IzyShift — BLACKBREAD LTD

Data Processing Agreement

Version 1.0 · Effective 7 October 2026 · https://izishift.cc/legal/dpa/

This Data Processing Agreement (the **"DPA"**) is made between:

- the **Customer**, the business that has registered a company workspace in IzyShift and accepted the IzyShift Terms of Service (the **"Controller"**); and
- **BLACKBREAD LTD**, HE 352187, Agias Zonis 5, 3027 Limassol, Cyprus (the **"Processor"**, **"we"**).

It sets out the terms required by Article 28(3) of the GDPR. It forms part of the Terms of Service and is entered into when the Customer accepts the Terms, at company registration, before a paid subscription, or by accepting updated terms in the app. No separate signature is needed. A PDF copy of this version can be downloaded from this page.

1. Definitions

- **"GDPR"** means Regulation (EU) 2016/679.
- **"Personal Data"** means personal data that the Processor processes on behalf of the Controller in providing the Service.
- **"Sub-processor"** means another processor engaged by the Processor.

Terms such as "processing", "data subject", "personal data breach" and "supervisory authority" have the meaning given in the GDPR.

2. Subject matter, duration, nature and purpose

2.1. **Subject matter.** The Processor processes Personal Data to provide the IzyShift Service to the Controller: staff scheduling, time and attendance, leave, shift notes, payroll preparation, notifications and the related reports and integrations.

2.2. **Duration.** The DPA applies for as long as the Processor processes Personal Data for the Controller. That is the term of the Customer's account, plus the retention and deletion period in section 10.

2.3. **Nature and purpose, data categories and data subjects.** These are described in **Annex 1**.

3. Instructions

3.1. The Processor processes Personal Data only on documented instructions from the Controller. That includes transfers to third countries, unless EU or Member State law requires otherwise. In that case the Processor informs the Controller before processing, unless the law prohibits this.

3.2. The Controller's documented instructions are:

- these Terms and this DPA;
- the Controller's configuration of the Service, such as features switched on, access levels and integrations connected;
- actions taken by the Controller's authorised Users in the Service;
- other written instructions agreed between the parties.

3.3. The Processor informs the Controller immediately if, in its opinion, an instruction infringes data protection law.

3.4. The Controller is responsible for the lawfulness of its instructions and of the processing it initiates. This includes the legal basis for it and informing data subjects.

4. Confidentiality

The Processor ensures that persons authorised to process Personal Data are bound by confidentiality. Access is limited to persons who need it to operate, support or secure the Service.

5. Security

The Processor implements the technical and organisational measures in **Annex 2**, as required by Article 32 GDPR. It may update these measures, provided the overall level of protection is not reduced.

6. Sub-processors

6.1. The Controller gives a **general authorisation** for the Processor to engage Sub-processors. The current list is published on the Sub-processors page and forms **Annex 3**.

6.2. The Processor will notify the Controller of any intended addition or replacement of a Sub-processor **at least 30 days in advance**. It does so by email to the account owner or by a notice in the app, and by updating the Sub-processors page. The Controller may object on reasonable data protection grounds within that period. If the parties cannot resolve the objection, the Controller may terminate the affected part of the Service and receive a pro-rata refund of prepaid fees.

6.3. Where an urgent replacement is needed for security or continuity, the notice may be shorter. The Processor will then notify the Controller as soon as possible.

6.4. The Processor imposes data protection obligations on each Sub-processor that are substantially the same as those in this DPA, where the Sub-processor offers such terms. It remains liable to the Controller for the Sub-processor's performance, as provided in Article 28(4) GDPR. Some providers do not offer data processing terms, and their use is optional for the Controller. Their status is stated on the Sub-processors page.

7. International transfers

The primary hosting of the Service (application and database) is in the European Union. Where a Sub-processor processes Personal Data outside the EEA, the Processor ensures an appropriate safeguard under Chapter V GDPR. Examples are an adequacy decision (including the EU–US Data Privacy Framework for certified recipients) or the Standard Contractual Clauses adopted by the European Commission. The mechanism for each Sub-processor is listed in Annex 3.

8. Assistance

8.1. **Data subject requests.** The Processor assists the Controller, through appropriate technical and organisational measures, to respond to requests from data subjects exercising their rights. If the Processor receives a request directly, it forwards it to the Controller without undue delay, and in any case within 5 business days. It does not respond itself except to confirm receipt and redirect the person, unless the Controller instructs otherwise. The Service lets the Controller view, correct and export staff data. Employees can request deletion of their own login account in the app, which the Controller is notified of.

8.2. **Other obligations.** Taking into account the nature of processing and the information available to it, the Processor assists the Controller with:

- security of processing;
- breach notifications;
- data protection impact assessments;
- prior consultations with supervisory authorities (Articles 32–36 GDPR).

9. Personal data breaches

9.1. The Processor notifies the Controller **without undue delay, and in any event within 48 hours**, after becoming aware of a personal data breach affecting the Controller's Personal Data.

9.2. The notification includes, as far as then known:

- the nature of the breach;
- the categories and approximate number of data subjects and records concerned;
- the likely consequences;
- the measures taken or proposed;
- a contact point.

Information may be provided in phases.

9.3. The Processor takes reasonable steps to contain the breach and mitigate its effects. Notifying supervisory authorities and data subjects is the Controller's responsibility, and the Processor assists with it.

10. Deletion or return at the end of the Service

10.1. During the Service, the Controller can export its data using the built-in exports. On request, the Processor provides a full export in a common machine-readable format.

