the Service (including any third-party services integrated to or embedded in the Service) you are asked to provide sensitive information, or you have a reason to suspect that sensitive information is collected, you are kindly requested to immediately report it to us. Please note that the definition of "sensitive information" may not have the same meaning in different jurisdictions.

Children's Privacy

1) Personal information about children who are under 13 years, or other minimum age which applies in your country (16 in most EU countries) is not knowingly or intentionally collected. If you are under that age, you are not permitted to use the Service, register to any Members Features, or use any aspect of the Service. If you have reason to suspect that children data is collected, you are kindly requested to immediately report it to us.

Use of collected information. Legal basis (GDPR only)

The information we collect will be used for the following purposes (please note the GDPR legal basis next to each purpose):

1) To provide you with the Service's functionalities, features and services (including, without limitation, personalized content and Location Based Services, if any), send you, from time to time, push notifications, SMS text messages, commercial emails and/or other communications from us. GDPR legal basis: depending on the context, consent, performance of a contract ((i.e. User \ Business End-User Terms of Use), legitimate interest (e.g. send you administrative communications);
2) To develop new Services or update or upgrade existing Services. GDPR legal basis: legitimate interest, performance of a contract (i.e. User \ Business End-User Terms of Use);
3) To manage the administrative and operational aspects of the Service. GDPR legal basis: legitimate interest, performance of a contract (i.e. User \ Business End-User Terms of Use);
4) To enforce this Policy and the User \ Business End-User Terms of Use and prevent unlawful activities and misuse of the Service. GDPR legal basis: legitimate interest, compliance with laws, performance of a contract (i.e. User \ Business End-User Terms of Use, this Policy);
5) To comply with any applicable law and assist law enforcement agencies when we have a good faith belief that our cooperation with them meets the applicable legal standards. GDPR legal basis: compliance with laws, legitimate interest; and
6) To take any action in any case of dispute involving you with respect to the Service. GDPR legal basis: Legitimate interest, compliance with laws.
7) If you have questions about these uses, please contact us. Please note that the legal basis is provided for GDPR purposes only.

Sharing and transferring collected information

The information outlined in the preceding sections, may be shared with, or transferred to our processors or vendors for the purposes of helping us provide the Service. This includes our processors, vendors and third parties which provide you with services, features or content in connection with the Service such as online ordering, ecommerce services, games, payments, communications, agencies, feedback, plugins or APIs, or companies that host the Service. If you wish to receive further information, please contact us.

In addition to the above, we may share the information as follows:

1) If you have breached the User \ Business End-User Terms of Use or this Policy, abused your rights to use the Service, or violated any applicable law, or in any other case of dispute, or legal proceeding of any kind involving you with respect to the Service, your information may be shared with competent authorities and with any third party, as may be required;
2) We may share information that we collect or obtain through the Service with the relevant authorities, entities or persons if we reasonably believe that we are required by law to share or disclose your information;
3) Personal data or identifiable information may be shared with, or transferred to, our affiliated corporate group entities (entities controlled by, under common control with, or controlling us, directly or indirectly);
4) Upon bankruptcy, dissolution or other liquidation or insolvency events or in the event of merger, sale or transfer of all or a portion of our assets or shares or other reorganization or reconstruction in our ongoing Subscriber, the information that we receive, collect or obtain, as outlined in the preceding sections, may be shared with or transferred to, that respective entity, provided that it will undertake to be bound by the provisions of this Policy, with reasonably necessary changes taken into consideration. Upon such transfer or sharing of information, that entity will assume full and exclusive responsibility for all subsequent use and processing it makes of the information and we will be released from any liability to you, regarding the succeeding entity's use and processing of the information by it.
5) In any case other than the above mentioned in this Policy, your personally identifiable information will be shared with others only if you provide your consent.
6) Aggregated or anonymized information
7) The Service collects anonymized as well as aggregated information, which does not identify you personally. In addition, we may anonymize your information and/or aggregate it with other Users\ Business End-Users' information. Such anonymized or aggregated information will be used by us in any way without restrictions or limitations.
8) Use of Automated Decision-Making
9) The Service uses automated decision-making. This is based on the information you provide and your usage of the Service, the number of transactions, frequency and volume. The consequence of this is that you will receive customized content and different offerings that we pre-customize to your profile.

