Kanriva™ security & GDPR pack

Version 1.0 · 29 June 2026 · Kaizen Kanri (KVK 42049431) · info@kaizenkanri.nl

This single file contains the complete pack: the Data Processing Agreement (with Annex I–III), the Security Statement including a pre-answered vendor security questionnaire, the Sub-Processor Register, the Backup, Retention and Exit Statement, and the Incident Response Procedure. Each document is also available separately. A Dutch version of the processing agreement is available on request.

#	Document
1.	Data Processing Agreement
2.	Security Statement
3.	Sub-Processor Register
4.	Backup, Retention and Exit
5.	Incident Response Procedure

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.

Security Statement

Kanriva™ operations platform and FlowCrew™ worker app

Version 1.0 · 29 June 2026 · Kaizen Kanri (KVK 42049431)

1. Purpose of this document

This statement describes how Kaizen Kanri hosts, protects and deletes the data you put into Kanriva™. It is written to be handed to an IT manager, a privacy officer or a works council without translation, and to replace the usual vendor security questionnaire — section 12 answers those questions directly.

Everything in this document is a statement of what is true today. Where a control is not yet in place, it is listed in section 11 rather than omitted. If you find a claim here that you cannot verify during a walkthrough, treat it as a defect and report it to info@kaizenkanri.nl.

2. What the platform processes

Kanriva™ plans, publishes and measures work. To do that it holds workforce data: names and employee numbers, department and function, contract hours, shifts and availability, absence and holiday, presence and actual times, productivity per person and per process, documented follow-up of formal conversations, uploaded documents such as certificates or damage photographs, and shift-linked messages and handovers.

That is personnel data, and it is treated as such. Two consequences:

- **Special categories are neither required nor wanted.** Absence can be recorded as a type or code. Medical details, diagnoses and occupational-health reports must not be entered; your users are contractually instructed not to.
- **Performance data is access-controlled.** Productivity and personnel screens are separate modules with their own roles, so a shift planner does not automatically see personnel records.

3. Hosting and data location

The application, the database and uploaded files run on infrastructure provided by **Strato AG in Germany**, inside the European Union, on a managed container platform operated together with our deployment partner. No workforce personal data is stored outside the European Union.

Three narrow exceptions are named rather than buried:

- the **payment provider** processes billing contact and payment data of your administrators, and never workforce data;
- the **transactional email provider** processes the recipient address and the content of platform emails;
- **mobile push delivery**: where push notifications are enabled on an Android device, hand-off to the device is performed by Google's notification service, and notification text is kept free of personnel details. Notifications inside the platform are generated and stored on our own EU infrastructure.

The first two are engaged under the European Commission's Standard Contractual Clauses. The complete list, with roles and locations, is in the **Sub-Processor Register**.

Everything else stays in the EU, including application logs, error logs, the audit trail, uploaded files and backups.

4. Encryption

- **In transit** — all browser and mobile traffic is encrypted with TLS. Plain HTTP is not served. Authentication cookies are marked Secure.

- **At rest** — the database, uploaded files and backups sit on provider-managed encrypted storage. To be precise, because a security reviewer will ask: this is **storage-level encryption with provider-managed keys**, not per-field application encryption, and not customer-managed keys.

5. Accounts, sessions and access

- Passwords are hashed with **bcrypt** and individually salted. They are never stored or logged in plain text, and cannot be read by Kaizen Kanri.
- Sessions use signed JSON Web Tokens delivered in **HttpOnly, Secure, SameSite** cookies, valid for a maximum of seven days, after which the user re-authenticates.
- Invitation and password-reset links are single-use and time-limited.
- Access is **role-based and enforced on the server** for every request. Hiding a button is never the only control.
- You administer your own users and roles. No customer role can reach another customer's data.
- One exception, stated openly: a **named Kaizen Kanri master-admin account** exists for tenant administration and support. Its use is limited to support, incident resolution and maintenance, and it is bound by the confidentiality and least-privilege terms of the DPA. Infrastructure-level access (hosting console and database tooling) inevitably sits with the operator, as it does with any hosted platform; it is not a separate back door, and it is covered by the same obligations.
- **Multi-factor authentication is not yet available.** See section 11.

