

Data Processing Agreement

Version 1.0 · 25 October 2026

The short version

- This agreement applies whenever FRONTROOM AI LTD processes personal data for a business that uses Frontroom. It is part of our [Terms](#), so it applies as soon as you accept them. There is nothing extra to sign.
- You, the restaurant, are the controller of the data you put into Frontroom. We are your processor: we only use that data to provide Frontroom to you, on your instructions.
- We keep it secure, tell you before we add or replace a subprocessor, tell you without undue delay about a breach, help you answer people's requests, and delete or return the data when you leave.
- If you would like a signed copy for your records, email support@frontroom.ai and we will send it to you for electronic signature. The [PDF](#) has the same text as this page.

1. Who this agreement is between

This Data Processing Agreement (this "DPA") is between **FRONTROOM AI LTD**, company number 17540446, registered office 11 Frating Crescent, Woodford Green, IG8 0DW, United Kingdom ("we", "us" or "our"), and the business that has a Frontroom account ("you" or "your").

It supplements our Terms at frontroom.ai/terms and the order or plan you have with us (together, the "Agreement"), and forms part of the Agreement. Section 13 of our Terms summarises the same commitments. This DPA sets them out in full.

2. Our roles

2.1 We as your processor. Where you are the controller of the personal data you put into or connect to Frontroom ("your personal data"), we are your processor and process it on your behalf.

2.2 We as your subprocessor. Where you process personal data for someone else, for example for another company in your group, you are a processor and we are your subprocessor. You confirm that the controller has approved our role, and that your contract with the controller allows the processing

this DPA describes. You will pass on to the controller anything from us that the controller needs.

2.3 What this DPA does not cover. It does not cover personal data we control ourselves, such as the details of your account owners and users that we need to run your account, billing records, the pseudonymous usage statistics described in our privacy policy, or data about visitors to our website. Our [privacy policy](#) covers that data.

3. How we process your data

3.1 Details. Annex 1 sets out the subject matter, nature, purpose and duration of the processing, the types of personal data, and the people the data is about.

3.2 Your instructions. You instruct us to process your personal data:

- (a) to provide, maintain, secure and support Frontroom;
- (b) as you choose through your settings and your use of Frontroom, for example the features you switch on and the people you give access to;
- (c) as set out in the Agreement and this DPA; and
- (d) as set out in any other written instructions you give us that we accept in writing.

We follow these instructions unless the law requires us to do something else. If it does, we will tell you before we process the data, unless the law forbids us from telling you. We will tell you straight away if we cannot follow an instruction, or if we think an instruction breaks data protection law.

3.3 Only for you. We process your personal data only as this DPA allows. We never sell it and never use it for advertising.

3.4 New or changed features. When we add or change features, we may update Annex 1 to match: the types of data and people, the nature and purpose of the processing, and how long it lasts. We will tell you about the update before it takes effect. Optional features, such as AI cameras, stay off until you switch them on.

4. Your responsibilities

4.1 Lawful use. You are responsible for having a lawful basis for the personal data you put into Frontroom, for giving people the information the law requires, and for getting any consent that is needed.

4.2 Lawful instructions. Your instructions to us must comply with the law.

4.3 AI cameras. If you use AI cameras, you must also display clear CCTV signs, tell your staff in writing what the cameras are used for, carry out a data protection impact assessment where the law requires one, have a valid condition under Article 9 of UK GDPR for any biometric data (for example for staff check-in by camera) and offer staff another way to clock in, and never cover private areas such as toilets or changing rooms. Section 7 of our Terms has the full list.

4.4 When you are a processor. Where you act as a processor (section 2.2), you will comply with the law that applies to you as a processor and with your contract with the controller, including its rules on subprocessors.

5. Our people

Everyone we allow to process your personal data is bound to keep it confidential, by contract or by law. They only access it when they need to, to run, support or secure Frontroom.

