Data Processing Agreement

Verwerkersovereenkomst — Article 28 GDPR

Version 1.0 · 29 June 2026 · Kanriva™ and FlowCrew™

1. Parties

Processor — Kaizen Kanri, a company registered in the Netherlands under Chamber of Commerce (KVK) number 42049431, hereinafter "Kaizen Kanri". Contact for all matters under this agreement: info@kaizenkanri.nl.

Controller — the customer organisation that has entered into a subscription or pilot agreement for the Kanriva™ platform, hereinafter "the Controller". The Controller's legal name, address and contact for data protection matters are recorded in Annex I.

The Controller determines the purposes and means of the processing of personal data. Kaizen Kanri processes personal data only on behalf of and on the documented instructions of the Controller. This agreement forms part of, and prevails over, the subscription agreement in respect of data protection.

2. Subject matter and duration

Kaizen Kanri provides the Kanriva™ operations platform and the FlowCrew™ worker application. In doing so it processes personal data relating to the Controller's workforce. The subject matter, nature, purpose, categories of personal data and categories of data subjects are described in Annex I.

This agreement takes effect on the date the Controller first obtains access to the platform, including any trial or pilot, and remains in force for as long as Kaizen Kanri processes personal data for the Controller. Clauses that by their nature extend beyond termination — in particular clauses 9, 11 and 12 — survive termination.

3. Instructions

1. Kaizen Kanri processes personal data solely on the documented instructions of the Controller. The subscription agreement, this agreement, the platform's documented functionality and the Controller's use of that functionality together constitute those instructions.
2. Kaizen Kanri does not process the personal data for its own purposes. It does not sell personal data, does not use it for advertising, and does not use it to train machine-learning models. See clause 8.
3. Kaizen Kanri informs the Controller without delay if, in its opinion, an instruction infringes the GDPR or other applicable data protection law, and may suspend execution of that instruction until it is confirmed or withdrawn.
4. Kaizen Kanri processes personal data only within the European Union, save for the limited exceptions set out in clause 7.

4. Controller obligations

1. The Controller warrants that it has a lawful basis for the processing it instructs, and that it has informed its workforce about the use of the platform in accordance with Articles 13 and 14 GDPR.
2. The Controller is responsible for the personal data it and its users enter. In particular, **the Controller instructs its users not to enter special categories of personal data** (Article 9 GDPR) into free-text fields, attachments or messages. Absence may be recorded as a type or code; medical details, diagnoses and occupational-health reports must not be entered. Kaizen Kanri's functionality does not require them.
3. The Controller is responsible for managing its own user accounts and roles: granting access only to those who need it, applying the least-privilege principle to modules containing personnel data, and removing access when a user leaves.

4. Where the Controller uses the platform for works-council-sensitive purposes such as performance measurement or documented personnel follow-up, the Controller is responsible for any consultation or agreement required under national employment law.

5. Confidentiality

1. Kaizen Kanri keeps all personal data confidential and does not disclose it to third parties except as permitted by this agreement or required by law. If disclosure is legally required, Kaizen Kanri informs the Controller in advance unless prohibited from doing so.
2. Every natural person acting under the authority of Kaizen Kanri who has access to personal data is bound by a duty of confidentiality that survives the end of their engagement.
3. Access to production data by Kaizen Kanri personnel is limited to what is strictly necessary for support, incident resolution and maintenance, and is exercised on a least-privilege basis.

6. Security measures

1. Kaizen Kanri implements appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of the processing.
2. The measures in force at the date of this agreement are set out in **Annex II**. Kaizen Kanri may update them, provided the level of protection is not reduced.
3. Kaizen Kanri publishes an honest statement of the measures it has **not** yet implemented in Annex II, section 12, so that the Controller can take them into account in its own risk assessment.

