HarmonyHR HRIS Terms of Service

Effective date: 12 May 2025

These HarmonyHR HRIS Terms of Service (the Terms) govern a business customer's use of HarmonyHR's human-resources information system (HRIS). The Terms include the data-processing terms in Schedule 1 and the SaaS service terms in Schedule 2. Together with an accepted quotation, invoice or written order confirmation that identifies the Customer and commercial scope, they form the agreement between the Parties (the Agreement).

Key definitions

Authorised User means an individual whom Customer permits to use the HRIS within the licensed scope. Customer Data means data entered into, uploaded to, stored in or generated through the HRIS by or for Customer. Documentation means HarmonyHR's then-current user and technical documentation made available for the HRIS. Personal Data means information relating to an identified or identifiable individual under applicable data-protection law. Professional Services means implementation, migration, configuration, training, integration, consulting or custom work expressly purchased by Customer. Third-Party Service means a product, service, integration or content not owned or operated by HarmonyHR.

1. Contracting parties and acceptance

Provider. HarmonyHR LLC, a limited liability company incorporated and operating under the laws of the Kyrgyz Republic, registration number 309328-3301-OOO, with its registered office at Imeni Baltagulova st., 27, Bishkek, Kyrgyz Republic (HarmonyHR, Provider, we, us).

Customer. The legal entity or individual that accepts the Agreement, places an order, pays an invoice or uses the HRIS (Customer, you). The person accepting for Customer represents that they have authority to bind Customer.

Customer accepts the Agreement when it accepts a quotation, signs an acceptance record, pays an invoice referring to these Terms, or first uses the HRIS. The applicable quotation, invoice or order confirmation may state licensed modules, authorised-user limits, fees, subscription term, deployment model, implementation scope and data region. It overrides these Terms only where it expressly identifies the clause it overrides and is signed by both Parties.

2. Services, deployment model and licence

HarmonyHR provides HRIS software for Customer's internal HR administration, only to the extent the relevant modules are enabled. The HRIS may include employee records, organisational data, leave and absence administration, surveys, performance reviews, compensation information, payroll-related information, benefits administration and role-based access management. It does not include applicant tracking, CV processing, recruitment workflows, biometric identification or medical-record management unless separately agreed in writing.

The HRIS is not legal, tax, accounting, employment, benefits, financial, banking or investment advice and does not make employment decisions for Customer. Customer is solely responsible for its HR practices, employment decisions, statutory filings, payroll calculations, benefits decisions, workforce notices and compliance with laws applicable to Customer and its personnel. HarmonyHR is not a party to any employment or other relationship between Customer and an individual whose data is in the HRIS.

Unless HarmonyHR expressly agrees in writing, Customer must not use the HRIS to store, process or transmit payment-card data subject to PCI DSS, protected health information subject to HIPAA, biometric data, medical records, highly sensitive government identifiers, or other categories requiring a specialised regulated-data arrangement. Customer is responsible for ensuring that an enabled module is suitable for its intended use.

On-Premise. Unless a purchase document expressly identifies SaaS, deployment is On-Premise. Customer selects, controls and operates the infrastructure. HarmonyHR has no standing remote access to Customer's environment and does not routinely receive, host, monitor, analyse or use Customer Data.

SaaS. A provider-hosted SaaS deployment is available only when an accepted purchase document expressly identifies it as SaaS. Schedule 2 applies only to that deployment. Before SaaS activation, HarmonyHR will provide the Customer with the then-current service details required by Schedule 2, including the selected data region, applicable subprocessors, security measures, support channel, export method and transfer safeguards. No Customer obtains SaaS access solely because these Terms mention it.

Subject to payment and compliance with the Agreement, HarmonyHR grants Customer a limited, non-exclusive, non-transferable, non-sublicensable right during the subscription term to install and use the object-code HRIS and documentation for Customer's internal business purposes, within the licensed modules and authorised-user limits. This licence does not transfer ownership, source code, intellectual-property rights, a right to host for third parties, or any right not expressly granted.

3. Accounts and authorised users

Customer is responsible for all activity through its HRIS accounts and for ensuring that each Authorised User uses a unique account and keeps credentials confidential. Customer must promptly disable accounts for leavers and unauthorised users, maintain least-privilege role assignments, and notify HarmonyHR without undue delay of a suspected compromise, unauthorised use or security incident.

Customer may permit its employees, contractors and service providers to use the HRIS only for Customer's internal business purposes and only if they comply with the Agreement. Customer remains responsible for their acts and omissions. Customer must not share credentials, circumvent user limits or use automation that impairs the HRIS or bypasses security controls.

