Data Processing Agreement

Template - review with your counsel before first use.

v1.1 - July 2026

This Data Processing Agreement (the "DPA") is entered into between:

the client identified below, with its registered office at the address stated below (the "Controller"); and

Client (Controller) legal name

Client (Controller) registration number

Client (Controller) registered address

VALOR CONSULTING, Reg. no. 544967287, with its registered office at the address stated below (the "Processor"),

Processor registered address

each a "Party" and together the "Parties".

1. Background and scope

1.1 The Processor provides Azure cost-assessment and optimisation services to the Controller under an engagement agreement or accepted proposal between the Parties (the "Main Agreement"). In performing those services, the Processor processes limited personal data on the Controller's behalf: business contact data of the Controller's staff, and personal data incidentally contained in Azure invoices, cost and usage exports, and account metadata.

1.2 This DPA is entered into pursuant to Article 28 of Regulation (EU) 2016/679 (the "GDPR") and forms part of the Main Agreement. In case of conflict between this DPA and the Main Agreement regarding the processing of personal data, this DPA prevails.

1.3 Terms such as "personal data", "processing", "data subject", "personal data breach", and "supervisory authority" have the meanings given in the GDPR.

2. Subject matter, duration, nature and purpose

2.1 Subject matter. The processing of personal data contained in Azure billing and usage documentation shared by the Controller, and in Azure account and resource metadata viewed by the Processor through view-only access, in the course of the cost assessment and optimisation services.

2.2 Duration. The processing continues for the term of the Main Agreement and until the personal data has been returned or deleted in accordance with Clause 11.

2.3 Nature. Collection (receipt of files shared by the Controller), viewing via read-only access to the Controller's Azure environment, storage, analysis, and deletion. The Processor does not modify the Controller's Azure environment or the personal data within it.

2.4 Purpose. Analysing the Controller's Azure spend and usage in order to identify cost-optimisation

opportunities, and producing assessment reports and recommendations for the Controller.

2.5 The details in Clauses 2 and 3 constitute Annex A for the purposes of Article 28(3).

3. Categories of personal data and data subjects

3.1 Categories of personal data:

a. business contact data: names, business email addresses, business phone numbers, job titles, and organisational details of the Controller's staff involved in the engagement or named in billing documents;
b. billing and usage metadata contained in Azure invoices and exports: user principal names, account identifiers, subscription and tenant names, resource names and tags, and similar identifiers that may directly or indirectly identify individuals.

3.2 Categories of data subjects: employees, contractors, and other staff of the Controller (and, where applicable, of its affiliates) whose identifiers appear in the data described in Clause 3.1.

3.3 No special categories. The services do not require special categories of personal data (Article 9 GDPR) or data relating to criminal convictions (Article 10 GDPR), and the Controller shall not provide such data. If such data is nevertheless shared, the Processor will notify the Controller and delete it unless instructed otherwise in writing.

4. Instructions of the Controller

4.1 The Processor shall process personal data only on documented instructions from the Controller, including with regard to transfers to a third country or international organisation, unless required to do so by Union or Member State (or applicable EEA state) law to which the Processor is subject; in that case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information.

4.2 The Main Agreement, this DPA, and its Annexes constitute the Controller's documented instructions. Additional instructions must be given in writing and must be consistent with the Main Agreement.

4.3 The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes the GDPR or other applicable data protection law, and may suspend the affected processing until the instruction is confirmed or amended.

5. Obligations of the Processor

5.1 The Processor shall:

a. ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
b. implement and maintain the technical and organisational measures described in Clause 6 and Annex B;
c. respect the conditions in Clause 7 for engaging sub-processors;
d. taking into account the nature of the processing, assist the Controller by appropriate technical and organisational measures, insofar as this is possible, in fulfilling the Controller's obligation to respond to requests from data subjects exercising their rights under Chapter III GDPR;
e. assist the Controller in ensuring compliance with Articles 32 to 36 GDPR (security, breach

notification, data protection impact assessments, and prior consultation), taking into account the nature of the processing and the information available to the Processor;

f. at the Controller's choice, delete or return all personal data after the end of the provision of services, in accordance with Clause 11; and

g. make available to the Controller all information necessary to demonstrate compliance with Article 28 GDPR and allow for and contribute to audits in accordance with Clause 9.

5.2 The Processor shall not sell personal data, use it for its own purposes, or use it to train or improve any product or model.

5.3 If a data subject contacts the Processor directly about personal data processed under this DPA, the Processor shall forward the request to the Controller without undue delay and shall not respond on the merits except on the Controller's documented instruction.

6. Security of processing

6.1 The Processor shall implement appropriate technical and organisational measures under Article 32 GDPR, appropriate to the risks to data subjects, including at minimum:

a. View-only access: any access to the Controller's Azure environment is granted on a read-only basis (for example, the built-in Reader and Cost Management Reader roles); the Processor does not request or use write, contributor, or owner permissions during the assessment;

b. Encrypted transit: all data shared with or accessed by the Processor is transmitted over encrypted channels (TLS 1.2 or higher), and files at rest on Processor systems are stored encrypted;

c. Access logging: access by Processor personnel to shared files and to the Controller's environment is limited to named individuals on a need-to-know basis and is logged; logs are retained for the duration of the engagement and made available to the Controller on request;

d. Deletion on request: shared files and derived working materials are deleted at the Controller's request at any time, and in any event in accordance with Clause 11.

