DATA PROCESSING AGREEMENT
(Revision November 2018)

This Data Processing Agreement sets out the principles and commitments concerning the primary processing of personal data. The Parties agree that, for some aspects of the processing, the Parties may have different roles and alternatively act as Data Controller and data Processor, or joint Data Controllers. The obligations arising in these specific circumstances are set out in Schedule A.

RECITAL

This Data Protection Agreement ("DPA") forms an integral part of any written agreement between Mindbaz (hereinafter defined as "Mindbaz » or « Processor) and the Data Controller, including the Mindbaz General Terms and Conditions of Service, the order form(s) and/or invoice(s) for the purchase of services provided by Mindbaz (hereinafter defined as "Contract").

The Parties agree that this DPA remplaces and/or governs all provisions relating to personal data protection. In the event of any conflict or inconsistency between this DPA and the Contract, the DPA shall prevail.

I - Objet

The purpose of this Data Processing Amendment is to set out the conditions on which (i) the Data Processor undertakes to carry out the data processing tasks set out below on behalf of the Data Controller and (ii) the Data Controller shall provide instructions to the Data Processor for any processing of personal data.

As part of their contractual relationship, the Parties undertake to comply with prevailing regulations on the processing of personal data, in particular Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 applicable from 25 May 2018 (the "**GDPR**").

II - Description of the data processing activities

A. Nature and purpose of processing

The Processor is authorised to process on behalf of the Data Controller the personal data necessary to provide the email routing service(s) as detailed in Contract.

The purpose of processing is strictly limited to the service as described above, to the exclusion of any other purpose. In this respect, the Controller expressly undertakes (i) not to access

and/or use the said data, unless this is strictly necessary to provide the said email routing service and (ii) not to use or process the said data for its own purposes and in particular not to use or process the said data for profiling, data mining or direct marketing purposes.

B. Relevant categories of personal data

In order to perform its email routing service in accordance with the request of the Data Controller (and only for this purpose), the Processor may be required to process the categories of personal data pursuant to current regulations that do not require special and specific security measures, other than those implemented by the Processor and detailed at the following address: https://www.mindbaz.com/en/gdpr/

C. Categories of persons concerned

The categories of persons whose personal data are likely to be processed as part of the emailing routing service may include: your end users of products and/or services, your customers, prospects, candidates, employees, suppliers, external service providers, processor and sub-processor.

D. Additional categories of personal data and additional person concerned/Sensitive Data

As a technical service provider providing a Saas solution (hereinafter referred to as the "Mindbaz application"), the Processor contents itself with providing the Data Controller with a secure IT infrastructure accessible online. Thus, a customer using the e-mailing routing service has the freedom to choose which data they wish to process on the infrastructure made available to them, for what purposes and how they wish to protect this data. Given the nature of the service that it provides, the Processor does not have to know which data is processed by the Data Controller and consequently cannot distinguish whether it concerns personal data or not. To this end, Mindbaz undertakes to provide a level of security appropriate to all types of data, with the exception of certain sensitive data.

Consequently, all categories of data or persons concerned other than those described herein above must be specifically communicated to the Processor by the Data Controller. The Data Controller undertakes not to host sensitive data pursuant to current regulations without first notifying the Processor. In any event, the Data Controller undertakes not to host data requiring the implementation of special and specific security measures, other than those implemented by the Processor and detailed at the following address:
https://www.mindbaz.com/en/gdpr/

III - Term of agreement

If the date of conclusion of the Contract is prior to May 25, 2018, this DPA shall be effective from May 25 2018 for the duration stipulated in the Contract.

If the date of conclusion of the Contract is later than May 25 2018, this DPA shall enter into force on the effective date of the Contrat and for the duration stipulated in the Contract.

