PaperDrop Data Processing Agreement

Version 2.0 — 14 September 2026

This Data Processing Agreement ("DPA") forms part of the Agreement between PaperDrop Limited (company number 14319420, Allia Future Business Centre, London Road, Peterborough PE2 8AN) ("PaperDrop") and the Customer identified in the Order Form. It applies where PaperDrop processes personal data on the Customer's behalf in providing the Service under the PaperDrop General Terms and Conditions (the "General Terms"). Words defined in the General Terms have the same meaning here.

In short — how your data is handled (not part of the DPA)

You own the data you and your team put into PaperDrop. We process it only to run the Service for you and on your instructions. It is hosted by Microsoft Azure in the UK. We use a small number of suppliers to run the Service; they are listed in Annex 3 with where they process data (hosting is in the UK or EU and our support desk is in Norway, but several suppliers are US companies and some processing happens in the USA, under UK-approved safeguards), and we give you 30 days' notice before adding one. If we suffer a security breach affecting your data we tell you within 48 hours. When the Agreement ends you have 60 days to export your data, and we delete it from the live Service within 60 days after that (or after we have returned it, if you ask for it back); copies in backups expire within 12 months and are not used in the meantime. If anything on this page differs from the clauses below, the clauses apply.

1. Scope, roles and precedence

1.1. For personal data contained in Customer Data, the Customer is the controller and PaperDrop is the processor. The subject matter, duration, nature and purpose of the processing, the types of personal data and the categories of data subjects are set out in Annex 1.

1.2. PaperDrop is an independent controller of personal data it processes for its own purposes, such as the Customer's account, billing and contact details, User login and support administration records needed to administer the Agreement (Customer Data contained in support tickets remains covered by this DPA, see clause 11.2), and usage data used to operate, secure and improve the Service. That processing is described in PaperDrop's Privacy Notice and is outside this DPA.

1.3. This DPA prevails over the other documents forming the Agreement in relation to the processing of personal data (General Terms clause 2.1). In all other respects, including liability, the General Terms govern.

1.4. "Data Protection Legislation" has the meaning given in the General Terms. "Personal Data Breach", "processing", "controller", "processor", "data subject" and "sub-processor" have the meanings given in the UK GDPR.

2. Duration

2.1. This DPA applies for as long as PaperDrop processes personal data on the Customer's behalf, which is the Subscription Term together with the export and deletion periods in clause 11.

3. The Customer's obligations

3.1. The Customer is responsible for the lawfulness of the personal data it and its Users enter into the Service, including having a lawful basis for processing the personal data of its employees, workers, subcontractors and other individuals, and for giving those individuals the transparency information the Data Protection Legislation requires (General Terms clause 17.3).

3.2. The Customer decides what personal data to put into the Service. The employee profile includes an optional medical conditions field, intended to record fitness for site work and health and safety information the Customer needs; it can be seen and edited only by Users the Customer has given the relevant permission. Where the Customer uses that field, or records health and safety incidents, fitness-to-work information or other special category data in forms, RAMS or job notes, the Customer is responsible for identifying an appropriate condition for processing it under Article 9 UK GDPR and, where required, a condition (and any appropriate policy document) under Schedule 1 of the Data Protection Act 2018, and for limiting who can see it. The Service is not designed for, and the Customer must not use it to process, criminal offence data or data relating to children, except incidentally within ordinary business records.

3.3. Where the Customer uses location, tracking or geofencing features, the Customer is responsible for the matters set out in General Terms clause 13.5, including any data protection impact assessment.

3.4. The Customer's instructions to PaperDrop must comply with the Data Protection Legislation. The Customer will not instruct PaperDrop to do anything that would put PaperDrop in breach of it.

4. PaperDrop's instructions

4.1. PaperDrop will process personal data only on the Customer's documented instructions, including in relation to transfers outside the United Kingdom, unless required to do otherwise by law applicable to PaperDrop, in which case PaperDrop will inform the Customer of that requirement before processing unless the law prohibits it.

4.2. The Customer's documented instructions are: (a) the Agreement, including this DPA; (b) the Customer's and its Users' configuration and use of the Service's features; and (c) any further written instructions agreed by PaperDrop. PaperDrop may charge at its standard rates for instructions that go beyond the ordinary operation of the Service.

4.3. PaperDrop will inform the Customer without undue delay if, in its opinion, an instruction infringes the Data Protection Legislation. PaperDrop may suspend the relevant

processing until the instruction is amended or withdrawn, or PaperDrop is satisfied that it is lawful.

