



Data Processing Agreement

Standard version 2.2

Reference: Esperto Data Processing Agreement v2.2.docx
Version: 2.2
Date: 6 September 2026
Page: 1

Esperto B.V. standard version 2.2, 6 September 2026. This version replaces version 2.1 of 5 September 2026 and the Esperto Data Processing Agreement of June 2025 (reference Esperto-I-2025). Text between **[[double brackets]]** is completed by the Parties before signing.

Parties

1. **Esperto B.V.**, a private limited company under Dutch law, with its registered office at Europalaan 93, 3526 KP Utrecht, the Netherlands, registered with the Dutch Chamber of Commerce under number 88522237, VAT number NL864666536B01 ("Esperto"); and
2. **[[Customer legal name]]**, **[[legal form]]**, with its registered office at **[[address]]**, registered under number **[[registration number]]** ("Customer").

Esperto and Customer are each a "Party" and together the "Parties".

Background

- (A) Esperto operates an online assessment platform on which Customer runs assessments with respondents, and provides related reporting and support services (the "Services") under **[[the agreement, order, partnership agreement or online terms between the Parties dated ...]]** (the "Agreement").
- (B) In providing the Services, Esperto processes personal data on behalf of Customer or, where Customer itself acts for a client, on behalf of that client.
- (C) Article 28 of the General Data Protection Regulation requires that such processing is governed by a written contract. This Data Processing Agreement ("DPA") is that contract. It is written so that it works in both situations described in Article 2, without amendment.

1. Definitions

Terms defined in the GDPR, such as personal data, processing, controller, processor, personal data breach and supervisory authority, have the meaning given there. In addition:

- 1.1 "Agreement" means the agreement referred to in Background (A), including any order, partnership agreement, quotation accepted by Customer or online terms under which Esperto provides the Services, and any later amendment.
- 1.2 "Applicable Data Protection Law" means the GDPR, the Dutch GDPR Implementation Act (Uitvoeringswet AVG) and any other law on the protection of personal data that applies to the Processing.

- 1.3 "Controller" means the party that determines the purposes and means of the Processing of Customer Personal Data. This is Customer where Customer runs assessments for its own purposes (Article 2.1), and Customer's client (the "End Client") where Customer runs assessments on behalf of that client (Article 2.2).
- 1.4 "Customer Personal Data" means all personal data that Esperto processes in providing the Services on behalf of Customer or the Controller, as described in Annex 1. It does not include the data for which Esperto is itself a controller (Article 2.4).
- 1.5 "Expert Partner" means the owner of the methodology underlying an assessment that is made available on the platform under a partnership agreement with Esperto.
- 1.6 "GDPR" means Regulation (EU) 2016/679.
- 1.7 "Instructions" means the documented instructions of the Controller for the Processing, consisting of this DPA, the Agreement, the settings Customer applies within the platform and any further written instruction given under Article 3.
- 1.8 "Processing" means processing within the meaning of Article 4(2) GDPR, in relation to Customer Personal Data.
- 1.9 "Respondent" means a natural person who is invited to complete, or completes, an assessment on the platform.
- 1.10 "Sub-processor" means any third party engaged by Esperto to process Customer Personal Data, as listed in Annex 3.
- 1.11 "Standard Contractual Clauses" means the standard contractual clauses for the transfer of personal data to third countries adopted by the European Commission in Implementing Decision (EU) 2021/914, or any replacement adopted by the Commission.

2. Roles of the Parties

- 2.1 Esperto as processor. Where Customer runs assessments with its own employees, clients, coachees or other Respondents for its own purposes, Customer is the Controller and Esperto is the processor.
- 2.2 Esperto as sub-processor. Where Customer runs assessments on behalf of an End Client, for example as a consultancy or assessment provider delivering a programme

to that End Client, the End Client is the Controller, Customer is the processor and Esperto is a sub-processor of Customer within the meaning of Article 28(4) GDPR.

