Data processing agreement

Processor IMGN Technologies (Pty) Ltd, registration number 2015/026469/07
Version 3, 16 November 2026
Published at precedent.biz/dpa

1. About this agreement

1.1 This data processing agreement (“**DPA**”) is between **IMGN Technologies (Pty) Ltd**, a private company registered in South Africa under number 2015/026469/07, with its registered office at 20 Krynauw Street, Worcester, Western Cape, 6850, South Africa, which operates Precedent (“**IMGN**”, “we”), and the organisation that uses the hosted Precedent service under the terms of service (the “**Customer**”, “you”).

1.2 It forms part of the terms of service (precedent.biz/terms) that govern the Customer’s use of the hosted service at precedent.biz (the “**Terms**”) and takes effect when the Customer accepts the Terms. It needs no signature to apply. A Customer whose procurement process requires a countersigned copy can sign the PDF version of this page, which has the same text.

1.3 It applies to personal data that IMGN processes on the Customer’s behalf when providing the service. It does not apply to personal data that IMGN processes as a controller, such as account, billing and security records and visits to the public website, which the privacy policy (precedent.biz/privacy) covers.

1.4 If this DPA conflicts with the Terms, this DPA prevails on the protection of personal data. If it conflicts with the Clauses or the UK Addendum incorporated by section 11, they prevail.

1.5 It does not apply to copies of Precedent that the Customer or anyone else runs on their own infrastructure. IMGN has no access to those deployments.

2. Definitions

2.1 In this DPA:

- **Data Protection Law** means every law on the protection of personal data that applies to the processing under this DPA, including the EU General Data Protection Regulation 2016/679 (“**GDPR**”), the GDPR as it forms part of the law of the United Kingdom together with the Data Protection Act 2018 (“**UK GDPR**”), the Swiss Federal Act on Data Protection (“**FADP**”), and South Africa’s Protection of Personal Information Act 4 of 2013 (“**POPIA**”).
- **Customer Personal Data** means personal data, including personal information as POPIA defines it, that IMGN processes on the Customer’s behalf under this DPA, as described in Annex 1.
- **Controller** includes a responsible party under POPIA, and **processor** includes an operator under POPIA.
- **Security Incident** means a personal data breach as the GDPR and UK GDPR define it, and any situation in which there are reasonable grounds to believe that Customer Personal Data has been accessed or acquired by an unauthorised person, as section 21(2) of POPIA describes.
- **Sub-processor** means a third party that IMGN engages to process Customer Personal Data.
- **Workspace** means a workspace in the hosted service that the Customer owns or administers, with everything its members and connected assistants put into it.
- **Clauses** means the standard contractual clauses annexed to European Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
- **UK Addendum** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, version B1.0, issued by the UK Information Commissioner under section 119A of the Data Protection Act 2018 and in force from 21 March 2022.

2.2 Other terms, such as personal data, processing, data subject and supervisory authority, have the meanings that Data Protection Law gives them.

3. Roles

3.1 The Customer is the controller of Customer Personal Data and IMGN is its processor. Where the Customer is itself a processor acting for another controller, IMGN is its sub-processor, and the Customer confirms that its controller has authorised IMGN's appointment on these terms.

3.2 The Customer is responsible for having a lawful basis for the processing, for the notices it gives to data subjects, for the accuracy of what it puts into the Workspace, and for the lawfulness of its instructions.

3.3 The Customer chooses which integrations, model accounts and assistants to connect to its Workspace. A service the Customer connects under its own account, such as its Slack, Microsoft Teams, Jira, GitHub or model provider account, processes data under the Customer's own agreement with that provider and is not IMGN's Sub-processor.

3.4 The service is not designed for special categories of personal data (special personal information under POPIA), data about criminal convictions, or personal information about children. The Customer will not put such data into the Workspace unless a decision record needs it and the Customer has assessed that the measures in Annex 2 are appropriate for it.

4. Details of the processing

4.1 The subject matter, nature, purpose and duration of the processing, the types of personal data and the categories of data subjects are described in Annex 1.

5. Instructions

5.1 IMGN processes Customer Personal Data only on the Customer's documented instructions, including with regard to transfers, unless a law to which IMGN is subject requires otherwise. In that case IMGN will tell the Customer about the legal requirement before processing, unless that law prohibits it on important grounds of public interest.