5. Confidentiality

5.1. PaperDrop will ensure that every person it authorises to process personal data (including employees, contractors and agency staff) is bound by a written or statutory duty of confidentiality and has access only to the personal data needed for their role.

6. Security

6.1. PaperDrop will implement and maintain the technical and organisational measures described in Annex 2, and any others required to provide a level of security appropriate to the risk under Article 32 UK GDPR, taking account of the state of the art, the cost of implementation and the nature of the processing.

6.2. PaperDrop may update the measures in Annex 2 from time to time, provided the updated measures do not materially reduce the overall level of security. The current Annex 2 is published at the permanent link stated in the Order Form.

6.3. The Customer is responsible for the security of its own devices, networks and User credentials, for enabling multi-factor authentication where PaperDrop makes it available, and for managing its Users' access rights within the Service (General Terms clause 12.2).

7. Sub-processors

7.1. The Customer gives PaperDrop general written authorisation to engage the sub-processors listed in Annex 3 and, subject to this clause 7, other sub-processors. Annex 3 states each sub-processor's purpose and the location of processing.

7.2. PaperDrop will give the Customer at least 30 days' written notice before appointing a new sub-processor or replacing an existing one, by updating Annex 3 at the permanent link and sending notice to the Customer's notice address under General Terms clause 26.1.

7.3. The Customer may object within that 30-day period on reasonable grounds relating to data protection. PaperDrop will then discuss the objection in good faith and may offer a reasonable alternative, such as not using the new sub-processor for the Customer's data. If no alternative is agreed within 30 days of the objection and the change would materially and adversely affect the protection of the Customer's personal data, the Customer may terminate the affected part of the Service, or the Agreement if the affected part cannot be separated, by written notice taking effect no earlier than the date the new sub-processor starts processing its data. In that case PaperDrop will refund any prepaid Fees for the period after termination, the Customer remains liable for Fees accrued to that date, and no Committed Remaining Value is payable. This is the Customer's sole remedy for an objection.

7.4. PaperDrop will impose on each sub-processor, by written contract, data protection obligations that provide at least the same level of protection as this DPA, and remains liable to the Customer for the performance of each sub-processor's obligations.

7.5. The following are not sub-processors: (a) payment providers (such as GoCardless or Stripe) that process the Customer's own payment details as independent controllers; (b) third-party services the Customer chooses to connect to the Service (such as Xero, QuickBooks or its own Microsoft 365 tenant for sign-in and sending email), which receive data on the Customer's instruction under the Customer's own agreement with that provider (General Terms clause 14); (c) Google Maps Platform, which receives address text typed into address fields as an independent controller; and (d) recipients of emails or documents the Customer sends using the Service.

8. International transfers

8.1. PaperDrop hosts and stores Customer Data in the United Kingdom (Annex 2). Some sub-processors listed in Annex 3 process Customer Data in the European Union and in Norway (support desk), and some are US companies or process Customer Data in the United States, under the transfer mechanisms stated in Annex 3. PaperDrop will not otherwise transfer personal data outside the United Kingdom, or permit a sub-processor to do so, except: (a) to a sub-processor listed in Annex 3 whose location is stated there; and (b) using a transfer mechanism permitted by the Data Protection Legislation, such as adequacy regulations or the UK International Data Transfer Agreement or Addendum, together with any supplementary measures required.

8.2. If the Customer is established outside the United Kingdom, PaperDrop returning or making Customer Data available to the Customer is a transfer on the Customer's instruction and is not a restricted transfer by PaperDrop.

9. Assistance with data subject rights

9.1. The Service includes tools that allow the Customer to access, correct, export and delete personal data itself. The Customer will use those tools to respond to data subject requests where it can.

9.2. If PaperDrop receives a request from a data subject relating to the Customer's personal data, PaperDrop will forward it to the Customer within 5 Business Days and will not respond to the data subject except to say that the request has been passed to the Customer, unless required by law.

9.3. Where the Customer cannot deal with a request using the Service's tools, PaperDrop will provide reasonable assistance within a timescale that allows the Customer to meet its statutory deadline, taking account of the information PaperDrop holds. PaperDrop may charge at its standard rates for assistance that goes beyond the Service's standard tools, unless the need for assistance arises from PaperDrop's breach of this DPA.

10. Personal Data Breach and other assistance

10.1. PaperDrop will notify the Customer without undue delay, and in any event within 48 hours, after becoming aware of a Personal Data Breach affecting the Customer's personal data. The notice will describe, so far as then known, the nature of the breach, the categories and approximate numbers of data subjects and records affected, the likely consequences,

the measures taken or proposed, and a contact point. PaperDrop may provide the information in stages as it becomes available.

