

LEGAL

Data Processing Agreement

Version 1.0 · Effective 2026-06-26 · UK GDPR + Data Protection Act 2018

Need a signed copy? Download the source DPA below. Pre-signed by Jeanus; countersign and return to hello@pixelandshovel.co.uk for a fully executed PDF in return.

1. Parties

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

- **The Customer** (the "Controller"), being the entity that has subscribed to the Jeanus B2B CRM service ("Service") on its own behalf; and
- **Pixel & Shovel Ltd**, a company registered in England and Wales, trading as Jeanus, with registered office in Brighton, United Kingdom (the "Processor").

ICO registration: [ZC068491](https://ico.org.uk/registration/zc068491). Contact: hello@pixelandshovel.co.uk.

2. Background

The Parties have entered into a subscription agreement under which the Processor provides the Service to the Controller (the "Principal Agreement"). In the course of providing the Service, the Processor processes Personal Data on behalf of the Controller. This DPA governs that processing and forms part of the Principal Agreement.

3. Definitions

Terms not defined here take the meaning given in the UK General Data Protection Regulation ("UK GDPR", the UK's implementation of the EU GDPR) and the Data Protection Act 2018 (together, "Data Protection Laws").

- **Personal Data:** any data relating to an identified or identifiable natural person that the Controller (or its end users) submits to the Service.
- **Processing:** as defined in the UK GDPR.
- **Subprocessor:** a third party engaged by the Processor to process Personal Data on the Controller's behalf, listed at [/subprocessors](#).

- **We use cookies.**
Strictly-necessary cookies make Jeanus work (login, security, tenant context) - these are always on. Analytics cookies help us see which features get used; they only fire if you accept. You can change this any time via [our privacy notice](#).

4.

AI-assisted features, transactional email, and subscription billing.

- **Nature:** storing, organising, displaying, transmitting, copying, querying, exporting, and (where the Controller triggers AI features) submitting Personal Data to AI subprocessors for the purpose of generating drafts, summaries, briefings or enrichment.
- **Purpose:** enabling the Controller to operate its B2B sales, customer and account workflows.
- **Duration:** the term of the Principal Agreement, plus any retention period under section 13.

5. Categories of Personal Data and Data Subjects

The Controller determines what Personal Data it submits. The Service accommodates:

- **Data Subjects:** the Controller's own customers, prospects, leads, contacts, suppliers, candidates (for recruitment users), and the Controller's own employees and authorised users.
- **Personal Data categories:** identification (name, job title), contact (email, phone, business address), commercial (orders, quotes, pricing, billing), interaction (notes, activity, emails, call logs), and any other Personal Data the Controller chooses to record.
- **Special category data:** the Service is not designed to process special category data under Article 9 of the UK GDPR. The Controller agrees not to submit special category data unless the Parties have agreed additional terms in writing.

6. Controller obligations

The Controller:

1. is the data controller of the Personal Data it submits and is responsible for the lawfulness, accuracy and lawful basis of that processing;
2. is responsible for providing all required notices to, and (where required) obtaining all required consents from, Data Subjects;
3. will give the Processor lawful, documented instructions; the Principal Agreement, this DPA, and the Controller's use of the Service within its documented features constitute documented instructions;
4. will not submit special category data or data relating to criminal convictions without prior written agreement; and
5. will keep its account credentials secure and take reasonable steps to off-board users whose access should be revoked.

7.

We use cookies.

Th
1. Strictly-necessary cookies make Jeanus work (login, security, tenant context) - these are always on. Analytics cookies help us see which features get used; they only fire if you accept.
2. You can change this any time via [our privacy notice](#).

3. implement the technical and organisational security measures set out in Appendix A below and at [/security](#);
4. engage Subprocessors only in accordance with section 8;
5. taking the nature of the processing into account, assist the Controller by appropriate technical and organisational measures with its obligations to respond to Data Subject requests under Articles 12-22 of the UK GDPR;
6. assist the Controller with its obligations under Articles 32-36 of the UK GDPR (security, breach notification, data protection impact assessments and prior consultation);
7. notify the Controller without undue delay, and in any event within 48 hours, after becoming aware of a Personal Data Breach affecting the Controller's data;
8. at the Controller's election, delete or return all Personal Data at the end of the Service, subject to section 13; and
9. make available all information reasonably necessary to demonstrate compliance with this DPA and allow for and contribute to audits, in accordance with section 11.

8. Subprocessors

The Controller gives the Processor general authorisation to engage Subprocessors, subject to:

1. the Processor maintaining a current list of Subprocessors at [/subprocessors](#);
2. before engaging a new Subprocessor, the Processor imposing data protection obligations on that Subprocessor no less protective than this DPA;
3. the Processor giving at least 30 days' notice of any intended changes (by updating the page and notifying tenant admins by email);
4. if the Controller reasonably objects on data protection grounds, the Parties discussing in good faith; if the Processor cannot offer an alternative, the Controller may terminate the Principal Agreement without penalty for the remainder of the current billing period;
5. the Processor remaining liable to the Controller for the acts and omissions of its Subprocessors as if they were its own.

