Privacy Policy

Introduction

This Privacy Policy (the "Policy") describes Brainsonic's practices, with respect to the privacy of its clients and/or users (the "User", or "you").

The purpose of this policy is to ensure the conformity of personal data processing and the respect of the concerned persons' rights. The legal reference of this policy are : the RGPD (General Regulation for Data Protection) and the French Data Protection Act (called « Loi Informatique et Libertés »). The notions used in this policy are used in accordance with their definition in the RGPD, in particular the notions of processing, personal data or data of a personal nature, etc.

Personal data

The categories of personal data that we may collect fairly and lawfully are as follows:

- First name and surname ;
- Professional e-mail address;
- Telephone number ;
- Business mailing address ;
- Your job title ;
- The name of the company you work for.

Use of personal data

We mainly use your personal data for the following purposes:

- In order to contact you regarding satisfaction surveys or market researches ;
- For commercial prospecting,
- In order to communicate informations, or to invite you to events ;
- For commercial exchanges.

Under no circumstances will the data collected by Brainsonic be yielded or sold to third parties. E-mail addresses will not be transmitted to third parties, including our partners, without the express consent of the concerned parties (opt-in). All our employees are subject to confidentiality clauses expressly stated in their employment contract.

Rights of the person concerned

In accordance with the regulations in force, collected data may be processed. Pursuant to the provisions of the « Loi Informatique et Libertés » of January 6, 1978, and the General Data Protection Regulations (GDPR), you have the right to access, oppose, correct, the right to portability and to delete all personal data which concerns you:

- Right of access. You may request an extract of the personal information stored and processed.

- Right of rectification. You can ask to modify erroneous information

- Right to forget. You can ask to delete one or more personal information.

- Right of opposition: This allows you to object to your data being used by an organization for a specific purpose. You must put forward "reasons relating to your particular situation", except in the case of commercial prospecting, to which you can object without any reason.

- Right to portability. You have a right of portability of your data. However, since the processed data are contact data or data replicated from customer's information systems, data portability is not necessary in case of a change to another similar service provider.

Brainsonic undertakes to respond as soon as possible (one month maximum by default, extended to 2 months in case of particular technical difficulties) to legitimate requests to exercise the aforementioned rights. For all these requests, you can contact us through the following email address: privacy@brainsonic.com.

For any request an identity verification will be carried out through a check of the ID card. Answers to the requests will be sent in electronic format

Justification for any denial of access will be indicated in the request log and that such denial will be traced back to the "client". Any disagreement will also be recorded in the request log and reported to the "client".

If you identify an error in this data or if you find it to be incomplete or ambiguous, you may also ask us to correct, complete or clarify it. For all these requests, you can contact us via the following email address: privacy@brainsonic.com.

For any request, please indicate your last name, first name, email adress, as well as the expected modification.

A review of the requests is carried out monthly by Brainsonic in order to verify that all requests have been resolved.

Storage and retention of your personal data

Your personal data is stored in our Microsoft Azure SaaS.

Your personal data will be stored in the most secure way possible, and only for the time necessary to achieve the processing's purpose. With this in mind, we take the appropriate physical, technical and organizational measures in order to prevent, as much as possible, any alteration or loss of your data or any unauthorized access to them.

Transfer of your personal data

The service's data is hosted within the European Union and cannot be transferred to countries outside the European Union.

For more information about transfers to non-European Union country or about the specific security measures which are applicable, you can contact us at: privacy@brainsonic.com.

Cookie Management

In order to optimize and improve the quality of the services that are offered to you and their adequacy with your expectations, Brainsonic is likely to use "cookies". When you acess Brainsonic's websites and pursue your navigation on it, you may agree to or configure the implementation and the use of cookies on your terminal. Doing so, you acknowledge that you have read the information provided to you

concerning the use of these cookies, and you acknowledge the means at your disposal to oppose them. Cookies are valid for at least the duration of the session and for a maximum period of 2 years. To learn more about the management of Cookies, please contact us at the following address: privacy@brainsonic.com.

The Brainsonic site may place cookies on your computer and use them to customize, secure and improve your experience on the website.

Publisher

The site www.brainsonic.com is published by Brainsonic SAS.

Hosting

The site brainsonic.com is hosted by Brainsonic SAS, via Microsoft Azure.

Data breach process and notification to authorities and individuals

In case of a personal data breach, Brainsonic has implemented, in accordance with the regulations, a process in order to notify the competent control authorities, as well as the data controller whenever required.

In the event a data breach has been established, any actual or suspected incident shall be reported immediately after the breach is perceived by our teams. Brainsonic, represented by its DPO, shall notify the customer (identified as the data controller) of the data breach before any public disclosure unless required by law. Brainsonic will then inform the CNIL within a maximum of 72 hours after the incident if it is certified. Brainsonic will inform about this breach by transmitting a "**Data breach notification**". If the impact on the concerned persons is certified as significant, Brainsonic also undertakes to notify these persons as well, and as soon as possible (customers, prospects, employees, staff representative bodies, or third parties).

Data retention and destruction policy

1. Purpose, Scope and Users

This policy defines the preservation periods required for specified categories of personal data and the minimum standards to be met regarding the destruction of hereinafter designated Brainsonic information.

This policy applies to all business units, processes and commercial systems in all countries in which Brainsonic undertakes its professionnal activities and/or has commercial and/or other business relationships with third parties.

This policy applies to all directors, managers, employees, agents, affiliates, suppliers, consultants, advisors or service providers, working for and/or with Brainsonic, who may collect, process or have access to data (including personal and/or sensitive data). It is the responsibility of the aforementioned persons to familiarize themselves with this policy and to ensure that they strictly comply with it.

