Personal data processing documentation

I. Quality Charter

TEHTRIS undertakes to comply with the Quality Charter, which guarantees the quality of its services in all areas of the TEHTRIS Service that are not provided free of charge or offered.

1. *Availability*

TEHTRIS undertakes to implement internal controls to ensure that the User can access and use the TEHTRIS Service in accordance with the terms and conditions set forth in the Agreement. In particular, TEHTRIS has implemented redundant systems to ensure that service is provided with minimum risk of interruption. TEHTRIS shall ensure response times based on the items set forth in the Agreement, with respect to the Appliances at the User's premises, the Users and the TEHTRIS datacenter located in France. In the event of an outage, TEHTRIS shall provide an availability report to verify the parameters defined in this Charter.

In particular, TEHTRIS uses the following technologies: dual power supplies, dual inverters, dual network connections at least Gigabit, dual switches, dual HSRP routing and dual physical links to the Internet

2. *Integrity*

From the point of view of the development and testing of the TEHTRIS Solutions prior to their use in production, TEHTRIS undertakes to implement effective controls to provide reasonable assurance that the applications made available to the User process the Data entrusted to them without risk of omission, alteration, distortion or any other form of anomaly that could adversely affect the integrity of the results obtained from these applications.

3. *TEHTRIS Staff*

TEHTRIS uses only personnel who have a contractual relationship with TEHTRIS. TEHTRIS staff are subject to confidentiality obligations and to the signature of the TEHTRIS ethics and IT charters. No member of TEHTRIS' staff is registered in bulletin no. 3 of the criminal record.

4. *Security and privacy*

TEHTRIS shall endeavor to secure access to and use of the TEHTRIS Service, taking into account the threats, in accordance with industry practice and the state of the art. TEHTRIS regularly conducts penetration tests against its own facilities and tools to check for security vulnerabilities. These tests are regularly re-run after each modification requiring the revalidation of the complete security cycle.

TEHTRIS has implemented effective controls to protect against unauthorized physical and electronic access to TEHTRIS' operating systems and applications, as well as Users' confidential information, to provide reasonable assurance that access to Client systems and data is limited to authorized individuals and that confidential information is protected from improper use.

TEHTRIS has set up a daily data backup in the TEHTRIS datacenter. The backups are kept for 14 consecutive days. The data backed up are the following: complete operating systems, and all associated data, used for the User in the TEHTRIS datacenter. The time required to restore the backups will depend on the performance of the host and the size of the data to be restored and may be several days in the most complex cases. All data backups are protected by cryptographic means. On optional request, the media can be stored in two separate locations, which will serve as an additional quote. TEHTRIS provides, as part of an obligation of means, a business recovery plan. Any request for additional commitment will be subject to additional billing and contractual conditions.

User Data is protected by cryptographic means in the TEHTRIS Appliances hosted at the User's premises, and in the TEHTRIS datacenter that centralizes the results of TEHTRIS Solutions for the User. The encryption keys are protected and are not present in the operating systems that will use them. They are securely distributed at the time of startup of the operating systems hosting the TEHTRIS Solutions. If these keys are not retrievable, for security reasons or network concerns, the Data on the hard disk is not accessible by the operating systems. When operating systems are running, the Data remains permanently encrypted in all areas using non-volatile memory.

a. *Physical security*

The TEHTRIS main building is equipped with physical security with biometric fingerprint authentication for authorized personnel.

The telecom room used for the link with the operator has a reinforced physical security limiting the possibility to enter it (armored door, etc.). In particular, it is electronically monitored with a real-time alert system available 24 hours a day, 365 days a year in case of physical intrusion.

TEHTRIS' premises do not contain any unencrypted persistent Data that is linked to the TEHTRIS Service or the User. Any theft of physical disks would result in the inability to read the associated Data. User Data used by the TEHTRIS Service is not stored on TEHTRIS' premises. It is stored in the datacenters of the TEHTRIS datacenter host. Physical intrusion into TEHTRIS's premises shall not result in theft with the possibility of reading or using the User Data present in the TEHTRIS datacenter.

