wizville

# Data Processing Policy

Applicable from November 1st, 2022

# Table des matières

# 1. Scope of the data processing policy

The present data processing policy applies to any data that are processed by **WIZVILLE** on behalf of its clients; **WIZVILLE** is a simplified joint stock company with a share capital of € 936,90, whose registered office is located at 51, rue de Chabrol – 75010 Paris, registered in the Business and Trade Registry under unique identification number 751 226 606 R.C.S. PARIS.

It applies to all contracts (hereinafter referred to as the "Contract") relating to the **WIZVILLE** software solution (hereinafter referred to as the "Solution") entered into by and between **WIZVILLE** and the client (hereinafter referred to as the "Client"), involving the processing of data, especially the processing of the personal data of the Client or its own clients (hereinafter referred to as the "End Clients").

In the context of their contractual relations, the parties undertake to comply with any valid regulations applicable to the processing of personal data and, not least, EU Regulation no. 2016/679 of the European Parliament and of the Council, of 27 April 2016, applicable as of 25 May 2018 (hereinafter referred to as the "GDPR"), and French Law n° 78-17 dated January 6 1978.

In this capacity, **WIZVILLE** is acting in its capacity as a processor of the Client within the meaning of the GDPR.

The Client expressly authorises **WIZVILLE**, acting in its capacity as processor, to process, on its behalf, any personal data required for the use of the Solution.

The data are processed for the purposes of monitoring the satisfaction of any End Clients who have agreed to receive marketing correspondence by email, in the context of their use of the products and services of the Client.

The categories of data subjects are as follows:

- Any End Clients or natural persons who have used the products and services of the Client, after agreeing to receive marketing correspondence by email, SMS, web or mobile push notifications, and after completing a satisfaction questionnaire;
- Any workers of the Client with access to the Solution.

**WIZVILLE** undertakes to:

- Process the data exclusively for the purpose(s) established above,
- Process the data in accordance with the instructions of the Client. If **WIZVILLE** deems that an instruction violates the GDPR or any other provision of EU law or the law of any Member State relating to the protection of personal data, it shall immediately inform the controller. Moreover, if **WIZVILLE** is required to transfer any data to a third country, by virtue of EU law or the law of any Member State to which it is subject, it shall inform the Client of this legal obligation prior to the processing operation, unless the corresponding law precludes any such disclosure for important

reasons of public interest.
- Guarantee the confidentiality of the data processed under the Contract.
- Make sure that any person authorized to process the personal data under the Contract:
    - Undertakes to respect the confidentiality or is bound by an appropriate legal obligation of confidentiality,
    - Receives the necessary data protection training,
- With regard to his/her tools, products, applications or services, takes into account data protection principles from conception and default data protection principles.

**The Client undertakes to:**

- Obtain the consent of End Clients in relation to the use of their personal data and the corresponding processing in the context of the use of the Solution,
- Formalize in writing any instruction issued to **WIZVILLE** concerning the processing of any personal data entrusted to the latter,
- Inform **WIZVILLE** of any request of an End Client relating to the processing of its personal data at the earliest possible time.

**WIZVILLE** reserves the right to make any changes that it deems useful and necessary to the present data processing policy, not least in view of any legal, case-law or technical developments.

If the present data processing policy is modified, the Client shall be informed at least thirty (30) days before the entry into force of the modifications.

## 2. Categories of data collected

The use of the Solution involves the collection and processing of the data of the Client and/or the following End Clients:

| Categories | Types |
|---|---|
| Direct personal data | Surname |
| | First name |
| | E-mail address |
| | Telephone numbers (landline or mobile) |
| | Client number |
| | Loyalty card number |
| Indirect personal data | Civil status |
| | Client category (VIP, New, etc.) |
| | Transaction date |

| | |
|---|---|
| Transactional Data | Transaction amount |
| | Transaction type (purchase, service, delivery, call, contact, visit, etc.) |
| | Goods or services concerned by the transactions and all their characteristics |
| | Agency, point of sale or point of contact related to the transaction |
| | Unique transaction number |
| Personal Data of the Client's workers | Colleague's first name |
| | Colleague's surname |
| | Colleague's e-mail |
| | Colleague's role |
| Web browsing data of Client's workers | Internet browser used |
| | Operating system |
| | Number of pages visited |
| | Pages visited |
| | Number of visits |
| | Type of device used |

## 3. Procedures and timeframes for the storage of the collected data

The data collected and processed by **WIZVILLE** are stored according to the following procedures and timeframes:

## 4. Data relating to End Clients

- Direct Personal Data, Indirect Personal Data and Transactional Data relating to an End Client are stored for a period of twenty-four (24) months as of their disclosure by the Client; any new disclosure of data by the Client relating to an End Client within this period shall mark the beginning of a new period of twenty-four (24) months prior to the implementation of data anonymization measures.
- If the Client does not disclose any new data relating to the End Client within the period of twenty-four (24) months, as indicated above, **WIZVILLE** implements an irreversible anonymization measure which consists of:
    - Deleting the Direct Personal Data of the End Client from its databases;
    - Exclusively storing, without any time limit, the Indirect Personal Data and the Transactional Data which means that **WIZVILLE** is unable to identify the End Client

concerned.

## 5. Personal Data of the Client's workers

- The Personal Data of the Client's workers and web browsing Data are stored for the duration of the Contract;
- If the Contract is terminated or expires, the Personal Data of the Client's workers and web browsing Data are deleted within a period of ninety (90) calendar days.

## 6. Assistance of the Client for the purposes of exercising the rights of the End Clients

**WIZVILLE** undertakes to assist the Client for the purposes of exercising the rights of the End Clients, subject to the following terms and conditions:

| Rights of the End Client | Timeframes |
|---|---|
| Access rights | Contact via email at data@wizville.fr |
| | Extraction of data in CSV format within 48 hours |
| Right to rectification | Contact via email at data@wizville.fr |
| | Modification of data within 48 hours |
| Right to be forgotten and to erasure | Contact via email at data@wizville.fr |
| | Deletion of data from the active database within 48 hours |
| | Deletion of saved and archived data within 90 days |
| Right to restriction of processing | Contact via email at data@wizville.fr |
| | Restriction of processing of data within 7 days |
| Right to notification | Contact via email at data@wizville.fr |
| | Notification to third parties within 48 hours |
| | Confirmation to the Client within 72 hours |
| Right to data portability | Contact via email at data@wizville.fr |
| | Extraction of data in CSV format within 5 days |
| | Disclosure of data in CSV format within 7 days |

Unless contractually established otherwise, if the requests to exercise the rights of the Client's End Clients exceed 10 requests per calendar month, any additional request is invoiced to the Client on the basis of applicable pricing terms.

# 7. Data backup and recovery

The Customer's data, including the personal data of the End Customers, is hosted by IGUANE SOLUTIONS, which provides:

- A server monitoring service;
- Notification in case of incident;
- A redundant backup of data on a separate server every **24 hours** with access to previous backups in case of difficulty over a period of 30 days;
- Data access recovery within 4 hours maximum from Monday to Friday during office hours UTC Paris, France, and within 6 hours maximum on weekends, nights and holidays, except in cases of force majeure.

If the active server is unavailable, a backup server is activated within a period of **4 hours** except in a case of force majeure.

Moreover, some documentary data may be hosted on the Google Cloud service (documentary host service provider - PDF, Excel files and images sent to and generated by the Solution).

# 8. Data security

**WIZVILLE** guarantees the security of any data disclosed by the Client by implementing the following measures:

## A. Physical security

The Customer's data is hosted on a remote server managed by the company IGUANE SOLUTIONS and hosted by the company SCALEWAY (ILIAD), in a secure data center (DC3), located in France, in Vitry-sur-Seine. These data may be hosted in other data centers operated by IGUANE SOLUTIONS and located in France.

**IGUANE SOLUTIONS** guarantees the physical security of servers 24/7.

Access to data centers is strictly controlled and monitored.

**Security is managed by:**

- A permanent presence of security guards (24/7);
- Access limited exclusively to the employees of IGUANE SOLUTIONS or **WIZVILLE** who are required to physically access the IT servers;
- Access controlled by passes and biometric scanners;
- 24/7 video surveillance;
- Rooms equipped with smoke and humidity detection systems;
- Technical staff present 24/7.

**The data center (DC3) has the following certifications:**

- **ISO 27001** certification, guaranteeing the effective implementation of an information security management system (risk management and information security management);
- **ISO 50001** certification (ENMS609673), guaranteeing the effective implementation of an optimized energy management system;
- **TIER III** Design certification issued by Uptime Institute (2014), ensuring that the physical topology of the data center infrastructure avoids the risk of shortage or weak links;
- **PCI-DSS** standard (in the process of being acquired), to ensure the compliance of network infrastructures with the PCI DSS security standard for data security for the use of payment cards.
- **HADS** accreditation: The HADS accreditation, "Hébergeur Agréé de Données de Santé" (Agremented Health Data Hoster) , has been created to guarantee the confidentiality, integrity, availability and traceability of this sensitive information. This approval implies the respect of numerous requirements at both the technical and the organizational level.

