WORKFORCE, OPS & HSE

Trust & Compliance Brief

Version 1.0 · 29 November 2026

For the IT, security and data protection review of HR Cluster. Each statement is taken from HR Cluster's published Security, Privacy, Subprocessors, DPA and Cookies pages. The page and section are named under each part.

This brief reflects HR Cluster's published legal pages as of that date. The live pages (hrcluster.app/security, /privacy, /subprocessors, /dpa, /cookies) prevail.

What HR Cluster processes, and in which role

- HR Cluster handles workforce data: personal details, schedules, attendance records, incident reports, and competence certificates and qualifications.
- For the workforce data that customers enter into or generate in the platform, the customer organisation is the data controller and HR Cluster AS is the data processor. HR Cluster AS is the controller for its own processing, such as billing, account administration, security logging of platform access and, with consent, usage analytics.

Sources: hrcluster.app/security, section 1; hrcluster.app/privacy, section 2; hrcluster.app/dpa, section 2

Hosting and data residency

- HR Cluster runs on Hetzner Cloud servers in the EU. Application servers, production databases and uploaded files are hosted in the EU, primarily in Helsinki, Finland, with a standby database replica in Nuremberg, Germany.
- The database service is not reachable from the internet. It accepts connections only over our private network and encrypted replication tunnels.

Sources: hrcluster.app/security, section 2; hrcluster.app/subprocessors, section 2

Encryption

- In transit: TLS (HTTPS) on every request, terminated at our managed load balancer with an auto-renewing certificate.
- At rest: sensitive identifiers such as national ID numbers and bank details are encrypted with AES-256-GCM before they reach the database, using a key that is stored outside the database. This applies to those fields; it is not a statement about all stored data.
- Passwords and PINs: passwords are hashed with bcrypt; clock-in PINs are hashed separately. HR Cluster never stores either in plain text or writes them to its logs. A new PIN sent by email is in that email, which the email provider keeps for its retention period.

Sources: hrcluster.app/security, section 3

Tenant isolation

- HR Cluster is multi-tenant. Queries on customer-owned data are scoped to the customer's account, either directly by account_id or through a parent record whose account has been checked. Public links, such as signing and supplier links, are looked up by their own secret token and then act only within that record's account. Platform administration and scheduled maintenance jobs work across accounts by design.
- File uploads are stored outside the webroot, organised per account, and served only through application handlers that check access: for signed-in users, membership of the account and the relevant permission; for signing and request links, that link's token, limited to its own record. File type is checked before a file is served.
- Platform admin access uses a separate login, cookie, and auth table from customer accounts.

Sources: hrcluster.app/security, section 4 and 5

Access control and audit logging

- Password sign-in creates a random session token that is held only in a secure, HttpOnly, SameSite cookie in the browser. The database stores only a hash of it, and every signed-in request is checked against the database, with an idle timeout and an absolute time limit.
- Role-based access control (account admin, manager, worker) with per-permission overrides.
- CSRF protection on state-changing requests from signed-in users: forms and API calls must carry a token bound to the sign-in session, and sign-in cookies are set with SameSite=Lax. Requests that do not come from a signed-in browser are protected in other ways: provider webhooks by a shared secret or signature, the clock-in terminal by the worker's PIN, and password-protected live screens by their password. Rate limiting on authentication endpoints.
- We log administrative actions, data exports, and permission changes per account.

Sources: hrcluster.app/security, section 4 and 7

Backups and monitoring

- HR Cluster AS maintains layered backup and disaster recovery measures designed to support service continuity and data resilience.
- Off-site backups are transferred over SSH to Hetzner backup storage in the EU. Separate backup copies are kept in Norway, within the European Economic Area (EEA).
- Server-level logs include errors, slow queries, and authentication events. Logs are retained for security and accountability purposes.

