

Data Processing Policy

Version of 28 October 2026.

Pursuant to the Agreement concluded between Vantage and the Client, Vantage provides the Deliverables and the Services to the Client. The provision of the Deliverables and the Services leads to the collection and processing of Personal Data by Vantage, in its capacity as a data processor, on behalf of the Client. Therefore, Vantage provides the Client with this Data Processing Policy (“DPP”) which sets out (i) how Vantage shall manage, process and secure the Personal Data; as well as (ii) all Parties’ obligations to comply with the Privacy Legislation.

By concluding the Agreement with Vantage, the Client has indicated that it has read, understands and accepts the conditions in this DPP, which forms an integral part of said Agreement.

This DPP may be updated from time to time by Vantage, in which case Vantage shall notify the Client through its Website or via e-mail. In any event, the latest version of this DPP, and its previous versions, can always be accessed on the Website.

1. Definitions

Capitalised terms shall have the meaning as set out below.

- 1.1 **Agreement** means the combined term for (i) the Statement Of Work; (ii) the Service Agreement, where one applies; (iii) this DPP; and (iv) the Terms And Conditions;
- 1.2 **Client** means the Party with whom Vantage has concluded the Agreement;
- 1.3 **Data Subject** means the natural person to whom the Personal Data relates, as described in Annex I;
- 1.4 **Deliverables** means the Deliverables as described in the Agreement;
- 1.5 **Personal Data** means personal data (within the meaning of Privacy Legislation) relating to the Data Subjects, as described in Annex I;
- 1.6 **Privacy Legislation** means the (supra)national privacy legislation applicable to the processing of personal data by the Client or Vantage within the scope of the Agreement, such as, but not limited to: (i) the General Data Protection Regulation 2016/679 of April 27, 2016 (“GDPR”); (ii) the ePrivacy Directive 2002/58/EC of 12 July 2002, including future amendments and revisions thereof; and/or (iii) (future) national legislation regarding the implementation of the GDPR;
- 1.7 **Services** means the services provided by Vantage, as set out in the Agreement;
- 1.8 **Sub-processor** means other third parties engaged by Vantage to process the Personal Data on behalf of the Client and in accordance with the Client’s instructions, as identified in Annex III;
- 1.9 **Vantage** means Vantage AI B.V., a private limited company (besloten vennootschap) with its registered office at Keizersgracht 452, 1016 GD Amsterdam, the Netherlands, registered with the Dutch Chamber of Commerce (KVK) under number 42186948;
- 1.10 **Website** means the Vantage website, namely www.vantagegroup.ai, including any and all of its subdomains.
- 1.11 The (uncapitalised) terms “controller”, “personal data breach”, “process”, “processing” and “processor” shall have the meaning attributed to them in the Privacy Legislation.
- 1.12 Other capitalised terms shall have the same meaning as defined elsewhere in the Agreement.

2. Role of the Parties

- 2.1 The Parties acknowledge with regard to the processing of Personal Data under the Agreement that the Client shall be considered the 'controller' and Vantage the 'processor' in accordance with the Privacy Legislation. Vantage may engage a Sub-processor pursuant to the provisions of Section 7.
- 2.2 Each Party shall comply with its respective obligations under the Privacy Legislation with respect to the processing of the Personal Data.