- 2.3 One set of obligations for both situations. Every obligation Esperto accepts in this DPA is accepted towards Customer and, in the situation of Article 2.2, also for the benefit of the Controller. In that situation:
- (a) Customer passes the Controller's instructions on to Esperto and is Esperto's single point of contact. Esperto may treat an instruction from Customer as an instruction from the Controller.
 - (b) Customer may exercise every right of the Controller under this DPA, including the rights to information, assistance and audit, on the Controller's behalf, and may pass on to the Controller any information, report or assistance Esperto provides.
 - (c) The response times in this DPA are set so that Customer can in turn meet its own obligations towards the Controller.
 - (d) Customer represents that it has the Controller's authorisation to engage Esperto as a sub-processor and that its contract with the Controller imposes on Customer data protection obligations at least equivalent to those Esperto accepts here. On Esperto's request Customer confirms this in writing for a specific End Client.
- 2.4 Data for which Esperto is controller. Esperto is itself the controller, and this DPA does not apply, for the personal data of Customer's contact persons and account holders that Esperto processes for its contractual and commercial relationship with Customer: contract and account administration, invoicing, support and, subject to the applicable rules, marketing. Esperto's privacy statement at espertoassessments.com/privacy-policy applies to that data.
- 2.5 Expert Partners. Where the assessment Customer deploys is provided by an Expert Partner, and the Agreement or the information shown to Respondents before the assessment states that the Expert Partner receives assessment data (usage data at aggregate level or, in some partnerships, individual responses, for example where the Expert Partner debriefs the results), Esperto makes that data available to the Expert Partner on Customer's Instruction. The Expert Partner is an independent controller for its own use of that data. Annex 1 records what the Expert Partner receives. In any other case Esperto does not disclose Customer Personal Data to an Expert Partner.

3. Instructions

- 3.1 Esperto processes Customer Personal Data only on the Instructions and only to provide the Services, unless Union or Member State law to which Esperto is subject requires otherwise. In that case Esperto informs Customer of that legal requirement before Processing, unless the law prohibits this on important grounds of public interest.
- 3.2 Esperto does not use Customer Personal Data for any purpose of its own, including marketing, profiling for its own account or the development of new products, unless the Controller instructs otherwise in writing. Statistical use of assessment data, such as the development of norm groups and the validation of an assessment, takes place only on pseudonymised data, from which the name, email address and other direct identifiers of the Respondent have been removed and kept separately, and never results in a report or disclosure at the level of an individual Respondent. By entering into this DPA the Controller authorises that statistical use; it may withdraw the authorisation for its own Customer Personal Data by written notice at any time.
- 3.3 Customer may give further written instructions, including by email to privacy@esperto.one. An instruction that goes beyond the Services as described in the Agreement, or that requires a change to the platform, is performed only once Esperto has agreed to it, where applicable against the fees set out in the Agreement or otherwise agreed in writing.
- 3.4 If Esperto considers that an Instruction infringes Applicable Data Protection Law, it informs Customer without delay and may suspend performance of that Instruction until Customer has confirmed or amended it.

4. Confidentiality

- 4.1 Esperto treats Customer Personal Data as confidential. Esperto ensures that every person acting under its authority who has access to Customer Personal Data, its employees and any contractor or freelancer working for Esperto included, is bound by a written confidentiality obligation or by an appropriate statutory obligation of confidentiality, and processes the data only on the Instructions.
- 4.2 Access is granted on a need-to-know basis and limited to what a person needs in order to perform the Services. The confidentiality obligation continues after the person's engagement ends and after this DPA ends.

5. Security

- 5.1 Esperto implements and maintains the technical and organisational measures described in Annex 2, so as to ensure a level of security appropriate to the risk in accordance with Article 32 GDPR, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing.
- 5.2 Esperto may update Annex 2 as technology and practice develop, provided the overall level of protection is not reduced. Esperto informs Customer of material changes and provides the current version of Annex 2 on request.
- 5.3 Customer is responsible for the security of the credentials of its own users and administrators, for the configuration of single sign-on where it chooses to use it, and for the choices it makes within the platform, such as which data it enters and which users it grants access.

