Data Processing Agreement CloudtoShare

Standard data processing agreement under the CloudtoShare General Terms and Conditions (Article 14). In case of any discrepancy, the Dutch version prevails.

Parties

1. **[Client name]**, having its registered office in [city], Chamber of Commerce no. [number], represented by [name], hereinafter: "Controller"; and
2. **CloudtoShare B.V.**, High Tech Campus 5, 5656 AE Eindhoven, Chamber of Commerce no. 88581306, represented by [name], hereinafter: "Processor".

Where the Controller itself acts as a processor for an End Customer, CloudtoShare acts as sub-processor. This agreement then applies in the same way, and "Controller" also includes the End Customer where the context requires.

Recitals

- The parties have concluded one or more Agreements to which the CloudtoShare General Terms and Conditions apply.
- In performing them, the Processor processes personal data on behalf of the Controller, usually because the Processor's consultants are given access to the Controller's systems, such as Salesforce.
- The parties record their arrangements in this agreement, as required by Article 28 of the General Data Protection Regulation (GDPR).

Article 1 – Definitions

1.1 Terms from the GDPR, such as personal data, processing, controller, processor, data subject and personal data breach, have the meaning given in the GDPR.

1.2 **Agreement:** the agreement or agreements between the parties for the provision of services by the Processor. **End Customer:** the customer of the Controller, where the Controller purchases the services for the benefit of a third party. **Data Breach:** a personal data breach. **In writing:** on paper or by e-mail.

Article 2 – Subject matter and scope

2.1 This agreement applies to all processing of personal data that the Processor carries out for the Controller under the Agreement.

2.2 The subject matter, nature and purpose of the processing, the types of personal data and the categories of data subjects are set out in Annex 1.

2.3 The Controller determines the purpose and means of the processing. The Processor has no control over the personal data and does not use them for its own purposes.

2.4 The Processor is not set up to process special categories of personal data, criminal data or national identification numbers. The Controller will only have the Processor process such data after prior written agreement on appropriate additional measures.

Article 3 – Instructions

3.1 The Processor processes personal data only on the Controller's written instructions. The Agreement, this data processing agreement and instructions given by the Controller through the agreed contact persons count as such instructions.

3.2 The Processor may process personal data without instructions where required by law. The Processor then informs the Controller in advance, unless the law prohibits this.

3.3 The Processor immediately informs the Controller if, in its opinion, an instruction infringes the GDPR or other data protection law, and may suspend the execution of that instruction.

3.4 The Controller warrants that the processing is lawful, that a valid legal basis exists and that data subjects have been adequately informed.

Article 4 – Confidentiality

4.1 The Processor ensures that everyone processing personal data under its authority, including employees and engaged consultants, is bound by confidentiality.

4.2 The Processor only grants access to personal data to persons who need it to perform the Agreement.

Article 5 – Security

5.1 The Processor takes appropriate technical and organisational measures to protect personal data against loss and unlawful processing, as referred to in Article 32 GDPR, taking into account the state of the art, implementation costs, the nature and scope of the processing and the risks to data subjects.

5.2 The measures the Processor takes in any event are set out in Annex 2. The Processor may adjust these measures, provided the level of security is not reduced.

5.3 Because the Processor mostly works in the Controller's systems, the Controller is responsible for the security of those systems, including user management, permissions, multi-factor authentication and the timely revocation of the Processor's consultants' access.

5.4 The Processor does not guarantee that security is effective under all circumstances.

Article 6 – Sub-processors

6.1 The Controller gives the Processor general authorisation to engage sub-processors. The sub-processors the Processor uses when this agreement is concluded are listed in Annex 3.

6.2 The Processor informs the Controller at least ten (10) working days in advance of a new or replacement sub-processor. The Controller may object In writing on reasonable grounds within that period. The parties will then discuss a solution. If they cannot agree, either party may terminate the relevant part of the Agreement.

6.3 The Processor imposes on sub-processors at least the same obligations as in this agreement, and remains responsible towards the Controller for their compliance.

6.4 Employees of the Processor are not sub-processors.

Article 7 – Transfers outside the EEA

7.1 The Processor processes personal data within the European Economic Area (EEA).

7.2 Transfer to, or access from, a country outside the EEA is only permitted on an appropriate basis under Chapter V GDPR, such as an adequacy decision of the European Commission, the EU-US Data Privacy Framework or the European Commission's standard contractual clauses. Annex 3 states where each sub-processor processes data.

Article 8 – Assistance

8.1 The Processor assists the Controller, as far as reasonably possible, in handling requests from data subjects, such as requests for access, rectification or erasure. If the Processor receives such a request directly, it forwards it to the Controller without delay and does not handle it itself.

8.2 Taking into account the nature of the processing and the information available to it, the Processor provides reasonable assistance with the Controller's obligations under Articles 32 to 36 GDPR, such as a data protection impact assessment (DPIA) or a prior consultation of the supervisory authority.

8.3 The Processor may charge the reasonable costs of assistance under this article at its applicable rates, unless the assistance is required because of a failure by the Processor.

Article 9 – Data Breaches

9.1 The Processor informs the Controller without undue delay, and no later than forty-eight (48) hours after discovering a Data Breach, using the contact details provided by the Controller.

9.2 The Processor provides, as far as known: the nature of the Data Breach, the categories and approximate number of data subjects and records concerned, the likely consequences, and the measures taken or proposed to address the Data Breach and mitigate its effects. Information not yet available is provided as soon as possible.