Third parties services

1) You may provide information through certain areas, features, frames or sections of the Service, that are operated by or for third parties. Those third parties may include, e-commerce platforms, scheduling partners, payment services providers and payment processors ("Third Parties" and "Third Parties Services").
2) It is those Third Parties, and not us, that are responsible for their data collection practices associated with such Third Parties Services. We encourage you to read the privacy policy of each Third Party.
3) Third Parties Services will share with us information they collect from you or you voluntarily provide to them which is related to or within the scope of the Service.

atriis

Transfer of Data Outside Your Territory (GDPR only)

1) We host your personal information in connection with the Service either in the European Economic Area, in the US, in the country where we are located, or in countries deemed as providing an adequate level of data protection.
2) Your data will be accessible in the country where we or our service providers are located, the UK, the US, and countries deemed as providing an adequate level of data protection.
3) Please contact us if you need further information about this.

Your Rights with the Data

1) Please be informed that under applicable privacy laws, you may have certain rights such as the right to access, rectification, erasure, restriction of processing, objection, withdraw consent (without affecting lawfulness of the processing based on consent before its withdrawal) or data portability. These rights may not be available in certain jurisdictions and/or may be subject to certain derogations or limitations.
2) If you choose to exercise any User \ Business End-User Right, we will handle these requests in accordance with applicable law but please note that exercise of some of those rights may have commercial consequences. For example, depending on the right exercised, you may be disconnected from the Service and cease to be a Registered Member.
3) You have the right to lodge a complaint with a supervisory authority but, before filing a claim, we encourage you to resolve the issue in question directly with us in good faith.

Data Retention

1) We keep your data for as long as we have a valid legal basis, reason or need to keep your data.
2) Please note that removal of the Service from your device does not cause a deletion or anonymization of the information you voluntarily provided or information that we collected in accordance with this Policy. You should contact us if you would like your data to be deleted.

Changes to this Policy

1) This Policy may be changed from time to time. Substantial changes will take effect 30 days after an initial notification is posted through the Service. Other changes will take effect 7 days after their initial posting within the Service or other electronic means. However, if the Policy is amended to comply with legal requirements or for urgency reasons, the amendments will become effective immediately upon their initial posting, or as required. The most up-to-date Policy is accessible through the Service's settings or information menu or other electronic means.
2) Your continued use of the Service after the changed take effect will indicate your acceptance of the amended Policy. If you do not agree with the amended Policy, you must uninstall the Service and avoid any further use of it.

Contact Us

You may send requests, responses, questions and complaints by contacting us at support@gtp-marketplace.com

(GDPR only) If your question relates to our data protection officer (DPO) or representative in the EU, we will forward the request accordingly.

For your convenience, this Policy may be translated from English to several other languages. Please note that in any discrepancies between the translation available to you (if any) and the English version, the English version shall prevail.

Appendix C - Personal Data Protection Policy

Purpose, Scope and Users

Atriis Technology Ltd., hereinafter referred to as the “Company”, strives to comply with applicable laws and regulations related to Personal Data protection in countries where the Company operates. This Policy sets forth the basic principles by which the Company processes the personal data of consumers, customers, suppliers, business partners, employees and other individuals, and indicates the responsibilities of its business departments and employees while processing personal data.

This Policy applies to the Company and its directly or indirectly controlled wholly owned subsidiaries conducting business within the European Economic Area (EEA) or processing the personal data of data subjects within EEA.

The users of this document are all employees, permanent or temporary, and all contractors working on behalf of The Company.

Reference Documents

- EU GDPR 2016/679 (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC)
- Employee Personal Data Protection Policy
- Data Retention Policy
- Data Protection Officer Job Description
- Guidelines for Data Inventory and Processing Activities
- Data Subject Access Request Procedure
- Data Protection Impact Assessment Guidelines
- Cross Border Personal Data Transfer Procedure
- Information security policies
- Breach Notification Procedure

Definitions

The following definitions of terms used in this document are drawn from Article 4 of the European Union’s General Data Protection Regulation:

Personal Data: Any information relating to an identified or identifiable natural person ("**Data Subject**") who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Sensitive Personal Data: Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data Controller: The natural or legal person, public authority, agency or any other body, which alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor: A natural or legal person, public authority, agency or any other body which processes personal data on behalf of a Data Controller.