6. Personal data breaches

- 6.1 Esperto notifies Customer of a personal data breach affecting Customer Personal Data without undue delay and in any event within 48 hours after becoming aware of it. The notification goes to the email address Customer designates for this purpose in Article 14.5 or, failing that, to Customer's contact person under the Agreement.
- 6.2 The notification contains, as far as known at that moment, the information the Controller needs in order to meet its obligations under Articles 33 and 34 GDPR: the nature of the breach, the categories and approximate number of Respondents and records concerned, the likely consequences, the measures taken or proposed, and a contact point at Esperto. Where not all information is available at once, Esperto provides it in phases without undue delay.
- 6.3 Esperto takes the measures reasonably necessary to contain the breach and to limit its consequences, documents the breach, and cooperates with Customer and, through Customer, with the Controller in their investigation.
- 6.4 Notifying a supervisory authority or Respondents is the Controller's responsibility. Esperto does not itself notify the supervisory authority or Respondents of a breach affecting Customer Personal Data, unless Applicable Data Protection Law requires it to do so or Customer asks it to.
- 6.5 A notification under this Article is not an acknowledgement of fault or liability.

7. Assistance to the Controller

- 7.1 Rights of Respondents. Taking into account the nature of the Processing, Esperto assists Customer by appropriate technical and organisational measures in responding to requests from Respondents to exercise their rights under Chapter III GDPR: access, rectification, erasure, restriction, data portability and objection. If Esperto receives such a request directly, it does not respond on the merits but forwards the request to Customer without undue delay and informs the Respondent that it has done so. Reports and Respondent data can be exported from the platform in a structured, commonly used and machine-readable format.
- 7.2 Security, breaches, impact assessments and prior consultation. Taking into account the nature of the Processing and the information available to it, Esperto assists Customer in ensuring compliance with Articles 32 to 36 GDPR: security, breach notification, data protection impact assessments and prior consultation of the supervisory authority. The description of the Processing in Annex 1, the measures in Annex 2 and the list in Annex 3 are provided for that purpose and may be passed on to the Controller and to a supervisory authority.
- 7.3 Costs. Assistance under Article 7.1 and the provision of the information in the Annexes are included in the Services. Assistance under Article 7.2 that goes beyond providing that information, and assistance under Article 7.1 that is excessive in number or scope, is provided at Esperto's then current hourly rates, unless the need for assistance results from Esperto's breach of this DPA.

8. Sub-processors

- 8.1 General authorisation. Customer gives Esperto general authorisation, and in the situation of Article 2.2 confirms that it holds the Controller's general authorisation, to engage the Sub-processors listed in Annex 3 and to replace or add Sub-processors in accordance with this Article.
- 8.2 Notice and objection. Esperto informs Customer in writing, email included, of any intended addition or replacement of a Sub-processor at least 30 days before the new Sub-processor starts processing Customer Personal Data. Customer may object within that period on reasonable grounds relating to data protection. The Parties then discuss the objection in good faith. If Esperto cannot accommodate the objection within a reasonable time, Customer may terminate the affected part of the Services by written notice without penalty, and Article 11 applies to the data concerned. If Customer does not object within the period, the Sub-processor is deemed approved.

- 8.3 Flow-down. Esperto enters into a written contract with each Sub-processor that imposes data protection obligations at least equivalent to those in this DPA, in particular on instructions, confidentiality, security, assistance, deletion and audit. Where a Sub-processor processes Customer Personal Data outside the EEA, Article 9 applies.
- 8.4 Responsibility. Esperto remains fully liable to Customer for the performance of each Sub-processor's obligations.
- 8.5 Information. On request Esperto provides Customer with the information it needs to assess a Sub-processor, including a summary of the data protection terms agreed with it. Esperto may redact commercial terms.