6. Security

We keep appropriate technical and organisational measures in place to protect your personal data against accidental or unlawful destruction, loss, change, disclosure or access, taking into account the risks involved, as Article 32 of UK GDPR requires. Annex 2 describes them. We may change these measures over time, but we will not reduce the overall level of protection they give.

7. Subprocessors

7.1 Your approval. You give us general written authorisation to use the subprocessors listed at frontroom.ai/subprocessors (Annex 3), each for the tasks and in the places shown there.

7.2 Changes and objections. We will tell you by email (to your account owner) and on that page at least 10 business days before we add or replace a subprocessor that handles your personal data, with the information you need to decide whether to object. If you object, tell us in writing, with your reasons, within 30 days of our notice. Otherwise you are treated as accepting the change. If you object, we will work with you in good faith to resolve your concern. You can also end the Agreement at any time, as our Terms allow.

7.3 Our contracts with subprocessors. We have a written contract with each subprocessor that allows it to use your personal data only as needed for the work we give it, and that requires it to protect the data with data protection obligations no less protective than those in this DPA, as Article 28(4) of UK GDPR requires. On request, we will give you a copy of, or a link to, the data protection terms we have with a subprocessor. We may remove commercial or confidential details first.

7.4 Our responsibility. We remain fully responsible to you for the work of our subprocessors, including what they do or fail to do with your personal data. We will tell you if a subprocessor fails to meet a material obligation about your personal data.

8. Transfers outside the UK

8.1 Where data is kept. Frontroom's application, database and backups run on our own servers in the United Kingdom. Some subprocessors process personal data in other countries, as Annex 3 shows. You authorise these transfers where they are needed to provide Frontroom.

8.2 Safeguards. Every transfer of your personal data out of the UK is covered by UK adequacy regulations (for example for the European Economic Area, or for US companies certified under the UK Extension to the EU-US Data Privacy Framework), or by appropriate safeguards under Article 46 of UK

GDPR, such as the International Data Transfer Agreement or the UK Addendum to the EU standard contractual clauses, both issued by the Information Commissioner.

8.3 If you are in the European Economic Area. Sending your personal data to us in the UK is covered by the European Commission's adequacy decision for the UK. If that decision stops applying, the EU standard contractual clauses (Module Two, or Module Three where you are a processor) apply between you as data exporter and us as data importer, and are part of this DPA, completed as follows: clause 7 does not apply; in clause 9, option 2 applies, with the notice period in section 7.2; the optional wording in clause 11 does not apply; in clauses 17 and 18, the law and courts of Ireland apply; and the annexes of this DPA complete the clauses' annexes.

9. Personal data breaches

When we become aware of a personal data breach affecting your personal data, we will:

- (a) tell you without undue delay, and in any case within 72 hours;
- (b) give you the information you need about it as soon as we have it, or as you reasonably ask, including what happened, the types of data and the number of people affected, the likely consequences, and what we are doing about it;
- (c) promptly take reasonable steps to contain it, investigate it and reduce the harm; and
- (d) help you tell the Information Commissioner's Office and the people affected, where the law requires.

Telling you about a breach, or responding to it, does not mean we accept fault or liability for it.

10. Help with requests and assessments

10.1 Requests from people. If someone asks us to use their data protection rights over your personal data, we will pass the request to you without undue delay and will not answer it ourselves, except to tell them we have passed it on, unless you ask us to. Frontroom lets you find, correct, export and delete records yourself. Where you need more help to answer a request, we will give it, taking into account the nature of the processing.

10.2 Requests from authorities. If a court, regulator or other public body asks us for your personal data, we will tell you, unless the law forbids it, and we will disclose only what we are legally required to. Where the law allows, we will follow your reasonable instructions about the request and keep you updated. If you take legal steps in response to such a request, we will cooperate and give you reasonable help, at your cost.

10.3 Impact assessments. We will reasonably help you with data protection impact assessments, transfer risk assessments, and prior consultation with the Information Commissioner's Office, where the law requires them, taking into account the nature of the processing and the information we have. For AI cameras, we can give you a description of how they work to use in your assessment.