Sources: hrcluster.app/security, section 6 and 7

Email and message retention

WHERE	WHAT IS KEPT	FOR HOW LONG
Postmark (AC PM, LLC), email delivery, United States	Message content and metadata. Processed in the United States under Standard Contractual Clauses and, where applicable, the EU-US Data Privacy Framework.	7 days, the retention period set for HR Cluster's Postmark account.
Lettermint B.V., email delivery, EU	Message content and attachments; delivery and engagement events; residual encrypted backups. Open and click tracking is turned off.	Content and attachments: 7 days. Events: up to 90 days. Residual encrypted backups: up to 14 days after active deletion.
Inside HR Cluster	Message content (the text and subject of SMS and email notifications and of messages sent through the platform) and the delivery records of those messages.	Content: removed 90 days after sending. Delivery records: deleted 90 days after sending has finished.

- Both email providers may keep suppression records, such as addresses that bounced or unsubscribed, for longer than message content. Postmark keeps these records indefinitely.
- Messages a provider accepted before its retention setting was changed on 19 November 2026 may still follow the earlier period: 45 days for Postmark and 28 days for Lettermint.

Sources: hrcluster.app/privacy, section 11 and 13; hrcluster.app/subprocessors, section 2

Data Processing Agreement

- The standard Data Processing Agreement is published at hrcluster.app/dpa. It forms part of the contract and supplements the Terms of Service and the Privacy Policy.
- A signed PDF is available on request: email privacy@hrcluster.com with your organisation name and registered address. It is typically returned within two business days.
- Customers are notified in advance of any material change to the subprocessor list, typically by email to the account administrator.

Sources: hrcluster.app/subprocessors, section 5; hrcluster.app/dpa, section 1 and 10

Subprocessors and other providers

PROVIDER	PURPOSE	LOCATION	ROLE AND SAFEGUARDS
Hetzner Online GmbH	Hosting, compute, storage, backups, database replica	Helsinki, Finland and Nuremberg, Germany (EU)	Subprocessor. EU data processing. ISO 27001 certified: this is Hetzner's certification, not one held by HR Cluster.
Postmark (AC PM, LLC)	Transactional email delivery	United States	Subprocessor. Standard Contractual Clauses; EU-US Data Privacy Framework where applicable.
Lettermint B.V.	Transactional email delivery	EU; delivered through the recipient's email provider	Subprocessor. EU data processing under Lettermint's data processing agreement.
Google Ireland Limited (Google Analytics)	Usage analytics on hrcluster.app, including the signed-in application, and on hrcluster.com	United States / global Google infrastructure	Subprocessor. Loaded only after consent on that browser. On hrcluster.app Google receives page names, never page addresses or record identifiers; on hrcluster.com it receives the public page address and title, campaign tags and the referrer. Advertising features and Google signals are off; Standard Contractual Clauses.
Google Ireland Limited (reCAPTCHA Enterprise)	Spam and abuse protection on password-reset forms, on the sign-in form after repeated failed attempts, on public forms where the customer has turned it on, on the clock-in terminal, and on the contact form on hrcluster.com	United States / global Google infrastructure	Subprocessor. Used only as a security measure, not for analytics or advertising; Standard Contractual Clauses; EU-US Data Privacy Framework where applicable.
46elks AB	Delivery of SMS sent by the platform, where the relevant feature is enabled	EU, according to 46elks; delivered through the recipient's mobile network operator	Not a subprocessor. Independent controller, as stated by 46elks, as a registered electronic communications provider.
Stripe	Card payments for SMS credit packages bought in the platform	Ireland (EU); also the United States and other Stripe locations	Not a subprocessor. Processes payment data for HR Cluster AS's own billing. Card details never reach HR Cluster's servers.

Sources: hrcluster.app/privacy, section 11; hrcluster.app/subprocessors, section 2, 3 and 4; hrcluster.app/cookies

Company and contact

- HR Cluster AS, Norwegian org. no. 937 565 690. Privacy: privacy@hrcluster.com. Security: security@hrcluster.com.
- The Data Processing Agreement is governed by the laws of Norway. The supervisory authority named in the Privacy Policy is the Norwegian Data Protection Authority (Datatilsynet).

Sources: hrcluster.app/security, section 11; hrcluster.app/privacy, section 17; hrcluster.app/dpa, section 2 and 9