TEHTRIS premises are protected 24/7/365 by a reinforced physical surveillance system (sensors, detections, video surveillance, etc.).

Access to TEHTRIS premises is limited to TEHTRIS staff. Trainees or non-CDI employees work in physically separate rooms and on physically separate networks. Meetings with external personnel are held in rooms adjacent to TEHTRIS. External companies (maintenance and cleaning) may not work on TEHTRIS premises unless they are physically supervised directly and locally by TEHTRIS.

TEHTRIS does not print sensitive documents for security reasons. The working documents that are nevertheless printed, are then destroyed when they are no longer used, with a shredder (confetti with cross-cutting guaranteeing a level of security adapted to confidential documents), before being managed as waste. The main building of TEHTRIS has been certified to the ISO 14001 standard.

b. *Logical security*

All hard drives of TEHTRIS Appliances at the User's premises or in the TEHTRIS datacenter (which are used in servers) are encrypted via FDE (Full Disk Encryption) with keys that are stored off-site in a restricted, protected and encrypted space.

All hard drives on TEHTRIS workstations (which are used to remotely administer the TEHTRIS Service) are encrypted via FDE. Workstations with elevated privileges are physically protected and inaccessible outside of business hours.

All system authentications are performed by using a crypto-processor in a French branded smart card, with a PIN code typed on an external French branded reader, and/or by an ANSSI certified external key.

All operating systems used in TEHTRIS Appliances at the User's site or in the TEHTRIS Datacenter are protected by secure Linux kernels, modified and compiled by TEHTRIS, with the use of advanced security technologies, including for example: RBAC integration in the kernel with role assignment and security policies for all processes; technologies against overflow attacks; special protections against Data leakage in memory

Applications hosted in TEHTRIS Appliances at the User's location or in the TEHTRIS Datacenter, built by TEHTRIS in order to provide the TEHTRIS Service, may use technologies such as obfuscation, encryption and anti-reverse engineering, in order to limit and slow down attempts to recover functionality.

All communications related to the TEHTRIS Service are encrypted between TEHTRIS workstations and the TEHTRIS Datacenter. All communications between TEHTRIS Appliances are encrypted including in the TEHTRIS Datacenter. All communications between TEHTRIS employees regarding the Agreement are encrypted (email, instant messaging).

TEHTRIS' internal network access security contains scalable modules to combat physical and logical intrusion threats, for example: authentication on the network with 802.1X; technologies against network attacks, such as DHCP attacks, ARP spoofing attacks, IP spoofing attacks, etc. TEHTRIS employees do not have any access to the TEHTRIS internal network from a remote location, as the network behaves like a diode with respect to the Internet.

Access to the TEHTRIS datacenter infrastructure is protected by: (i) identity restrictions: strong authentication dedicated to each employee based on physical tokens with French-branded crypto-processors and physical protection; (ii) time restrictions: with limitations on hours and days based on roles; (iii) geographic restrictions: with limitation to known areas defined as work source; (iv) network restrictions: with firewalls that are designed, installed, controlled and maintained solely by TEHTRIS from end to end; (v) DDOS restrictions: with the use of anti-DDOS technologies at the entrance to the TEHTRIS Datacenter; (vi) application restrictions: with the use of certificates to access application areas like the TEHTRIS Console.

All TEHTRIS Data in local or cloud areas is on encrypted media.