9. Transfers outside the EEA

- 9.1 Assessment data, being the Respondent data, responses, scores and reports described in Annex 1, is stored and processed on servers in the Netherlands and is not transferred outside the European Economic Area.
- 9.2 Esperto does not transfer other Customer Personal Data to a country outside the EEA that is not covered by an adequacy decision of the European Commission, and does not permit a Sub-processor to do so, unless (a) the transfer is covered by the Standard Contractual Clauses or another transfer instrument under Chapter V GDPR entered into by Esperto or the Sub-processor, (b) Esperto has assessed whether the law and practice of the destination country require supplementary measures and has implemented those measures, and (c) the transfer is listed in Annex 3 together with the transfer mechanism used.
- 9.3 Where an Instruction itself requires a transfer outside the EEA, for example because Customer asks Esperto to send a report to a recipient outside the EEA, the Controller is responsible for the lawfulness of that transfer.

10. Information and audits

- 10.1 Esperto makes available to Customer all information necessary to demonstrate compliance with Article 28 GDPR and this DPA. In the first instance this consists of this DPA and its Annexes, Esperto's answers to a reasonable written security questionnaire, and any recent report or attestation that Esperto or its hosting partner holds. An audit under Article 10.2 takes place only where that information does not reasonably suffice.

- 10.2 Customer, or an independent auditor mandated by Customer who is not a competitor of Esperto and is bound by confidentiality, may audit Esperto's compliance with this DPA. An audit (a) takes place at most once in every period of twelve months, unless a personal data breach has occurred, a supervisory authority requires it, or the information provided under Article 10.1 gives reasonable grounds for concern; (b) is announced in writing at least 30 days in advance, stating its scope; (c) is conducted during business hours in a manner that does not unreasonably disrupt Esperto's operations; and (d) is limited to the systems, documents and personnel involved in the Processing of Customer Personal Data. Sub-processors are audited through the information and audit rights Esperto holds towards them.
- 10.3 Costs. Each Party bears its own costs of an audit. Where an audit requires more than one working day of Esperto's time, Esperto may charge the additional time at its then current hourly rates, unless the audit reveals a material breach of this DPA by Esperto, in which case Esperto bears its own costs in full.
- 10.4 In the situation of Article 2.2, the Controller exercises the rights in this Article through Customer, or directly on the same terms where Customer's contract with the Controller so requires. Customer may share the results with the Controller. Customer and its End Clients together are entitled to one audit per period of twelve months, unless an exception in Article 10.2(a) applies.

11. Duration, end of the Services, deletion and return

- 11.1 This DPA applies for as long as Esperto processes Customer Personal Data, regardless of the term of the Agreement.
- 11.2 Within 30 days after the end of the Services, or in the situation of Article 2.2 after the end of the Services for a specific End Client, Customer instructs Esperto in writing whether it wants Customer Personal Data returned or deleted. Return takes place through an export from the platform in a structured, commonly used and machine-readable format, after which Esperto deletes the data. If Customer gives no instruction within that period, Esperto deletes the data.
- 11.3 Esperto deletes Customer Personal Data, and ensures that its Sub-processors delete it, within 30 days after the instruction to delete or after the end of the period in Article 11.2, and confirms deletion in writing on request.
- 11.4 Backups. Data contained in backups made by the hosting partner before deletion is not deleted from those backups individually. It is overwritten in the hosting partner's normal backup cycle, with a standard retention of seven days, after deletion from the platform. Until then the data remains protected by the measures in Annex 2, is not

restored except where necessary to recover the platform after an incident, and in that case is deleted again from the restored environment without undue delay.

- 11.5 Esperto may retain Customer Personal Data to the extent and for as long as Union or Member State law requires, and protects it in accordance with this DPA during that period.