5.2 The Customer's instructions are the Terms, this DPA, and what the Customer and its users do in the service: the content they enter, the settings administrators choose, the integrations and assistants they connect, the retention policy and legal holds they set, and the exports and deletions they make. Further instructions need IMGN's written agreement.

5.3 IMGN will tell the Customer promptly if, in its opinion, an instruction infringes Data Protection Law.

5.4 IMGN processes Customer Personal Data only with the Customer's knowledge or authorisation, as section 20 of POPIA requires. It does not sell Customer Personal Data, use it for advertising, or use it to train machine learning models.

6. Confidentiality

6.1 IMGN treats Customer Personal Data as confidential and does not disclose it except as this DPA allows or the law requires.

6.2 IMGN gives access to Customer Personal Data only to personnel who need it to provide, secure or support the service, and ensures that each of them is bound by a contractual or statutory duty of confidentiality.

6.3 If a public authority asks IMGN for Customer Personal Data, IMGN will refer it to the Customer where it can, will tell the Customer unless the law forbids it, and will disclose only what it is legally compelled to disclose.

7. Security

7.1 IMGN implements and maintains the technical and organisational measures described in Annex 2. They are designed to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure and access, as Article 32 of the GDPR and sections 19 and 21 of POPIA require.

7.2 IMGN may change those measures as the service develops, but will not reduce the overall level of protection they give.

7.3 The Customer is responsible for the security choices within its control, including whom it invites and which role

each person holds, which assistants and integrations it connects, whether to require single sign-on, and keeping its own credentials safe.

8. Sub-processors

8.1 The Customer gives IMGN general written authorisation to engage Sub-processors. The current list, with what each one does and where it processes data, is published at precedent.biz/sub-processors and forms Annex 3.

8.2 IMGN will give at least 30 days' notice before a new Sub-processor starts processing Customer Personal Data, by updating the list and by email to the Customer's workspace administrators.

8.3 The Customer may object to a new Sub-processor on reasonable grounds relating to data protection by writing to info@precedent.biz within the notice period. The parties will discuss the objection in good faith. If IMGN cannot resolve it, for example by not using that Sub-processor for the Customer's Workspace, the Customer may end the affected service before the change takes effect and receive a refund of fees it has prepaid for the period after the end.

8.4 IMGN imposes on each Sub-processor, by written contract, data protection obligations no less protective than those in this DPA, to the extent relevant to the service the Sub-processor provides, including sufficient guarantees of appropriate security. IMGN remains fully liable to the Customer for each Sub-processor's performance of those obligations.

8.5 On request, IMGN will give the Customer a copy of a Sub-processor's data protection terms. It may remove commercial information that is not about data protection first.

9. Data subject requests and assistance

9.1 If IMGN receives a request from a data subject about Customer Personal Data, it will pass the request to the Customer without undue delay. It will not answer the request itself, other than to say that it has passed it on, unless the Customer authorises it to.

9.2 The service lets the Customer answer most requests itself. Workspace administrators can export the whole Workspace as a JSON file, with links to its uploaded files, under Settings, General; correct a decision by revising it; remove a member or cancel an invitation; revoke an assistant's connection; set a retention policy that permanently deletes archived decisions after a chosen period; and delete the Workspace.

9.3 A revision keeps the earlier text in the decision's history. To remove personal data from that history, the Customer can archive the decision and let its retention policy delete it, or ask IMGN for help.

9.4 Where the service is not enough, IMGN will give the Customer reasonable further assistance in responding to data subjects, taking into account the nature of the processing and the information available to IMGN.

9.5 IMGN will give the Customer the information about the service that it reasonably needs to carry out a data protection impact assessment, to consult a supervisory authority before processing, and to meet its own obligations on security and on notifying Security Incidents.

10. Security incidents

10.1 IMGN will notify the Customer of a Security Incident affecting Customer Personal Data immediately, and in any event within 48 hours, after becoming aware of it. That leaves the Customer time to meet its own obligations, including the 72 hours the GDPR allows for notifying a supervisory authority, and POPIA's requirement to notify the Information Regulator and data subjects as soon as reasonably possible.

