VERSION 05.2024

DATA PROCESSING AGREEMENT

INTRODUCTION

If F.INSTITUTE process Personal Data of Client when performing the Services, parties agree that this data processing agreement sets forth their obligations with respect to the processing and security of Personal Data in connection with the services provided by F.INSTITUTE. The Data Processing Agreement will be part of the Service Agreement between parties.

ARTICLE 1 GENERAL AND DEFINITIONS

1.1 F.INSTITUTE B.V. is a private company with limited liability organized and existing under the laws of the Netherlands, having its registered office at Rondweg 50, 3474 KG Zegveld and registered with the trade register of the Chamber of Commerce under number 73674257 (hereafter referred to "**F.INSTITUTE**"). The party to which F.INSTITUTE will provide its services - under a service agreement - will hereafter be referred to as "**Client**".

1.2 Terms with a capital in this agreement are definitions and are set out in this clause. All terms in this agreement not defined in this clause, but defined in the Data Protection Legislation will have the meaning as assigned thereto in the Data Protection Legislation.

1.3 The definitions:

a) **"Confidential Information"** All Personal Data and other information about the processing, including the terms of the DPA.

b) **"DPA"** This data processor agreement including any annex(es) thereto

c) **"Data Protection Legislation"** Any legislation that applies to the processing of the Personal data, such as, but not limited to, the General Data Protection Regulation (GDPR), the Dutch Implementing Act of the GDPR, and any code of conduct and/or any (non-)EEA local laws applicable to the processing of the Personal data.

d) **"Force Majeure Event"** means any events or circumstances, or any combination of such events or circumstances, which are beyond the reasonable control of and not otherwise attributable to the affected party.

e) **"Member State law"** Any applicable law issued by a Member State of the European Union.

f) **"Personal Data"** Any personal data processed by F.INSTITUTE and/or its Subcontractors in connection with any Services.

g) **"Personal Data Breach":** A breach of security or confidentiality possibly leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Confidential Information.

h) **"Regulator"** A supervisory authority such as the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens)* or any other governmental body with supervisory authority over Client.

i) **"Services"** Any services provided by F.INSTITUTE for Client

j) "**Service Agreement**" The agreement in which the assignment performed by F.INSTITUTE to Client is being described in detail.

k) **"Subcontractor"** Any Third Party engaged by F.INSTITUTE for the processing of Personal Data

l) **"Third Party"** All other parties and entities other than Client or F.INSTITUTE itself, such as Subcontractors, agents, other clients, business partners or group members of F.INSTITUTE

m) **"Union law"** Any applicable law issued by (institutions of) the European Union

ARTICLE 2 INSTRUCTIONS

2.1 The F.INSTITUTE will be considered as a data processor for the processing of Personal Data of the Client.

2.2 The F.INSTITUTE will comply with the Data Protection Legislation in relation to the Personal Data of the Client.

2.3 The F.INSTITUTE will only process Personal Data:

a) for the provision of the Services;

b) on documented instructions from Client, including, but not limited to, the instructions as set out in **Annex A**; or

c) if required to do so by Union or Member State law to which the F.INSTITUTE is subject. In that case, the F.INSTITUTE will notify the Client of that legal requirement before the processing, unless those laws prohibit such notification.

2.4 The F.INSTITUTE will as soon as reasonable possible inform the Client if, in the F.INSTITUTE's opinion, an instruction of the Client infringes the DPA or the law.

ARTICLE 3 SECURITY

3.1 The F.INSTITUTE shall take appropriate technical and organisational measures to protect the Personal Data in accordance with the Data Protection Legislation. These measures are described in **Annex B**.

3.2 The Parties acknowledge that security measures need to be frequently updated in order to comply with the Data Protection Legislation. The F.INSTITUTE will therefore regularly evaluate and, if necessary, take any follow-up measures to maintain compliance with the Data Protection Legislation.

ARTICLE 4 SUBCONTRACTORS

4.1 The Client gives a general authorization for the use of Subcontractors by F.INSTITUTE. F.INSTITUTE provides information concerning the Subcontractor upon request. If the Client does not agree with a new Subcontractor it shall inform F.INSTITUTE as soon as possible and the Parties will discuss the possibilities of continuing the Services.

4.2 F.INSTITUTE shall obligate all Subcontractors to comply with the same obligations F.INSTITUTE has under the DPA.

4.3 F.INSTITUTE shall remain fully liable towards the Client for any acts or omissions by Subcontractors on the processing of Personal Data of the Client.