7. Sub-processors and international transfers

1. The Controller grants Kaizen Kanri general authorisation to engage the sub-processors listed in **Annex III**.
2. Kaizen Kanri imposes on each sub-processor data protection obligations no less protective than those in this agreement, and remains fully liable to the Controller for the performance of its sub-processors.
3. Kaizen Kanri notifies the Controller in writing at least **thirty (30) days** before adding or replacing a sub-processor that processes workforce personal data. The Controller may object on reasonable data protection grounds within that period; if the objection cannot be resolved, the Controller may terminate the affected part of the subscription without penalty.
4. All workforce personal data is hosted within the European Union. Two sub-processors may process a strictly limited data set outside the EU: the payment provider (billing contact data of the Controller's administrators, never workforce data) and the transactional email provider (recipient email address and message content of platform notifications). Both are engaged under the European Commission's Standard Contractual Clauses. Annex III states this per sub-processor.

8. No AI training and no secondary use

1. The staffing recommendation engine in Kanriva™ is deterministic and rule-based. It runs on Kaizen Kanri's own infrastructure and produces an explainable outcome from the Controller's own workload, availability and shift-rule data. A planner confirms every outcome.
2. **No third-party artificial intelligence or large-language-model service processes the Controller's personal data.** No personal data is sent to any AI provider, and no personal data is used to train, fine-tune or evaluate any model, by Kaizen Kanri or by any sub-processor.
3. Kaizen Kanri does not use production personal data for product development, benchmarking, analytics or marketing. Test and demonstration environments use invented data only.

9. Personal data breaches

1. Kaizen Kanri notifies the Controller of a personal data breach affecting the Controller's data **without undue delay and in any event within 48 hours** of becoming aware of it, in writing, to the contact in Annex I. The 48-hour limit is an outer bound on the *initial* notification, not a promise that the investigation is complete within it.
2. Notification is explicitly phased, so that speed never becomes a reason to delay:

- **Initial notification** — sent within the 48-hour window, stating what is known, what is not yet known, and what has already been done to contain the incident. It is marked provisional.
- **Information available at that moment** — the nature of the breach, the categories and approximate number of data subjects and records concerned as far as then established, the likely consequences, the measures taken or proposed, and the name and contact details of the person from whom further information can be obtained.
- **Investigation updates** — provided as facts are established, without further undue delay, and always immediately if the assessed severity or scope changes.
- **Confirmed scope** — a written confirmation of the categories and numbers actually affected once the investigation is complete.
- **Remediation and closure** — a written report of root cause, the structural measures taken, and any action recommended on the Controller's side.

3. A partial notification within 48 hours is always preferred over a complete one that is late. Kaizen Kanri does not withhold a notification because the picture is incomplete.
4. Kaizen Kanri assists the Controller with any notification to a supervisory authority or to data subjects. The decision to notify rests with the Controller.
5. The full procedure, including the internal severity classification and timings, is published in the Incident Response Procedure that accompanies this agreement.

10. Data subject rights and assistance

1. Kaizen Kanri assists the Controller in fulfilling requests from data subjects exercising their rights of access, rectification, erasure, restriction, portability and objection. The platform's role-based screens and Excel/PDF exports allow the Controller to answer most requests itself without involving Kaizen Kanri.
2. If a request is addressed directly to Kaizen Kanri, it does not act on it, but forwards it to the Controller without undue delay.
3. Kaizen Kanri assists the Controller, at the Controller's request, with data protection impact assessments and with prior consultation of a supervisory authority, to the extent the information is available to Kaizen Kanri.
4. Reasonable assistance is provided at no charge. Disproportionate effort may be invoiced at the agreed hourly rate, after written notice.

11. Audit

1. Kaizen Kanri makes available to the Controller all information necessary to demonstrate compliance with Article 28 GDPR, in the form of this agreement, the Security Statement, the Sub-Processor Register, the Backup, Retention and Exit Statement and the Incident Response Procedure.
2. The Controller may, at its own cost and no more than once per twelve months, audit that compliance, either itself or through an independent auditor bound by confidentiality. An audit is announced at least thirty (30) days in advance, takes place during business hours, and may not disrupt operations or expose other customers' data.
3. Kaizen Kanri does not currently hold an ISO 27001 certificate or a SOC 2 report, and has not commissioned an external penetration test. This is stated openly rather than implied; see Annex II, section 12.