12. Obligations of Customer

- 12.1 Customer is responsible for the lawfulness of the Processing it instructs, including for having a legal basis, for informing Respondents or ensuring that the Controller does so, and for the accuracy of the Respondent data it enters into the platform.
- 12.2 Customer ensures that its Instructions comply with Applicable Data Protection Law and, in the situation of Article 2.2, with its contract with the Controller.
- 12.3 No decisions based solely on an assessment outcome. Customer shall not use, and shall ensure that the Controller and any recipient of a report do not use, an assessment outcome as the sole basis for a decision that produces legal effects concerning a Respondent or similarly significantly affects a Respondent, in particular a decision on selection, recruitment, promotion, remuneration, or the termination of employment or an engagement. Every such decision involves a meaningful assessment by a natural person who has the authority and the competence to depart from the assessment outcome. The assessments are designed as input for development, dialogue and decision-making by people, not as a decision-making mechanism. Esperto's own Processing does not include any decision within the meaning of Article 22 GDPR.
- 12.4 Special categories of data. Customer shall not enter into the platform, and shall instruct Respondents not to enter, special categories of personal data within the meaning of Article 9 GDPR or data relating to criminal convictions and offences within the meaning of Article 10 GDPR. The assessments do not ask for such data and free-text fields carry an instruction not to enter it. If Esperto nonetheless notices such data, it deletes it and informs Customer.

13. Liability

- 13.1 The liability of each Party under or in connection with this DPA is governed by the limitations and exclusions of liability in the Agreement, which apply to this DPA as if set out in full here.

- 13.2 Where the Agreement contains no limitation of liability, the total liability of each Party under or in connection with this DPA, for all events in a calendar year together, is limited to the total fees paid or payable by Customer to Esperto under the Agreement in the twelve months preceding the event giving rise to the liability, with a maximum of EUR 25,000. This limit does not apply to liability arising from a Party's wilful misconduct or gross negligence.
- 13.3 Each Party bears the administrative fines that a supervisory authority imposes on it. Compensation owed to data subjects under Article 82 GDPR is allocated between the Parties in accordance with that Article, so that a Party that has paid full compensation may claim back from the other Party the part corresponding to that Party's responsibility.

14. General

- 14.1 Precedence. Where this DPA and the Agreement or any other arrangement between the Parties conflict on the Processing of Customer Personal Data, this DPA prevails. Where this DPA and the Standard Contractual Clauses conflict, the Standard Contractual Clauses prevail.
- 14.2 Changes in law. If Applicable Data Protection Law changes, or a supervisory authority or court gives guidance that makes an amendment necessary, the Parties amend this DPA in good faith. Esperto may issue an updated standard version and offer it to Customer; it applies once both Parties have signed it.
- 14.3 Amendments. This DPA can only be amended in writing signed by both Parties, except that Annex 2 and Annex 3 may be updated by Esperto as provided in Articles 5.2 and 8.2.
- 14.4 Severability. If a provision of this DPA is invalid or unenforceable, the remainder stays in force and the Parties replace the provision with a valid one that comes as close as possible to its purpose.
- 14.5 Notices. Notices under this DPA are given in writing, email included. Esperto's address for privacy matters and breach notifications is privacy@esperto.one. Customer's address for privacy matters and breach notifications is [\[\[email address\]\]](#).
- 14.6 Governing law and jurisdiction. This DPA is governed by the laws of the Netherlands. Disputes arising from or in connection with this DPA are submitted exclusively to the competent court of the District Court of Central Netherlands (Rechtbank Midden-Nederland), location Utrecht, without prejudice to the right of a data subject or a supervisory authority to bring proceedings elsewhere where the GDPR so provides.

14.7 Survival. Articles 4, 11, 13 and 14 remain in force after this DPA ends.

Signatures

Esperto B.V.	Customer: [[legal name]]
Name: [[name]]	Name: [[name]]
Title: [[title]]	Title: [[title]]
Date: [[date]]	Date: [[date]]
Signature:	Signature:

Annex 1. Description of the Processing

This Annex describes the Processing for both situations in Article 2. Where a field is Customer-specific it is marked as such; the other fields apply to every Customer.