6. Separation between customers

Every customer is a separate tenant. Every database query, export, report and background job is scoped to the authenticated user's tenant on the server side. There is no shared list, no global search and no cross-customer reporting.

This is the control we take most seriously, because it is the one that would matter most if it failed. It is therefore covered by **automated regression tests** that call the platform as one tenant and assert that no record belonging to another tenant is ever returned. The covered surfaces are the REST API and its list and detail endpoints, Excel and PDF exports, file downloads, search, reports and dashboards, background jobs, and the FlowCrew mobile endpoints. Those tests run as part of the release process, and the test report can be shared on request.

The claim is deliberately scoped: isolation is enforced in the application layer on every request, and verified by tests on the surfaces listed above. It is not a claim about the hosting provider's own infrastructure tooling, which is covered by the administrative route described in section 5.

7. Traceability

The platform keeps a change history of operational records: who changed what, when, and what the previous value was. Schedules, workload figures, presence corrections, handovers and personnel entries are therefore reconstructable, which is what makes the data usable in a formal conversation or a dispute.

Application errors are logged for troubleshooting only. Logs are not a monitoring tool and are not used to observe individual employees.

8. Backups and recovery

Full backups are taken **monthly** and stored within the European Union. Restores are tested when a change affects the data model.

Be aware of what that means: the recovery point objective is **up to one month**, and there is no point-in-time recovery. For most planning operations this is acceptable because the schedule is rebuilt weekly and exports are held locally, but if your risk assessment requires daily backups, say so before signature — it can be arranged per

customer. Details are in the **Backup, Retention and Exit Statement**.

9. Deletion, export and exit

- You can export from every module to Excel or PDF at any time, without asking us. That is deliberate: your data should never be hostage to a subscription.
- Deleting an account archives it and keeps it recoverable for **thirty days**, so an accidental or disputed cancellation does not destroy your records. After thirty days an automated process permanently removes the tenant and its records from the production database.
- On written request we provide a complete structured export before deletion, and confirm in writing when the last backup containing your data has been overwritten.

10. Artificial intelligence — what we do not do

The staffing recommendation engine is **deterministic and rule-based**. It calculates required hours from the workload you enter, compares them with availability, contract hours and shift rules, and proposes a staffing per department. Every proposal is explainable, reproducible, and confirmed by a planner before it becomes a schedule.

Consequently:

- **No third-party AI or large-language-model service processes your data.** No employee record, message or productivity figure is sent to any AI provider.
- **No model is trained, fine-tuned or evaluated on your data**, by us or by any sub-processor.
- **No production data is used for benchmarking, analytics or marketing.** Demonstration environments, including the public demo tour on our website, contain invented names and invented figures only.

If a supplier cannot tell you plainly where employee data goes when they say "AI", that is the question worth asking. Here, it does not leave the platform.

11. What is not in place — stated openly

- **Multi-factor authentication** for platform accounts is not yet available. It is on the roadmap. Compensating controls: strong unique passwords, seven-day session expiry, prompt removal of leavers, role-limited access to personnel modules.
- **No external penetration test** has been commissioned, and we hold **no ISO 27001 certificate and no SOC 2 report**. We will not imply otherwise to win a tender.
- **Backups are monthly**, not daily, with no point-in-time recovery.
- **Kaizen Kanri is a small, owner-operated company.** Continuity is addressed by version control, written architecture and handover documentation per module, managed EU hosting that runs independently of any individual, and data that you can export at any time. The continuity statement on the website describes this in full.
- **No formal ISMS or certified audit programme.** What exists instead: this document, the sub-processor register, the incident response procedure, automated isolation tests, and a standing offer to let your IT lead inspect the setup during a walkthrough.