The documentary data hosted on Google Cloud depends on data centers operated by GOOGLE IRELAND LIMITED and located in the EU, outside of France. On the date hereof, these data centers are located in the following cities and countries:

- St. Ghislain, Belgium
- London, UK
- Frankfurt, Germany
- Eemshaven, Netherlands

The data may be hosted in other data centers operated by **GOOGLE IRELAND LIMITED** located in the EU.

## B. Server security

Access to services is secured by robust authentication processes based on a strict policy of password management and the deployment of two-factor authentication measures (private and secure SSH keys).

The servers used for the Solution are not directly accessible via the internet.

Only authorized staff members of **WIZVILLE** and the Client's workers have access to the data.

Data is transferred from the Client to **WIZVILLE** by means of an sFTP server which involves the encryption of data interchanges, with a username and password.

Any data transfers from **WIZVILLE** to its processors are carried out by means of HTTPs protocol.

The Client's data is never stored on peripheral devices such as USB, CD, DVD or any other kind of detachable storage device.

The encryption for the disk is activated on all workstations, portable computers and mobile devices used by the staff of **WIZVILLE**, with identification by username and password.

### C. Client Security

Access to the Solution is secure in HTTPs with a username and a password.

The passwords of Client's workers are created by means of an e-mail sent directly to the e-mail addresses provided by the Client.

The Client's workers are able to create passwords with minimum strength criteria.

Client connections using its username/password are monitored and are time-stamped and recorded.

The Solution provides precise user right management functionalities which guarantee that the Client's workers may only access the data which they are entitled to access.

### D. Protection against attacks, IT viruses and malware

Access to servers is protected by a fail2ban device in the event of repeated attempts to access the servers without the adapted access.

**WIZVILLE** also uses security devices such as firewalls etc. The firewall filters incoming traffic, thereby guaranteeing the security of the perimeter and preventing unauthorised access from the internet. It also integrates anti-intrusion mechanisms.

The network and functioning of the Solution are monitored at all times. Surveillance includes real-time alerts in the event of an attempted intrusion.

## 9. Incident management

The incident management procedure of **WIZVILLE** includes the following stages:

1. **Alerts:** the support teams of **WIZVILLE** are informed of the incident either by the server surveillance tools, by the Solution surveillance tools or by the Client's workers.

2. **Identification:** the support teams of **WIZVILLE** determine the conditions under which the incident has taken place and its impact on the Solution, the servers and the data. If necessary, they attempt to reproduce the incident in a test environment. When an incident is detected by the Client, it shall provide **WIZVILLE** with all the data at its disposal with a view to allowing the incident to be reproduced.

3. **Isolation:** the support teams make sure that the impact of the incident is limited by confining it and protecting the data.

4. **Backup:** the support teams proceed with a backup operation to preserve evidence of the incident and its consequences for the investigation.

5. **Investigation:** the support teams investigate the incidents and verify the resources that have been stolen, altered or destroyed, as well as the duration of the incidents. This phase particularly makes it possible to qualify the severity of the incident and dismiss any anomalies that have no consequences.

6. **Treatment:** the support teams restore any affected systems or remove them. Verification tools are used to check that the incident renewal risk is limited or eradicated.

7. **Restoration:** the Solution, servers or data are restored and the integrity of the system is checked and tested.

8. **Reporting:** the support teams produce a comprehensive incident report, including the date and time of the incident, any information contained in the registers, systems or data affected. This report particularly includes the procedures used to resolve the incidents, the permanent or temporary nature of the procedures and the risk that the incident will reoccur.

9. **Improvement:** if necessary, the Solution is the subject of a documented update in order to stop the incident from reoccurring.

## 10. Security violation

**WIZVILLE** informs the Client of any data security violation within a period of 48 working hours after becoming aware of the incident and by email.

This notification is accompanied by any useful documentation to allow the processor, if necessary, to notify this violation to the competent supervisory authority.

The notification contains the following information:

- The description of the nature of the data violation including, where possible, the categories and approximate number of data subjects concerned by the violation and the categories and approximate number of data records concerned;
- The name and contact details of the data protection officer or any other point of contact from whom additional information may be obtained;
- The description of the probable consequences of the data violation;
- The description of the measures taken or those to be implemented with a view to resolving the

data violation, including, if necessary, any measures to mitigate any adverse consequences.

## 11. Return of data

Upon the expiration of the Contract, **WIZVILLE** returns the corresponding data to the Client within a period of thirty (30) days.