10.2. After the account ends, or after the Controller deletes its company, the Processor keeps Personal Data for **90 days**. This allows restoration or a final export on the Controller's request. After that period, the Processor deletes or anonymises the Personal Data in its live systems. Copies in encrypted backups are overwritten within a further 60 days.

10.3. Section 10.2 does not apply where EU or Member State law requires the Processor to keep the data.

11. Audits and information

11.1. The Processor makes available to the Controller the information necessary to demonstrate compliance with Article 28 GDPR. This includes answers to reasonable security questionnaires.

11.2. The Controller (or an independent auditor it mandates, bound by confidentiality) may audit the Processor's compliance:

- no more than once in any 12-month period, unless a breach or a supervisory authority requires otherwise;
- with at least 30 days' written notice;
- during business hours;
- in a way that does not disrupt the Service or compromise other customers' data.

Each party bears its own costs, unless the audit reveals a material breach by the Processor.

12. Liability and precedence

12.1. Liability under this DPA is subject to the limitations in the Terms of Service, except where the law prohibits such limitation.

12.2. In case of conflict between this DPA and the Terms on the processing of Personal Data, this DPA prevails.

12.3. This DPA is governed by the laws of the Republic of Cyprus. The courts of Limassol have jurisdiction.

Annex 1 — Details of processing

Data subjects:

- the Controller's employees, managers, administrators and owners who are Users of its workspace;
- candidates or staff the Controller adds without giving them a login;
- persons named in shift notes, where the Controller's Users write about them.

Categories of Personal Data:

- identity and contact data (name, work email, phone, login, password hash, language, Telegram user ID and name if linked);
- employment organisation data (venue, department, position, access level, hire and termination dates, maximum hours, staff-card notes, personal rules);
- schedule and leave data (shifts, breaks, notes, leave requests and balances, absence type);
- attendance data (punch times, method, approvals and corrections, lateness and no-shows, punctuality ranking). Depending on the Controller's settings, this also includes the device IP address, GPS position at the moment of punching, and the terminal PIN;
- pay data (pay type and rates, adjustments, calculated hours and pay);
- bank details for salary payouts, only if the Controller uses the payroll payouts feature (name on the bank account, IBAN, optional BIC), payroll runs (net amounts to pay as entered or approved by the Controller, adjustments with comments, approval and payment status);
- shift notes (text, photos without EXIF metadata, transcripts of voice messages if enabled);
- technical data (sessions, audit log, notification logs).

Special categories: none are intended. The Service records an absence type (e.g. sick leave) without medical details. The Controller must not enter special categories of data in free-text fields unless lawful and necessary.

Nature of processing: collection, recording, organisation, storage, retrieval, calculation, display to authorised Users, transmission of notifications (web, email, Telegram), transcription of voice notes (if enabled), export, deletion.

Purpose: providing the Service to the Controller: scheduling, time and attendance, leave management, payroll preparation, preparing salary payment files (and, if the Controller chooses one, passing payment instructions to a payment provider) on the Controller's approval, shift reporting, labour-cost reporting with POS sales data, and the related notifications and support.

Frequency: continuous, for the duration of the Service.

Retention: as set out in section 10 and the Controller's own configuration and deletions.

Annex 2 — Technical and organisational measures

1. **Hosting and location.** Servers operated by Hetzner Online GmbH in the EU (Germany and Finland). The provider is certified to ISO/IEC 27001 for its data centres.
2. **Encryption in transit.** All web, API and app traffic uses HTTPS (TLS). HTTP is redirected to HTTPS. Session cookies are `Secure`, `HttpOnly`, `SameSite=Lax`.
3. **Encryption of backups and secrets.** Daily backups are encrypted (GPG, AES-256) before leaving the server. The key is held only by the Processor. Credentials for the Controller's POS integration and employees' bank details (IBAN) are stored encrypted at rest; bank details are shown masked and the full IBAN only on an explicit request by an owner or administrator, which is logged.
4. **Authentication.** Passwords are stored only as salted PBKDF2 hashes. Login attempts are rate-limited per account and per IP address. Telegram logins are verified by cryptographic signature. Invitation, terminal and file links are random tokens with expiry or revocation.
5. **Access control.** Permissions are checked on the server for every request, by action (employee, manager, department manager, administrator, owner). Each customer's data is separated by company identifier in every query. Pay data is visible only to owners and administrators.
6. **Administrative access.** Server access is restricted to the Processor's authorised administrators. Administrative (root) login to the server accepts SSH keys only. Secrets are kept outside the code repository with restricted file permissions.
7. **Data minimisation.** Geolocation is captured only at punch time and only if the Controller enables it. EXIF metadata is removed from photos. Voice audio is not stored after transcription. There is no analytics or advertising tracking.
8. **Availability and resilience.** Daily encrypted backups, with local and off-site copies. Restore tests run regularly. Service monitoring alerts the Processor about failures.
9. **Logging.** An audit log covers administrative changes (roles, ownership, rules), every change to bank details, every view of a full IBAN, and every step of a payroll run (approval, export, payment marks). Web server logs are kept for 14 days for security.
10. **Development and change management.** Code is under version control. Automated tests and staged checks run before deployment. Database backups are taken before schema changes. Tests run on copies of data in isolated sandboxes and never send messages to real users.
11. **Incident handling.** Breaches are assessed and the Controller is notified as in section 9.
12. **Personnel.** Access is limited to persons bound by confidentiality, on a need-to-know basis.

Annex 3 — Sub-processors

The current list, with each Sub-processor's purpose, location and transfer mechanism, is published at izishift.cc/legal/subprocessors/ and is incorporated by reference.