12. Vendor security questionnaire — pre-answered

Company and contract

#	Question	Answer
1	Legal entity and registration	Kaizen Kanri, Netherlands, KVK 42049431

#	Question	Answer
2	Role under GDPR	Processor. The customer is the controller.
3	Is a DPA available?	Yes — downloadable immediately in English and Dutch, counter-signed on request before any employee data is entered. Your own template is also acceptable for review.
4	Data protection contact	info@kaizenkanri.nl
5	Is a DPO appointed?	No statutory obligation to appoint one; the owner is the accountable contact.
6	Sub-processors disclosed?	Yes — Sub-Processor Register, with 30 days' notice of changes and a right to object.

Data and location

#	Question	Answer
7	Where is data hosted?	Strato AG, Germany (EU).
8	Is data ever outside the EU?	Workforce data: no. Three exceptions: billing contact data (payment provider) and platform email content (email provider), both under Standard Contractual Clauses, and Android push hand-off through Google's notification service with no personnel details in the notification text.
9	Categories of personal data	Identity, employment, scheduling, absence, presence and actuals, productivity, documented follow-up, uploaded documents, app account data, shift-linked messages, audit metadata.
10	Special category data	Not required and not permitted; users are instructed not to enter it.
11	Data retention	Term of the subscription plus a 30-day recovery window, then permanent deletion.
12	Data portability	Excel and PDF exports in every module, self-service; full structured export on request.

Security controls

#	Question	Answer
13	Encryption in transit	Yes, TLS; HTTP not served; Secure cookies.
14	Encryption at rest	Yes — storage-level encryption with provider-managed keys, covering database, uploaded files and backups. Not per-field application encryption; no customer-managed keys.
15	Password storage	bcrypt with per-password salt.
16	Session management	Signed JWT in HttpOnly/Secure/SameSite cookie, maximum seven days.
17	Multi-factor authentication	Not yet available; on the roadmap.
18	Single sign-on / SAML	Not available today.

#	Question	Answer
19	Role-based access control	Yes, granular per module, enforced server-side.
20	Customer separation	Separate tenant per customer; every application query scoped server-side; automated regression tests cover API, exports, file downloads, search, reports, background jobs and mobile endpoints.
21	Audit trail	Yes — who changed what, when, and the previous value.
22	Admin access to customer data	A named master-admin account for tenant administration and support, least privilege, bound by the DPA. Infrastructure-level access sits with the operator, as with any hosted platform.
23	Penetration test	None commissioned to date.
24	ISO 27001 / SOC 2	Not held.
25	Vulnerability management	Dependencies updated on release; security-relevant updates applied promptly.
26	Anti-virus / endpoint	Standard endpoint protection on development machines; server workloads are managed containers.

Operations

#	Question	Answer
27	Backup frequency	Monthly full backups, stored in the EU.
28	Recovery point / time objective	RPO up to one month; RTO target one business day. A shorter RPO can be agreed per customer.
29	Restore testing	Tested when a change affects the data model.
30	Disaster recovery plan	Redeploy from version control onto managed hosting and restore the latest backup; documented per module.
31	Uptime commitment	Continuous availability while hosting infrastructure is operational. No SLA percentage on trials/pilots; SLA available on annual agreements.
32	Planned maintenance	Announced in advance; scheduled outside shift-change peaks where possible.
33	Breach notification	Within 48 hours of becoming aware, in writing, per the Incident Response Procedure.
34	Incident response plan	Yes — published document, reviewed annually.
35	Support channel and response time	info@kaizenkanri.nl; reply within one business day, usually faster during CET business hours.

Development and AI

#	Question	Answer
36	Source control and change history	Yes, every change attributable.

#	Question	Answer
37	Automated testing	Yes — authentication, tenant isolation, planning logic and exports.
38	Production data in test environments	No. Test and demo environments use invented data.
39	AI / LLM processing of customer data	None. The staffing engine is deterministic and rule-based, running on our own infrastructure.
40	Customer data used for model training	Never, by us or by any sub-processor.
41	Third-party analytics or tracking in the app	None in the application.
42	Mobile app distribution	FlowCrew™ on Google Play (com.flow_crew). iOS under consideration.