They are deleted from the active database within this same period.

They are deleted from the archived backups within a period of ninety (90) days.

The deletion of the backup data becomes irreversible by overwriting the disk sectors used.

Following the aforementioned periods, **WIZVILLE**:

- Proceeds with a data deletion test, to confirm that the deleted data may not be fully or partially reconstructed using a piece of data reconstruction software;
- Issues the Client with a written destruction certificate;
- Retains the details of the return and destruction operations, as well as any test reports which are registered and retained.

## 12. Data transfers outside of the EU

The Client's data are hosted in France and in the EU and are not transferred outside of the EU, unless a specific request is submitted by the Client and provided that any applicable rules, in accordance with the GDPR, are respected.

## 13. Outsourcing

On the date hereof, **WIZVILLE** engages the services of the following processors for the purposes of processing any data that are entrusted to it by the Client:

| Processors | Purpose |
|---|---|
| Sinch | E-mail & SMS delivery service provider |
| Iguane solutions | Server management provider |
| Scaleway (Online) | Data hosting provider |
| Google Cloud | Documentary data hosting |

In the event of a change of processor, **WIZVILLE** undertakes to previously inform the Client, specifying the outsourced processing activities, the identity and contact details of the processor and the outsourcing agreement dates.

The Client has a minimum period of thirty (30) days, from the receipt of this information, to submit any objections. This outsourcing may only take place if the Client has not submitted any objection within the established period.

The processor of **WIZVILLE** is required to fulfill the obligations of this instrument on behalf of and according to the instructions of the Client. **WIZVILLE** is responsible for ensuring that its processors are concerned by sufficient guarantees in terms of implementing appropriate technical and organisational measures such that the data are processed in a manner that meets the requirements of applicable legislation.

If a processor of **WIZVILLE** does not fulfill its data protection obligations, **WIZVILLE** is fully liable vis-à-vis the Client for the fulfillment of the corresponding obligations.

## 14. Data Protection Officer (DPO)

**WIZVILLE** has designated the following party as Data Protection Officer (DPO):

The legal firm **SMARTUP AVOCATS**, a limited liability company (sarl) with a share capital of €30,000, whose registered address is located at 3, rue Anatole de la Forge – 75017 Paris, registered in the Business and Trade Registry under unique identification no. 821 811 700 R.C.S. PARIS.

The Data Protection Officer may be contacted at the following address: contact@smartup-avocats.fr

## 15. Processing activity register

**WIZVILLE** states that it keeps a written record of all categories of processing activities carried out on behalf of the Client, including:

- The name and contact details of the controller on behalf of which it is acting,
- The categories of processing activities carried out on behalf of the Client,
- If previously authorized by the Client, any data transfers to a third country, including the identification of this third country and, in the event of the transfers referred to in Article 49, paragraph 1, section two of the GDPR, any documents which confirm the existence of appropriate guarantees;
- Where possible, a general description of any technical and organization security measures, including, as appropriate:
    - The pseudonymisation and encryption of personal data;
    - Any means by which it is possible to guarantee the constant confidentiality, integrity, availability and resilience of processing systems and services;
    - Any means by which it is possible to restore the availability of personal data and access to the same in a timely fashion, in the event of a physical or technical incident;
    - A procedure that seeks to test, analyze and regularly assess the efficiency of technical and organizational measures with a view to guaranteeing the security of the processing

operation.

# 16. Prior impact analysis procedure

At the request of the Client and subject to the approval by the latter of the applicable financial terms, **WIZVILLE** takes part in all prior impact analyses.

In the absence of a specific procedure of the Client, the procedure used by **WIZVILLE** includes the following stages:

## A. Study of the context

This phase involves identifying the corresponding personal data processing operations, by:

- Presenting an overview of the corresponding processing operation, its nature, its scope, its context, its purposes and its issues;
- Identifying the controller and any processors;
- Listing any standards that are applicable to the processing operation, useful or to be respected, especially any approved codes of conduct (Article 40 of the GDPR) and data protection certification (Article 42 of the GDPR);
- Defining and describing the scope in detail:
    - The personal data concerned, their recipients and retention periods;
    - A description of the processes and the data media for the whole life cycle of the data (from their collection to their erasure).