3. Subject matter

- 3.1 The Client acknowledges that by making use of the Deliverables and/or Services, pursuant to the Agreement, it may provide (certain sets of) Personal Data to Vantage for processing. The nature and purpose of said processing, as well as a description of the Personal Data and categories of Data Subjects processed under the Agreement, are further specified in Annex I.
- 3.2 The Client shall not provide Vantage with special categories of personal data within the meaning of Article 9 GDPR, or with personal data relating to criminal convictions and offences within the meaning of Article 10 GDPR, unless the Parties have expressly agreed otherwise in writing in the Statement Of Work.
- 3.3 Vantage shall process the Personal Data in a proper and careful way and in accordance with the Client's instructions, the Privacy Legislation and other applicable rules/best-practices concerning the processing of personal data. More specifically, Vantage shall:
 - (a) during the performance of the Services, provide all its know-how in order to perform the Agreement according to the rules of art, as it fits a specialised and 'good' data processor; and,
 - (b) adopt, to the best of its abilities, the necessary security measures (see Annex II) and provide all its know-how in order to perform the Services in accordance with the rules of art.
- 3.4 The Client keeps full control concerning the following: (i) how the Personal Data must be processed by Vantage; (ii) the types of Personal Data processed; (iii) the categories of Data Subjects whose Personal Data is subjected to the processing; (iv) the purpose of the processing; and (v) the fact whether such processing is proportionate.

4. Instructions from and responsibility of the Client

- 4.1 Instructions. Vantage shall only process the Personal Data upon the Client's request and in accordance with the Client's lawful instructions in Annex I, unless any legal obligation states otherwise. Vantage shall inform the Client if, in its opinion, the instructions infringe the Privacy Legislation. If the Client subsequently cannot guarantee the validity or legality of the instruction or fails or refuses to change the unlawful instruction so that it no longer violates the Privacy Legislation, Vantage shall be entitled to (i) suspend/refuse the performance of said instruction and (ii) at its discretion, either continue to process the Personal Data in accordance with previously provided instructions or stop the processing altogether, until the Client has revised its instruction so that it no longer violates the Privacy Legislation.
- 4.2 Responsibilities. Furthermore, the Client acknowledges that it is responsible for:
 - (a) the accuracy, quality and legality of (the collection and transfer of) the Personal Data;
 - (b) compliance with all transparency and lawfulness requirements under the Privacy Legislation for the collection and processing of the Personal Data and the transfer thereof to Vantage;
 - (c) processing Personal Data on the basis of the correct legal grounds;

- (d) fulfilling its transparency obligations in accordance with the Privacy Legislation; and,
 - (e) ensuring compliance of its instructions (see Annex I) with the Privacy Legislation.
- 4.3 The Client shall inform Vantage without undue delay if it is not able to comply with its responsibilities under this Section or the Privacy Legislation.

5. Use of the Deliverables

- 5.1 In relation to (the processing of) the Personal Data, the Client recognises that:
- (a) Vantage acts as a facilitator by providing its Services and the Deliverables. Therefore, the Client shall be responsible for how and to what extent it makes use thereof;
 - (b) it is responsible for all acts and omissions of its employees, directors and affiliates;
 - (c) Vantage allows the Client to make adjustments and/or changes to the Personal Data and shall never adjust such Personal Data for itself and/or process the Personal Data for its own purposes, unless the Client requests Vantage to do so;
 - (d) it is responsible for the material and/or data (including Personal Data) provided (directly and/or indirectly) by the Data Subject. The Client is, as controller, thus responsible for complying with the Privacy Legislation and/or any other regulations with regard to aforementioned material and/or data;
 - (e) it shall comply with all laws and regulations (such as, but not limited to, with regard to the retention period or rights of the Data Subject) imposed on it by making use of the Services.
- 5.2 In case of any misuse of the Deliverables by the Client in relation to the Personal Data and/or under this DPP or the Privacy Legislation, Vantage can never be held liable in this respect nor for any damage that would occur.
- 5.3 The Client shall avoid any misuse of the Deliverables in relation to the Personal Data and/or under this DPP or the Privacy Legislation. Therefore, the Client shall indemnify Vantage when such misuse would occur as well as for any claim from a Data Subject and/or third party due to such misuse.

