Personal Data Processing Policy – STid Mobile ID®

STid assigns the utmost importance to the protection of personal privacy. Any information collected concerning individuals, when you have decided to provide this information, is intended to enable us to perform the services that you have entrusted to us.

The personal data collected by STid is protected by French data law ("Informatique et Libertés") no. 78-17 of January 6, 1978, as amended in 2004, and by Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016. (Hereinafter referred to as "Personal Data")

All our customers' data remains held on our premises and the premises of our trusted third parties stated below. Only personnel requiring this data to perform their duties are authorized to access your Personal Data. Furthermore, all employees are made aware of the updated practices that they must comply with regarding security and Personal Data.

Use of the STid Mobile ID® service requires us to process Personal Data concerning you and Users as referred to in the Terms of Use, and that of their employees, customers and third parties. However, we draw your attention to the fact that this Personal Data is encrypted and that STid does not have access to the content of encrypted information.

The User remains the data controller (as defined by the applicable regulations) of the Personal Data of their employees, customers and third parties that they may use in connection with use of the STid Mobile ID® service.

Before disclosing any of your employees' and/or third parties' Personal Data to STid, you must obtain their prior consent for both the data collected and the purposes envisaged. The customer holds STid harmless against any remedy sought by their employees regarding the information that the customer may disclose to STid in connection with use of the STid Mobile ID® service.

0.1 - Collection of the Personal Data

The Personal Data collected on this site (or "Platform") is as follows:

- Opening a user account

When a User Account is created, the platform records the following data: title, first and last names, profession, landline and cell phone number, fax number, email address, name, registration number, VAT / EU VAT number and EORI number for natural persons, director's name, date established, capital, profile (distributor or end customer), company website and preferred language (French, English) for communicating with STid.

- Login

When the User logs into the Platform, this login process records, among other information, their ID and password.

- Profile

Use of the services provided on the Platform enables a profile to be completed, which may include the following data: logo, user's first and last name, email address and phone number in addition to any data they wish to record (customizable fields), configuration associated with the user badge, type of ID used (private or STid Mobile ID+) and a photo of the user.

- Cookies

The platform does not use tracking cookies.

Cookies are used in connection with use of the site. The User has the option to disable cookies in their navigator settings.

However, disabling some cookies risks limiting the use of some of the site's features.

The cookies used on this site are as follows:

- Authentication cookie
  Used by the ASP.NET Identity framework (OWIN).
  Automatically expires after 24 hours (even if the user is continually using a web application) and after 10 minutes of inactivity.
  Secure and requires SSL for transmission.
  HttpOnly cookie is enabled, which reduces the risk of intersite scripts being created. Attribute preventing access to cookies via the script on the customer's side.

- Language cookie
  - Used for the language version
    Non-secure, in which HttpOnly is disabled.
    Initialized the first time that the user opens the web application.

0.2 - Use and retention of the Personal Data

The purpose of the Personal Data collected from Users is to provide the services of the Platform, improve them and maintain a secure environment.

More specifically, the use of the Personal Data is as follows:

- access to and use of the Platform by the User;
- operational management and optimization of the Platform;
- verification, identification and authentication of the data transmitted by the User;
- implementation of User assistance;

- prevention and detection of scams, malware (malicious software) and management of security incidents;
- management of any disputes with Users;
- the uses referred to in Article 0.7 below in connection with relations with subcontractors.

The Personal Data is retained for as long as the account remains active. The account is deactivated at the User's request or when the account was last logged into more than three years ago.

0.3 - Sharing of the Personal Data with third parties

The Personal Data may be shared with third-party companies in the following cases:

- if required by law, the Platform may transmit data to take action in response to claims made against the Platform and to comply with administrative and judicial procedures;

- if the Platform is involved in a merger, acquisition, asset transfer operation, or reorganization under the supervision of the court, it may have to transfer or share all or part of its assets, including the Personal Data. In such a case, STid will inform the Data Controller before any transfers to third parties. The Data Controller is then responsible for informing the Users, so that they can exercise their rights, as stated in 0.5, if necessary.

0.4 - Security and confidentiality

The Platform implements organizational, technical, software and physical measures in relation to digital security to protect the Personal Data from being impaired, destroyed or accessed without authorization. However, it should be noted that the Internet is not an entirely secure environment, and that the Platform cannot guarantee the secure transmission or storage of information via the Internet.

0.5 - Exercising of Users' rights

In accordance with the regulations applicable to Personal Data, Users may update, modify or delete the Data concerning them by logging into their account and configuring the settings of this Account;

Additionally, by writing to the email address: dpo@stid.com may exercise the following rights:

- they may delete their Account, or oppose the processing of their Personal Data,

- they may exercise their right of access, to obtain information on the Personal Data concerning them. In this case, before this right is exercised, STid may request proof of identity in order to verify their identity,

- if Personal Data held by the platform is incorrect, they may request that this information be updated,

- they can request the portability of their Personal Data,

- they can make a complaint to the CNIL.