Processing: An 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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of the data.

Anonymization: Irreversibly de-identifying personal data such that the person cannot be identified by using reasonable time, cost, and technology either by the controller or by any other person to identify that individual. The personal data processing principles do not apply to anonymized data as it is no longer personal data.

Pseudonymization: The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. Pseudonymization reduces, but does not completely eliminate, the ability to link personal data to a data subject. Because pseudonymized data is still personal data, the processing of pseudonymized data should comply with the Personal Data Processing principles.

Cross-border processing of personal data: Processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the European Union where the controller or processor is established in more than one Member State; or processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State;

Supervisory Authority: An independent public authority which is established by a Member State pursuant to Article 51 of the EU GDPR;

Lead supervisory authority: The supervisory authority with the primary responsibility for dealing with a cross-border data processing activity, for example when a data subject makes a complaint about the processing of his or her personal data; it is responsible, among others, for receiving the data breach notifications, to be notified on risky processing activity and will have full authority as regards to its duties to ensure compliance with the provisions of the EU GDPR;

Each "**local supervisory authority**" will still maintain in its own territory, and will monitor any local data processing that affects data subjects or that is carried out by an EU or non-EU controller or processor when their processing targets data subjects residing on its territory. Their tasks and powers includes conducting investigations and applying administrative measures and fines, promoting public awareness of the risks, rules, security, and rights in relation to the processing of personal data, as well as obtaining access to any premises of the controller and the processor, including any data processing equipment and means.

"Main establishment as regards a controller" with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

"Main establishment as regards a processor" with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

Group Undertaking: Any holding company together with its subsidiary.

Basic Principles Regarding Personal Data Processing

The data protection principles outline the basic responsibilities for handling personal data. Article 5(2) of the GDPR stipulates that "*the controller shall be responsible for, and be able to demonstrate, compliance with the principles*."

Lawfulness, Fairness and Transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

Purpose Limitation

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Data Minimization

Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. The Company must apply anonymization or pseudonymization to personal data if possible to reduce the risks to the data subjects concerned.

Accuracy

Personal data must be accurate and, where necessary, kept up to date; reasonable steps must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified in a timely manner.

Storage Period Limitation

Personal data must be kept for no longer than is necessary for the purposes for which the personal data are processed.

Integrity and confidentiality

Taking into account the state of technology and other available security measures, the implementation cost, and likelihood and severity of personal data risks, the Company uses appropriate technical or organizational measures to process Personal Data in a manner that ensures appropriate security of personal data, including protection against accidental or unlawful destruction, loss, alternation, unauthorized access to, or disclosure.

Accountability

Data controllers must be responsible for and be able to demonstrate compliance with the principles outlined above.

Building Data Protection in Business Activities

In order to demonstrate compliance with the principles of data protection, the Company build data protection into its business activities.

Notification to Data Subjects

(See the Fair Processing Guidelines section.)

Data Subject's Choice and Consent

(See the Fair Processing Guidelines section.)

Collection

The Company strives to collect the least amount of personal data possible. If personal data is collected from a third party, Information Security Officer must ensure that the personal data is collected lawfully.

Use, Retention, and Disposal

The purposes, methods, storage limitation and retention period of personal data must be consistent with the information contained in the Privacy Notice. The Company must maintain the accuracy, integrity, confidentiality and relevance of personal data based on the processing purpose. Adequate security mechanisms designed to protect personal data must be used to prevent personal data from being stolen, misused, or abused, and prevent personal data breaches. Data Protection Officer is responsible for compliance with the requirements listed in this section.

Disclosure to Third Parties

Whenever the Company uses a third-party supplier or business partner to process personal data on its behalf, Data Protection Officer must ensure that this processor will provide security measures to safeguard personal data that are appropriate to the associated risks. For this purpose, the Processor GDPR Compliance Questionnaire must be used.

The Company must contractually require the supplier or business partner to provide the same level of data protection. The supplier or business partner must only process personal data to carry out its contractual obligations towards the Company or upon the instructions of the Company and not for any other purposes. When the Company processes personal data jointly with an independent third party, the Company must explicitly specify its respective responsibilities of and the third party in the relevant contract or any other legal binding document, such as the Supplier Data Processing Agreement.