ARTICLE 5 CONFIDENTIALITY

5.1 F.INSTITUTE shall keep all Confidential Information strictly confidential and not disclose Confidential Information, except if specifically approved in writing by the Client or if this is otherwise permitted under the DPA.

5.2 F.INSTITUTE may share Confidential Information to its employees, to Third Parties such as (but not limited to) lenders, subsidy agents and equity partners to obtain financing or Subcontractors insofar as this is necessary to perform the Services.

5.3 F.INSTITUTE will ensure that its employees, specific Third Parties and Subcontractors are bound by the same confidentiality terms and conditions as F.INSTITUTE under the DPA.

5.4 This clause does not apply insofar as the relevant information has become part of the public domain without violation of the DPA.

5.5 In the event of a conflict with other contractual arrangements between the Parties regarding confidentiality, the DPA prevails.

ARTICLE 6 NOTIFICATION OF A PERSONAL DATA BREACH

6.1 In the event of a Personal Data Breach F.INSTITUTE will notify the Client without undue delay after becoming aware of a personal data breach. F.INSTITUTE will cooperate with the Client in order to enable the Client to properly respond to a Personal Data Breach.

6.2 F.INSTITUTE will not inform the affected data subjects nor a Regulator of a Personal Data Breach, unless this is required by Union or Member State law. In that case, F.INSTITUTE will inform the Client thereof as soon as possible.

ARTICLE 7 INTERNATIONAL DATA TRANSFERS

7.1 F.INSTITUTE may transfer Personal Data between member states of the European Economic Area (EEA); or to any country or territory outside the EEA with an adequate level of protection (according to the European Commission for which an approved adequacy decision has been published). When such a decision is not in place, F.INSTITUTE may transfer Personal Data to a third country outside the EEA and will take all necessary measures as set out in the Data Protection Regulation and inform the Client of such transfer (e.g. signing the applicable EU model clauses).

ARTICLE 8 RETENTION

8.1 F.INSTITUTE will retain the Personal Data as long as necessary for providing the Services, as set out in more detail in **Annex A.**

8.2 Unless agreed otherwise in writing, F.INSTITUTE will delete all Personal Data of the Client, and will confirm in writing to the Client that all Personal Data have been deleted:

(a) Upon the Client's written request thereto; or

(b) within 30 calendar days after termination of this Agreement.

8.3 If F.INSTITUTE cannot delete all Personal Data of the Client because of technical reasons, or because Union law or Member State law requires longer storage of the Personal Data of the Client, F.INSTITUTE will inform the Client as soon as possible. In that event, F.INSTITUTE will still take all necessary steps to:

(a) come closest to a complete and permanent return and/or deletion of the Personal Data of the Client; and

(b) make the Personal Data of the Client unavailable for further processing.

ARTICLE 9 LIABILITIES

9.1 To the extent permitted by applicable law, the contractual or non-contractual liability of F.INSTITUTE for damages resulting from or in connection with possible shortcomings in the performance of the Services shall be limited to the amount of the invoices excluding VAT as paid by the Client in the 12 months prior to the date the shortcoming (first) occurred and which relates to the specific services provided with respect to which F.INSTITUTE has failed to perform.

9.2 In no event will either Party be liable for indirect damages, including loss of use, loss of profits or interruption of business, however caused or on any theory of liability in relation to the DPA.

9.3 The limitations to F.INSTITUTE's total liability provided in this clause do not apply when arising out of gross negligence or willful misconduct of F.INSTITUTE.

ARTICLE 10 FORCE MAJEURE

10.1 If, due to a Force Majeure Event, the F.INSTITUTE is unable to comply with its obligations under this Agreement, the F.INSTITUTE will inform the Client thereof as soon as possible.

ARTICLE 11 TERM AND TERMINATION

11.1 The Agreement will be effective from the commence date according to the Service Agreement or the commence date of providing the Services (date that comes first will be the effective date).

11.2 Unless terminated earlier in accordance with the Agreement, this Agreement will terminate by operation of law if the F.INSTITUTE no longer has access to or otherwise processes Personal Data for the Client.

11.3 The Agreement may be terminated by either Party in writing with immediate effect in the event that the other Party:

(a) is declared bankrupt;

(b) has been granted suspension of payments.

