Frends Data Processing Agreement

1. Background and Purpose

This Data Processing Agreement ("DPA") forms part of the agreement entered into by Frends Technology ("Frends") and customer identified in the agreement ("Customer"), which governs the provision of the Frends Platform by Frends to Customer and Customer's use of said platform and related services ("Agreement"). This DPA sets out the terms and conditions under which Frends processes Customer's Personal Data in relation to the Agreement. The purpose of this DPA is to take into account the responsibilities and obligations set by the GDPR in the Agreement.

Customer is the data controller of Customer's Personal Data processed in connection with the service agreed in the Agreement. Frends processes the said Personal Data on behalf of and by the order of Customer as agreed in this DPA. The Parties shall agree more specifically in Schedule 1 and Schedule 2 on the categories of data subjects, data security procedures and the purpose for which Frends processes Customer's Personal Data.

The Parties understand that authorities may issue orders and guidelines within the scope of the GDPR after the signing of this DPA. The Parties commit to, if necessary, amend this DPA based on such orders and guidelines.

Any terms not defined in this DPA shall have the meaning set forth in the Agreement. In the event of a conflict between

the terms and conditions of this DPA and the Agreement, the terms and conditions of this DPA shall take precedence with regard to the subject matter of this DPA.

2. Definitions

"Authorized Individual(s)" means the persons processing Personal Data on behalf of and under the control of Frends pursuant to the Agreement and this DPA; "Data Processing Agreement" or "DPA" means this agreement on processing of Personal Data and its schedules;

"Data Protection Legislation" means the national data protection legislation in force at the time in question and the GDPR;

"GDPR" means the General Data Protection Regulation of the European Union (2016/679/EU);

"Personal Data" means any information relating to an identified or identifiable natural person, from which the person can be identified, directly or indirectly;

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

3. Responsibilities of Customer

Customer shall process the Personal Data in compliance with the Data Protection Legislation. Customer is responsible for the lawfulness and completeness of the instructions on the processing of Personal Data set out in Schedule 3. Possible changes to the instructions set out in Schedule 3 and possible cost effects in relation thereto shall always be

agreed on separately in writing.

Customer is responsible for the Personal Data provided to Frends and for the lawfulness of the Personal Data. Frends does not monitor the content, quality or timeliness of the Personal Data provided by Customer.

Customer shall ensure that the purpose and grounds for processing are in compliance with the Data Protection Legislation. Customer shall also ensure that Personal Data has been collected in accordance with the Data Protection Legislation and that Customer has the right to transfer the Personal Data to be processed by Frends.

4. Responsibilities of Frends

Frends shall process the Personal Data in accordance with the Data Protection Legislation and the written instructions set out in Schedule 3, unless otherwise required by law applicable to Frends. In such case, Frends shall inform Customer of such legal requirement before the processing, unless the applicable law prohibits such notification.

Taking into account the nature of the processing, Frends shall assist Customer with appropriate technical and organisational measures chosen by Frends so that Customer can fulfil its obligation to respond to requests concerning the exercise of the following rights of the data subjects, as set out in Chapter III of the GDPR (provided that the data subject has the said right under the GDPR):

1. right of access to the Personal Data;
2. right to rectification and erasure;
3. right to restriction of processing;
4. right to Personal Data portability; and
5. right to object to processing of Personal Data.

In case a Party receives a request concerning the use of the data subject's rights, the Party receiving the request shall notify the other Party of the request immediately and at the latest on the day following the receipt of the request, if fulfilment of the request requires any actions from the other Party. The notification will contain all information necessary to the other Party to fulfil the request. Frends is entitled to charge Customer for all actions taken to fulfil the request of the data subject on a time and material basis in accordance with its price list applicable at the time. Frends shall assist Customer in ensuring compliance with the following obligations under Articles 32–36 of the GDPR (taking into account the nature of the processing and the information available to Frends):

1. ensuring the security of processing by implementing appropriate technical and organisational measures;
2. notifying supervisory authority and the data subjects of Personal Data Breaches;
3. participating in data protection impact assessment if such impact assessment is necessary under Article 35 of the GDPR; and
4. participating in the prior consultation of the supervisory authority if such prior consultation is necessary under Article 36 of the GDPR.

Frends is entitled to charge Customer for the aforementioned measures on a time and material basis in accordance with its price list applicable at the time.