Cross-border Transfer of Personal Data

Before transferring personal data out of the European Economic Area (EEA) adequate safeguards must be used including the signing of a Data Transfer Agreement, as required by the European Union and, if required, authorization from the relevant Data Protection Authority must be obtained. The entity receiving the personal data must comply with the principles of personal data processing set forth in Cross Border Data Transfer Procedure.

Rights of Access by Data Subjects

When acting as a data controller, Data Protection Officer is responsible to provide data subjects with a reasonable access mechanism to enable them to access their personal data, and must allow them to update, rectify, erase, or transmit their Personal Data, if appropriate or required by law. The access mechanism will be further detailed in the Data Subject Access Request Procedure.

Data Portability

Data Subjects have the right to receive, upon request, a copy of the data they provided to us in a structured format and to transmit those data to another controller, for free. Data Protection Officer is responsible to ensure that such requests are processed within one month, are not excessive and do not affect the rights to personal data of other individuals.

Right to be Forgotten

Upon request, Data Subjects have the right to obtain from the Company the erasure of its personal data. When the Company is acting as a Controller, Data Protection Officer must take necessary actions (including technical measures) to inform the third-parties who use or process that data to comply with the request.

Fair Processing Guidelines

Personal data must only be processed when explicitly authorised by Data Protection Officer.

The Company must decide whether to perform the Data Protection Impact Assessment for each data processing activity according to the Data Protection Impact Assessment Guidelines.

Notices to Data Subjects

At the time of collection or before collecting personal data for any kind of processing activities including but not limited to selling products, services, or marketing activities, Data Protection Officer is responsible to properly inform data subjects of the following: the types of personal data collected, the purposes of the processing, processing methods, the data subjects' rights with respect to their personal data, the retention period, potential international data transfers, if data will be shared with third parties and the Company's security measures to protect personal data. This information is provided through Privacy Notice.

Where personal data is being shared with a third party, Data Protection Officer must ensure that data subjects have been notified of this through a Privacy Notice.

Where personal data is being transferred to a third country according to Cross Border Data Transfer Policy, the Privacy Notice should reflect this and clearly state to where, and to which entity personal data is being transferred.

Where sensitive personal data is being collected, the Data Protection Officer must make sure that the Privacy Notice explicitly states the purpose for which this sensitive personal data is being collected.

Obtaining Consents

Whenever personal data processing is based on the data subject's consent, or other lawful grounds, Data Protection Officer is responsible for retaining a record of such consent. Data Protection Officer is responsible for providing data subjects with options to provide the consent and must inform and ensure that their consent (whenever consent is used as the lawful ground for processing) can be withdrawn at any time.

Where collection of personal data relates to a child under the age of 16, Data Protection Officer must ensure that parental consent is given prior to the collection using the Parental Consent Form.

When requests to correct, amend or destroy personal data records, Data Protection Officer must ensure that these requests are handled within a reasonable time frame. Data Protection Officer must also record the requests and keep a log of these.

Personal data must only be processed for the purpose for which they were originally collected. In the event that the Company wants to process collected personal data for another purpose, the Company must seek

the consent of its data subjects in clear and concise writing. Any such request should include the original purpose for which data was collected, and also the new, or additional, purpose(s). The request must also include the reason for the change in purpose(s). The Data Protection Officer is responsible for complying with the rules in this paragraph.

Now and in the future, Data Protection Officer must ensure that collection methods are compliant with relevant law, good practices and industry standards.

Data Protection Officer is responsible for creating and maintaining a Register of the Privacy Notices.

Organization and Responsibilities

The responsibility for ensuring appropriate personal data processing lies with everyone who works for or with the Company and has access to personal data processed by the Company.

The key areas of responsibilities for processing personal data lie with the following organisational roles:

The board of directors makes decisions about and approves the Company's general strategies on personal data protection.

The **Data Protection Officer (DPO),** is responsible for managing the personal data protection program and is responsible for the development and promotion of end-to-end personal data protection policies, as defined in Data Protection Officer Job Description;

The **Legal Affairs Department/Counsel together with the Data Protection Officer,** monitors and analyses personal data laws and changes to regulations, develops compliance requirements, and assists business departments in achieving their Personal data goals.

The **Data Protection Officer (DPO),** is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.