## B. Study of fundamental principles

This phase involves establishing compliance arrangements as regards principles of privacy protection, by:

- Assessing the measures which guarantee proportionality and the need for the processing, involving:
    - Explaining and justifying the choices made to comply with the following requirements:
        - **Purpose:** specific, explicit and legitimate (Article 5.1 (b) of the GDPR)
        - **Basis:** lawfulness of processing, prohibition on purpose diversion (Article 6 of the GDPR)
        - **Data minimisation:** adequate, relevant and limited (Article. 5.1 (c) of the GDPR);
        - **Quality of data:** accurate and up-to-date (Article 5.1 (d) of the GDPR);
        - **Retention period:** limited (Article 5.1 (e) of the GDPR).

- Checking that it is not convenient, or not possible, to improve the way in which each point is considered, explained and justified, in accordance with the GDPR;
- If necessary, reviewing their description or proposing additional measures.
- Assessing the measures used to protect the rights of data subjects, involving:
- Identifying or determining, and describing, the measures used (existing or considered) to comply with the following requirements (requiring an explanation about how they are expected to be

implemented):

- Informing of data subjects (fair and transparent processing, Article 12, 13 and 14 of the GDPR);
- Obtaining consent, if necessary: express, demonstrable, retractable (Article 7 and 8 of the GDPR);
- Exercise of the rights to access and portability (Article 15 and 20 of the GDPR);
- Exercise of the rights to rectification and erasure (Article 16 and 17 of the GDPR);
- Exercise of the rights to restriction of processing and opposition (Article 18 and 21 of the GDPR);
- Outsourced processing: identified and formalized by virtue of a contract (see Article 28 of the GDPR);
- Transfers: fulfillment of obligations concerning the transfer of data outside the EU (Article 44 to 49 of the GDPR).
- Checking that it is not convenient, or not possible, to improve each measure and its description, in accordance with the GDPR;
- If necessary, reviewing their description or proposing additional measures.

## C. Study of risks related to data security

Each phase involves identifying risks and their consequences in the field of data security and assessing any existing or considered security measures, with a view to gaining a good understanding of the measures that contribute to security, by:

- Establishing the types of risks by which the data may be concerned (unlawful access to data, unwanted modification of data, disappearance of data);
- Assessing how the vulnerabilities of data media might be exploited;
- Identifying any data that are likely to be compromised;
- Assessing the severity of the risk in view of its scope and the prejudicial nature of potential impacts;
- Estimating potential impacts on the privacy of data subjects and the use that may be made of the compromised data, involving:
  - Setting out potential impacts on the privacy of data subjects, in the event that they occurred;
  - Estimating their severity, especially according to the prejudicial nature of potential impacts and, if necessary, any measures that may modify them;
  - Identifying any threats to data media and risk sources that may be the cause thereof;
  - Estimating their likelihood, especially according to any data media vulnerabilities, capacities of risk sources to exploit them and measures that may modify them.
- Identifying or setting out any existing or considered measures (already engaged), which may be characterized in any of the following three ways:
  - Measures relating specifically to the data of the processing operations: encryption, anonymisation, compartmentalisation, access control, traceability, etc.;
  - General security measures of the system in which the processing operation takes place: security of exploitation, backups, equipment security, etc.;

    - Organizational measures (governance): policy, project management, staff management, incident and violation management, third-party relations, etc.
- Checking that it is not convenient, or not possible, to improve each measure and its description, in accordance with good security practices;
- If necessary, specifying their description or proposing additional measures;
- Determining whether the identified risks can be regarded as acceptable in view of any existing or considered measures;
- If not, proposing additional measures and re-assessing the level of each risk in consideration of the measures, with a view to determining residual risks.

## D. Validation of the Privacy Impact Assessment (PIA)

This phase makes it possible to determine whether or not to accept the PIA as regards the results of the study, by:

- Consolidating and conditioning the results of the study, which involves:
    - Producing a visual representation of the chosen measures to respect fundamental principles, according to their compliance with the GDPR;
    - Producing a visual representation of the chosen measures to contribute to data security, according to their compliance with good security practices;
    - Producing a visual cartography of residual risks according to their severity and likelihood
    - Producing an action plan based on any additional measures identified in the previous stages and, for each measure, determining at least the person responsible for its implementation, its cost (financial and/or in terms of load) and projected timeframe.

- Formalizing the consideration of stakeholders:
    - The advice of the Data Protection Officer (Article 35 (2) of the GDPR);
    - The opinion of data subjects or their representatives, if necessary (Article 35 (9) of the GDPR).
- Formally validating the PIA, by determining the acceptability of the chosen measures, residual risks and action plan, based on reasoned arguments, as regards the previously identified issues and the opinion of the stakeholders;
- Or, if applicable by executing the previous stages again to ensure that the PIA is able to be validated.