4. Customer responsibilities and On-Premise environment

For On-Premise, Customer is solely responsible for its infrastructure and its lawful operation, including servers or cloud tenancy, operating systems, databases, network, firewalls, endpoint protection, backup, recovery, physical security, administrator accounts, identity management, configurations, integrations and user access.

Customer must maintain appropriate technical and organisational measures for the risk of its processing, including role-based access, encryption where appropriate, logging, patching, backups and a tested recovery process. Customer is responsible for the accuracy, legality and completeness of Customer Data; all notices and lawful bases for its processing; and its decisions about data retention, visibility, access permissions and data location.

Customer must not use the HRIS in a manner that is unlawful, fraudulent, infringing, discriminatory, abusive or harmful; upload malicious code; interfere with the service or another customer's environment; or use the HRIS in breach of applicable export-control, sanctions, anti-bribery or employment laws. Customer is responsible for obtaining any required rights, permissions and consents for Customer Data and Third-Party Services that it connects to the HRIS.

HarmonyHR is not responsible for outages, loss, corruption, security incidents or failed integrations caused by Customer's environment, Customer configuration, Customer users or administrators, third-party services, or Customer's failure to apply a supported update. This does not limit HarmonyHR's liability for its own wilful misconduct or gross negligence.

5. Implementation, support and remote access

Implementation, migration, training, integrations and custom development are included only if expressly agreed in writing. Customer is responsible for supplying timely information, access and personnel reasonably necessary for agreed implementation work.

HarmonyHR provides reasonable technical support through the support channel communicated to Customer. Standard support hours are Monday through Friday, 09:00-18:00 UTC+2, excluding public holidays in the Kyrgyz Republic. HarmonyHR targets an initial response within 24 hours during those hours. A response target is not a guaranteed resolution time, availability commitment or service credit.

Remote access to an On-Premise environment is exceptional. It requires Customer's prior written authorisation for the specific purpose, systems and period. Customer may require a separate NDA, its own access procedure, supervision, multi-factor authentication or logging. HarmonyHR will use authorised access only for the approved support activity, will not copy Customer Data except where necessary and authorised, and will promptly end access when the activity is completed.

Unless otherwise agreed, Customer installs updates. HarmonyHR may make updates, fixes and documentation available and may require reasonably necessary security updates for continued support. HarmonyHR will not automatically alter Customer's On-Premise environment without Customer's authorisation.

Third-Party Services are governed by the third party's terms and privacy notice. Customer is responsible for procuring and maintaining rights to use a Third-Party Service, configuring the integration and determining which Customer Data is exchanged. HarmonyHR is not responsible for availability, security, functionality, data handling or changes of a Third-Party Service, except to the extent directly caused by HarmonyHR's breach of the Agreement.

6. Fees, taxes and commercial changes

Fees, billing frequency, payment currency, licensed scope and subscription term are stated in the applicable purchase document. Fees are payable in advance unless that document says otherwise. Customer is responsible for taxes, duties and governmental charges associated with its purchase, excluding taxes based on HarmonyHR's net income, property or employees.

Each invoice will identify the Provider, invoice number and date, Customer, licensed HRIS scope, deployment model, relevant subscription or service period, amount, currency, due date and payment instructions. Where required by law or available to HarmonyHR, the invoice will also state the Provider's applicable tax identification number. Customer must quote the invoice number in the payment reference and pay from an account in Customer's name, unless HarmonyHR has approved another arrangement in writing.

If an undisputed invoice remains unpaid for 14 calendar days after HarmonyHR's written notice, HarmonyHR may suspend support and, where technically applicable, access or the licence until payment is received. Customer remains responsible for the fees due during a suspension caused by its non-payment.

HarmonyHR may change fees for a renewal by giving at least 60 calendar days' notice. A change does not alter fees already paid for the current subscription term. Customer may elect not to renew before the revised fees take effect.

7. Customer Data and confidentiality

Customer Data means all data, including Personal Data, that Customer or its Authorised Users enter into, upload to, store in or generate through the HRIS. Customer retains all rights in Customer Data. HarmonyHR does not sell Customer Data, use it for advertising, train artificial-intelligence models on it, data mine it, aggregate it for unrelated analytics, or use it for any purpose outside the Agreement.

HarmonyHR may collect and use limited operational, diagnostic and performance information about the HRIS and its technical environment, such as version, configuration state, feature usage, error events, latency and security telemetry (Service Telemetry), only to operate, secure, support and improve the HRIS. HarmonyHR will not use Service Telemetry to identify Customer or an individual in external publications, marketing or benchmarking without Customer's written consent. Where Service Telemetry contains Personal Data, it is Customer Data and Schedule 1 applies.