5. *TEHTRIS Datacenter Hosting*

The access provider and provider of the cloud hosting used by TEHTRIS is the company "OVH". The guarantees offered by OVH for the TEHTRIS Datacenter are applied to the Agreement. The certifications obtained by OVH, relating to IT security and operational safety of the security standards for the hosting of the TEHTRIS Datacenter are as follows: PCI-DSS level 1; ISO/IEC 27001:2005; SOC 1 type II (SSAE x 2 type II).

a. Physical security of the data centers that host the TEHTRIS Datacenter

Access to the compound is strictly monitored with fences and barbed wire. A video surveillance and motion detection system also operates continuously. Activity in the data centers and outside the buildings is monitored and recorded on secure servers, while surveillance teams are on call 24/7.

In order to control and monitor access to the facility, strict security procedures are in place. Each member of staff is equipped with a personal RFID badge to which access rights are assigned. These are regularly reviewed, depending on the duties of each employee. To gain access to the premises, each employee must first submit his or her badge for verification and then pass through a secure airlock.

Inside, the data centers benefit from even greater protection, since only authorized personnel can enter them. The hosting company is the sole operator of its facilities. Each room in each datacenter is equipped with a fire detection and extinguishing system and fire doors. The host respects the APSAD R4 rule for the installation of portable and mobile fire extinguishers, and has the N4 certificate of compliance for all its datacenters.

b. Logical security of the datacenters hosting the TEHTRIS datacenter

The host deploys its fiber optic network throughout the world. The equipment is chosen for its performance, then installed and maintained by the hosting company's engineering teams. The host has also chosen to build its network in a totally redundant way: several security loops have been put in place to eliminate any risk of unavailability. This multiplicity of links allows the data to take the shortest route and therefore to display minimum latency.

This proprietary network delivers a high quality of service with a bandwidth of 3Tbps in Europe, around 8000Gbps in North America, and a connection to 33 peering points on 3 continents.

A human presence is ensured 24/7/365 in the data centers by the teams of the host, in order to ensure a permanent maintenance. In the event of a technical incident, their reaction is immediate so that the servers are restored as soon as possible.

The servers used by TEHTRIS are also equipped with a dual power supply and a dual network card: the infrastructure is thus redundant from end to end. The data centers are powered by two independent power supplies and are also equipped with inverters and generators with a 48-hour autonomy in case of a power failure. The hosting provider integrates protection against all types of DDoS attacks and has set up three anti-DDoS infrastructures of 160 Gbps each in the data centers used by TEHTRIS, to be able to mitigate up to 480 Gbps, 24 hours a day, 7 days a week.

A double authentication process secures the connection to the administration tools of the hosting company, with OTP (One Time Password) options in addition to the traditional login - password combination. This OTP is a randomly generated one-time password. Each time a connection is attempted, it is sent by SMS or generated in separate physical tokens, and it is necessary for the finalization of authentications.

II. Personal data's processing

In this appendix:

- the terms personal data and controller have the same definition as in Article 4 of the GDPR;
- TEHTRIS is a subcontractor within the meaning of the said Article 4 ;
- The data controller is the User of the TEHTRIS Service.

1. *TEHTRIS' Obligations to the data controller*

In this regard, TEHTRIS undertakes to:

- To cooperate with and assist the data controller in fulfilling its obligations,
- Process the data controller's personal data only for the purposes for which they are processed as described above, process them only in accordance with the data controller's written instructions and refrain from any personal or commercial use,
- If TEHTRIS considers that an instruction constitutes a violation of the applicable regulations on the protection of personal data, it shall immediately inform the controller. TEHTRIS reserves the right not to carry out any unlawful instruction of the controller, without any liability on its part,
- Ensure the confidentiality of the personal data processed under the Agreement,
- Ensure that persons authorized to handle personal data are subject to a duty of confidentiality,
- Consider the principles of personal data protection by design and by default,
- Comply with an internal security program in accordance with the ISO/IEC 27001 Standard or its equivalent as agreed between the Parties including the controls of ISO/IEC 27002,
- To assist the data controller in carrying out impact analyses relating to the protection of personal data and, where appropriate, in carrying out the prior consultation with the supervisory authority,
- Refrain from using or allowing or facilitating the use by third parties, on the part of a subcontractor or a person acting under the authority or on behalf of TEHTRIS, for purposes other than the performance of the services, as well as from any use or processing or any other operation or exploitation without the prior authorization of the controller.