10.2 IMGN will send the notice by email to the Customer's workspace administrators. It will describe, as far as IMGN knows at the time, the nature of the incident; the categories and approximate number of data subjects and records concerned; the identity of the unauthorised person, if known; the likely consequences; the measures taken or proposed; and whom to contact for more information. Where IMGN cannot give all of this at once, it will send what it knows and follow up as it learns more.

10.3 IMGN will take reasonable steps to contain and investigate the incident and to reduce its effects, and will cooperate with the Customer's own investigation and notifications. IMGN will not notify the Customer's data subjects or supervisory authorities on the Customer's behalf without the Customer's agreement, unless the law requires it to.

10.4 A notice under this section is not an admission of fault or liability.

11. International transfers

11.1 IMGN is established in South Africa. In the hosted service at precedent.biz, Workspace databases and uploaded files are stored in the European Union, in Ireland. Some Sub-processors, including providers of hosting, email delivery and the AI features, are established or process data in the United States or other countries, as the list at precedent.biz/sub-processors shows. IMGN's personnel may access Customer Personal Data from South Africa to provide and support the service.

11.2 **European Union.** To the extent that the Customer's processing is subject to the GDPR and making Customer Personal Data available to IMGN is a transfer to a third country, the Clauses are incorporated into this DPA by reference, with Module Two (controller to processor), the Customer as data exporter and IMGN as data importer, and completed as follows:

- Clause 7, the docking clause, applies.
- Clause 9(a): Option 2, general written authorisation, with the notice period in section 8.2.
- Clause 11(a): the optional language does not apply.
- Clause 13: the competent supervisory authority is the one identified in Annex 1, part C.
- Clause 17: Option 1. The Clauses are governed by the law of Ireland.
- Clause 18(b): disputes are resolved by the courts of Ireland.
- Annex I of the Clauses is completed by Annex 1 of this DPA, Annex II by Annex 2, and Annex III by Annex 3.

11.3 **United Kingdom.** To the extent that the Customer's processing is subject to the UK GDPR, the UK Addendum is incorporated into this DPA and applies to the Clauses as completed in section 11.2. In Table 1, the parties and their details are those in Annex 1, part A. In Table 2, the Addendum EU SCCs are the Clauses as incorporated by section 11.2, with Module Two and the options chosen there. In Table 3, the Appendix Information is in Annexes 1, 2 and 3. In Table 4, neither party may end the UK Addendum under its section 19.

11.4 **Switzerland.** To the extent that a transfer is subject to the FADP, the Clauses apply as completed in section 11.2 with these changes: the Swiss Federal Data Protection and Information Commissioner is the competent supervisory authority for that transfer; references to the GDPR are read as references to the FADP; and the term "Member State" does not prevent data subjects habitually resident in Switzerland from bringing claims where they live, under Clause 18(c).

11.5 **South Africa.** Where the Customer is subject to POPIA, this DPA is the binding agreement contemplated by section 72(1)(a) of POPIA for transfers of Customer Personal Data to IMGN's storage and Sub-processors outside South Africa. IMGN will transfer Customer Personal Data outside South Africa only to a recipient that is subject to a law, binding corporate rules or a binding agreement that provides an adequate level of protection, as section 72 requires.

11.6 **Onward transfers.** IMGN will transfer Customer Personal Data to a Sub-processor in a country outside the European Economic Area, the United Kingdom, Switzerland and South Africa only where Data Protection Law recognises the transfer: under an adequacy decision or regulations, including the EU-US Data Privacy Framework and its UK Extension for a Sub-processor certified under them; under standard contractual clauses, including Module Three of the Clauses (processor to processor) with the UK Addendum where UK data is concerned; or, for POPIA, under a binding agreement that meets section 72.

11.7 **Transfer impact note.** As Clause 14 of the Clauses requires, IMGN has assessed the laws and practices of the countries to which Customer Personal Data is transferred. The Customer may rely on this note in its own assessment:

- **South Africa.** IMGN is subject to POPIA, a comprehensive data protection law overseen by an independent regulator, the Information Regulator. Access by public authorities to data that IMGN holds is governed by statute, including the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 and the Criminal Procedure Act 51 of 1977, and generally requires prior authorisation by a judge or magistrate. IMGN has no reason to believe that these laws prevent it from meeting its obligations under the Clauses.
- **United States.** Some Sub-processors are subject to US laws that allow public authorities to require access

to data, such as section 702 of the Foreign Intelligence Surveillance Act and Executive Order 12333. Executive Order 14086 added limits on that access and a redress mechanism, which the European Commission relied on when it adopted its adequacy decision for the EU-US Data Privacy Framework on 10 July 2023.