The **Director of Sales - EMEA**, is responsible for:

- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with the Data Protection Officer to ensure marketing initiatives abide by data protection principles.

The **VP Operation & Product** is responsible for:

- Improving all employees' awareness of user personal data protection.
- Organizing Personal data protection expertise and awareness training for employees working with personal data.
- End-to-end employee personal data protection. It must ensure that employees' personal data is processed based on the employer's legitimate business purposes and necessity.

The **Data Protection Officer (DPO)** is responsible for passing on personal data protection responsibilities to suppliers, and improving suppliers' awareness levels of personal data protection as well as flow down personal data requirements to any third party a supplier they are using. The Procurement Department must ensure that the Company reserves a right to audit suppliers.

Guidelines for Establishing the Lead Supervisory Authority

Necessity to Establish the Lead Supervisory Authority

Identifying a Lead supervisory authority is only relevant if the Company carries out the cross-border processing of personal data.

Cross border of personal data is carried out if:

a) *processing of personal data is carried out by subsidiaries of the Company which are based in other Member States;*

or

b) *processing of personal data which takes place in a single establishment of the Company in the European Union, but which substantially affects or is likely to substantially affect data subjects in more than one Member State.*

If the Company only has establishments in one Member State and its processing activities are affecting only data subjects in that Member State than there is no need to establish a lead supervisory authority. The only competent authority will be the Supervisory Authority in the country where Company is lawfully established.

Main Establishment and the Lead Supervisory Authority

Main Establishment for the Data Controller

The CEO needs to identify the main establishment so that the lead supervisory authority can be determined.

If the Company is based in an EU Member State and it makes decisions related to cross-border processing activities in the place of its central administration, there will be a single lead supervisory authority for the data processing activities carried out by the Company.

If Company has multiple establishments that act independently and make decisions about the purposes and means of the processing of personal data, CEO needs to acknowledge that more than one lead supervisory authority exists.

Main Establishment for the Data Processor

When the Company is acting as a data processor, then the main establishment will be the place of central administration. In case the place of central administration is not located in the EU, the main establishment will be the establishment in the EU where the main processing activities take place.

Main Establishment for Non-EU Companies for Data Controllers and Processors

If the Company does not have a main establishment in the EU, and it has subsidiary(ies) in the EU, then the competent supervisory authority is the local supervisory authority.

If the Company does not have a main establishment in the EU nor the subsidiaries in the EU, it must appoint a representative in the EU, and the competent supervisory authority will be the local supervisory authority where the representative is located.

Response to Personal Data Breach Incidents

When the Company learns of a suspected or actual personal data breach, Data Protection Officer must perform an internal investigation and take appropriate remedial measures in a timely manner, according to the Data Breach Policy. Where there is any risk to the rights and freedoms of data subjects, the Company must notify the relevant data protection authorities without undue delay and, when possible, within 72 hours.

Audit and Accountability

The CEO is responsible for auditing how well business departments implement this Policy.

Any employee who violates this Policy will be subject to disciplinary action and the employee may also be subject to civil or criminal liabilities if his or her conduct violates laws or regulations.

Conflicts of Law

This Policy is intended to comply with the laws and regulations in the place of establishment and of the countries in which Atriis Technologies Ltd operates. In the event of any conflict between this Policy and applicable laws and regulations, the latter shall prevail.

Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Data Subject Consent Forms	Atriis Travel Platform Database @Microsoft Azure	Data Protection Officer	Only authorized persons may access the forms	10 years
Data Subject Consent Withdrawal Form	Atriis Travel Platform Database @Microsoft Azure	Data Protection Officer	Only authorized persons may access the forms	10 years
Parental Consent Form	Atriis Travel Platform Database	Data Protection Officer	Only authorized persons may access the forms	10 years

	@Microsoft Azure			
Parental Consent Withdrawal Form	Atriis Travel Platform Database @Microsoft Azure	Data Protection Officer	Only authorized persons may access the forms	10 years
Supplier Data Processing Agreements	Atriis Travel Platform Database @Microsoft Azure	Data Protection Officer	Only authorized persons may access the folder	5 years after the agreement has expired
Register of Privacy Notices	Atriis Travel Platform Database @Microsoft Azure	Data Protection Officer	Only authorized persons may access the folder	Permanently