Each Party must protect the other Party's Confidential Information using at least reasonable care and may use it only to perform or exercise rights under the Agreement. Confidential Information includes Customer Data, security information, pricing, business plans, software and technical information. It excludes information that the recipient can demonstrate was lawfully known without restriction, becomes public without breach, is independently developed without use of the other Party's Confidential Information, or must be disclosed by law. Where disclosure is legally required, the recipient will, where legally permitted, give advance notice and limit disclosure to what is required.

Customer is the controller, holder or owner of Customer Data and determines the purposes and means of processing. HarmonyHR acts as Customer's processor only to the extent described in Schedule 1. For information HarmonyHR processes as an independent controller, including business contacts, website data and billing data, the Privacy Policy applies.

8. Security and incident management

Each Party is responsible for security of the systems it controls. HarmonyHR will maintain reasonable organisational and technical measures for its personnel, support processes and systems, taking account of the risk and the nature of the relevant processing. HarmonyHR will not make a claim of a certification, audit standard or security framework unless that claim is accurate and current.

Customer must promptly notify HarmonyHR of a suspected vulnerability or incident involving the HRIS and reasonably cooperate in remediation. If HarmonyHR becomes aware of a Personal Data breach in systems or activities under its control that affects Customer Data, it will notify Customer without undue delay and, where practicable, within 24 hours after awareness during the support hours in section 5. The notice will describe the information then available. HarmonyHR will reasonably assist Customer with investigation and remediation. Customer is responsible for notifications to individuals and regulators unless applicable law requires otherwise.

9. Intellectual property and restrictions

HarmonyHR and its licensors retain all rights, title and interest in the HRIS, documentation, updates, service materials and all related intellectual property. Customer must not, and must not allow another person to: copy the HRIS other than

reasonable backup copies; rent, lease, sell, sublicense, assign or transfer it; make it available to a third party other than Authorised Users; circumvent security or licence controls; reverse engineer, decompile or disassemble it except to the limited extent mandatory law prohibits that restriction; introduce malicious code; interfere with its operation; or remove proprietary notices.

Feedback is voluntary. If Customer provides feedback, HarmonyHR may use it without restriction or payment, provided it does not identify Customer or disclose Customer Confidential Information.

10. Warranties and disclaimers

HarmonyHR warrants that it has the right to grant the licence in the Agreement and that the HRIS will materially conform to the applicable documentation when used in a supported environment. Customer's exclusive remedy for breach of this warranty is HarmonyHR's reasonable effort to repair, replace or work around the affected feature. If that is not commercially reasonable, Customer may terminate the affected subscription and receive a pro-rata refund of prepaid fees for the unused period.

Except for the express warranties in the Agreement, the HRIS is provided on an "as available" basis. To the maximum extent permitted by law, HarmonyHR disclaims implied warranties, including merchantability, fitness for a particular purpose and non-infringement. HarmonyHR does not warrant that the HRIS will be uninterrupted, error-free, meet every legal requirement applicable to Customer, or prevent every security incident.

11. Indemnity and limitation of liability

Customer will defend and indemnify HarmonyHR against third-party claims arising from Customer Data, Customer's unlawful use of the HRIS, or Customer's breach of the Agreement. HarmonyHR will defend Customer against a third-party claim that the unmodified HRIS, used as permitted, infringes that third party's intellectual-property rights, and will pay final damages awarded or settlements approved by HarmonyHR. This does not apply to claims caused by Customer Data, Customer modifications, combinations not supplied by HarmonyHR, or use outside the Agreement. The indemnified Party must promptly notify the other, allow it to control the defence and settlement, and provide reasonable cooperation.

Neither Party is liable for indirect, incidental, special, punitive or consequential loss, or for lost profits, revenue, business, goodwill or data, even if advised of the possibility. Subject to the enhanced limit below, each Party's aggregate liability arising from the Agreement is limited to the fees paid or payable by Customer to HarmonyHR for the 12 months immediately preceding the event giving rise to liability.

HarmonyHR's aggregate liability for breach of its confidentiality obligations, Schedule 1, Schedule 3, or its intellectual-property indemnity is limited to two times the fees paid or payable by Customer to HarmonyHR for the 12 months immediately preceding the event giving rise to liability. The enhanced limit is an aggregate cap, not an additional cap; Customer may not recover the same loss twice. Nothing in this section limits liability for fraud, death or personal injury caused by negligence, wilful misconduct, or liability that cannot lawfully be limited. Nothing in this section limits Customer's liability for infringement of HarmonyHR intellectual-property rights.

12. Suspension, term, termination and exit

HarmonyHR may suspend use or support to the extent reasonably necessary to prevent a security risk, comply with law or a binding requirement of a financial institution or payment provider, address Customer's material breach, or respond to non-payment under section 6. It will give notice where practicable and restore the affected service when the reason is resolved. HarmonyHR will not be liable for a delay or suspension required by applicable sanctions, anti-money-laundering, counter-terrorist-financing, export-control or similar compliance obligations.