6.2 The full set of technical and organisational measures is described in Annex B. The Processor may update Annex B from time to time, provided the updates do not materially reduce the overall level of protection.

7. Sub-processors

7.1 The Controller grants the Processor general written authorisation to engage the sub-processors listed in Annex C.

7.2 The Processor shall inform the Controller in writing of any intended addition or replacement of a sub-processor at least thirty (30) days in advance, giving the Controller the opportunity to object on reasonable, data-protection-related grounds. If the Parties cannot resolve an objection in good faith, the Controller may terminate the affected services without penalty.

7.3 The Processor shall impose on each sub-processor, by way of contract, the same data protection obligations as set out in this DPA, in particular providing sufficient guarantees to implement appropriate technical and organisational measures. Where a sub-processor fails to fulfil its data protection obligations, the Processor remains fully liable to the Controller for the performance of that sub-processor's obligations.

8. Personal data breach notification

8.1 The Processor shall notify the Controller without undue delay, and in any event within forty-eight (48) hours, after becoming aware of a personal data breach affecting personal data processed under this DPA.

8.2 The notification shall, to the extent the information is available, describe the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, the measures taken or proposed, and a contact point. Information may be provided in phases as it becomes available.

8.3 The Processor shall cooperate with the Controller in investigating, mitigating, and remediating the breach, and shall not notify any supervisory authority or data subject on the Controller's behalf unless required by law or instructed by the Controller in writing.

9. Audit rights

9.1 The Processor shall make available to the Controller all information necessary to demonstrate compliance with Article 28 GDPR and this DPA, including, on request, summaries of relevant policies, access logs, and any available third-party attestations or certifications.

9.2 The Controller (or an independent auditor mandated by it and not a competitor of the Processor) may audit the Processor's compliance with this DPA once per twelve (12) months, on at least thirty (30) days' written notice, during normal business hours, and without unreasonable disruption to the Processor's operations. Additional audits are permitted where required by a supervisory authority or following a personal data breach. Each Party bears its own audit costs.

10. International transfers

10.1 The Processor shall process personal data within the European Economic Area (EEA), or in a third country recognised by the European Commission as providing an adequate level of protection, unless Clause 10.2 applies.

10.2 Any transfer of personal data to a third country without an adequacy decision shall take place only on the basis of appropriate safeguards under Chapter V GDPR, in particular the European Commission's Standard Contractual Clauses (Decision (EU) 2021/914) ("SCCs"), supplemented where necessary by additional measures identified through a transfer impact assessment. Where the SCCs apply, they are incorporated by reference and prevail over this DPA to the extent of any conflict.

10.3 Sub-processor locations and applicable transfer mechanisms are documented in Annex C.

11. Return and deletion on termination

11.1 On expiry or termination of the Main Agreement, or earlier at the Controller's written request, the Processor shall, at the Controller's choice, return to the Controller or securely delete all personal data processed under this DPA, including copies in working files and derived analyses, unless Union or Member State (or applicable EEA state) law requires storage of the personal data.

11.2 Unless the Controller instructs otherwise, the Processor shall complete deletion within thirty (30) days of the end of the services and shall confirm completion in writing. Personal data in encrypted backups is deleted in the ordinary backup rotation and remains protected by this DPA until deleted.

11.3 The Controller is responsible for revoking the Processor's view-only access to its Azure environment; the Processor shall not attempt to use or re-establish such access after the end of the services.

12. Liability, term and general

12.1 Each Party is liable for damage caused by its processing in accordance with Article 82 GDPR. Limitations of liability agreed in the Main Agreement apply to this DPA to the extent permitted by applicable law.

12.2 This DPA takes effect on the date of the last signature below and remains in force for as long as the Processor processes personal data on the Controller's behalf.

12.3 This DPA is governed by the same law and subject to the same venue as the Main Agreement or, if none is specified there, by the laws and courts of [Governing law / venue], provided always that mandatory provisions of the GDPR and applicable Member State (or applicable EEA state) data protection law prevail.

Annexes

Annex A - Details of processing

The subject matter, duration, nature, and purpose of the processing, the categories of personal data, and the categories of data subjects are as set out in Clauses 2 and 3, which constitute Annex A for the purposes of Article 28(3) GDPR. The Controller's contact for data protection matters is:

Controller's data-protection contact (name · role · email)

Annex B - Technical and organisational measures (TOMs)

The Processor's security measures are described in Clause 6, including the view-only access model, encryption in transit and at rest, named-individual access control and access logging, personnel confidentiality undertakings, and deletion-on-request procedures. Any engagement-specific additions to these measures are recorded in writing between the Parties and form part of this Annex B.

Annex C - Approved sub-processors

The Processor's standing infrastructure providers fall into the following categories, each of which is a POSSIBLE sub-processor that may touch engagement data: hosting and infrastructure, transactional email delivery, and productivity and meetings suite. Whether a provider in fact processes personal data under this DPA is confirmed per engagement. Each confirmed sub-processor is listed below with its name, registered address, processing location, services provided, and the transfer mechanism relied on where processing occurs outside the EEA (Clauses 7 and 10).

Approved sub-processors at the date of signature (name · address · location · services · transfer mechanism; or "none")

Signatures

Signatures

For Client (Controller)

Signature: _____
Signature

Name: _____
Name

Title: _____
Title

Date: _____
Date

For VALOR CONSULTING (Processor)

Signature: _____
Signature

Name: _____
Name

Title: _____
Title

Date: _____
Date