If your questionnaire contains a question that is not answered above, send it to info@kaizenkanri.nl. It will be answered in writing, including the awkward ones.

Kanriva™ and FlowCrew™ are trademarks of Kaizen Kanri.

Sub-Processor Register

Kanriva™ and FlowCrew™

Version 1.0 · 29 June 2026 · Kaizen Kanri (KVK 42049431)

1. Purpose

This register lists every third party that processes personal data on behalf of Kaizen Kanri in the delivery of the Kanriva™ platform and the FlowCrew™ worker app. It is referenced as Annex III of the Data Processing Agreement and is maintained as a living document, so that a customer can always see who touches their data.

Each sub-processor is engaged under a written data processing agreement with obligations no less protective than those Kaizen Kanri owes its customers. Kaizen Kanri remains fully liable for their performance.

2. Current sub-processors

Sub-processor	Role in the service	Personal data processed	Location	Transfer basis
Strato AG (Germany)	Hosting of the application, the database and uploaded files	All platform data, including workforce personal data	Germany, European Union	Not applicable — processing within the EU
Emergent Labs	Managed deployment platform and object storage for files uploaded by users	Platform data; uploaded documents and images	EU region; the current storage location is confirmed in writing on request	Standard Contractual Clauses where any processing occurs outside the EU
Stripe	Subscription payments, invoicing and payment-method handling	Billing contact details and payment data of the customer's administrators. **No workforce personal data.**	EU / United States	Standard Contractual Clauses
Resend	Transactional email: invitations, account notifications, deletion confirmations, system notices	Recipient email address and the content of the message sent	EU / United States	Standard Contractual Clauses

No other third party receives personal data. In particular:

- **No artificial intelligence or large-language-model provider** processes customer data. The staffing recommendation engine is deterministic and runs on Kaizen Kanri's own infrastructure.
- **No analytics, advertising or tracking provider** is embedded in the application.
- **No data broker, reseller or marketing partner** receives customer data in any form.

3. What each sub-processor can and cannot see

Strato AG hosts the infrastructure. As a hosting provider it has, by nature, the technical ability to access stored data, and is contractually bound not to. Data at rest is encrypted.

Emergent Labs provides the managed platform on which the application is deployed and the object storage used for user-uploaded files such as certificates and damage photographs. It does not receive database exports and does not process workforce data for its own purposes.

Stripe receives only what is needed to charge a subscription: the administrator's name, email, company and payment method, plus invoice amounts. It never receives employee names, schedules, presence data or

personnel records.

Resend receives the recipient address and the body of platform emails — for example an invitation to activate a FlowCrew™ account, or the confirmation of an account deletion. It does not receive database content beyond what appears in the message itself.

4. Changes to this register

1. Kaizen Kanri notifies customers **in writing at least thirty (30) days in advance** before adding or replacing a sub-processor that processes workforce personal data.
2. A customer may object on reasonable data protection grounds within that period. If the objection cannot be resolved, the customer may terminate the affected part of the subscription without penalty.
3. Changes to sub-processors that process **no** workforce personal data — for example a change of payment provider — are notified without the thirty-day waiting period, but are recorded here.
4. Every version of this register is dated. The version in force at the date of signature is attached to the Data Processing Agreement.

5. Subscribe to change notifications

To receive notifications automatically, send a request to info@kaizenkanri.nl stating the customer name and the address that should receive them. Confirmation is sent in writing.

Kanriva™ and FlowCrew™ are trademarks of Kaizen Kanri.

Backup, Retention and Exit Statement

Kanriva™ and FlowCrew™

Version 1.0 · 29 June 2026 · Kaizen Kanri (KVK 42049431)

1. Why this document exists

Two questions decide whether an operations platform is safe to depend on: *what happens if the data is lost*, and *what happens if we leave*. This document answers both in plain terms, including where the answer is less comfortable than a marketing page would suggest.