- **The data concerned.** Workspace content consists of business decision records, their rationale and evidence, and the names and email addresses of the people involved. The primary copy is stored in Ireland. What reaches a US Sub-processor is limited to what that Sub-processor needs: a request to an AI model contains only the content needed for that task.
- **Supplementary measures.** Data is encrypted in transit, and credentials for connected tools and model accounts are encrypted again by the application before they are stored. IMGN will review any request from a public authority for Customer Personal Data, challenge it where there are reasonable grounds to, and disclose the minimum the law requires, as Clause 15 of the Clauses sets out.

11.8 IMGN will tell the Customer promptly if it has reason to believe that it, or a Sub-processor, can no longer meet the obligations in this section.

12. Audits

12.1 IMGN will make available to the Customer the information reasonably necessary to demonstrate compliance with this DPA and Article 28 of the GDPR, and will allow for and contribute to audits as this section describes.

12.2 The standard way to verify the processing within the Customer's Workspace is the signed audit export. Workspace administrators can download it under Settings, Data. It contains every decision event and every assistant (MCP) tool call in a chosen date range, with the people and clients involved named, together with Ask AI usage records, retention runs and earlier exports. Each export is signed with an Ed25519 key over its exact bytes, so the Customer or its auditor can check, against the public key published at precedent.biz/.well-known/precedent-audit-key.json, that the file has not been changed since IMGN produced it. Every export is itself recorded.

12.3 The audit export records activity in the Workspace through the application and its assistant interface. It does not record IMGN's own operational access to the underlying infrastructure. For that, IMGN will answer the Customer's reasonable written questions about its security and processing, including a security questionnaire, once a year, and again after a Security Incident.

12.4 If that information is not enough to demonstrate compliance, or a supervisory authority requires it, the Customer may audit IMGN's processing of Customer Personal Data itself or through an independent auditor bound by confidentiality. The Customer will give at least 30 days' written notice, audit during business hours, not more than once in any 12 months except after a Security Incident or at an authority's request, and in a way that does not compromise the security of other customers' data. Each party bears its own costs. Where an audit concerns a Sub-processor, IMGN may meet it by providing that Sub-processor's own audit reports or certifications.

12.5 Nothing in this section limits the Customer's rights under the Clauses or the UK Addendum, or the powers of a supervisory authority.

13. Retention, return and deletion

13.1 IMGN keeps Customer Personal Data for as long as the Workspace exists, subject to the retention policy and deletions the Customer chooses.

13.2 **Retention policy.** Administrators can set a retention policy under Settings, Data. A daily job then permanently deletes archived decisions older than the chosen period, with their revisions, events, evidence and uploaded files, and deletes operational logs older than their chosen period: assistant tool call logs, email and chat delivery logs, and Ask AI usage records. A retention policy never deletes a decided decision. An archived decision that replaced an earlier decision is also kept, because it explains why the earlier one was superseded.

13.3 **Legal hold.** Administrators can place the whole Workspace on legal hold, which pauses every retention run, or place a single decision on hold, which keeps it through any purge until an administrator clears the hold. Every retention run is recorded, including one skipped because of a hold. A legal hold is the Customer's instruction to keep data. It does not stop an administrator deleting the whole Workspace, and the Customer is responsible for not deleting data it is obliged to keep.

13.4 **Deleting a Workspace.** Deleting a Workspace under Settings, General permanently removes it from the database, with its Areas, decisions, revisions, events, memberships and assistant grants, and queues its uploaded files for deletion from file storage. The files are deleted straight away, and a deletion that fails is retried by the daily job.

13.5 **Backups.** Deleted data can remain in the database provider's daily backups for up to 7 days, until they are overwritten. IMGN restores from a backup only to recover the service from a failure. If it does, it will delete again any Customer Personal Data the Customer deleted after the backup was taken.

13.6 **At the end of the service.** Administrators can export and delete the Workspace at any time, including after its trial or subscription has ended and it has become read-only. If the Customer asks IMGN in writing to delete its Workspace after the Terms end, IMGN will do so within 30 days and confirm it in writing. If the Customer does neither within 90 days after the Terms end, IMGN may delete the Workspace after giving its administrators at least 30 days' notice by email.