12. Return and deletion

1. On termination of the subscription, and at any time on written request, Kaizen Kanri deletes or returns all personal data processed for the Controller.
2. The account is first archived and remains recoverable for **thirty (30) days**, so that an accidental or disputed termination does not destroy the Controller's records. After that period an automated process permanently deletes the account and all associated records from the production database.
3. Before deletion the Controller may export its data through the platform's Excel and PDF exports. On written request Kaizen Kanri provides a complete structured export of the Controller's data.
4. Backups are overwritten in the normal backup cycle. Kaizen Kanri does not selectively delete individual records from historical backups; it confirms in writing when the last backup containing the Controller's data has been overwritten.
5. Details, including the exact retention periods, are in the Backup, Retention and Exit Statement.

13. Liability and law

1. Liability under this agreement is governed by the liability provisions of the subscription agreement, without prejudice to the rights of data subjects under Articles 79 and 82 GDPR.
2. This agreement is governed by Dutch law. Disputes are submitted to the competent court in the Netherlands.
3. If any provision is invalid or unenforceable, the remaining provisions stay in force and the parties replace the invalid provision with a valid one of equivalent effect.

14. Signature

Signed for and on behalf of the parties:

	Processor	Controller
Organisation	Kaizen Kanri (KVK 42049431)	.....
Name	.....	.....
Role	.....	.....
Date	.....	.....
Signature	.....	.....

A counter-signed copy is returned by email. A Dutch-language version of this agreement is available on request.

Annex I — Description of the processing

Controller details — to be completed on signature.

Field	Value
Legal name	.....
Address	.....
Contact for data protection	.....
Email for breach notification	.....

Subject matter — provision of the Kanriva™ operations platform and the FlowCrew™ worker application: workforce planning against measured workload, publication of schedules, registration of presence and actuals, absence and holiday administration, shift handover, productivity analysis, continuous-improvement registers and documented personnel follow-up.

Nature of the processing — collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, export, restriction, erasure and destruction, all by automated means within the platform.

Purpose — enabling the Controller to plan, publish, execute, measure and improve the work of its own workforce, and to communicate with that workforce.

Duration — for the term of the subscription, plus the thirty-day recovery window described in clause 12.

Categories of data subjects

- Employees of the Controller.
- Temporary workers, agency workers and contractors deployed by the Controller.
- Planners, team leaders, supervisors and administrators of the Controller.

Categories of personal data

Category	Examples
Identity and contact	Name, employee or UZK number, work email, telephone, preferred language
Employment data	Department, function, contract hours, start date, employment status, cost or rate band where entered
Scheduling data	Shifts, start and end times, planned hours, department assignment, availability, skills and qualifications
Absence and holiday	Absence type or code, holiday requests and balances, leave periods
Presence and actuals	Clock or confirmation times, attendance status, lateness, no-shows, overtime and surcharge bands
Performance data	Productivity per person and per process, plan-versus-actual results, benchmark comparisons
Documented follow-up	Records of formal conversations, agreements and deviations entered by authorised roles
Documents	Files and images uploaded by authorised users, such as certificates or damage photographs
App account data	FlowCrew™ account identifier, language preference, device push token, login timestamps
Communication	Messages linked to a shift, day or department, and shift handover entries
Technical metadata	Audit trail of changes, including user, timestamp and previous value; application error logs

Special categories of personal data — none are required or requested. The Controller instructs its users not to enter them; see clause 4.2.

Children's data — none. The platform is used by working adults; where national law permits employment from sixteen, the Controller remains responsible for the lawfulness of that processing.

Annex II — Technical and organisational measures

These are the measures in force on 29 June 2026.

1. Hosting and data location

Application and database run on infrastructure provided by Strato AG in Germany, within the European Union, on a managed container platform operated together with Kaizen Kanri's deployment partner. No workforce personal data is stored outside the European Union.

2. Encryption

- **In transit** — all traffic between browser or mobile app and the platform is encrypted with TLS. Plain HTTP is not served; authentication cookies are marked Secure.
- **At rest** — the database and stored files are encrypted at rest.