5. Data Security

The Parties undertake to implement the technical and organisational measures commonly used in the industry to protect the Personal Data from accidental or unlawful processing or disclosure of Personal Data. Such measures

include e.g.:

1. pseudonymisation and encryption of Personal Data;
2. the ability to ensure the continuing confidentiality, integrity, availability and resilience of processing systems and services;
3. the ability to restore the availability of and access to Personal Data in a timely manner in the event of a physical or technical incident; and
4. process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures to ensure the security of data processing.

The aforementioned measures are examples of how the Parties may ensure the security of the processing of Personal Data. The Parties shall separately agree in Schedule 1 and Schedule 2 on the aforementioned measures or other data security procedures that Frends shall implement in the processing of Personal Data. Customer shall ensure appropriate and sufficient data security of the equipment and IT environment under its control. Unless agreed otherwise in the Agreement, Customer shall be responsible for taking backups of the Personal Data and the verification of the functionality of the backups.

Frends shall ensure that the Authorized Individuals processing Personal Data are committed to confidentiality or are under an appropriate statutory obligation of confidentiality. Frends shall implement necessary measures to ensure that the said persons only process Personal Data in accordance with the instructions set out in Schedule 3.

6. Transfer of Personal Data

Unless otherwise agreed in Schedule 3, Frends has the right to transfer Personal Data outside the EU or EEA in accordance with the Data Protection Legislation. Frends

shall be entitled to transfer the Personal Data freely within the EU or EEA for the purpose of providing the agreed service.

7. Subcontractors

Frends is entitled to use subcontractors (including its Affiliates) in the provision of the service and the related processing of Personal Data. At the time of signature of this DPA, Frends' authorized subcontractors include third-party subcontractors and Frends' Affiliates listed at https://frends.com/legal/sub-processors. Frends shall be responsible that its subcontractors process the Personal Data in accordance with the Data Protection Legislation.

Frends shall notify Customer if it plans on changing or adding subcontractors participating in the processing of Personal Data. Customer is entitled to object to such changes on reasonable grounds. Customer shall notify Frends of the objection without undue delay after receiving the said notice from Frends. Should Customer not accept the change or the addition of a subcontractor, Frends has the right to terminate the Agreement with thirty (30) days' notice.

8. Personal Data Breaches

Each Party shall notify the other Party without undue delay if it becomes aware of a Personal Data Breach. When notifying Frends of a Personal Data Breach, Customer shall provide to Frends all information that can be deemed to help in the investigation, restriction and prevention of the Personal Data Breach. When notifying Customer of a Personal Data Breach Frends shall, to the extent such information is available to Frends, provide Customer with the

following information:

1. a description of the nature of the Personal Data Breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned (as far as the information is available to Frends);
2. the contact information of the Frends' Chief Information Security Officer or other contact point where more information can be obtained;
3. a description of the likely consequences of the Personal Data Breach; and
4. a description of the measures taken by Frends to address the Personal Data Breach and the measures taken by Frends to mitigate the adverse effects of the Personal Data Breach.

If the Personal Data Breach is caused by a reason that is under the responsibility of Customer, Customer shall be liable for all costs resulting from the Personal Data Breach. Customer shall be responsible for notifying the supervisory authority and the data subjects of the Personal Data Breach as set out in the GDPR.

9. Records of Processing Activities

Frends shall maintain a record of processing activities carried out on behalf of Customer. The record contains the following information:

1. the name and contact details of Customer, Frends and Frends' possible data protection officer and information about possible subcontractors;
2. the categories of Personal Data processed on behalf of Customer;
3. information on transfers of Personal Data outside the EU or EEA; and
4. where possible, a general description of the technical and

organisational safety measures implemented in accordance with Section 5 of this DPA.

10. Right to Audit

During the term of this DPA, Customer or an independent third party auditor appointed by Customer, which third party may not be Frends' competitor, may audit Frends' compliance with the obligations addressed to it under this DPA. The subject of the audit will be Frends' relevant material related to the processing of Customer's Personal Data and Frends' systems and premises used in the processing of Customer's Personal Data. The audit may be carried out no more than once per calendar year and Frends shall be provided with a notification of the audit in writing at least thirty (30) days in advance, accompanied with a detailed audit plan which describes the proposed scope, duration, and start date of the audit. Frends shall review the proposed audit plan and communicate any concerns or questions to the Customer in relation thereto. Customer shall address said concerns and questions to the extent possible.

Frends shall participate in the audit and provide to the auditor information required to demonstrate Frends' compliance with the requirements addresses to it under this DPA. The audit may not interfere with Frends' operation of services and the auditor will not be entitled to access information of Frends' customers or partners. Should Customer not be the one performing the audit, the auditor will enter into a confidentiality agreement with Frends prior to the execution of the audit.