0.6. Changes to this clause

The Platform reserves the right to make any changes to this clause relating to Personal Data protection at any time. If a change is made to this Personal Data protection clause, the Platform undertakes to publish the new version on the Platform. The Platform will also inform Users of the change by email, within a minimum of 15 days before the effective date. If the User does not agree with the terms of the new wording of the Personal Data protection clause, he/she has the option to request the deletion of his/her Account.

0.7. GDPR/Contract for the processing of personal data

Within the meaning of the applicable regulations, User remains responsible for processing the Personal Data of its customers and/or employees in the course of the use of the services.

The Parties agree that, in view of the General Data Protection Regulation:

The **Data Controller** is: The User

The **Data Processor** is: STid

The **Tier 2 Data Processor** is: Jaguar Network

In view of the encryption of the Data, the Data Processor and the Tier 2 Data Processor will not have access to the details of the Personal Data that will be processed by the User. Additionally, concerning the Personal Data, the service of the Data Processor delegated to the Tier 2 Data Processor is limited to providing Users with software enabling them to directly enter and to process the Personal Data themselves, without any intervention by the Data Processor or the Tier 2 Data Processor.

Data will be hosted by the Tier 2 Data Processor.

The following obligations will be set out in a separate act between the Data Processor and Tier 2 Data Processor, such that the Data Processor will be able to meets its obligations vis-à-vis the Data Controller.

Section I. Purpose

The purpose of these clauses is to define the conditions under which the Data Processor agrees to perform on behalf of the Data Controller the Personal Data processing operations defined below.

Section II. Description of Data Processor's processing

The Data Processor is authorized to process, on behalf of the Data Controller, the data and the Personal Data necessary for the purpose of the use of the Platform.

Management of data and Personal Data (GDPR)

Hosting of data on the premises of STid or the customer

Creation of an account associated with STid - End customer / Distributor

			Data hosted on the SAAS Cloud STid platform			Data hosted on the SAAS On Premise platform (on the customer's premises)		
Data	**Type of data**	**Purpose**	**STid**	**Cloud Jaguar Network**	**Customer**	**STid**	**Customer**	**Customer's customer**
Title Mr / Mrs	User	Enable the user to use the platform	Application supervision & security 24x7x365 Platform access security Database encryption Implementation and use of the platform Quarterly security audit Encrypted outsourced backup	Storage of "raw" STid data Availability of data for the application Historization of STid data (VM image 7 calendar days) Level-1 maintenance - GTR Business 24x7x365 - Facilities management of the OS + hardware Customer server support 24/7 via customer extranet	Management of usernames/passwords Entry of personal data	Supply of software tools	Data storage Availability of data Backup of data Maintenance Customer platform support	Management of usernames/passwords Entry of personal data
First name	User	Enable the user to use the platform						
Last name	User	Enable the user to use the platform						
Position	User	Enable the user to use the platform						
Landline phone number	User	Enable the user to use the platform						
Cell phone number	User	Enable the user to use the platform						
Fax number	User	Enable the user to use the platform						
Email address	User	Enable the user to use the platform						
Company name	Company	Accounting entry						
Registration no.	Company	Accounting entry						
VAT no.	Company	Accounting entry						
EORI	Company	Accounting entry						
CEO	Company	Accounting entry						
Date established	Company	Accounting entry						
Capital	Company	Accounting entry						
Type of company (distributor or end customer)	Company	Accounting entry						
Country	Company	Accounting entry						
Full address	Company	Accounting entry						
Website	Company	Accounting entry						

Creation of an account associated with a sub-distributor - End customer

Data	**Type of data**	**Purpose**	**STid**	**Cloud Jaguar Network**	**Customer**	**STid**	**Customer**	**Customer's customer**
Company name	Company	Enable the user to use the platform	Application supervision & security 24x7x365 Platform access security Database encryption Implementation and use of the platform Quarterly security audit Encrypted outsourced backup	Storage of "raw" STid data Availability of data for the application Historization of STid data (VM image 7 calendar days) Level-1 maintenance - GTR Business 24x7x365 - Facilities management of the OS + hardware Customer server support 24/7 via customer extranet	Management of usernames/passwords Entry of personal data	Supply of software tools	Data storage Availability of data Backup of data Maintenance Customer platform support	Management of usernames/passwords Entry of personal data
Type of company (distributor or end customer)	Company	Enable the user to use the platform						
Pricing category	Company	Enable the user to use the platform						
First name	User	Enable the user to use the platform						
Last name	User	Enable the user to use the platform						
Email address	User	Enable the user to use the platform						
Phone number	User	Enable the user to use the platform						
Fields customizable by the customer	User	Enable the user to use the platform						