Item	Esperto as processor (Article 2.1)	Esperto as sub-processor (Article 2.2)
Controller	Customer	End Client: [[name and address of the End Client, if the Parties choose to record it]]
Processor	Esperto	Customer
Sub-processors	The parties listed in Annex 3	Esperto, and the parties listed in Annex 3
Subject matter	Provision and operation of the online assessment platform on which Respondents complete assessments, answers are scored and reports are generated, with related support.	Same.
Nature of the Processing	Collection of answers through an online questionnaire; storage; automated scoring; generation of individual and, where applicable, team or organisation reports; making reports available to authorised users of Customer; export; deletion. The scoring and reporting constitute profiling within the meaning of Article 4(4) GDPR. Esperto takes no decision about any Respondent.	Same.
Purpose	The purposes determined by the Controller, such as [[leadership development, team development, coaching, organisational diagnosis]]. Esperto has no purpose of its own.	The purposes determined by the End Client and passed on by Customer.
Duration	The term of the Agreement, plus the deletion period in Article 11.	The duration of Customer's engagement for the End Client, plus the deletion period in Article 11.
Categories of data subjects	Respondents: employees, managers, team members, clients, coachees or other persons invited by Customer. Users of Customer who set up and manage assessments in the platform, to the extent their activity relates to Respondent data.	Respondents: employees, managers, team members, clients, coachees or other persons invited by or on behalf of the End Client. Users of Customer and, where applicable, of the End Client.
Categories of personal data	Name; email address; organisation; role or team where applicable; answers to the questionnaire; scores; the generated report; free-text entries by the Respondent.	Same.
Special categories of data	None requested. See Article 12.4.	Same.
Retention instruction	[[Retention period set by Customer, or "until the end of the Services" (default)]]	[[Retention period set by the End Client and passed on by Customer, or "until the end of the Services for this End Client" (default)]]



Item	Esperto as processor (Article 2.1)	Esperto as sub-processor (Article 2.2)
Expert Partner	[[None / receives usage data at aggregate level only / receives individual responses; name of the Expert Partner]]	Same, as passed on to the End Client by Customer.
Location of the Processing	The Netherlands (assessment platform). See Annex 3 for the other Sub-processors.	Same.

Annex 2. Technical and organisational measures

This Annex describes the measures Esperto applies to Customer Personal Data. It follows the order commonly used in security schedules of larger organisations. Where a heading is not listed, Esperto makes no statement about it.

Measure	What Esperto does
Pseudonymisation and encryption	All traffic between Respondents, users and the platform is encrypted in transit (TLS). Respondents are identified by name and email address only; no government identification numbers are collected.
Confidentiality	Access to Customer Personal Data is granted on a need-to-know basis through individual named accounts, with strong, unique passwords for administrator access. Everyone who works for or with Esperto is bound by a confidentiality obligation (Article 4). Esperto has data processing agreements with the suppliers that process personal data on its behalf (Annex 3).
Availability, resilience and ability to restore	The platform is hosted in data centres in the Netherlands operated by hosting partner ACC ICT. The hosting partner makes automated daily backups of the hosted application landscape on a disk-to-disk-to-disk basis and replicates them to a second, geographically separate data centre in the Netherlands, so that an incident at one location cannot affect the environment and its backups together. Standard backup retention is seven days and can be adjusted on request. Restores are tested periodically, including a check that restored data is usable and not merely present. Active storage is replicated to a storage environment outside the data centre in which it runs. The hosting partner manages incident handling around the clock.
Testing, assessing and evaluating the measures	Esperto reviews the measures in this Annex at least once a year and whenever the platform, its hosting or a Sub-processor changes, and updates this Annex accordingly (Article 5.2).
User identification and authorisation	Users of Customer sign in with individual accounts. Organisations that run assessments in their own environment can switch on single sign-on and enforce it for their users. Access then follows the organisation's own identity provider, including any multi-factor requirement that provider applies. Where single sign-on is not switched on, users sign in with an email address and a password. Respondents access their questionnaire through a personal invitation. Esperto's own administrator access uses individual accounts with strong, unique passwords. Access to the hosting partner's management portal requires two-factor authentication with a software token; this applies to the hosting partner's portal only and is separate from the single sign-on option for Customer environments described above.
Protection of data during transmission	All traffic is encrypted in transit (TLS).
Protection of data during storage	Assessment data is stored on servers in data centres in the Netherlands managed by ACC ICT. All data centres involved, including the location that holds the replicated backups, are in the Netherlands, and stored data does not leave the Netherlands. Access to the servers is limited to the hosting partner and to Esperto administrators, each through individual accounts.