6. Security

- 6.1 Vantage takes the security of the processing activities very seriously. Vantage implements appropriate technical and organisational measures, as set forth in Annex II, to ensure, to the best of its abilities, the protection of (i) the Personal Data, including protection against careless, improper, unauthorised or unlawful use and/or processing and against accidental loss, destruction or damage; and (ii) the confidentiality and integrity of the Personal Data. When implementing said measures, Vantage has taken into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

7. Sub-processors

- 7.1 Approval of Sub-processors. The Client acknowledges and agrees that Vantage may engage Sub-processors in connection with the provision of the Services or the development of the Deliverables (and the performance of the Agreement). In such a case, Vantage shall ensure that the Sub-processors are at least bound by the same obligations by which Vantage is bound under this DPP.
- 7.2 Vantage has currently appointed the Sub-processors as listed in Annex III.

- 7.3 Vantage shall be liable for the acts and omissions of its Sub-processors to the same extent as if it would be performing the Services/processing of the Personal Data itself, directly under the terms of this DPP.
- 7.4 Update of the Sub-processor list. Vantage shall:
- (a) update the list whenever a Sub-processor changes (e.g. a new Sub-processor was added, a Sub-processor was substituted, etc.);
 - (b) clearly indicate the changes in the list; and,
 - (c) add a timestamp (i) when the list was updated, and (ii) when the change of the Sub-processor went or will go into effect.
- 7.5 Vantage shall notify the Client through its Website and via e-mail when changes to the list are made. The Client can find the archived Sub-processor lists on the Website.
- 7.6 Objection. If the Client wishes to exercise its right to object to a new Sub-processor, it shall notify Vantage in writing (see Section 15) and based on reasonable grounds by the latest within thirty (30) days after the notification. If the Client does not object or fails to object within the aforementioned timeframe it shall be deemed to have waived its right to object and to have authorised Vantage to engage the new Sub-processor.
- 7.7 In the event the objection is valid and reasonable grounds are formulated clearly, the Parties will discuss the Client's concerns with a view to achieving a reasonable solution. Such solution may include, at Vantage's discretion, to (i) make available to the Client a change in the Services or Deliverables provided; or (ii) recommend a commercially reasonable change to the Client's use of the Deliverables to avoid the processing of the Personal Data by the objected new Sub-processor without unreasonably burdening the Client.
- 7.8 If the Parties are, however, unable to come to a solution within a reasonable period of time (which shall not exceed thirty (30) days following the objection of the Client), the Client may terminate the Agreement (in whole or in part) by providing written notice thereof to Vantage (see Section 15) within a reasonable time, if:
- (a) the Services/Deliverables cannot be used by the Client without appealing to the objected new Sub-processor; or,
 - (b) such termination solely concerns that part of the Services/Deliverables which cannot be provided by Vantage without appealing to the objected new Sub-processor.
- 7.9 Termination of the Services within the meaning of clause 7.8 shall be without liability to either Party (but without prejudice to any fees incurred by the Client prior to suspension or termination of the Services).

8. Transfer of Personal Data to third countries

- 8.1 Vantage processes the Personal Data within the European Economic Area ("EEA") where its Sub-processors allow it. Annex III states where each Sub-processor processes the Personal Data.
- 8.2 However, the Client recognises that Vantage is entitled to transfer and store the Personal Data to countries outside the EEA for the purpose of providing the Services, development of the Deliverables and fulfilling its obligations under the Agreement, provided that such transfer/storage is done in accordance with the Privacy Legislation regarding additional safeguards. In particular, any transfer of Personal Data outside the EEA by Vantage to a third party whose domicile or registered office is in a country which does not fall under an adequacy decision enacted by the European Commission shall be additionally subject to one or more of the following EU-approved safeguards:

- (a) a European Commission adequacy decision, including the EU-U.S. Data Privacy Framework for recipients certified under it;
 - (b) a data transfer agreement with the third country recipient, which shall contain the standard contractual clauses as referred to in the European Commission implementing decision of 4 June 2021 (Decision (EU) 2021/914) on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, including the performance of a transfer impact assessment. Before the transfer takes place, the recipient of the Personal Data/Sub-processor of Vantage in the third country has to guarantee Vantage that an adequate level of privacy compliance is ensured in this third country;
 - (c) binding corporate rules. As is the case for standard contractual clauses, the recipient of the Personal Data/Sub-processor of Vantage in the third country has to guarantee Vantage that an adequate level of privacy compliance is ensured in the third country; and/or,
 - (d) certification mechanisms.
- 8.3 In the event the transfer (or disclosure) of the Personal Data to a third country is required by EU law or EU member state law to which Vantage is subject, Vantage shall inform the Client of that legal requirement before the transfer/disclosure, unless that law prohibits such information on important grounds of public interest.

9. Confidentiality

- 9.1 Vantage shall keep the Personal Data confidential and thus not disclose nor transfer the Personal Data to third parties without the Client's permission, unless such disclosure and/or transfer is required by law or by a court or other government decision (of any kind). In such case Vantage shall, prior to any disclosure and/or announcement, inform the Client in full transparency on the scope and manner thereof.
- 9.2 Vantage ensures the Client that individuals engaged in the performance of the Services (such as personnel, representatives, officers, directors, agents, advisors, affiliates and consultants) are (i) informed of the confidential nature of the Personal Data; (ii) well aware of their responsibilities; and (iii) bound by written confidentiality agreements. Vantage ensures that such confidentiality obligations survive the termination of their employment or services contract.
- 9.3 Vantage ensures the Client that the access of its personnel to the Personal Data is limited to such personnel performing the Services in accordance with this DPP.

10. Notification obligations and assistance

- 10.1 Notification. Vantage shall use its best efforts to inform the Client as soon as reasonably possible when it:
- (a) receives a request for information, a subpoena or a request for inspection or audit from a competent public authority (including a supervisory authority) in relation to the processing of the Personal Data;
 - (b) receives a request from a Data Subject invoking its privacy rights under the Privacy Legislation (see clause 10.3);
 - (c) has the intention to disclose Personal Data to a competent public authority (including a supervisory authority); or,

- (d) determines or reasonably suspects that a personal data breach has occurred in relation to the Personal Data.
- 10.2 Personal data breach. In case of a personal data breach, Vantage:
- (a) shall notify the Client without undue delay after becoming aware of this personal data breach and, to the extent possible, provide the information as required by the Privacy Legislation (e.g. Article 33.3 GDPR). Upon request of the Client, Vantage shall provide, to the extent possible, assistance with respect to the Client's reporting obligation under the Privacy Legislation;
 - (b) undertakes, as soon as reasonably possible, to take appropriate remedial actions to put an end to the personal data breach (if such has occurred under its responsibility) and to prevent and/or limit any future personal data breaches.
- 10.3 Rights of Data Subjects. Vantage shall promptly notify the Client if it receives a request from a Data Subject invoking its privacy rights under the Privacy Legislation. Vantage shall not respond to any such Data Subject request without the Client's prior written consent, except to confirm that the request relates to the Client, to which the Client hereby agrees.
- 10.4 If a Data Subject requests to exercise his/her/their rights, it is the Client's responsibility to assist the Data Subject in its request. Only if the Client does not have the ability to correct, amend, block or delete the Personal Data (as required by the Privacy Legislation), Vantage shall assist the Client (as long as commercially reasonable). Notwithstanding the foregoing, the Client remains responsible for compliance of such Data Subject requests.
- 10.5 Data Protection Impact Assessment. Taking into account the nature of the processing and to the extent that (i) the Client is required to perform a data protection impact assessment under the Privacy Legislation as a consequence of the Agreement and (ii) the required information is reasonably available to Vantage and the Client does not otherwise have access to said information, Vantage shall, upon request of the Client, provide reasonable assistance to the Client with the execution of a data protection impact assessment and possible prior consultation with the competent supervisory authorities. To the extent permitted by the Privacy Legislation, the Client shall be responsible for any costs arising from Vantage's provision of such assistance.