2. *Data controller obligations to TEHTRIS*

The data controller undertakes to TEHTRIS to:

- Provide TEHTRIS with the personal data referred to in this Section,
- Document in writing any instructions regarding the processing of personal data performed by TEHTRIS,
- To ensure that the applicable obligations regarding the protection of personal data are respected throughout the processing,
- Provide TEHTRIS with the contact details of its representative and, if applicable, of its Data Protection Officer.

3. *Subcontractor of personal data processing*

TEHTRIS undertakes to inform the data controller in advance of any subcontracting operation involving the processing of personal data.

TEHTRIS undertakes to inform the data controller of the location of personal data processing sites.

TEHTRIS undertakes to impose on its subcontractor all necessary obligations, at least equivalent to those provided for in this Appendix and the provisions relating to security, to ensure that the confidentiality, security and integrity of the personal data are respected, and that the said data cannot be transferred or leased to a third party, whether free of charge or not, or used for purposes other than those defined in the Agreement, and shall ensure that the said service provider(s) or subcontractor(s) comply with their obligations.

4. *Communication of personal data to third parties*

The personal data shall not be disclosed to any third party, including TEHTRIS' subcontractor, except as provided in the Agreement or as required by law or regulation. TEHTRIS shall put in place procedures to ensure that any third parties it authorizes to access the personal data respect and maintain the confidentiality and security of the personal data.

5. *Application of the European regulation regarding data transfers outside the European Union*

TEHTRIS undertakes to use exclusively means of processing Personal data located in the territory of a member country of the European Economic Area ("EEA") and/or in a country recognized as adequate by the European Commission. TEHTRIS undertakes not to disclose or transfer personal data, even for transit purposes or by means of remote access, to any third party or subcontractor operating in a country outside the EEA. TEHTRIS shall ensure that no personal data of the controller is transferred outside the EEA by its own subcontractor and by persons acting under the authority or on behalf of TEHTRIS. To the extent strictly necessary for the performance of the Agreement and subject to the consent of the data controller, TEHTRIS may use processing facilities located in a country that does not provide an adequate level of protection within the meaning of the GDPR, in the following case: TEHTRIS, has previously entered into a data transfer agreement with the data controller in accordance with the terms and conditions set out in the European Commission's standard contractual clauses for the transfer of personal data to processors established in third countries.

6. *Right of data subjects*

It is the responsibility of the data controller to provide information to data subjects of the processing operations at the time of collection of the personal data. To the extent possible, TEHTRIS shall assist the data controller in fulfilling its obligation to respond to requests to exercise the rights of data subjects with respect to the processing of Personal data performed by TEHTRIS on behalf of the data controller. However, as the processing performed by TEHTRIS is based on the legitimate interest pursued by the controller, the exercise of certain rights of data subjects is limited by the GDPR.

If a data subject should contact TEHTRIS directly to exercise his or her right of access, rectification, deletion and/or objection, TEHTRIS shall forward the request directly to the data controller.

7. *Personal data breaches' notification*

TEHTRIS shall notify the data controller of any breach of the personal data as soon as possible by means of a signed email. As an exception to the above, if TEHTRIS is unable to provide all the information available to it at the same time, the information may be provided in a staggered manner without undue delay.

This notification shall be accompanied by any useful documentation to enable the data controller, if necessary, to notify the breach to the competent supervisory authority within seventy-two (72) hours at the latest after becoming aware of it, unless the breach in question is not likely to give rise to a risk to the rights and freedoms of the data subjects. In general, it is the responsibility of the data controller to communicate directly to the data subjects the violation of the personal Data, when it is likely to generate a high risk for the rights and freedoms of the data subjects.

