OmniAccess Stellar Asset Tracking – Data Privacy Notice

OmniAccess Stellar Asset Tracking Release 1.0.5

Definitions

“Affiliates” means any entity which is controlled by, controls or is in common control with ALE.

“ALE” means the ALE Group or any of its Affiliates.

“ALE Group” means ALE and its Affiliates engaged in the Processing of Personal Data.

“CCPA” stands for the California Consumer Privacy Act and is a state statute intended to enhance privacy rights and consumer protection for residents of California.

“Data Controller” means the entity which determines the purposes and means of the Processing of Personal Data. In the context of Stellar Asset Tracking Service, the Data Controller is the End-Customer, using the Service.

“Data Processor” means the entity which Processes Personal Data on behalf of the Data Controller. In the context of the Stellar Asset Tracking Service, Data Processor is any Service Supplier, ALE business partners, ALE and ALE sub-contractors which contribute to the delivery of the Stellar Asset Tracking Service.

“Data Protection Laws” means all laws and regulations, including laws and regulations of the European Union (“EU”), the European Economic Area (“EEA”) and their member states, and the CCPA, applicable to the Processing of Personal Data.

“Data Subject” means the individual to whom Personal Data relates. In the Stellar Asset Tracking service context, the Data Subject is the User or the people tracked, using the Service.

End-Customer: means a company or legal entity contracting with the Service Supplier for the purpose of using the Stellar Asset Tracking Service for its own community of Users

“Personal Data” means any information relating to an identified or identifiable person.

“Processing” means any operation or set of operations which is performed upon Personal Data, whether by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction (“Process”, “Processes” and “Processed” shall have the same meaning).

“Data Breach” is a security incident in which sensitive, protected, personal or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.

“GDPR” stands for the General Data Protection regulation” and is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU).

"Services" means the provision of the Stellar Asset Tracking service.

"Service Supplier" means ALE International or an Authorized Reseller from which the End-Customer has purchased the Stellar Asset Tracking service.

"Standard Contractual Clauses" means the agreement executed by and between ALE and some of its sub-contractors, pursuant to the European Commission's decision of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

"Stellar Asset Tracking Service": The Service of Asset tracking identifies the location of equipment or people, in real-time, using tags with GPS, BLE or RFID technology to broadcast their location. One can track more than just the whereabouts of your assets. One can learn about equipment usage patterns and locations – even when it's not in use. Asset tracking analytics provide information about how items are used, which departments use them the most, how often they get moved around the premises, how far they travel on a daily basis and even when the asset was last maintained. This information helps organization optimize asset usage.

"User" means the individual who accesses the Stellar Asset Tracking Service. The User is the Data Subject.

A. General

This document is intended to be the support of understanding i) how ALE International, the editor of the Stellar Asset Tracking Service is managing its obligations under the various Personal Data protection regulations, of which, first and foremost, but not limited to, GDPR & CCPA and ii) what are the responsibilities amongst the stakeholders.

How does the Service work?

Asset tracking is built using asset tags, Stellar gateways, autocalibration tags, the Stellar Asset Tracking Cloud, a web management tool and an Android mobile app. The asset tags is tied to an asset (in health context: a bed or a medical device or appliance) or an individual (e.g. Health Patient) and sends out a periodic BLE (Bluetooth low energy) signal and the gateways listen for the BLE signals and the information is sent to the asset tracking cloud where the various signals from different gateways are used to calculate the location. The app and web management tool show the asset tag locations that are stored in the asset tracking cloud.

The tags can be programmed (mapped) by the Data Controller with information like the patient name (in a healthcare context) so that patients that need to be tracked, like infants and elderly, can be tracked to ensure their safety. Similarly, assets such as beds or medical devices or appliances can be tracked and monitored. The information on the tag is set up during tag assignment but can be modified as well. There is no patient health or personal data associated with these tags by ALE. For example, the Data Controller can use "John S. room 1201" as a tag identifier so this is very innocuous information.

For the sake of clarity, as Data Processor, while operating the Stellar Asset Tracking Service, ALE or any other Service Supplier does not have access to the personal data eventually mapped to the tags by the Data Controller, nor has it access to the location data collected from tags and processed by the Service. Administration access is given to the End Customer upon Service subscription. ALE may gain administration access to such data as mentioned beforehand only upon formal instruction from the Data Controller and upon support request. In this case, ALE's accesses and activities are logged and can be monitored by the End Customer or its delegate.

What are the stakeholders?

ALE is the editor and the operator of the Service when data collected from BLE Tags is flowing into its cloud.

As per the definitions, the End Customers are the Data Controllers and the resellers and ALE are the Data Processors. For information, in a health/ hospital context, patients or caring personal would be the Data Subjects, the hospital would be the End Customer and the Data Controller.

For the sake of clarity, all parties to a Stellar Asset Tracking distribution or sales contract acknowledge and warrant, in the data protection agreement they establish between them and that supplement Master Service agreement or equivalent, that they are aware of their respective legal obligations as Data Controller or as Data Processor.