11. Information and audits

11.1 Information. We will give you all the information reasonably needed to show that we meet this DPA

and Article 28 of UK GDPR.

11.2 Questionnaires. We do not hold third-party security certifications today. Instead, you may send reasonable security and due diligence questions in writing to support@frontroom.ai, once a year, or at any time after a personal data breach affecting your personal data or when a regulator requires it. We will answer them.

11.3 Audits and inspections. If our answers are not enough to show that we meet this DPA, or a regulator requires it, you, or an independent auditor you appoint who is bound to keep our information confidential, may audit us, including by inspection. You must give us at least 30 days' written notice, and the audit must take place during normal business hours, without disrupting the service or putting other customers' data at risk. Each party pays its own costs. We may limit access to information where giving it would break our duties of confidentiality to others or weaken our security.

11.4 Records. We keep records of our compliance with this DPA for 3 years after it ends.

12. Deleting or returning data

12.1 While you use Frontroom. You can delete records in Frontroom in the ways the app allows. Camera pictures and clips attached to events are deleted automatically after the number of days you set. Posted accounting entries are never edited or deleted: they are corrected by reversals, so your books stay complete. When you ask us to delete something, we will do it as soon as reasonably practical, unless the law requires us to keep it.

12.2 When the Agreement ends. You have 30 days to export your data. After that, we delete your personal data, or return it to you if you ask before the 30 days end, unless the law requires us to keep it. Copies in our backups are deleted as the backups roll over, within 30 days.

12.3 Data the law requires us to keep. If the law requires us to keep some of your personal data, or returning or deleting it is not possible, we will keep protecting it and will only process it for that purpose.

12.4 Confirmation. On request, we will confirm in writing that we have deleted your personal data.

13. Liability

Each party's liability under or in connection with this DPA is subject to the limits and exclusions of liability in the Agreement (section 11 of our Terms), as far as data protection law allows. This DPA does not limit anyone's liability to individuals for their data protection rights, or any liability that the law does not allow to be limited, including under the International Data Transfer Agreement, the UK Addendum or the EU standard contractual clauses. Only you, as the party to the Agreement, may bring claims against us under this DPA.

14. Which document applies first

If documents conflict, this order applies: (1) the International Data Transfer Agreement, the UK Addendum or the EU standard contractual clauses, where they apply; (2) this DPA; and (3) the rest of the Agreement.

15.1 Term. This DPA starts when you accept our Terms, or when you sign it if that is earlier, and lasts as long as the Agreement. After that, both of us stay bound by it, and by data protection law, for as long as we process your personal data.

15.2 Changes. We may update this DPA to reflect changes in the law, in guidance from the Information Commissioner's Office, or in Frontroom. We will publish each new version on this page with its date, and tell account owners at least 30 days before an important change takes effect. A change will not reduce the protection this DPA gives your personal data, unless the law requires it.

16. Law and courts

This DPA is governed by the law of England and Wales, and the courts of England and Wales deal with any dispute about it, except where section 8.3 says otherwise for the EU standard contractual clauses.

17. Meanings

- **UK GDPR** means the UK General Data Protection Regulation, as it applies with the Data Protection Act 2018 and later amendments, including by the Data (Use and Access) Act 2025.
- **Controller, processor, personal data, processing, personal data breach and special category data** have the meanings they have in UK GDPR, or in the data protection law that applies to you if you are outside the UK.
- **Subprocessor** means a company we use to process your personal data for us.
- **International Data Transfer Agreement** and **UK Addendum** mean the documents of those names issued by the Information Commissioner under section 119A of the Data Protection Act 2018.
- **EU standard contractual clauses** means the clauses annexed to European Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
- **Business day** means a day other than a Saturday, a Sunday or a public holiday in England.