Creation of a customer site

Data	**Type of data**	**Purpose**	**STid**	**Cloud Jaguar Network**	**Customer**	**STid**	**Customer**	**Customer's customer**
User's first name	User	Enable the user to use their virtual badge	Application supervision & security 24x7x365 Platform access security Database encryption Implementation and use of the platform Quarterly security audit Encrypted outsourced backup	Storage of "raw" STid data Availability of data for the application Historization of STid data (VM image 7 calendar days) Level-1 maintenance - GTR Business 24x7x365 - Facilities management of the OS + hardware Customer server support 24/7 via customer extranet	Management of usernames/passwords Entry of personal data	Supply of software tools	Data storage Availability of data Backup of data Maintenance Customer platform support	Management of usernames/passwords Entry of personal data
User's last name	User	Enable the user to use their virtual badge						
Configuration associated with the user badge	User	Enable the user to use their virtual badge						
Type of ID: private ID or STid Mobile ID+	User	Enable the user to use their virtual badge						
User's email address	User	Enable the user to use their virtual badge						
User's cell phone number	User	Enable the user to use their virtual badge						
Variable field concerning the user	User	Enable the user to be identified with a custom badge						
User's photo	User	Enable the user to be identified with a custom badge						
Configurator's first name	User	Enable the user to use their configuration badge						
Configurator's last name	User	Enable the user to use their configuration badge						
Configurator's email address	User	Enable the user to use their configuration badge						
Configurator's cell phone number	User	Enable the user to use their configuration badge						
Field customizable by the customer (configurator)	User	Enable the user to use their configuration badge						
Company logo	Company	Enable the user to be identified with a custom badge						

Creation of an account user

Data	Type of data	Purpose	STid	Cloud Jaguar Network data center	Customer	STid	Customer	Customer's customer
First name	User	Enable the user to use the platform	Application supervision & security 24x7x365 Platform access security Database encryption Implementation and use of the platform Quarterly security audit Encrypted outsourced backup	Storage of "raw" STid data Availability of data for the application Historization of STid data (VM image 7 calendar days) Level-1 maintenance - GTR Business 24x7x365 - Facilities management of the OS + hardware Customer server support 24/7 via customer extranet	Management of usernames/passwords Entry of personal data	Supply of software tools	Data storage Availability of data Backup of data Maintenance Customer platform support	Management of usernames/passwords Entry of personal data
Last name	User	Enable the user to use the platform						
Email address	User	Enable the user to use the platform						
Phone number	User	Enable the user to use the platform						
Fields customizable by the customer	User	Enable the user to use the platform						

Section III. Obligations of the Data Processor vis-à-vis the Data Controller

The Data Processor agrees to:

1. process the data for **the sole purpose(s)** that is/are the subject of the processing

2. process the data **in accordance with the documented instructions** of the Date Controller in the schedule to this Schedule. If the Data Processor considers that an instruction constitutes a violation of the General Data Protection Regulation or any other provision of Union law or of the data protection law of the Member States, the Data Processor must **immediately inform** the Data Controller. In addition, if the Data Processor is required to transfer data to a third country or to an international organization, under Union law or the law of the Member State to which it is subject, it must inform the Data Controller of this legal obligation prior to processing, unless the right concerned prohibits such disclosure for important reasons of public interest

3. guarantee the **confidentiality** of Personal Data processed under the Terms of Use

4. ensure that **persons authorized to process Personal Data** under the TOU:

- agree to comply with **confidentiality** obligations or are subject to an appropriate legal obligation of confidentiality

- receive the necessary **training** in the protection of Personal Data

5. take account, with respect to its tools, products, applications or services, of the principles of **data protection from the design** and **protection of data by default**

6. Data Processing

The Data Processor may use a second Tier 2 Data Processor (hereinafter, the **"Subsequent Tier 2 Data Processor"**) to conduct specific processing activities. In this case, it informs the Data Controller in advance of any proposed changes concerning the addition or replacement of other data processors. This information must clearly indicate what is being outsourced, the Data Processor's identity and contact information, and the dates of the data processing. The Data Controller has a minimum period of eight days from the date of receipt of this information to present its objections. This data processing can only be performed if the Data Controller has not objected within the agreed period.