IV - Data Processor's obligations to the Data Controller

The Data Processor undertakes to:

1. process the data **solely for the purpose(s)** for which the data processing is carried out
2. process the data **in accordance with the instructions** of the Data Controller. To this end, the Processor provides the Data Controller with **the necessary functionalities enabling it to instruct the processing** using the Mindbaz application itself. Indeed, the Processor provides the Data Controller with an on demand and self-managed virtual infrastructure. In particular, the said infrastructure allows it to download personal data and, where applicable, determine how this personal data is processed. If it needs to provide additional instructions, the Data Controller may at any time send the Data Processor any written instructions that it deems necessary by email with read receipt requested: serviceclient@mindbaz.com.
3. If the Data Processor considers that an instruction constitutes a breach of the GDPR, any other provision of European Union law or the laws of the Member States on data protection, it shall **immediately notify** the Data Controller. In addition, if the Data Processor is required to transfer data to a third country or to an international organisation pursuant to European Union law or the laws of the Member State by which it is governed, it must inform the Data Controller of that legal obligation before carrying out the processing, unless the relevant law prohibits it from making such a notification on material public interest grounds.
4. ensure that the **persons authorised to process personal data** under this Data Processing Agreement:
    a. undertake to keep the information **confidential** or are subject to an appropriate legal confidentiality obligation
    b. receive the necessary **training** on the protection of personal data
5. incorporate the principles of **data protection by design** and **data protection by default** into the tools, products, applications and services they use.
6. **Sub-Processors**

The Processor may engage another Processor (hereinafter "***the Sub-Processor***") to conduct specific processing activities in connection with the provision of the Contract.

The list of current Sub-Processors is available on the following page:
https://www.mindbaz.com/en/gdpr/

The Processor shall inform the Controller by email, at the addresses indicated by the Controller within this DPA, beforehand of any change concerning the addition or replacement of SubProcessors(s) in order to allow the Controller to object to these changes.

Any objection must be duly justified and promptly addressed by the Controller. The Controller has a minimum timeframe of ten (10) working days from the date on which it receives said information to object thereto. Such sub-contracting is possible where the Controller has not objected thereto within the agreed timeframe.

If the Controller objects to a new Sub-Processor and the provision of the Contract cannot be provided without the use of this objected Sub-Processor, Mindbaz and the Controller may terminate:

- The Contract, if the entire Contract cannot be provided without the use of this objected new sub-Processor ; or

- The part of the Contract relating to the service that cannot reasonably be provided without the use of this objected new Sub-Processor.

The Contract may be terminated by registered letter with acknowledgement of receipt subject to thirty (30) days' notice from the date of dispatch of the said letter, as evidenced by the postmark. The sums due for services already performed cannot be contested by the Controller.

The Processor undertakes to enter into a legal agreement with the Sub-Processor and to impose the same obligations as those applicable to the Processor under this DPA. If the further Processor does not fulfil his data protection obligations, the Processor shall remain fully liable to the Controller for the performance by the other Processor of his obligations.

The Sub-Processor is obliged to comply with the obligations hereunder on behalf of and on instructions from the Controller. It is the initial Processor's responsibility to ensure that the Sub-Processor provides the same sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing meets the requirements of the GDPR. Where the Sub-Processor fails to fulfil its data protection obligations, the initial Processor remains fully liable with regard to the Controller for the Sub-Processor's performance of its obligations.

7. Data subjects’ right to information

The Data Controller is responsible for providing information to data subjects of the processing operations at the time the data is collected.

8. Exercing personal rights

To the extent possible, the Data Processor must assist the Data Controller in meeting its obligation to follow up requests made by data subjects to exercise their rights to access, rectification and erasure, their rights to object and to restrict processing, their right to data portability, and their right not to be subject to an individual decision based on automated processing (including profiling).

9. Notification of personal data breaches

The Data Processor shall inform the Data Controller of any personal data breach of which it becomes aware within the statutory deadlines, by sending an email (with read receipt requested) to the email address set out in the DPA. This notification shall enclose any relevant documentation to enable the Data Controller, where necessary, to notify the breach to the competent supervisory authority.

The documentation must, at the very least, contain:

- ✓ a description of the nature of the personal data breach, including, if possible, the categories and approximate number of persons affected by the breach and the categories and approximate number of recordings of personal data affected;
- ✓ the name and contact details of the data protection officer or another contact point from whom additional information may be obtained;
- ✓ a description of the likely consequences of personal data breaches; ✓ a description of the measures that have been taken or that the Data Processor proposes to take to remedy the personal data breach, including, where applicable, any measures to mitigate any adverse consequences.

If and to the extent that it is impossible to provide all this information at the same time, the information may be communicated in stages without undue delay.

10. Assistance to be provided by the Data Processor to the Data Controller in meeting its obligations

The Data Processor shall assist the Data Controller in carrying out data protection impact assessments. The Data Processor shall help the Data Controller in its preliminary consultation of the supervisory authority.