11.4 Termination or expiration of the Agreement will not discharge the F.INSTITUTE from its confidentiality obligations under the Agreement nor any other obligations which by their nature are meant to survive termination.

ARTICLE 12 MISCELLANEOUS

12.1 Amendments and additions to this Agreement and the relevant annexes thereto will only be valid and binding if these amendments and additions are agreed in writing and have been (digitally) signed by both parties.

12.2 This Agreement is governed by the laws of the Netherlands. The competent courts of Amsterdam will have exclusive jurisdiction.

ANNEX A – DETAILS ABOUT THE PROCESSING OF PERSONAL DATA

Action	Details
F.INSTITUTE will process the Personal Data for providing the Services, e.g. drafting financial advice and reports, and once done it will archive the Personal Data.	
F.INSTITUTE will process the following data	Name, address, e-mail address, telephone number, IP address social security number, financial details
Category of data subjects	Client's employees, directors and board members, contractors and temporary workers, partners, stakeholder, owners
Retention period of the Personal Data	As long as necessary to perform the Services or set by applicable law. For more information please contact your F.INSTITUTE contact person.
Special categories of data processed by the F.INSTITUTE	N/A
Subcontractors	On request a list of applicable subcontractors will be made available

In case of a **Personal Data Breach**, F.INSTITUTE will, as soon as possible, notify the Client, by the manner and with the details provided by Client by email or included in the Services Agreement of the following:

- the nature of the Personal Data Breach (including date and time and, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned);
- the contact details where more information can be obtained;
- the likely consequences of the Personal Data Breach for the Client or data subjects;
- the measures taken or proposed to be taken by F.INSTITUTE to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

ANNEX B – DETAILS ABOUT THE SECURITY MEASURES

F.INSTITUTE has implemented and will maintain for Personal Data in the Services the following security measures, which in conjunction with the security commitments in this DPA are F.INSTITUTE's only responsibility with respect to the security of that data.

Domain	Practices
Organization of Information Security	**Security Ownership**. F.INSTITUTE has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures. **Security Roles and Responsibilities**. F.INSTITUTE personnel with access to Personal Data are subject to confidentiality obligations.
Asset Management	**Asset Inventory**. F.INSTITUTE maintains an inventory of all media on which Personal Data is stored. Access to the inventories of such media is restricted to F.INSTITUTE personnel authorized in writing to have such access. **Asset Handling** - F.INSTITUTE classifies Personal Data to help identify it and to allow for access to it to be appropriately restricted. - F.INSTITUTE imposes restrictions on printing Personal Data and has procedures for disposing of printed materials that contain such data.
Physical and Environmental Security	**Protection from Disruptions**. F.INSTITUTE uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.
Access Control	**Access Policy**. F.INSTITUTE maintains a record of security privileges of individuals having access to Personal Data. **Access Authorization** - F.INSTITUTE maintains and updates a record of personnel authorized to access F.INSTITUTE systems that contain Personal Data.- - F.INSTITUTE identifies those personnel who may grant, alter or cancel authorized access to data and resources. - F.INSTITUTE ensures that where more than one individual has access to systems containing Personal Data, the individuals have separate identifiers/log-ins. **Least Privilege** - F.INSTITUTE restricts access to Personal Data to only those individuals who require such access to perform their job function. **Integrity and Confidentiality** - F.INSTITUTE instructs F.INSTITUTE's personnel to disable administrative sessions when leaving premises F.INSTITUTE controls or when computers are otherwise left unattended. **Authentication** - F.INSTITUTE uses industry standard practices to identify and authenticate users who attempt to access information systems.

	- Where authentication mechanisms are based on passwords, F.INSTITUTE requires that the passwords are renewed regularly. -- F.INSTITUTE monitors, repeated attempts to gain access to the information system using an invalid password. - - F.INSTITUTE uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage. **Network Design**. F.INSTITUTE has controls to avoid individuals assuming access rights they have not been assigned to gain access to Personal Data they are not authorized to access.
Information Security Incident Management	**Incident Response Process** - F.INSTITUTE maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data. - For each security breach that is a Personal Data Breach, notification by F.INSTITUTE (as described in the "Notification of a Personal Data Breach" section above) will be made without undue delay and. - F.INSTITUTE tracks, disclosures of Personal Data, including what data has been disclosed, to whom, and at what time.
Business Continuity Management	- F.INSTITUTE's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Personal Data in its original or last-replicated state from before the time it was lost or destroyed.