11. Liability

- 11.1 Both Parties are solely liable for all damage, claims and/or fines of third parties, competent supervisory authorities or Data Subjects that are the result of their own breach of or non-compliance with (i) the provisions of this DPP, and (ii) the Privacy Legislation or other applicable rules concerning Personal Data. Each Party shall indemnify the other Party in this regard.
- 11.2 In case of breach/non-compliance as described in clause 11.1, the infringing Party is liable to the other Party and must reimburse the latter for all damages and costs, including reasonable attorney's fees, (legal) expenses and damage resulting from such a breach/non-compliance.
- 11.3 In case of a proven breach by Vantage of its obligations under this DPP or under the Privacy Legislation, Vantage shall:
- (a) be liable for the proven direct damages incurred by the Client;
 - (b) not be liable for indirect, immaterial and/or consequential damages, including (but not limited to) loss of profit, loss of opportunities, loss of and/or damage to data, loss of reputation, sanctions and/or fines, and unforeseeable damages.
- 11.4 Vantage's liability towards the Client shall in any case be limited to the total amount paid by the Client to Vantage during the last twelve (12) months under the Agreement.

- 11.5 The provisions in this Section shall be without prejudice to any other liabilities and limitations of liability as agreed upon in the Agreement.

12. Term

- 12.1 The total term of this DPP shall be the term of the Agreement. If no term is determined, this DPP shall remain in force as long as the Services have not come to an end.

13. Retention, return and deletion of Personal Data

- 13.1 Vantage shall only retain the Personal Data as long as needed to provide the Services or for the term of the Agreement (see Section 12). The Client accepts that Vantage may create back-ups of the Personal Data stored for the execution of its Services.
- 13.2 Upon termination of the Services or the Agreement, the following shall apply:
- (a) the Client may request the Personal Data to be returned ('export') within ninety (90) days following the end of the Agreement, upon which Vantage shall assess whether such export is possible from a technical perspective. In any event, Vantage may, at its sole discretion, determine the format of the export. Vantage reserves the right to charge any costs relating to such exports to the Client;
 - (b) after said ninety (90) day period, the Personal Data shall be deleted within one (1) month, unless it is required by applicable law to retain the Personal Data; and,
 - (c) the Personal Data may be present on back-ups. The Personal Data shall be deleted once the last back-up containing the Personal Data is rotated.
- 13.3 Data or material provided to or submitted to Vantage by the Client during the use of the Services that does not contain Personal Data may be further stored by Vantage following the termination of the Agreement or the Services, in accordance with the specifications set out in the Agreement.

14. Compliance and inspections

- 14.1 Compliance. Upon the Client's request, Vantage shall make available to the Client all information necessary, and to the extent required by law, to demonstrate its compliance with its obligations under this DPP.
- 14.2 Inspections. Vantage shall allow the Client (or a third party on its behalf) to carry out inspections, such as, but not limited to, an audit, and shall provide the necessary assistance thereto.
- 14.3 However, the Client shall limit its initiatives to perform an inspection to a maximum of once a year. The Client must notify Vantage at least thirty (30) working days in advance. The performance of inspections may in any case not cause any delay in the performance of the Services by Vantage.
- 14.4 Vantage can in any case refuse any inspection if the subject of the inspection was already certified by a renowned certifying organisation.
- 14.5 The Client shall impose sufficient confidentiality obligations on its (internal/external) auditors. To ensure the confidentiality of other Vantage clients, Vantage has the right to require the Client and its auditors to sign a non-disclosure agreement before the start of the inspection and to limit the scope of the inspection or the access of the Client's auditors to certain premises.

- 14.6 All inspection costs are exclusively borne by the Client, except if (and to the extent that) a severe security incident/personal data breach (at Vantage/under Vantage's responsibility) or a violation of this DPP is determined during the inspection.