13.7 IMGN may keep Customer Personal Data after that only where a law to which it is subject requires it, for no longer and to no greater extent than that law requires, keeping it confidential and processing it for no other purpose.

14. Liability

14.1 Each party's liability under this DPA is subject to the limitations and exclusions of liability in the Terms. Nothing in this DPA or the Terms limits a party's liability to data subjects under the Clauses or the UK Addendum, or any liability that cannot be limited by law.

15. Duration, changes and governing law

15.1 This DPA lasts for as long as IMGN processes Customer Personal Data, and survives the end of the Terms until IMGN has deleted that data under section 13.

15.2 IMGN may update this DPA to reflect changes in the law, regulatory guidance or the service. It will publish each new version on this page with its date, and give workspace administrators at least 30 days' notice by email of a change that materially affects the Customer, unless the law requires the change sooner. No update will reduce the protection given to Customer Personal Data or the Customer's rights under the Clauses.

15.3 Where the parties have signed a copy of this DPA, the signed version governs. A later version applies to that Customer only if it agrees in writing or the law requires the change.

15.4 This DPA is governed by the law that governs the Terms. The Clauses are governed by the law chosen in section 11.2, and the Clauses as they apply under the UK Addendum are governed by the laws of England and Wales, as the UK Addendum provides.

15.5 IMGN's contact for data protection matters, including questions about this DPA, is its Information Officer, Gordon Byron, at info@precedent.biz.

15.6 Notices to IMGN under this DPA are given by email to info@precedent.biz or by post to its registered office at 20 Krynauw Street, Worcester, Western Cape, 6850, South Africa. IMGN gives notices to the Customer by email to its workspace administrators.

Annex 1: Details of the processing

A. List of parties

Data exporter: the Customer, as named when it accepted the Terms or on a signed copy of this DPA, with the address and contact details given there. Activities: using the hosted Precedent service to record and share its decisions. Role: controller, or processor as section 3.1 describes. Signature and date: acceptance of the Terms, or the signature on a signed copy.

Data importer: IMGN Technologies (Pty) Ltd, registration number 2015/026469/07, 20 Krynauw Street, Worcester, Western Cape, 6850, South Africa. Contact for data protection matters: Gordon Byron, Information Officer, info@precedent.biz. Representative in the European Union under Article 27 of the GDPR: none appointed. Activities: providing the hosted Precedent service. Role: processor. Signature and date: as for the data exporter.

B. Description of the processing

- **Categories of data subjects:** the Customer's workspace members and invited users; people named or discussed in decisions, evidence and captured chat threads, such as employees, contractors, customers and suppliers; client portal invitees; and people whose chat accounts are linked to the Workspace.
- **Categories of personal data:** names, email addresses and profile pictures; workspace roles, group membership, invitations and how each membership came about; the content of decisions, including rationale, alternatives, assumptions, review conditions, comments and evidence, uploaded files and captured chat threads, and any personal data within them; chat user and team identifiers and display names for linked chat accounts; the history of who did what to each decision; and for assistant connections, the client, the permissions approved, and the tool name, duration and outcome of each call, but not its content.
- **Special categories of data:** none intended; see section 3.4. If the Customer includes any, the measures in Annex 2 apply, including access limited by Area and role.
- **Frequency of the transfer:** continuous, for as long as the Customer uses the service.
- **Nature of the processing:** hosting, storage, organisation, retrieval and display; search, including turning decision text into search embeddings; making content available to the people and assistants the Customer authorises; sending the emails and chat messages the Workspace is set up to send; the AI-assisted features the Customer uses, such as conflict checks, drafting decisions from chat threads and transcripts, and suggestions; export; and deletion.
- **Purpose:** providing the hosted service to the Customer under the Terms, including support, security and preventing abuse.
- **Duration and retention:** for the term of the Terms and until deletion under section 13, subject to the Customer's retention policy and legal holds.
- **Transfers to Sub-processors:** for the subject matter, nature and duration set out in Annex 3.