ALE has designed and is enforcing policies and procedures with respect to Personal Data collection & processing through i) ALE Global Privacy Policy and ii) the provisions in the present Stellar Asset Tracking Data Privacy Notice complementing the ALE Global Privacy Policy.

ALE has nominated a data protection officer who can be addressed at:

ALE Data Protection Officer

32 avenue Kleber, 92700, Colombes, France

dataprivacy@al-enterprise.com

B. The obligations of Data Controller and Data Processor

B.1 Obligation of the Data Controller

The Data Controller:

is committed to abide by all laws and regulations, in this context, those pertaining to data privacy, personal data protection and security.

shall instruct its Data Processors to collect and process personal data in accordance with all the relevant provisions of the applicable data protection laws, in particular, with respect to the security, protection and disclosure of personal data; in particular also upon support requests

shall inform the Data Subjects i) of the use of their personal data (see sections C below) ii) of the involvement of data processors to process their personal data and iii) that their personal data may be processed outside the EEA (European Economic Area).

shall respond in reasonable time and to the extent reasonably possible to enquiries by Data Subjects regarding the Processing of their Personal Data by the Data Controller, and it will give appropriate instruction to the Data Processor in a timely manner.

shall respond in a reasonable time to enquiries from the Data Protection Supervisory authority.

Shall protect personal data in a manner that is deemed “adequate”; where means meeting generally accepted data security standard such as ISO 27001. It is expected that the Data Controller provides the TOM-s (technical organizational measures) by which personal data is protected. TOM-s may be provided by the Data Processors.

Beyond the GDPR obligations listed above, there are also obligations specific to the CCPA whereby Data Controllers should:

1. Disclose to consumers/ Data Subjects that they sell or share personal information; in the Stellar Asset tracking context, this means that End Customers, if they intent to sell or share Data Subject information, should disclose this in an explicit manner at the time they collect such data or before they do. For the sake of clarity, without this being construed as an advice, and for example in the Health context, a hospital (Data Controller) should disclose this information at the time the Data Subjects are enrolled in the Service.

2. Add a “Do Not Sell My Personal Information” option to their websites, and a toll-free phone number for consumer requests; in the Stellar Asset tracking context, the process by which this would be carried out should be managed by the Data Controlled with its own means since people being tracked by the in the Stellar Asset Tracking Service do not all have access to it (patients).

3. Affirmatively collect consent to sell data from any consumer under 16, or from a parent or guardian for any consumer under 13: see 2.

4. Treat customers equally on service and price regardless of whether they have exercised their rights under the law. This is solely under the responsibility of the Data Controller.

B.2 Obligations of the Data Processor

The Data Processor:

is committed to abide by all laws and regulations, in this context, those pertaining to data privacy, personal data protection and security.

Instruction:

The Data Processor only processes Personal Data on behalf of and in accordance with Data Controller’s instructions,

Individuals accessing personal data:

The Data Processor ensures that whenever its staff is involved in the Processing of Personal Data, such staff is informed of the confidential nature of the Personal Data, has received appropriate training on its responsibilities and is subject to obligations of confidentiality. Such obligations survive the termination of that individual’s involvement with the Data Processor.

The Data Processor shall take commercially reasonable steps to ensure the reliability of any staff involved in the Processing of Personal Data.

The Data Processor ensures that its access to Personal Data is limited to those staff who requires such access to perform the Service or the instructions given by the Data Controller.

Personal data protection and personal data security

The Data Processor must maintain highest protection of data, including personal data, and has therefore designed and enforced internal data security policy and procedures for the protection and the security, confidentiality and integrity of Personal Data. In general, data security is described in the technical and organizational measures (TOM-s).

Data Breach:

If the Data Processor becomes aware of any unlawful access to any Data Subject's Personal Data stored on its equipment or in its facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Data Subject's Personal Data (Data Breach), the Data Processor will promptly: (a) notify the relevant Data Protection Authority (DPA) and potentially after DPA's approval, notify the concerned Data Subject and Service provider thereof of the Data Breach, through any appropriate mean; (b) investigate the Data Breach and provide Data Protection Authority and the Data Subject with information about the Data Breach, through any appropriate mean; and (c) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Data Breach.

Where:

(i) An unsuccessful Data Breach attempt will not be subject to this Section. An unsuccessful Data Breach attempt is one that results in no unauthorized access to Data Subject's Personal Data or to any of its equipment or facilities storing Data Subject's Personal Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond IP addresses or headers) or similar incidents; and

(ii) The Data Processor 's obligation to report or respond to a Data Breach under this Section is not and will not be construed as an acknowledgement by this latter of any fault or liability with respect to the Data Breach.

Notification(s) of Data Breaches, if any, will be delivered to the Data Subjects by any means that the Data Processor selects, including via email. It is the recipient's sole responsibility to ensure it maintains accurate contact information in the Asset tracking Service at all times.