15. Notification and contact

- 15.1 Notifications by the Client under this DPP and/or any questions or concerns with regard to the provisions of this DPP must be directed to contact@vantagegroup.ai.

16. Governing law and jurisdiction

- 16.1 This DPP, including its Annexes, shall be governed by the law and subject to the jurisdiction clause as provided in the Agreement.

Annex I: Data Processing

This Annex describes the processing for each service Vantage provides. The Statement Of Work states which services apply to the Client, and may add to or narrow what is listed here.

1. Capture

Data Subjects

- employees and directors of the Client who take part in interviews, or who appear in the material the Client provides (such as an organisation chart or staff list);
- authorised users of the Client who receive or access the Deliverables.

Personal Data

- name and first name;
- job title, role and department;
- work e-mail address;
- interview answers, and voice input where the Client's staff answer an interview by voice. The voice input is processed to produce a transcript; Vantage does not keep the audio;
- employment cost per employee, where the Client provides it. Vantage asks for this data in anonymised form.

Nature of the processing

Collecting, consulting, structuring, analysing, saving, transferring to the Sub-processors listed in Annex III, and deleting.

Means of processing

Through the Services and the Deliverables, including artificial intelligence models provided by the Sub-processors listed in Annex III.

Purpose of the processing

Identifying where artificial intelligence can be applied in the Client's business, and reporting the findings to the Client, as set out in the Statement Of Work.

2. Context Platform (Compound)

Data Subjects

- employees, directors and authorised users of the Client;
- persons whose details appear in the documents and process knowledge the Client makes available for the Context Platform, such as contacts at the Client's customers and suppliers.

Personal Data

- name and first name;
- work e-mail address, role and department;
- user account and access log data;
- personal data contained in the Client Materials made available for the Context Platform.

Nature of the processing

Collecting, consulting, structuring, analysing, modifying, saving, transferring to the Sub-processors listed in Annex III, and deleting.

Means of processing

Through the Context Platform and the Deliverables.

Purpose of the processing

Providing the Services and access to and use of the Context Platform and the Deliverables pursuant to the Agreement.

3. Duration

For the term of the Agreement (see the Terms And Conditions applicable to the Client). Upon termination of the Agreement (for whatsoever reason), access to the Deliverables shall be deactivated and the Personal Data shall either be deleted or returned to the Client as provided in Section 13.

Annex II: Security

1. Management of information security

- (i) Vantage has implemented an appropriate information security policy.
- (ii) Information security is the responsibility of Vantage's management.
- (iii) Vantage management requires employees and third-party contractors with access to Client information to commit to written confidentiality and privacy responsibilities with respect to that information. These responsibilities survive termination or change of employment or engagement.
- (iv) Vantage management provides information security awareness information to employees and relevant third-party contractors.

2. Access control

User access management

- (i) Vantage implements access control policies to support the creation, amendment and deletion of user accounts for systems or applications holding or allowing access to Client information.
- (ii) Vantage implements a user account and access provisioning process to assign and revoke access rights to systems and applications.
- (iii) The use of "generic" or "shared" accounts is prohibited without system controls enabled to track specific user access and prevent shared passwords.
- (iv) Vantage monitors and restricts access to utilities capable of overriding system or application security controls.
- (v) User access to systems and applications storing or allowing access to Client information is controlled by a secure logon procedure.

Physical access management

- (i) Physical access to facilities where Client information is stored or processed is protected in accordance with good industry practices.
- (ii) Physical documents shall always be kept in secluded spaces to which access shall only be granted on a need-to-know basis.

3. Communications and cloud security

- (i) Vantage logically segregates Client data within a shared service environment.
- (ii) Vantage secures network segments from external entry points where Client data is accessible.
- (iii) External network perimeters are hardened and configured to prevent unauthorised traffic.
- (iv) Inbound and outbound points are protected by firewalls and by the network security measures of the cloud services listed in Annex III.
- (v) Ports and protocols are limited to those with specific business purposes.
- (vi) Vantage synchronises system clocks on network servers to a universal time source (e.g. UTC) or network time protocol (NTP).