The Subsequent Tier 2 Data Processor is required to comply with the TOU obligations on behalf of and in accordance with the instructions of the Data Controller. It is the responsibility of the initial Tier 2 Data Processor to ensure that the Subsequent Tier 2 Data Processor provides the same sufficient safeguards for the implementation of appropriate technical and organizational measures to ensure that the processing meets the requirements of the General Data Protection Regulation. If the Subsequent Tier 2 Data Processor does not fulfil its data protection obligations, the original Tier 2 Data Processor remains wholly liable to the Data Controller for the performance by the Subsequent Tier 2 Data Processor of its obligations.

7. Right of information of data subjects

The Data Controller is required to provide information to data subjects affected by the processing of data at the time the data is collected.

8. Exercise of rights by data subjects

Since the data is encrypted and the Data Processor cannot access the content of the data, the Data Controller shall fulfill its obligation to grant any requests by the Data Subjects to exercise their rights: the right of access, rectification, erasure and opposition, right to limitation of processing, right to portability of data, right not to be the subject of an automated individual decision (including profiling).

When the Data Subjects make requests to the Data Processor to exercise their rights, the Data Processor will send these requests to the Data Controller.

9. Notification of Personal Data breaches

The Data Processor notifies the Data Controller of any violation of Personal Data by e-mail within 24 hours of being informed. This notification is accompanied by any useful documentation that will enable the Data Controller to inform the competent Supervisory Authority of this violation.

10. Data Processor's assistance in the Data Controller's fulfilment of its obligations

The Data Processor assists the Data Controller in conducting data protection impact assessments.

The Data Processor assists the Data Controller in carrying out the prior consultation of the supervisory authority.

11. Security Measures

The Data Processor agrees to implement the following security measures:

Control of physical access: at jaguar network.

Logical access Control: Access to the platform (servers) in Administrator mode is only possible after Windows authentication of an authorized IP pool. This authentication is not correlated in any way with the one that allows access to the database.

Breakdown of the functional roles of the STid Mobile ID solution.
In addition, the two functional elements of the STid Mobile ID solution, namely the WEB platform, and the Addition of pseudonyms (usernames), encryption and authentication of Personal Data.

Authentication of people with access to the platform, with different levels of access.

Only authenticated persons can read/edit/delete Personal Data according to the rights assigned to them.
Customization of the protection keys for each entity (Resellers/sub-resellers can only access their accounts and have their own set of protection keys).

Breakdown of the management roles of the database, the administrator does not have knowledge of the protection keys of each reseller and cannot interpret the data managed by the database, and the database manager has no knowledge of the master key of the database.
All user data are signed, and authenticated, which allows for protection against corruption and falsification.

The availability of this data is subject to the SLAs of the Jaguar Network.
The time to restore access to this data is also subject to the SLA of the Jaguar Network, and according to the usage history of the VM 7js.

12. Output data

On completion of the services related to the processing of these data, the Data Processor agrees to:

- destroy all Personal Data; or
- return all Personal Data to the controller; or
- return the Personal Data to the Data Processor appointed by the Data Controller

The return must be accompanied by the destruction of all existing copies in the Data Processor's information systems. Once destroyed, the Data Processor must provide proof of the destruction in writing.

13. Data Protection Officer

The Data Processor provides the Data Controller with **the name and contact details of its Data Protection Officer**, if one has been designated one in accordance with Article 37 of the General Data Protection Regulation.

14. Register of categories of processing activities

The Data Processor maintains a written register of all categories of processing activities performed on behalf of the Data Controller including:

- the name and contact details of the Data Controller on whose behalf it is acting, any Data Processors and, where applicable, the Data Protection Officer;

- the categories of processing performed on behalf of the Data Controller;

- where appropriate, transfers of Personal Data to a third country or to an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in Article 49(1), second paragraph of the General Data Protection Regulation, documents proving the existence of appropriate safeguards;

- to the extent possible, a general description of the technical and organizational security measures, including, inter alia, as appropriate:

    - pseudonymisation and encryption of Personal Data;
    - measures to ensure the ongoing confidentiality, integrity, availability and resilience of treatment systems and services;
    - measures to timely restore the availability of and access to Personal Data in the event of a physical or technical incident;

- a procedure to test, analyse and regularly evaluate the effectiveness of technical and organizational measures to ensure secure processing.

15. Documents

The Data Processor provides the Data Controller with the necessary documentation to demonstrate compliance with its obligations and to enable audits and inspections to be carried out by the Data Controller or other auditor engaged by the Data Controller and contribute to these audits.

Section IV. Obligations of the Data Controller vis-à-vis the Data Processor

The Data Controller agrees to:

1. provide the Data Processor with the data referred to in Section II of these clauses,

2. document in writing any instructions regarding the data processing by the Data Processor,

3. ensure, in advance and throughout the duration of the processing, compliance with the obligations provided by the General Data Protection Regulation by the Data Processor,

4. supervise processing, including conducting audits and inspections with the Data Processor.