TEHTRIS undertakes to carry out any useful investigation into breaches of the aforementioned protection rules and/or any threats in order to remedy such breaches and/or threats and prevent their recurrence in the future.

The relevant documentation will be provided to the data controller by means of a written report by TEHTRIS consisting of:

- The nature of the failures to comply with the rules for the protection of personal data as defined in the Contract,
- A description of the corrective actions taken or proposed to be taken by TEHTRIS to remedy the deficiencies identified, or where appropriate, measures to mitigate any adverse consequences,
- The name and contact details of the Data Protection Officer or other point of contact from whom further information can be obtained.

TEHTRIS is aware that any failure to comply with the rules for the protection of personal data may impose obligations on the data controller, in particular with regard to notification of data subjects and the authorities.

8. *Personal data' Use*

The controller shall be responsible for the use of the TEHTRIS Service in accordance with the provisions of the Agreement. The data controller shall indemnify TEHTRIS on first demand against any loss resulting from a third party challenging it for a breach of this warranty.

The data controller shall be solely responsible for the quality, lawfulness and relevance of the personal data and their content, which it transmits for use of the TEHTRIS Service. He also warrants that he holds the Intellectual Property Rights entitling him to use the Data and content. Accordingly, TEHTRIS shall not be liable for any failure of the Data and/or content to comply with laws and regulations, public policy or the needs of the controller.

More generally, the controller is solely responsible for the content and messages broadcast and/or downloaded via the Service. The controller remains the sole owner of the Data constituting the content of the Solutions. Malicious or suspicious items uploaded to the Solutions shall become the sole Property of TEHTRIS under the conditions set forth in Article - Property.

9. *Personal Data' Security*

Each of the Parties undertakes to implement the appropriate technical means to ensure the security of the personal data.

TEHTRIS undertakes to implement technical and organizational measures to prevent any access to or fraudulent use of the personal data and to prevent any loss, alteration or destruction of the personal data, in particular all of the undertakings set out in the TEHTRIS Quality Charter, attached to this Agreement.

10. *Description of the processing carried out on behalf of the data controller*

DPO contact details
TEHTRIS : Florine Belle - privacy@tehtris.com , TEHTRIS - Service DPO - 5, allée des lumières, Cité de la photonique, 33600, PESSAC, France
Purposes

Personal data might be collected from the security logs and recorded to organize the processing for incident monitoring. The purposes are to ensure the management and performance of the incident and event security monitoring system as well as the management of authentication accounts to the TEHTRIS XDR Platform and the continuous improvement of TEHTRIS Services (necessary to ensure the security of the IT infrastructure and the information of the controller).

Type of the processing

- Collection; Storage; Analysis; Removal

Persons concerned categories

- Any person with access to the data controller's information system on which the TEHTRIS Service is deployed (employees, service providers, customers, visitors, etc.).
- The controller's IT team ("User") accessing the XDR Platform.

Data category

TEHTRIS Solutions do not allow to open or have access to a client file of type .doc, .pdf, .xls. Only the technical security data are transmitted.
No "sensitive" data by default.