9. International transfers

Where the Processor or a Subprocessor transfers Personal Data outside the United Kingdom, the transfer is made on the basis of the UK International Data Transfer Addendum to the EU Standard

Co
La
10

We use cookies.

Strictly-necessary cookies make Jeanus work (login, security, tenant context) - these are always on. Analytics cookies help us see which features get used; they only fire if you accept.

You can change this any time via [our privacy notice](#).

The Processor will:

1. promptly notify the Controller of any request received directly from a Data Subject relating to the Controller's data, and will not respond directly except to confirm the request has been forwarded (unless instructed otherwise);
2. provide reasonable assistance, including by making available administrative tools in the Service (data export, deletion, rectification), to enable the Controller to fulfil its obligations under Articles 12-22 of the UK GDPR within statutory time limits.

11. Audits

1. The Processor will respond promptly to reasonable written requests for information necessary to demonstrate compliance with this DPA, including copies of relevant policies, attestations and Subprocessor DPAs.
2. Where the Controller can demonstrate the information provided is insufficient, the Controller may, on at least 30 days' written notice and not more than once in any twelve-month period (unless required by a supervisory authority), conduct an audit by a mutually agreed independent third-party auditor under reasonable confidentiality terms. The Controller bears the costs of any such audit unless it discovers a material breach.

12. Personal Data Breach

1. The Processor will notify the Controller of any Personal Data Breach affecting Controller data without undue delay and in any event within 48 hours of becoming aware.
2. The notice will include, to the extent then known: nature of the breach, categories and approximate number of Data Subjects and records concerned, likely consequences, and measures the Processor has taken or proposes to take.
3. The Processor will cooperate with and assist the Controller in complying with the Controller's own Article 33 and 34 notification obligations.

13. Return or deletion of Personal Data

1. On termination or expiry of the Principal Agreement, the Controller's tenant data will remain accessible for export for 30 days.
2. After the 30-day window, the Processor will delete all Controller Personal Data from active systems within a further 30 days, save where retention is required by law (including statutory requirements applicable to billing data).

3. **We use cookies.**
Strictly-necessary cookies make Jeanus work (login, security, tenant context) - these are always on. Analytics cookies help us see which features get used; they only fire if you accept.
4. You can change this any time via [our privacy notice](#).

14. Liability

The Parties' liability under this DPA is subject to the limitations of liability set out in the Principal Agreement.

15. Term

This DPA comes into force on the Effective Date and continues for as long as the Processor processes Personal Data on behalf of the Controller. Sections 12, 13, 14 and 16 survive termination.

16. Governing law

This DPA is governed by the law of England and Wales. The courts of England and Wales have exclusive jurisdiction over any dispute arising under or in connection with this DPA.

17. Order of precedence

In the event of a conflict between this DPA and the Principal Agreement on matters of data protection, this DPA prevails.

Appendix A - Technical and organisational security measures

The Processor implements at least the following measures, described in more detail at [/security](#):

1. **Encryption:** TLS 1.2+ in transit; AES-256 at rest (including backups).
2. **Tenant isolation:** three-layer defence - application-level tenant ID filter, Postgres Row Level Security, and an automated Playwright regression test against the live deployment that crawls every customer-facing page across all demo tenants and asserts no cross-tenant data renders.
3. **Authentication:** Supabase Auth with bcrypt hashing; TOTP MFA available to all users and required for staff/admin roles.
4. **Authorisation:** role-based access controls within a tenant. Management routes guarded server-side.
5. **Access management:** Supabase service-role key used server-side only; service-role calls logged.

- 6.
7. **We use cookies.**
Strictly-necessary cookies make Jeanus work (login, security, tenant context) - these are always on. Analytics cookies help us see which features get used; they only fire if you accept.
8. You can change this any time via [our privacy notice](#).

9. **Personnel:** all personnel with production access bound by confidentiality.

10. **Incident response:** documented playbook; 48-hour internal notification; 72-hour Controller notification.

Appendix B - Subprocessors

The current list of Subprocessors, with role, region, certifications and DPA, is at [/subprocessors](#). As at the Effective Date: Vercel Inc. (hosting, UK), Supabase Inc. (database + auth, UK/London), Anthropic PBC (AI features, US), Stripe Payments Europe Ltd. (billing, EU/Ireland), Resend Inc. (transactional email, US).

Signatures

ON BEHALF OF THE CONTROLLER

Name

Job title

Company

Email

Date

Signature

ON BEHALF OF THE PROCESSOR

Name
Sam Ball

Job title
Director / Founder

Company
Pixel & Shovel Ltd, t/a Jeanus

Email
hello@pixelandshovel.co.uk

Date
2026-06-26

Signature
Sam Ball (pre-signed)

To execute: download the DPA, complete the Controller block, and return to hello@pixelandshovel.co.uk. We will return a fully countersigned copy.

Bui

We use cookies.

Strictly-necessary cookies make Jeanus work (login, security, tenant context) - these are always on. Analytics cookies help us see which features get used; they only fire if you accept. You can change this any time via [our privacy notice](#).