10.2. PaperDrop will not notify the Information Commissioner or data subjects of a breach of the Customer's personal data on the Customer's behalf unless the Customer asks it to in writing or the law requires it. The decision whether to notify is the Customer's.

10.3. PaperDrop will provide the Customer with reasonable assistance in meeting its obligations under Articles 32 to 36 UK GDPR (security, breach notification, data protection impact assessments and prior consultation with the Information Commissioner), taking account of the nature of the processing and the information available to PaperDrop. PaperDrop may charge at its standard rates for assistance with data protection impact assessments and consultations unless the need arises from PaperDrop's breach of this DPA.

11. Return and deletion

11.1. During the Subscription Term, including during any suspension as set out in General Terms clause 21.2, and for 60 days after the Agreement ends, the Customer may export its Customer Data using the Service's standard export tools (General Terms clause 17.4). PaperDrop may charge at its standard rates for export assistance beyond those tools.

11.2. At the end of that 60-day period PaperDrop will, at the Customer's choice, return or delete the personal data in the Customer Data. Return is by the standard export tools; if the Customer tells PaperDrop before the end of the period that it needs personal data those tools do not cover, PaperDrop will provide it in a reasonable format, at its standard rates unless the gap is PaperDrop's fault. PaperDrop will then delete the personal data from the live Service within 60 days after the end of the export period or, where the Customer has asked for return, within 60 days after the return is made, except where United Kingdom law requires PaperDrop to retain it. The Customer instructs PaperDrop to keep support tickets, including any Customer Data in them, for 2 years so that support history is available, after which they are deleted (Annex 3). Personal data in backups is deleted when the backups expire under PaperDrop's backup cycle described in Annex 2 (point-in-time backups within 35 days; long-term monthly database backups within 12 months); until then it is held securely, is not restored to the live Service except where necessary to recover from a disaster affecting PaperDrop's systems generally, and is not otherwise processed. If such a recovery restores the Customer's personal data, PaperDrop will delete it again.

11.3. PaperDrop may retain, as controller, the records it needs to administer and evidence the Agreement, such as the Order Form, invoices, notices and account history, for the periods stated in its Privacy Notice.

11.4. On written request made within 90 days after deletion under clause 11.2, PaperDrop will confirm deletion in writing.

12. Information and audit

12.1. PaperDrop will make available to the Customer the information reasonably necessary to demonstrate compliance with this DPA and Article 28 UK GDPR, including this DPA, Annexes 2 and 3, and summaries of relevant third-party certifications or audit reports held by PaperDrop or its hosting provider.

12.2. If that information is not sufficient, the Customer (or an independent auditor appointed by it and bound by confidentiality) may audit PaperDrop's compliance with this DPA: no more than once in any 12-month period, on at least 30 days' written notice, during Business Days and business hours, in a manner that does not unreasonably disrupt PaperDrop's business or compromise the security of other customers' data. The scope and timing must be agreed in advance. The Customer bears its own costs and PaperDrop's reasonable costs of assisting, unless the audit reveals a material breach of this DPA by PaperDrop.

12.3. For infrastructure operated by PaperDrop's hosting sub-processor, the Customer accepts the hosting provider's independent certifications and audit reports in place of a physical audit, as PaperDrop has no right to audit those facilities itself.

12.4. Clause 12.2 does not limit an audit or inspection required by the Information Commissioner or by law, or an audit reasonably required following a Personal Data Breach affecting the Customer's personal data.

13. Liability

13.1. PaperDrop's liability arising out of or in connection with this DPA, whether in contract, tort (including negligence), breach of statutory duty or otherwise, is subject to the exclusions and limitations in clause 20 of the General Terms and counts towards the cap in clause 20.3. Nothing in this DPA limits either party's liability to data subjects or to the Information Commissioner where the Data Protection Legislation does not allow it to be limited.

14. Changes and versions

14.1. This DPA carries a version number and date. The version that applies to the Agreement is the version identified in the Order Form, supplied to the Customer before acceptance and available at the permanent link stated there (General Terms clause 2.6). No later version applies except as set out in this clause 14.

14.2. PaperDrop may change this DPA where required by a change in the Data Protection Legislation or by guidance of the Information Commissioner, by giving notice under clause 25 of the General Terms. Annex 2 may be updated under clause 6.2 and Annex 3 under clause 7.2.

14.3. PaperDrop retains an immutable copy of each version of this DPA and of Annexes 2 and 3 as they stood at each change, and will provide the version applicable to the Customer at any time on request.