Customer shall bear all costs resulting from the audit.

11. Termination of The Processing of Personal Data

Upon termination of the Agreement and provision of service related to the processing of Personal Data or upon termination of this DPA, Frends undertakes, in accordance with Customer's written request, to delete or return Customer's Personal Data to Customer.

Additionally, upon termination of the Agreement or this DPA, Frends shall delete all existing copies of Customer's Personal Data, unless otherwise required by applicable law or regulation.

Frends is entitled to charge Customer for the return or destruction of the Personal Data on a time and material basis in accordance with its price list applicable at the time.

12. Limitation of Liability

The limitation of liability clause of the Agreement is applied to this DPA. Notwithstanding the above-mentioned, the Parties' liability for the damages caused to the data subjects shall be determined in accordance with Article 82 of the GDPR.

13. Amendments

Amendments to this DPA are valid only if they are made in writing and signed by the authorized representatives of both Parties.

14. Term and Termination

This DPA will become effective when it has been duly signed by both Parties and will continue to be in effect as long as Frends processes Customer's Personal Data. This DPA will terminate upon the termination of the Agreement at the latest.

In case either Party materially breaches this DPA, the non-breaching Party will have the right to terminate this DPA, if the breaching Party has not remedied the breach within thirty (30) days from the non-breaching Party's written notification of the breach.

15. Applicable Law and Dispute Resolution

The dispute resolution clause of the Agreement is applied to this DPA.

Schedules

Schedule 1 Description of the Personal Data and Data Security Procedures Schedule 2 Frends Data Security Procedures

Schedule 1 – Description of the Personal Data and Data Security Procedures

The Parties may amend or update this schedule in writing, if necessary.

1. The Purpose of the Processing

Frends shall process the Personal Data only for the following purpose: provision of the Frends Platform and related Professional Services as stipulated in the Agreement.

2. Contents of the Processing

Frends shall perform the following processing activities on the Personal Data:

- Collection
- Adaptation, alteration
- Recording
- Making data available (disclosure of data by e.g. transmission or dissemination)
- Organisation
- Alignment or combination
- Storage
- Erasure and destruction

3. Categories of Data Subjects

Frends shall process the following, but not limited to, categories of data subjects:

• Customer's employees, independent contractors, agents, advisors and freelancers; • Customer's prospects, customers, business partners and vendors, or their respective employees and contact persons.

Frends shall process the following, but not limited to, categories of Personal Data in relation to the above-mentioned data subjects:

• First and last name • IP Address • Email

4. Applicable Data Security Procedures

Frends shall comply with its own data security guidelines when processing Personal Data, as outlined in Schedule 2.

Schedule 2 – Frends Data Security Procedures

Frends agrees that it:

1. Maintains an information security program which is approved by its management and regularly reviewed and updated according to ISO 27001 Certification.
2. Restricts access to Personal Data to Authorized Individuals who provide authentication that uniquely identifies them.
3. Restricts Authorized Individuals' rights to access or modify Personal Data based on business role and need.
4. Reviews access and authorization rights for Authorized Individuals regularly. Access or authorization rights are withdrawn or modified, as appropriate, promptly upon termination or change of role for such Authorized Individuals.
5. Ensures that physical access to systems storing or processing Personal Data is appropriately secured and monitored.
6. Encrypts Personal Data both at rest and in transit, using industry standard protocols and encryption algorithms.
7. Has implemented and maintains secure coding and development standards, incorporating security and privacy considerations.
8. Ensures that its personnel receive regular security and privacy training so that they are aware of their roles and responsibilities with regard to the treatment and protection of Personal Data.
9. Segregates internal systems storing or processing Personal

Data from public networks.

10. Has implemented monitoring and alerting capabilities on its systems.
11. Evaluates its systems for vulnerabilities and deploys required security updates on a schedule based on risk and severity.
12. Regularly tests the security of its systems including an annual penetration test performed by a qualified third party.
13. Evaluates the security and privacy practices of all authorized subcontractors.
14. Deploys redundant services and engages in practices including regular backups designed to provide continued availability and access to data despite disruptions to its infrastructure.
15. Maintains an incident response plan and commits to providing required notifications in case of a confirmed Personal Data Breach without undue delay.
16. Maintains systems and processes for complying with data privacy requirements including limited retention and processing of requests from data subjects.