- (vii) Client data, including Personal Data, is encrypted at rest.
- (viii) Vantage encrypts data during transmission between each application tier and between interfacing applications.

4. Operations security

Service management

- (i) Vantage has implemented formal operating procedures for system processes impacting Client data. This notification may occur through generic change logs. Procedures must track author, revision date and version number, and must be approved by management.
- (ii) Vantage monitors service availability.

Vulnerability management

- (i) Vantage tests the security of its systems and applications that store or allow access to Client data, including Personal Data, before release. Identified issues are remediated within a reasonable timeframe.
- (ii) Vantage has implemented a patch and vulnerability management process to identify, report and remediate vulnerabilities by implementing vendor patches or fixes, and by developing a remediation plan for critical vulnerabilities.
- (iii) Vantage has implemented controls to detect and prevent malware, malicious code and unauthorised execution of code. Controls must be updated regularly with the latest technology available (e.g. deploying the latest signatures and definitions).

Logging and monitoring

- (i) Vantage generates administrator and event logs for systems and applications that store or allow access to Client data.
- (ii) Vantage reviews system logs when investigating system failures, faults, or potential security incidents affecting Client information.

5. Resilience

- (i) Vantage relies on the backup and recovery measures of the cloud services listed in Annex III, so that the availability of and access to Client data can be restored in a timely manner in the event of a physical or technical incident that results in loss or corruption of Client data.

6. Third-party supplier management

- (i) Vantage has contractual agreements with third parties handling Client information which include appropriate information security, confidentiality and data protection requirements, as detailed in the Agreement. These agreements are reviewed when a Sub-processor is added or its terms change, to validate that information security and data protection requirements remain appropriate.
- (ii) Vantage selects its Sub-processors taking into account their information security measures and certifications.
- (iii) If required by the Client, Vantage provides the Client with a list of third parties with required access to Client data, including Personal Data.
- (iv) Vantage restricts access to Personal Data, but may permit access to Client data, including Personal Data, only as necessary to perform the services that the third party has contractually agreed to deliver.

7. Audit and compliance

- (i) Vantage periodically reviews whether its systems and equipment storing or enabling access to Client data, including Personal Data, comply with legal and regulatory requirements and contractual obligations owed to the Client, when it adds or changes a system and at least once a year.
- (ii) Vantage does not currently hold an independent certification such as ISO 27001. Its Sub-processors hold such certifications for the services they provide. Vantage will inform the Client if it obtains such a certification.

Annex III: Sub-processors

Last updated: 28 October 2026.

Vantage engages the following Sub-processors to assist in providing the Services as described in the Agreement. The Statement Of Work states which services apply to the Client; only the Sub-processors for those services process the Client's Personal Data.

1. All services

Name	Nature of processing	Territory and transfer safeguard
Microsoft (Microsoft 365)	E-mail, file storage and collaboration	EEA (Netherlands tenant)

2. Capture

Name	Nature of processing	Territory and transfer safeguard
Anthropic	AI model processing	Stored in the United States; processing may take place in other countries (global routing). Standard contractual clauses
ElevenLabs	Voice interviews: speech-to-text and conversation handling. ElevenLabs uses Anthropic models as its own sub-processor	United States (EU-U.S. Data Privacy Framework; standard contractual clauses)
Supabase	Database, file storage and authentication	EEA (Ireland). Standard contractual clauses
Vercel	Web application hosting	EEA (Dublin, Ireland). Standard contractual clauses

3. Context Platform (Compound)

Name	Nature of processing	Territory and transfer safeguard
Microsoft (Microsoft Azure)	Cloud hosting of the Context Platform	EEA (North Europe, Ireland)