15. Notices, contact and governing law

15.1. Notices under this DPA are given in accordance with clause 26.1 of the General Terms. Data protection matters should be sent to PaperDrop's data protection contact at dpo@paperdrop.com, PaperDrop Limited, Allia Future Business Centre, London Road, Peterborough PE2 8AN.

15.2. This DPA is governed by the laws of England and Wales, and clause 27 of the General Terms applies to any dispute.

Annex 1 — Details of the processing

Item	Description
Subject matter	Provision of the PaperDrop job management Service to the Customer: job management, timesheets, scheduling and planning, RAMS and forms, stock control, photos and documents, communications sent through the Service, reporting, integrations, onboarding and support.
Duration	The Subscription Term plus the export and deletion periods in clause 11.
Nature of processing	Hosting, storage, organisation, retrieval, display, transmission (including emails and documents the Customer sends through the Service), backup, export and deletion, and, where the Customer uses them, automated features such as scheduling suggestions, location capture and AI-assisted reading of scanned invoices, receipts and documents uploaded during set-up, using the sub-processors listed in Annex 3.
Purpose	To provide the Service and support to the Customer in accordance with the Agreement and the Customer's configuration and instructions.
Categories of data subjects	The Customer's employees, workers and subcontractors who use or are recorded in the Service; the Customer's own customers and their site contacts; suppliers and other third parties recorded in job records; any other individual whose details the

	Customer chooses to enter.
Types of personal data	Identification and contact details (name, job title, phone, email, address); employee profile details the Customer chooses to record (date of birth, nationality, next of kin, role, skills, certifications and training records, right-to-work or CSCS-type card details and their expiry dates); timesheet, attendance and scheduling records; location data captured by timesheet, scheduling or geofencing features where enabled; job records, notes, forms, RAMS and signatures; photos and documents uploaded by Users, which may show individuals; invoices, receipts and documents scanned or uploaded for automated reading, which may contain names, addresses and bank details; communications sent through the Service; expense and payment references relating to jobs.
Special category data	Not required by the Service. The optional medical conditions field in the employee profile (clause 3.2) is provided for fitness-for-site-work and health and safety purposes and is visible only to Users with the relevant permission. Special category data may also be present where the Customer records health and safety incidents, injuries or fitness-to-work information in forms, RAMS or job notes. The Customer is the controller of that data and is responsible under clause 3.2.
Criminal offence data	Not intended to be processed.

Annex 2 — Technical and organisational security measures

These are the measures PaperDrop currently applies. They describe industry-standard practice for cloud software of this kind and may be updated under clause 6.2.

Area	**Measure**
Hosting and location	The Service and Customer Data are hosted

	on Microsoft Azure in the United Kingdom (UK South region), with data and backups replicated to Azure's paired United Kingdom region (UK West). Microsoft Azure holds ISO 27001, ISO 27017, ISO 27018 and SOC 1/2/3 certifications for its infrastructure.
Encryption	Data is encrypted in transit using TLS 1.2 or higher and at rest using Azure platform encryption (AES-256).
Access control	Role-based access within the Service, controlled by the Customer's administrators, including permission-gated fields for sensitive employee information; Users sign in through PaperDrop's identity provider (Auth0) with email and password or with their Google or Microsoft work account, so the Customer can apply its own multi-factor authentication policy; PaperDrop staff access to production data and to the support console is restricted to named personnel on a need-to-know basis, individually authenticated with multi-factor authentication, and logged.
Backup and recovery	Database: Azure SQL automated backups (continuous transaction-log backup, daily differential, weekly full) with point-in-time restore to any moment in the preceding 35 days, plus long-term backups retained weekly for 12 weeks and monthly for 12 months; backup storage geo-redundant across UK South and UK West. Files and documents: Azure Blob Storage with versioning, soft delete and point-in-time restore for the preceding 30 days; storage geo-redundant across UK South and UK West. All data encrypted at rest and in transit. A documented restore test is carried out at least annually; the first is scheduled for December 2026 and the result is recorded.
Availability and resilience	Azure platform redundancy; monitoring and alerting of the production

	environment; documented incident response procedure.
Vulnerability and patch management	Regular application of security updates to the application and its dependencies; Azure manages patching of the underlying platform; security findings from PaperDrop's own reviews are tracked to closure on a security roadmap.
Logging and monitoring	Application and access logs retained under PaperDrop's retention schedule (normally 30 to 90 days) and used to detect and investigate security events and to evidence Service availability.
Data segregation	Each Customer's data is logically separated by tenant identifier and access is enforced at the application layer.
Personnel	Confidentiality obligations in employment and contractor agreements; data protection and security training on joining and periodically; access removed promptly when a person leaves or changes role.
Development and change	Separate development, test and production environments; production Customer Data is not used for development or testing except anonymised or with the Customer's consent; changes released through a controlled deployment process.
Sub-processor management	Due diligence before appointment; written data protection terms; review of certifications; Annex 3 kept current.
Certifications held by PaperDrop	PaperDrop does not currently hold its own certification. It relies on Microsoft Azure's certifications for the hosting infrastructure (above) and plans Cyber Essentials certification as a next step.