2. Backups

Item	Position today
Frequency	Full backup, **monthly**
Storage location	European Union
Encryption	Backups are stored encrypted
Recovery point objective (RPO)	Up to one month
Recovery time objective (RTO)	Target one business day after a confirmed request
Restore testing	Performed when a change affects the data model
Point-in-time recovery	Not available
Customer-triggered restore	On written request from an authorised contact

Read this honestly. A monthly cycle means that in a worst-case total loss, up to one month of changes could be lost. In practice the exposure is smaller than it looks, because schedules are rebuilt weekly, exports are held locally by most customers, and uploaded source files (for example volume forecasts) usually still exist outside the platform. But it is a real limitation, not a formality.

If your risk assessment requires a shorter RPO — daily backups, or point-in-time recovery — say so **before signature**. It can be arranged as part of the agreement rather than discovered afterwards.

3. What you can export yourself, at any time

Export is a first-class feature, not a concession:

- Schedules and the monthly schedule matrix — Excel and PDF.
- Workload, plan-versus-actual and productivity analyses — Excel.
- Presence, overtime and surcharge overviews — Excel.
- Absence and holiday overviews, per department and per period — Excel.
- Worker and department lists, including the fields you maintain — Excel.
- Shift handovers (Overdracht), including carry-over items — exportable for reports and overviews.
- Audits, improvement registers and action lists — Excel and PDF.

Every export is scoped to your own organisation and carries your own data only. No request to Kaizen Kanri is required, and no export is disabled at the end of a subscription while the account is still live.

4. Retention

Data	Retention
Operational records (schedules, presence, workload, handovers, audits, personnel follow-up)	For the term of the subscription, until you delete them, or as required by your own retention policy
Uploaded documents and images	As above
User accounts	Until removed by your administrator or until account deletion
Audit trail / change history	With the record it belongs to
Application error logs	Rolling, short-term, for troubleshooting only
Deleted account	Archived and recoverable for **30 days**, then permanently removed
Backups containing deleted data	Overwritten in the normal backup cycle

Kaizen Kanri does not impose a retention period on your operational data — that is the controller's decision. What it does guarantee is that deletion is real, automated and verifiable.

5. Deleting an account

1. An authorised administrator requests deletion, in the application or in writing.
2. A confirmation email is sent, so a deletion is never silent.
3. The tenant is **archived immediately**: it disappears from use, but remains recoverable.
4. For **30 days** the account can be restored on request. This window exists so that an accidental cancellation, a disputed termination or a departing administrator cannot destroy your records.
5. After 30 days an automated process permanently deletes the tenant and all associated records from the production database. No manual step is required and none can be forgotten.
6. Backups are overwritten in the normal cycle. Kaizen Kanri does not selectively delete individual records from historical backups; on request it confirms in writing when the last backup containing your data has been overwritten.

6. Exit checklist

If you decide to leave, this is the sequence that protects you:

1. **Export everything you need** from each module — see section 3 — or request a complete structured export in writing.
2. **Confirm the export is readable** in your own systems before anything is deleted.
3. **Request deletion in writing**, naming the authorised contact.
4. **Note the 30-day date.** Until then, restoration is possible; after it, the data is gone.
5. **Ask for the deletion confirmation** and, if your policy requires it, for written confirmation that backups have been overwritten.
6. **Remove FlowCrew™ access** for your workers — deleting the tenant already invalidates their accounts, but your own offboarding checklist should record it.

There is no exit fee, no export fee and no retention hostage. If a supplier makes leaving expensive, the product was never the reason you stayed.

7. Contact

Questions about backups, recovery, retention or exit: info@kaizenkanri.nl. Requirements that differ from the above can be agreed in writing per customer.

Kanriva™ and FlowCrew™ are trademarks of Kaizen Kanri.

Incident Response Procedure

Personal data breaches and security incidents

Version 1.0 · 29 June 2026 · Kaizen Kanri (KVK 42049431)

1. Scope and commitment

This procedure applies to any incident affecting the confidentiality, integrity or availability of customer data in the Kanriva™ platform or the FlowCrew™ worker app.

Kaizen Kanri commits to notifying an affected customer of a personal data breach **without undue delay and in any event within 48 hours** of becoming aware of it. That commitment is contractual: it appears in clause 9 of the Data Processing Agreement.