Personal data ***(applicable according to the services subscribed)***

TEHTRIS XDR Platform	For **authentication of User accounts** to the XDR Platform: User's first and last name, business email address and phone number, account login log. For **security incident tickets**: machine username, machine name, IP address, suspected log(s).
EDR, EPP, SIEM	For the **logs**: user name of the machine, name of the machine, IP address, paths and program indicating the name of a folder or the name of a file. For **Alerts**: machine user name, machine name, IP address, paths and program indicating the name of a folder or the name of a file.
MTD	**Device data**: device manufacturer and model, unique device identifier (UID), and MDM if applicable; enrollment date; last login date; device name entered by the user; number of CPUs, amount of RAM, device version, amount of total and available memory (the space on the phone's "disk"). **Device configuration data**, such as whether the device allows root access or whether its hardware restrictions have been removed (jailbreak). **Firmware/operating system data**, including the name of the manufacturer and model of the device, certain technical parameters of the device (including display size and firmware version), type and version of the device's operating system. **Application data**: including the metadata of all applications installed on your mobile device (including, but not limited to, application names and versions). Alerts reported by the application and their criticality level. The number of malware-type applications present on the devices. In some cases, we may also collect a copy of the application without the user data. **Analytics data**: used to analyze product performance on your device. **Identification data**: such as business email address for registration purposes, if applicable, or for analysis of a possible compromise, i.e. if the address is not part of a database of leaked identifiers. **Geolocation Data**: Geolocation only when activated by the End User and/or Employer where applicable; last known locations of the Device. **Network Data**: Metadata about the networks to which the Device connects (including, but not limited to, the SSID of the network or the unique MAC/BSSID of the network equipment) and the IP address; Name of the Wi-Fi network to which the Device is connected to identify whether the Wi-Fi network is at risk. **Web content data**: URLs and domain names associated with malicious content or content that requires further analysis. TEHTRIS MTD only collects metadata about the applications installed on the device and/or the application itself. TEHTRIS MTD does not collect the user data entered in these applications and therefore does not read or examine emails, SMS, photos or videos.
TEHTRIS Academy	Authentication of TEHTRIS Academy accounts: first name, last name, email address, account log.
TEHTRIS CTI	Suspicious file sent to TEHTRIS CTI for dynamic analysis that may contain personal data (for example, in the case of a script, properties such as the script's author)

Storage period

TEHTRIS XDR PLATFORM	Users' identifiers: during the contractual relationship or as soon as a User is changed or deleted. Incident tickets: the time of the contractual relationship.
EDR, EPP, SIEM	For Logs and Alerts: up to the storage capacity of the Appliances of the Solutions subscribed to and for a maximum of six (6) months, and for maximum three (3) months period for OPTIMUS offer.
MTD	Same as TEHTRIS EDR, EPP, SIEM, except if the Employer has authorized the capture of geolocation data, this data will only be kept for a maximum of 2 months.
TEHTRIS Academy	Username: during the contractual relationship or upon change/deletion of a User.
TEHTRIS CERT	The Data collected during a TEHTRIS CERT service are kept for the duration of the TEHTRIS CERT service, for a maximum of six (6) months from the day of collection.
TEHTRIS CTI	Personal data that may be contained in a TEHTRIS CTI analysis is kept for up to six (6) months after the last occurrence on the User's park and/or after its last consultation on TEHTRIS CTI.

Storage location

OVH Cloud - 2 rue Kellermann - 59100 Roubaix - France	**European Union** certifications obtained by OVH, relating to computer security and safety of operation of security standards for hosting the TEHTRIS Datacenter are: PCI-DSS level 1; ISO/IEC 27001:2005 ; SOC 1 type II (SSAE 16 and ISAE 3402), SOC 2 type II.
Twilio[1] – United States	**United States** certifications obtained by Twilio: ISO/IEC 27001 ISO/IEC 27017 & 27018 SOC 2 Type II ; PCI DSS Level 1 (https://www.twilio.com/legal/security-overview)

List of subcontractors

- OVHCloud, for hosting the TEHTRIS Service and data storage. OVHCloud does not have access to the data of the controller
- Twilio, only for professional phone numbers used for secure dual authentication to the TEHTRIS XDR Platform and the Alerting - notification option

Transfer outside the EEA

Yes, to Twilio, only for business phone numbers used for secure dual authentication to the TEHTRIS XDR Platform and Alerting - notification option. TEHTRIS will cease this transfer once Twilio allows the data to be hosted in Europe[2].

Security measures

[1] https://www.twilio.com/legal/privacy

[2] https://www.twilio.com/blog/expanded-data-protection-options-eu-schrems-ii

See TEHTRIS Quality Charter attached to the Agreement.