Measure	What Esperto does
Physical security of the processing locations	The platform is not hosted on Esperto's premises. The data centres in the Netherlands are operated by ACC ICT; physical security of those locations is the hosting partner's responsibility under its agreement with Esperto. Details are available to Customer on request.
Events logging	Server logs are kept and retained for a limited period, which Esperto states to Customer on request.
System configuration	Each Customer environment is configured by Esperto on Customer's instruction: assessments, branding and, where chosen, single sign-on. The questionnaires do not ask for special categories of data, and free-text fields carry an instruction not to enter such data.
Certifications	Esperto B.V. holds no security certification of its own; ISO 27001 certification of Esperto is in progress. Hosting partner ACC ICT holds ISO 27001:2022, ISO 9001:2015 and NEN 7510-1:2017 and has an ISAE 3402 Type II assurance report. The data centres used by the hosting partner hold ISO 27001, ISO 9001 and ISO 14001 as a minimum. Certificates are available to Customer on request.
Data minimisation	Only the data needed to invite a Respondent and to deliver the report is collected. Special categories of data are not requested. Any special category data that nonetheless reaches the platform is deleted once identified (Article 12.4).
Data quality	Respondents enter their own answers. Identity data (name, email address, role or team) is supplied by Customer, which can correct it in the platform. Esperto rectifies data on Instruction (Article 7.1). Scoring follows the documented logic of the assessment concerned.
Limited data retention	Retention is set by the Controller (Annex 1). Esperto deletes or returns the data as set out in Article 11. Backups are overwritten in the hosting partner's normal cycle.
Accountability	Esperto maintains this DPA, a published privacy statement (espertoassessments.com/privacy-policy) and data processing agreements with its suppliers. Privacy contact: privacy@esperto.one . Esperto is not required to appoint a data protection officer and has not appointed one.
Data portability and erasure	Reports and Respondent data can be exported from the platform in a structured, commonly used and machine-readable format. Data is deleted on Instruction within the period in Article 11, with written confirmation on request.
Assistance to the Controller	See Article 7. Requests from Respondents received by Esperto are forwarded to Customer without undue delay.
Measures for Sub-processors	See Article 8. Every Sub-processor is bound by a written contract with obligations at least equivalent to this DPA. Assessment data, including backups, is held only in data centres in the Netherlands and does not leave the Netherlands.

Annex 3. Sub-processors

Esperto engages the following Sub-processors for the Processing of Customer Personal Data. Changes are made in accordance with Article 8.

Name	Registered seat	Role	Location of processing	Transfer mechanism
ACC ICT	ACC ICT B.V., Nieuwegein, the Netherlands	Hosting and management of the assessment platform, including backups. Processes all assessment data.	The Netherlands	Not applicable (EEA)
Hostinger	Hostinger International Ltd., Larnaca, Cyprus	Hosting of the website espertoassessments.com and the checkout environment. Processes the data of persons who order through the website. Does not process assessment data.	Germany (data centre)	Not applicable (EEA)
Microsoft (Microsoft 365)	Microsoft Ireland Operations Limited, Dublin, Ireland	Email, document storage and collaboration used by Esperto staff for support and correspondence with Customer. May contain Customer Personal Data incidentally, for example a Respondent list sent by Customer by email.	European Union (Microsoft EU Data Boundary)	Standard Contractual Clauses in Microsoft's Data Protection Addendum, for any remaining transfer

For transparency: Esperto also uses ActiveCampaign (ActiveCampaign LLC, Chicago, United States) for newsletters and service emails to Customer's contact persons. That is data for which Esperto is controller (Article 2.4) and it does not include Respondent data. Transfer mechanism: ActiveCampaign is certified under the EU-US Data Privacy Framework. Stripe processes payments as an independent controller and is not a Sub-processor.