This policy applies to all information used within Brainsonic. The concerned documents include :

- E-mails

- Paper documents

- Digital documents

- Video and audio documents

- Data generated by physical access systems

2. Reference documents

- EU GDPR 2016/679 (EU Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC)

- Ordinance on the Federal Data Protection Act (VDSG/ OLPD)

- Code of Obligations (OR) - Art. 958f par. 1

- Personal data protection policy

3. Conservation By-law

3.1. General principle on conservation

Any document which does not pertain to a specifically aforedefined category, will be retained for a period of three (3) years from the date of creation of the document, except if another applicable law requires a different conservation period

3.2 General retention schedule

The data protection officer defines the period of time for which electronic documents and records are to be retained (hereinafter called « Retention period ») in the Data retention schedule.

Retention periods may be extended as an exception in the following cases :

- Ongoing investigations by European Union Member State authorities in the event personal data records are be necessary to prove compliance with legal requirements; or

- For the exercise of legal rights during lawsuits or similar legal proceedings recognized under local law.

3.3. Backup of data during the retention period

Possible degradation of the data medium used for archiving must be considered. If electronic storage is chosen, the procedures and systems that ensure that the information can be accessed during the retention period (whether for the data carrier or for the legibility of the formats) should also be maintained a way to protect it from data loss resulting from technological changes. The liability for storage lies with the IT Manager.

3.4. Destruction of data

Brainsonic and its employees are therefore required to regularly review all data (whether stored electronically or on paper) in order to decide whether to destroy or delete data once the purpose for which it was created was accomplished. Refer to the Appendices regarding the Data retention schedule. Overall liability related to the destruction of data rests with the IT Manager.

Once the decision is made to dispose of the data in accordance with the Data retention schedule, the data must be erased, shredded or otherwise destroyed in accordance with its value to others and its level of confidentiality. The method of disposal varies and depends on the nature of the record. For example, all documents containing sensitive or confidential information (and particularly sensitive personal data) should be disposed of as confidential waste and subjected to secure electronic deletion. Some expired or replaced contracts can be destroyed by simple internal shredding. The Disposal Schedule section defines the method of disposal.

The employee must carry out the duties and all liability related to the destruction of information in a compliant manner. The specific deletion or destruction process may be performed by an employee or by an internal or external service provider assigned to this task by the IT Manager.

All applicable general rule under the relevant data protection laws and/or Brainsonic's personal data protection policy shall be complied with.

Appropriate controls must be in place to prevent the irretrievable loss of essential company information due to malicious actions or unintentional destruction of information. These controls are described in the security of information policies (Security Policy - Brainsonic).

The IT Manager is responsible for documenting and shall approve of the entire destruction process. Applicable legal requirements for the destruction of information, including requirements of applicable data protection laws, must be fully complied with.

3.5. Violation, enforcement and compliance

It is the responsibility of the Data Protection Officer (the DPO) to ensure that each Brainsonic office complies with this policy. It is also the Data Protection Officer's obligation to assist local offices in obtaining information from any local data protection authority or government.

Any suspected violation of this policy must be reported immediately to the data protection officer. Any suspected breach of the Policy shall be investigated and action taken as appropriate.

Failure to comply with this policy may occur certain consequences, including loss of customer confidence, litigation and loss of competitive advantage, financial loss and damage to Brainsonic's reputation, injury, damage or loss. Non-compliance with this policy by permanent or temporary employees or contractors, or by third parties with access to Brainsonic's premises and/or information may result in disciplinary proceedings or the termination of the employment contract.

Such non-compliance may also result in legal action against parties involved in such activities.

4. Disposal of Documents

4.1. Systematic elimination schedule

The documents that may be automatically destroyed, except in the case of an ongoing legal or regulatory investigation, are the following:

- Announcements and notices of daily meetings and other events, including approvals and apologies ;

- Requests for any information such as travel itineraries ;

- Reservations for internal meetings at no charge / no external costs;

- Documents such as letters, fax headers, e-mails, transmittal slips, compliment slips and similar éléments which accompany documents, but do not add value;

- Personalized messages

- Updated mailing list, distribution lists, etc. ;

- Duplicates of documents such as CC copies and for information purposes, unmodified drafts, prints of screenshots or extracts from databases and daily files ;

- Internal publications of stocks that are obsolete or superseded; and

- Specialized magazines, supplier catalogs, brochures and newsletters from suppliers or other external organizations.

In any event, disposal is subject to disclosure requirements that may exist in the event of a dispute. For example, if there are ongoing legal proceedings, then all documents related to these proceedings cannot be disposed of.

4.2 Method of Destruction

Level I documents are those containing the most secret and confidential information. These documents must be disposed of as confidential waste (shredding and incineration) and/or must be subject to secure electronic deletion.

Disposal of documents must be demonstrated by proof of destruction.

Level II documents are proprietary documents that contain confidential information such as names, signatures and addresses of the parties, or that could be used by third parties to commit fraud. Level II documents must be shredded before disposal. Electronic documents will be subject to secure electronic deletion.

Level III documents are those that do not contain confidential information or personal data and are published by Brainsonic. They must be shredded and may include, but are not limited to, advertisements, catalogs, brochures and newsletters. These documents can be disposed of without verification.

5. Validity and management of documents

This document is valid from 15.03.2018.

The owner of this document is the DPO, who must check and, if necessary, update the document at least once a year.

We inform you that this privacy policy may be modified by us. If so, the changes will be made available on this page.