Additional terms for personal data transfers out of the EU/EEA and Switzerland:

This only applies to Data Subjects resident in the EU, EEA or Switzerland.

The Service is operated by ALE on servers in Germany, and the personal data collected by the Service is processed in Germany. However, during the Service, for example, in case of load balancing management, or use of sub-contractors to manage service tickets, ALE may transfer personal data outside the EU or the EEA.

In these cases, ALE has implemented the appropriate guarantees in order to ensure existence of an adequate level of protection of Personal Data upon export to territories deemed not having such adequate level of protection by EU (list of territories with adequate level of protection). This means that ALE has concluded contracts with those of its sub-contractors that may be importer of Personal data out of the EU/EEA in the form of European Standard Contractual Clauses approved by the European Commission.

Such clauses include the technical and organizational measures taken by the sub-contractor to protect personal data.

Engaging another Data Processor

ALE's Affiliates may be retained as Data Processors; and

ALE and ALE's Affiliates respectively may appoint sub-contractors in connection with the provision of the Services.

Any such sub-contractor will be permitted to obtain Personal Data only for the purpose of delivering the services for which ALE has appointed them, and they are prohibited from using Personal Data for any other purpose.

ALE will be liable for the acts and omissions of its sub-contractors to the same extent ALE would be liable if performing the services of each sub-contractor.

The Data Processor's Assistance

The Data Processor will assist the User and the Data Controller by using appropriate technical and organizational measures, insofar as this is commercially possible, for the fulfillment of the Users' rights (as Data Subjects) or for the fulfillment of its obligations as per the applicable Personal Data Protection laws and regulations.

To the extent the User or its Data Controller, in its use or receipt of the Services, does not have the ability to correct, amend, block or delete Personal Data, as required by Data Protection Laws, the Data Processor will assist to facilitate such actions to the extent the Data Processor is legally permitted or technically able to do so and to the extent such activity is commercially reasonable.

The Data Processor shall, to the extent legally permitted, promptly notify the Data Controller if it receives a request from a Data Subject for access to, correction, amendment or deletion of that User's Personal Data. The Data Processor shall not respond to any such Data Subject request without Data Controller's prior written consent except to advise the Data Subject that such request must be addressed to the Data Controller. The Data Processor shall provide the Data Controller with commercially reasonable cooperation and assistance in relation to handling of a Data Subject's request for access to that User's Personal Data, to the extent legally permitted and to the extent the Data Controller does not have access to such Personal Data through its use or receipt of the Services.

Personal data retention:

The Data Processor retains Personal Data for as long as it is needed to fulfill the purpose for which it was collected or as long as the Service is subscribed and within the limit of compliance with laws and regulations. For the sake of clarity, this means location data is deleted the shortest of either termination date or twelve months after data collection.

C. Personal Data ALE collects (as Data Processor) and uses to deliver the Stellar Asset Tracking Service

The Stellar Asset Tracking service collects and process technical from BLE tags which generate location data for those BLE tags. Data Controllers may associate personal data to the technical BLE tag identifier. The association is not viewed by the Data Processors, unless instructed to access the Service data base

for support purposes only. Therefore, Data Processors do not process personal data other than in the event of support.

Such support activity is logged and is available for review by the Data Controller.

Additionally, ALE does not use, sell or share personal data at all. All statistical use of the Service activity or behavioral data is anonymized.

D. ALE's Commitment to Data Security

ALE intends to protect the personal information entrusted to ALE and treats it securely in accordance with this Data Privacy Notice. ALE implements physical, administrative, and technical safeguards designed to protect any personal information from unauthorized access, use, or disclosure. ALE contractually requires that ALE's sub-contractors protect such information from unauthorized access, use, and disclosure. The Internet, however, cannot be guaranteed to be 100% secure, and ALE cannot ensure or warrant the security of any personal information Users provide to ALE.

ALE recommends not using unsecured wifi infrastructure or other unprotected networks to connect, use or submit BLE data to the Stellar Asset Tracking Service. ALE makes reasonable efforts to ensure the security of its systems and uses state of the art high level encryption to protect data in transit.

Should a User or an End-Customer become aware of a Data breach affecting its Stellar Asset Tracking Service account, then such User or End-Customer must notify its reseller or ALE immediately using dataprivacy@al-enterprise.com

E. Special Note to International End-Users

The Stellar Asset Tracking Service is hosted in Amazon Web Services Data centers in Frankfurt, Germany for Europe region. Furthermore, we have the necessary contractual material in place with the Data Center providers to ensure that the level of (personal but not limited to) data protection is adequate in the sense of the GDPR. Finally,

The designer and developer of the Stellar Asset Tracking Service is ALE International, a French corporation formed as a "Société par Action Simplifiée" with registered office address at 32, Avenue Kléber 92700 Colombes, France, registered at the Nanterre Commerce and Companies Registry under number 602 033 185 RCS Nanterre; more information available at https://www.al-enterprise.com .