Annex 1: Processing details

A. The parties

Party	Details	Role
You (data exporter)	The business named in the Frontroom account. Contact: the account owner, at the email address in the account.	Controller, or processor where section 2.2 applies
FRONTROOM AI LTD (data importer)	11 Frating Crescent, Woodford Green, IG8 0DW, United Kingdom. Contact: Moaed Yahia, Founder, support@frontroom.ai .	Processor, or subprocessor where section 2.2 applies

B. The processing

Item	Details
Service	Frontroom, the restaurant till and accounting system, with its optional AI features.
People the data is about	Your staff (employees, workers and contractors); the users you give access to; your guests and customers; your suppliers and their contacts; your other business contacts; and, if you switch on AI cameras, anyone who appears on your connected cameras, such as staff, guests and visitors.
Staff data	Name, contact details, role and branch; shifts and rota; attendance, such as clock-in and clock-out times; leave and absence; pay rates and payroll records; identity or tax reference numbers you choose to record; bank details for paying wages; HR documents and notes you add.
User data	Name, username, email address, phone number, role, sign-in records, and what each user does in the account, as recorded in the audit log.
Guest and customer data	Name, phone number, email address and address for orders and invoices; order history; loyalty points; notes you add.
Supplier and contact data	Names and contact details; invoices, bills and payments; bank details.
Content you add	Photos of invoices and receipts; voice notes and their text; questions typed in Ask and the answers; attachments.
Camera data (only if you switch AI cameras on)	Images from the cameras you connect; pictures and short clips attached to events, with sound only if you turn sound on; counts and events worked out from them; and, if you switch on staff check-in by camera, matches between people seen on camera and your staff list.
Special category data	Frontroom does not need special category data to work. Your data may include it if you choose: biometric data, if you switch on staff check-in by camera and it recognises people from their physical features; and health information, if you record sickness absence. Safeguards: camera features stay off until you switch them on; access follows the roles you set; camera pictures and clips are deleted automatically after the number of days you set (7 days unless you change it, 90 days at most); and you must meet section 4.3.
How often	Continuously, while you use Frontroom.
Nature of the processing	Receiving, recording, storing, organising, displaying, analysing (including with the AI features you use), sending emails that you or your users trigger, such as invitations, backing up, restoring, exporting and deleting.

Item	Details
Purpose	To provide Frontroom to you under the Agreement: the till and orders, kitchen screen, menu and stock, purchases, staff, rota and payroll, tax, banking and reports, and the AI features you choose to use; and to secure and support it.
Duration and retention	For as long as the Agreement lasts, then the 30 days you have to export your data and the time our backups take to roll over (section 12), or longer only where the law requires. While the Agreement lasts, you decide how long records are kept, and camera pictures and clips are kept for the number of days you set.
Transfers to subprocessors	As set out in Annex 3, for the tasks shown there, for as long as each task needs.

C. Supervisory authority

The Information Commissioner's Office (ICO) in the United Kingdom. Where the EU standard contractual clauses apply (section 8.3), the authority chosen under their clause 13.

Annex 2: Security measures

These are the technical and organisational measures we use today.

- **Encryption in transit.** All connections to Frontroom use TLS (HTTPS), and browsers are told to use HTTPS only. Our servers accept no direct connections from the internet: traffic reaches them through an encrypted tunnel from our network provider.
- **Access control and roles.** Every user signs in with their own account. The account owner decides each user's role, and our servers check that role for every action. Passwords are stored only as strong one-way hashes (Argon2), repeated failed sign-ins are slowed down, and sessions use secure cookies.
- **Separate accounts.** Each restaurant's records are kept separate, and every request is checked against the account it belongs to. Only the people the account owner gives access to can see them in Frontroom.
- **Our own access.** Only named Frontroom staff can reach production systems, using personal keys. We access customer data only when needed to run, support or secure the service. Keys and passwords for our systems are kept out of the code.
- **Audit log.** Frontroom records who did what in each account. Posted accounting entries are never edited or deleted: corrections are made by visible reversals.
- **Backups and recovery.** The database and files are backed up every night. Backups are kept on two machines, and an encrypted copy is kept off site, so the service and your data can be restored after a fault or an incident.
- **Error tracking with scrubbing.** When something breaks, an error report goes to our error tracking provider. Before it leaves our servers, we remove personal data from it: the user, IP addresses, cookies, the content of requests, email addresses, phone numbers, card and bank numbers, and

passwords and tokens.