Under the GDPR the customer is the controller. The customer decides whether a breach is reported to the supervisory authority (in the Netherlands, the Autoriteit Persoonsgegevens) and whether data subjects are informed. Kaizen Kanri's role is to detect, contain, inform and assist — not to decide on the customer's behalf.

2. Severity classification

Level	Definition	Examples	Customer notification
S1 — Critical	Confirmed unauthorised access to or loss of personal data, or confirmed cross-customer data exposure	Account compromise with data access; a defect returning another tenant's records	Immediately on confirmation, and in any event within 48 hours
S2 — High	Credible suspicion of unauthorised access, or loss of data integrity affecting operational records	Anomalous access pattern; corrupted schedule or presence data	Within 48 hours of becoming aware
S3 — Moderate	Security-relevant defect or misconfiguration without evidence of data exposure	Permission check too permissive, found internally and fixed	In the next release note, or immediately if the customer is affected
S4 — Availability	Platform unavailable or materially degraded, no data exposure	Hosting outage, failed deployment	As soon as the cause is known, with an expected restoration time

An incident is escalated, never quietly downgraded. If the classification changes, the customer is told that it changed and why.

3. Procedure

Step 1 — Detect and record (immediately)

The incident is recorded with the time of discovery, how it was discovered, what is known, and what is not yet known. Everything that follows is logged against that record, so the timeline is reconstructable afterwards.

Step 2 — Contain (within hours)

Priority is stopping the harm, not explaining it. Depending on the incident: revoke or rotate credentials and tokens, disable the affected function or endpoint, roll back the change that caused it, or take the affected component offline. Containment is never delayed to protect appearances.

Step 3 — Assess (within 24 hours)

Establish which customers are affected, which categories of personal data and roughly how many records and data subjects are involved, whether data was read, altered or exfiltrated, and the likely consequences for the individuals concerned.

Step 4 — Notify the customer (within 48 hours)

Written notification to the customer's registered data protection contact, containing:

- the nature of the incident and when it was discovered;
- the categories and approximate number of data subjects and records concerned;
- the likely consequences;
- the measures already taken and those proposed;
- the name and contact details of the person who can answer further questions.

If some facts are not yet established, the notification is sent anyway, marked as provisional, and updated without further undue delay. **A partial notification within 48 hours is always preferred over a complete one that is late.**

Step 5 — Remediate and verify

Fix the root cause, not the symptom. Where the incident touched access control or customer separation, an automated regression test is added so the same failure cannot return unnoticed. The fix is verified before the incident is closed.

Step 6 — Report and learn (within 10 business days of closure)

The affected customer receives a written report: timeline, root cause, data affected, actions taken, structural measures and — where relevant — what the customer should do on its side. Where the lesson is general, the Security Statement or this procedure is updated.

4. Availability incidents

For S4 incidents the customer is informed as soon as the cause is known, with an expected restoration time and, where the outage falls in a shift change, a practical workaround: schedules exported to Excel or PDF remain usable offline, which is one of the reasons exports exist in every module.

5. Reporting an incident to us

If you believe data is exposed, or you find a security defect:

- Email **info@kaizenkanri.nl** with "SECURITY" in the subject line.
- Describe what you observed, the URL or screen, the approximate time, and the account used.
- Do not test further, do not attempt to access data that is not yours, and do not publish the finding before it is fixed.

Reports from customers, workers and independent researchers are welcome and are acknowledged within one business day. Good-faith reporters are never pursued; Kaizen Kanri would rather be told than discover it later.

6. Contacts

Purpose	Contact
Security incidents and breach reports	info@kaizenkanri.nl (subject: SECURITY)
Data protection matters, DPA, sub-processors	info@kaizenkanri.nl

Purpose	Contact
Customer's own notification contact	Recorded in Annex I of the Data Processing Agreement

7. Review

This procedure is reviewed at least once a year and after every S1 or S2 incident.

Kanriva™ and FlowCrew™ are trademarks of Kaizen Kanri.