11. Security measures

The Data Processor undertakes to implement the technical and organisational measures set out at the following address: https://www.mindbaz.com/en/gdpr/

12. Dealing with data on conclusion of the services

At the term of the contractual relationship, the Data Processor will destroy all existing copies in its information systems. At the request of the Controller and once those copies

have been destroyed, the Data Processor shall provide written confirmation of their destruction.

13. Data Protection Officer

The Data Processor shall send the Data Controller **the name and contact details of its data protection officer**, if it has appointed one pursuant to Article 37 of the GDPR.

14. Register of categories of processing activities

The Data Processor represents that it **keeps a written register** of all categories of processing activity carried out on the Data Controller's behalf that includes:

- ✓ the name and contact details of the Data Controller for whom it is working, those of any data Processors and, where applicable, those of the data protection officer;
- ✓ the categories of processing carried out on the Data Controller's behalf; ✓ where applicable, transfers of personal data to a third country or to an international organisation, including the name of this third country or international organisation and, in respect of the transfers referred to in the second paragraph of Article 49(1) of the GDPR, the documents demonstrating the existence of suitable safeguards;
- ✓ to the extent possible, a general description of the technical and organisational security measures including, inter alia, as appropriate:
    - the pseudonymisation and encryption of personal data;
    - the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
    - the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
    - a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

15. Documentation

The Data Processor shall provide the Data Controller with all **documentation it needs to demonstrate that it has met all its obligations**.

16. Audit

The Data Controller may, at his own expense, carry out one (1) audit of the personal data protection and security measures taken by the Processor in relation to the personal data processed on behalf of the Data Controller, at most once every twelve (12) months, unless exceptional circumstances arise due to the violation of personal data attributable to the Processor justifying the conduct of an additional audit.

This audit may be carried out by the Data Controller or a third party auditor independent of the Processor duly mandated by the Data Controller, provided that this third party auditor does not himself also carry out an activity competing with that of the Processor and/or has no legal relation with a competitor of the Processor.

A confidentiality agreement must be signed beforehand between the Parties and the third party auditor.

The Controller shall inform the Processor in writing, subject to fifteen (15) working days' notice, of its intention to have such an audit carried out and of the identity of the third party auditor retained, if any (accompanied by the mandate given), as well as the scope of the planned audit.

The audit carried out by the Data Controller will focus solely on compliance with the Processor's obligations under the applicable personal data protection regulations, in particular in terms of security and protection of personal data processed on behalf of the Data Controller under the Contract.

In any event, the audit operations must not disrupt the functioning of the services and the activity of the Sub-Processor.

V. The Data Controller's obligations to the Data Processor

The Data Controller undertakes to:

1. document in writing any instructions on the processing of data provided by the Data Processor or use the functionalities provided to it to provide processing instructions in accordance with prevailing regulations.
2. ensure, before and throughout the processing period, that the Data Processor complies with its obligations under the GDPR
3. determine the purpose and means of processing in accordance with prevailing regulations. In this respect, it undertakes to comply with the principles of purpose limitation, data minimisation and limited storage periods and undertakes to notify data subjects and ensure that it has properly obtained their consent to the processing of data.
4. keep a detailed register of the processing activity it carries out
5. implement the technical and organisational measures required under prevailing regulations.
6. Use the service(s) offered by Mindbaz in accordance with applicable regulations.

SCHEDULE A - QUALIFICATION AND OBLIGATIONS IN RESPECT OF SUB-PROCESSING

Mindbaz acts as “Data Controller” when it determines the purpose and means of its own processing.

Mindbaz may be required to collect data for the purposes of invoicing, debt collection management, improving its services and performance or in connection with managing the accounts and passwords of your employees with access to the Application. In this respect, the data of some of your employees who interact with Mindbaz may be the subject of such processing.

Mindbaz undertakes to comply with all regulations in force in respect of the processing activity it carries out as Data Controller within the meaning of the GDPR and undertakes:

- To limit the collection of data to that data strictly relevant to the processing
- Not to use the collected data for purposes other than those for which it is collected
- To comply with all legal rules on the storage period for the data
- Not to transfer data to third parties other than those involved in the performance of the Agreement
- To take the appropriate technical and organisational measures to ensure a high level of security