- **Data minimisation.** We send each subprocessor only what it needs for its task. Product usage statistics use codes instead of names, and never include email addresses, phone numbers or IP addresses. Data exports never include passwords or secret codes, and only the account owner can download a full copy of the account's data.
- **AI features.** We send the AI provider only the content needed for the task you asked for. Nothing an AI feature drafts is posted to your books until a person approves it.
- **Cameras.** The camera engine connects out from your network, so you do not need to open your network to the internet. Pictures and clips attached to events are deleted automatically after the number of days you set.
- **Breaches.** We follow section 9 when something goes wrong, and record what happened and what we did.

Annex 3: Subprocessors

You approve these subprocessors (section 7). The current list is always at frontroom.ai/subprocessors, and we tell you before we add or replace one. On 25 October 2026 the list was:

Company	What it does for Frontroom	Data it handles	Where
Cloudflare	Delivers this website and the app, runs our domain names (DNS), protects both from attacks, carries traffic between browsers and our servers, and forwards email sent to our addresses.	Everything sent to or from Frontroom passes through its network, and email sent to our addresses.	Worldwide, at the data centre nearest the user
Resend	Sends account emails, such as invitations, password resets and service messages.	The recipient's name and email address, and the email itself.	European Union (Ireland)
Sentry	Error tracking: tells us when something in Frontroom breaks, so we can fix it.	Technical error reports. Before a report leaves our servers, we remove names, email addresses, phone numbers, IP addresses, card and bank numbers, passwords and the content of requests.	European Union (Germany)
Mixpanel	Product analytics: counts which features are used.	Pseudonymous usage events, such as a paid till order or an invoice photo read, labelled with codes. Never names, email addresses, phone numbers or IP addresses.	European Union

Company	What it does for Frontroom	Data it handles	Where
Amplitude	Product analytics: the same counts as Mixpanel.	The same pseudonymous usage events as Mixpanel, and nothing more.	European Union
OpenAI (AI model provider)	Runs the AI model behind Ask and photo reading.	The question or photo, and the records needed to answer it or to draft the entry.	United States
Speech-to-text provider	Turns voice notes into text.	The voice recording. The text comes back to Frontroom and is saved with the record it belongs to.	United States
Oracle Cloud	Stores an encrypted off-site copy of our nightly database backup.	Encrypted backup files only. They are encrypted before upload and only Frontroom holds the key, so Oracle cannot read them.	United Kingdom (London)
Google	Hosts the inbox for email you send to support@frontroom.ai.	The emails you send us and our replies.	United States and Europe

Frontroom's application, database and backups run on Frontroom servers in the UK that we own and operate.

Signatures

You do not need to sign this DPA: it applies once you accept our Terms. If you want a signed copy, both parties can sign here, or we can send it to you for electronic signature.

	FRONTROOM AI LTD	Customer
Business name	FRONTROOM AI LTD	
Name		
Title		
Signature		
Date		

About this document

Version 1.0, published 25 October 2026. Read it online at frontroom.ai/dpa or [download the PDF](#), which has the same text.

This DPA is based on the [Common Paper Data Processing Agreement Standard Terms, Version 1.1](#), by Common Paper, Inc., free to use under [CC BY 4.0](#). We changed it: we rewrote it in plain English as one document with its cover page, adapted it to UK GDPR and the Data Protection Act 2018, filled in the details and annexes for Frontroom, simplified the transfer terms, and added terms on AI cameras, audits and deletion. Common Paper is not a party to this DPA and does not endorse Frontroom. Common Paper offers its standard terms as they are, without warranties.