3. Authentication and session security

- Passwords are hashed with bcrypt, individually salted. Plain-text passwords are never stored or logged.
- Sessions use signed JSON Web Tokens (HS256) delivered in HttpOnly, Secure, SameSite cookies, with a maximum lifetime of seven days, after which re-authentication is required.
- Invitation and password-reset links are single-use and time-limited.

4. Access control

- Access is role-based and enforced server-side on every request; hiding a menu item is never the only control.
- Roles are granular per module, so that planning access does not imply access to personnel records.
- The Controller administers its own users and roles. Kaizen Kanri administrative access to production data is limited to named personnel and exercised only for support, incident resolution and maintenance.

5. Tenant separation

- Every customer is a separate tenant. Every database query is scoped to the authenticated user's tenant on the server, including exports, reports and background jobs.
- Tenant separation is covered by automated regression tests that run against the API and assert that no cross-tenant record is ever returned. These tests are part of the release process; the corresponding test report is available on request.

6. Logging and traceability

- The platform keeps a change history of operational records: who changed what, when, and what the previous value was.
- Application errors are logged for troubleshooting. Logs are not used for employee monitoring.

7. Backups

Full backups are taken **monthly** and stored within the European Union. Restores are tested when a change affects the data model. The resulting recovery point objective is up to one month; see section 12 and the Backup, Retention and Exit Statement.

8. Deletion and retention

Account deletion archives the tenant and keeps it recoverable for thirty days, after which an automated process permanently removes it. Retention periods per data category are in the Backup, Retention and Exit Statement.

9. Secure development and change management

- All source code is held in version control with a per-change history; every change is attributable.
- Each module has written architecture and handover documentation, maintained alongside the code, so the platform does not depend on one person's memory.
- Automated test suites cover authentication, tenant isolation, planning logic and exports, and are run before release.

- Development and demonstration environments use invented data. Production data is not copied into them.

10. Availability

The platform is continuously available while the hosting infrastructure is operational. Planned maintenance is announced in advance and scheduled outside Dutch shift-change peaks where possible. No uptime percentage is contractually guaranteed on trial or pilot subscriptions; a service level can be agreed in writing on an annual agreement.

11. Personnel

Kaizen Kanri is a small, owner-operated company. Everyone with access to production data is bound by confidentiality, applies least privilege, and is instructed on the handling of workforce personal data. Continuity does not depend on a single individual's local machine: source, documentation and hosting are managed and recoverable.

12. Measures not yet in place — stated openly

- **Multi-factor authentication** is not yet available for platform accounts. It is on the roadmap. Until then, strong unique passwords and prompt removal of leavers' accounts are the compensating controls, and the Controller should treat them as such in its risk assessment.
- **No external penetration test** has been commissioned, and Kaizen Kanri holds **no ISO 27001 certificate and no SOC 2 report**.
- **Backup frequency is monthly**, not daily, and there is no point-in-time recovery. A shorter recovery point objective can be arranged per customer before signature.
- **Single-operator company** — see clause 11 and the continuity statement published on the Kanriva™ website.

Kaizen Kanri prefers to state these limitations rather than let a buyer discover them after signature.

Annex III — Authorised sub-processors

Sub-processor	Role	Data processed	Location	Transfer basis
Strato AG	Hosting of application, database and files	All platform data	Germany (EU)	Not applicable — EU
Emergent Labs	Managed deployment platform and object storage for uploaded files	Platform data, uploaded documents and images	EU region; current location confirmed on request	Standard Contractual Clauses where any processing occurs outside the EU
Stripe	Subscription payments and invoicing	Billing contact and payment data of the Controller's administrators. **No workforce personal data.**	EU/US	Standard Contractual Clauses
Resend	Transactional email (invitations, notifications, account and deletion confirmations)	Recipient email address and message content	EU/US	Standard Contractual Clauses

The register, including the notification procedure for changes, is maintained as a separate document: **Sub-Processor Register**.

Kanriva™ and FlowCrew™ are trademarks of Kaizen Kanri. This agreement is provided for signature by Kaizen Kanri and the Controller. It has been drafted to align with Article 28 GDPR and the European Commission's standard contractual clauses for

controller-to-processor relationships; the Controller is free to submit its own template instead, which Kaizen Kanri will review and, where acceptable, sign.