C. Competent supervisory authority

For the Clauses, the supervisory authority that Clause 13(a) determines: the authority of the EU Member State in which the Customer is established; if the Customer is not established in the EU but has appointed a representative under Article 27(1) of the GDPR, the authority of the Member State where that representative is established; and otherwise the authority of one of the Member States in which the data subjects whose personal data is transferred are located. Under the UK Addendum, the UK Information Commissioner. For the FADP, the Swiss Federal Data Protection and Information Commissioner. For POPIA, the Information Regulator of South Africa.

Annex 2: Security measures

These are the measures IMGN applies to the hosted service. Each one describes how the service works today.

Access control and separation of customers

- Every request runs in a database transaction scoped to one Workspace, and PostgreSQL row-level security policies, enforced for the role the application uses, limit what that transaction can read or change to that Workspace. The application checks permissions as well.
- Within a Workspace, access follows roles (Viewer, Member, Maintainer and Admin) granted through groups linked to Areas. Every list, search, export and assistant tool call applies the same visibility rules.
- Uploaded files are served only through the application, to people who can see the decision they belong to.
- Deleting a Workspace and managing legal holds are available only in the web application, to administrators.

Authentication

- People sign in with an email link that expires after 15 minutes, with Google, or with the Customer's own single sign-on provider through OpenID Connect or SAML. Sessions expire after 30 days. Requests for sign-in links are rate limited.
- Administrators can require single sign-on for the Workspace. Requiring it revokes the assistant connections that non-administrators approved from another kind of sign-in.
- Assistants connect through OAuth 2.1 with PKCE. Each connection is limited to the Workspace or Area and the permissions its person approved, acts with that person's access, and can be revoked at any time under Settings,

Agents.

Encryption

- The service is served only over HTTPS, and the application reaches file storage over HTTPS.
- The database and file storage provider encrypts stored data at rest.
- Credentials for connected tools and model accounts are encrypted by the application with AES-256-GCM before they are written to the database, under a key kept apart from the database. They are never displayed again after they are entered.

Integrity and accountability

- Every decision keeps each of its revisions and an event history of who did what, when, and through which channel: the web application, an assistant, chat or an integration.
- The signed audit export described in section 12.2. Outside a local development copy, the application signs exports only with a dedicated signing key, kept apart from the key that protects sign-in sessions.
- Every export of Workspace data is recorded with who made it and how.

Data minimisation

- Assistant tool call logs record the tool, duration, outcome and any error, but not the content of the call.
- Ask AI usage records keep the provider, model, tools used, token counts, duration and outcome, but not the text of questions or answers.
- Application logs and error details stay with the hosting provider, Vercel, which keeps them for 30 days. They are not sent to a separate monitoring service.
- A request to the app-funded AI model contains only the content needed for that task, such as the decision text being checked or the thread being captured.

Location of data

- Each deployment serves one region and stamps every Workspace with the region it was created in. A deployment refuses to serve a Workspace stamped with another region. The hosted service at precedent.biz stores Workspace data in the European Union, in Ireland.

Retention and deletion

- Retention policies, legal holds, Workspace deletion and file cleanup work as section 13 describes. The database provider keeps daily backups for 7 days.

Outbound requests

- When the application fetches a title from a connected tool at an address the Customer configured, such as a self-hosted Jira or GitHub Enterprise site, it accepts only hostnames that resolve to public addresses and keeps TLS certificate checks on, so the service cannot be used to reach private networks.

Changes to the service

- Every change to the application goes through a reviewed pull request and automated unit, database and browser tests before it is merged. It is deployed to a staging environment first and promoted to production deliberately. Database migrations are checked for compatibility with the version already running.

People and incidents

- Access to Customer Personal Data is limited to personnel who need it and are bound by confidentiality, as section 6 describes.
- Vulnerabilities can be reported to info@precedent.biz. Security Incidents are handled as section 10 describes.
- Sub-processors are bound by written contract, as section 8 describes.

Annex 3: Sub-processors

The list of Sub-processors at precedent.biz/sub-processors forms this Annex and Annex III of the Clauses. It names each Sub-processor, what it does for the service and where it processes data. Changes to it follow section 8.

Signatures

Signed by the authorised representatives of the parties. By signing, each party also enters into the Clauses and the UK Addendum incorporated by section 11, where they apply.

For the Customer (data exporter)

Organisation _____

Address _____

Signature _____

Name _____

Title _____

Date _____

Privacy contact _____

For IMGN Technologies (Pty) Ltd (data importer)

Signature _____

Name _____

Title _____

Date _____