9.3 The Processor immediately takes reasonable measures to contain the Data Breach and prevent recurrence.

9.4 Assessing a Data Breach and notifying the Dutch Data Protection Authority and data subjects is the Controller's responsibility. The Processor does not notify the supervisory authority or data subjects itself, unless required by law.

Article 10 – Information and audits

10.1 On request, the Processor makes available to the Controller all information reasonably necessary to demonstrate compliance with this agreement and Article 28 GDPR. The Processor keeps a record of processing activities as referred to in Article 30(2) GDPR.

10.2 If that information is insufficient, the Controller may have an audit carried out on the terms of Article 17 of the CloudtoShare General Terms and Conditions: at most once per calendar year, with at least four (4) weeks' notice, by an independent expert bound by confidentiality, and at the Controller's expense, unless the audit reveals a material failure by the Processor.

10.3 An audit following a Data Breach or an order of a supervisory authority is also possible outside the annual frequency.

Article 11 – Requests from authorities

11.1 If the Processor receives a request or order from a public authority to disclose personal data, it informs the Controller without delay, unless the law prohibits this. The Processor discloses no more data than strictly necessary and only cooperates where legally obliged.

Article 12 – Return and deletion

12.1 After the Agreement ends, or earlier at the Controller's request, the Processor deletes the personal data it holds for the Controller, or returns them if the Controller so requests, within thirty (30) days, unless a statutory retention obligation applies.

12.2 Data that reside only in the Controller's systems, such as its Salesforce environment, remain there. The Processor does delete local copies, exports and test files, and the Controller revokes the Processor's access.

12.3 On request, the Processor confirms the deletion In writing.

Article 13 – Liability

13.1 The parties' liability for damage in connection with this data processing agreement is governed by Article 12 of the CloudtoShare General Terms and Conditions. Its limitations also apply to claims under this data processing agreement, to the extent permitted by mandatory law.

13.2 The Controller indemnifies the Processor against claims from data subjects and supervisory authorities resulting from an unlawful instruction or another failure by the Controller.

13.3 An administrative fine imposed on a party is borne by that party.

Article 14 – Term, precedence and governing law

14.1 This data processing agreement applies for as long as the Processor processes personal data for the Controller. Obligations that by their nature survive, such as confidentiality and deletion, continue to apply thereafter.

14.2 In case of conflict between this data processing agreement and the Agreement or the General Terms and Conditions, this data processing agreement prevails with regard to the processing of personal data, except for liability (Article 13).

14.3 Amendments are only valid if agreed In writing. If the GDPR or other data protection law changes, the parties will amend this agreement by mutual consultation.

14.4 This agreement is governed by Dutch law. Disputes are submitted to the District Court of Oost-Brabant, 's-Hertogenbosch location.

Signature

This data processing agreement also applies without signature where it has been declared applicable through the Agreement, an order form or the CloudtoShare website and accepted by the Controller.

	Controller	CloudtoShare B.V.
Name		
Title		
Date		
Signature		

Annex 1 – Description of the processing

- **Subject matter:** provision of Salesforce, data and AI services by the Processor, such as advice, configuration, development, data migration, testing, training, managed services and support.
- **Nature of the processing:** viewing, consulting, structuring, modifying, importing, exporting, migrating, testing and deleting data in the Controller's systems, such as Salesforce and connected applications.
- **Purpose:** performance of the Agreement.
- **Categories of data subjects:** employees, customers, prospects, leads, contact persons, suppliers and other business relations of the Controller or its End Customer.
- **Types of personal data:** name, job title, company details, e-mail address, telephone number, address, communication and activity data (such as e-mails, meetings and notes), sales and service data, user data and log files, and [any additional data per Agreement].
- **Special categories of personal data:** none, unless agreed otherwise In writing (Article 2.4).
- **Duration:** for the term of the Agreement, plus the deletion period in Article 12.
- **Processor's privacy contact:** [name, e-mail, telephone].
- **Controller's data breach contact:** [name, e-mail, telephone].

Annex 2 – Security measures

Organisational

- Confidentiality obligation for all employees and engaged consultants.
- Access to client data only for consultants involved in the assignment (need-to-know).
- Periodic awareness on information security and privacy.
- Procedure for reporting and handling Data Breaches.
- Consultants' access is ended when the assignment ends.

Technical

- Multi-factor authentication on all of the Processor's business accounts (Microsoft 365) and single sign-on where possible.
- Managed and encrypted laptops with up-to-date security patches and antivirus.
- Encrypted connections (TLS) when accessing the Controller's systems.
- Preferably working in sandboxes with anonymised or test data; production data only where needed for the assignment.
- No storage of client data on personal devices or in unapproved cloud services; exports are deleted after use.
- No input of the Controller's personal data into public AI tools, unless agreed In writing and with appropriate safeguards.

Annex 3 – Sub-processors

Overview at the time this agreement is concluded. Complete or delete as applicable.

1. **Microsoft Ireland Operations Ltd.**: Microsoft 365 (e-mail, Teams, storage of project documents). Location: EEA (EU Data Boundary).
2. **[Independent consultants or partners]**: performance of parts of the work. Location: [country].
3. **[Other tools, for example Slack or an AI service]**: [purpose]. Location: [country and transfer basis if outside the EEA].

Salesforce is generally not a sub-processor of the Processor: the Controller purchases Salesforce itself, and Salesforce is then directly the Controller's processor.