Annex 3 — Sub-processors

Current as at the version date. Changes are notified under clause 7.2. The current list is published at the permanent link stated in the Order Form. “UK Addendum” means the UK International Data Transfer Addendum to the EU Standard Contractual Clauses; “DPF” means the EU–US Data Privacy Framework with the UK Extension.

Sub-processor	Purpose	Location of processing
Microsoft Ireland Operations Limited / Microsoft Corporation (Microsoft Azure)	Cloud hosting, database, file storage, cache, logging and backup of the Service	United Kingdom (UK South; paired region UK West). Support access governed by Microsoft’s Data Protection Addendum.
Okta, Inc. (USA), provider of Auth0, under the Okta Master Subscription Agreement and Okta’s data processing addendum	User sign-in and authentication for the Service	Hosted in the EU (Auth0 EU region); UK Extension to the EU–US DPF.
ActiveCampaign, LLC (Postmark)	Sending emails from the Service on the Customer’s behalf, including invitations, invoices, quotations and documents Users choose to send	United States. DPF / UK Addendum. Email content is retained by Postmark for 7 days for delivery and troubleshooting.
Vercel Inc.	Hosting of the Service’s web forms, planner, document merge and scanning screens (spp.paperdrop.com)	United Kingdom (London region). Vercel is a US company; support access under DPF / UK Addendum.
Functional Software, Inc. (Sentry)	Error monitoring and fault diagnosis for the Service	Functional Software, Inc. (USA); hosted in the EU (Germany); UK Extension to the EU–US DPF and UK Addendum. Session replays are masked by default.
PostHog, Inc.	Product usage analytics within the Service	PostHog Inc. (USA); hosted in the EU (Germany), with some processing in the US by PostHog’s sub-processors; UK Extension to the EU–US DPF, with the UK International Data Transfer Addendum in PostHog’s

		DPA as the fallback.
Google Cloud EMEA Limited (Ireland), Vertex AI	Reading invoices and receipts scanned with DropScan (optical character recognition); primary provider	Processing in the EU (Netherlands); transfer basis: UK adequacy regulations for the EU. Google's onward transfers to its affiliates are covered by Google's Cloud Data Processing Addendum. No training on Customer Data; no prompt retention where the abuse-monitoring exception is in place.
OpenAI OpCo, LLC	Reading invoices and receipts scanned with DropScan; fallback provider for invoice reading	OpenAI OpCo, LLC (USA); processing in the US; transfer basis: UK Addendum to the EU Standard Contractual Clauses, under OpenAI's Data Processing Addendum. No training on Customer Data; retention up to 30 days for abuse monitoring unless zero data retention is approved.
Anthropic, PBC	Reading documents uploaded during onboarding; drafting follow-ups to support requests	United States. UK Addendum in the Anthropic Data Processing Addendum. No training on Customer Data; retention up to 30 days unless zero data retention is approved.
Product Fruits s.r.o., Rozdělovská 1999/7, 169 00 Prague, Czech Republic (company ID 09552618)	In-app onboarding guides, product tours and announcements in the main app (the User's email address, sent as the username, and their interaction with guides: tours completed or skipped, hints shown, announcements read, checklists completed)	Product Fruits s.r.o. (Czech Republic); hosted by Amazon Web Services in the EU (Ireland); UK adequacy regulations for the EU. Product Fruits' Data Processing Addendum (productfruits.com/policies/terms#dpa) forms part of its terms and covers its use of AWS and its own US sub-

		processors.
Jam Technologies, Inc. (jam.dev)	Screen recordings a User chooses to make and send to PaperDrop support to show a problem	United States. UK IDTA. Recordings are deleted when the support request is closed.
ITX Norge AS	Customer support desk, where support requests may contain Customer Data	Norway. UK adequacy regulations. Support tickets are deleted after 2 years.

Not sub-processors (clause 7.5): GoCardless and Stripe (payment collection, independent controllers of the Customer's payment details); Xero, QuickBooks, the Customer's own Microsoft 365 tenant and other integrations the Customer connects (data transferred on the Customer's instruction under its own agreement with that provider); Google Maps Platform (address autocomplete, independent controller).