The initial subscription term and renewal period are stated in the applicable purchase document. If none is stated, the term is one year and renews for successive one-year periods unless either Party gives at least 30 calendar days' written non-renewal notice. Either Party may terminate for material breach if the other Party fails to cure the breach within 30 calendar days after written notice, unless the breach cannot be cured.

On expiry or termination, Customer must stop using the HRIS and uninstall or disable all copies, except one archival copy retained solely where law requires it. Customer may retain Customer Data in its own On-Premise environment, subject to its own legal obligations. For SaaS, export and deletion are governed by Schedule 2. HarmonyHR will delete Personal Data contained in support records or diagnostic extracts within 30 days after closing the relevant support activity, unless retention is required by law or Customer instructs otherwise in writing.

13. General

The Parties are independent contractors. Customer may not assign the Agreement without HarmonyHR's written consent, except in connection with a merger, reorganisation or sale of substantially all assets, provided the assignee is not a direct competitor of HarmonyHR and agrees in writing to the Agreement. HarmonyHR may assign the Agreement to an affiliate or successor in connection with a merger, reorganisation or sale of substantially all assets, provided it gives notice to Customer.

Contract notices must be in writing in English and sent to the email address stated in the applicable purchase document or accepted correspondence. Notices to HarmonyHR must be sent to legal@harmonyhr.org. Informal messenger communications are not contractual notices.

HarmonyHR may amend these Terms for future purchases or renewals by giving at least 30 calendar days' notice. A material adverse change to an active paid subscription takes effect at renewal unless required by law or necessary to address an immediate security risk. A Customer that does not accept a material adverse renewal change may elect not to renew before it takes effect.

Neither Party is responsible for a delay or failure to perform caused by events beyond its reasonable control, including natural disaster, war, terrorism, civil unrest, epidemic, labour dispute, government action, internet or utility failure, or third-party infrastructure failure, except that this does not excuse payment obligations for amounts already due. The affected Party will use reasonable efforts to mitigate the effect and notify the other Party where practicable.

No failure or delay to exercise a right is a waiver. A waiver is effective only in writing. The Agreement does not create rights for third parties except a permitted successor or assignee. Neither Party may use the other Party's name, logo or trademarks in publicity without prior written consent, except that HarmonyHR may identify Customer as a customer only if Customer has separately agreed in writing.

The Agreement is governed by the laws of the Kyrgyz Republic, without regard to conflict-of-laws rules. The courts of Bishkek, Kyrgyz Republic have exclusive jurisdiction, unless the Parties agree another dispute-resolution process in writing. If a provision is unenforceable, the remaining provisions remain effective. The Agreement is the entire agreement regarding the HRIS and supersedes prior discussions on that subject.

Schedule 1. Data Processing Terms

1. Scope and roles

This Schedule applies only when HarmonyHR processes Personal Data for Customer: (a) during authorised On-Premise remote support or handling of an authorised diagnostic extract; or (b) during a SaaS deployment. Customer is the controller and, where relevant, holder or owner. HarmonyHR is the processor. If HarmonyHR processes Personal Data for its own business administration, billing, legal compliance or website communications, it acts as an independent controller under the Privacy Policy.

2. Processing details

Subject matter and duration. Processing is limited to the authorised support activity or, for SaaS, the subscription term plus the deletion and backup period in Schedule 2.

Nature and purpose. For On-Premise: narrowly scoped diagnosis, remediation, maintenance or implementation approved by Customer. For SaaS: hosting, operation, support, security, backup, recovery and other documented HRIS services requested by Customer.

Data subjects. Customer's employees, former employees, contractors, Authorised Users, emergency contacts and other people whose information Customer lawfully enters.

Categories of Personal Data. Identity and business-contact details; job, organisation, leave, absence, survey, performance-review, compensation, payroll and bank-account information; employment documents; DMS membership or benefit eligibility; and system access and audit data. The HRIS is not designed for biometric, candidate, CV, recruiting or medical data. Customer must not enter special-category or similarly sensitive data unless it has a lawful basis, a documented need and appropriate safeguards.

3. Instructions and Customer obligations

HarmonyHR will process Personal Data only on Customer's documented instructions, including configurations and support requests Customer approves, unless processing is required by applicable law. If HarmonyHR considers an instruction unlawful, it will inform Customer unless law prohibits doing so. Customer is responsible for notices, consent or other lawful bases, data-subject requests, role-based access, and the lawfulness of its instructions and Customer Data.

4. Confidentiality, security and personnel

HarmonyHR will ensure that persons authorised to process Personal Data are bound by confidentiality obligations and will apply appropriate organisational and technical measures for systems and activities it controls. In On-Premise deployments, Customer remains responsible for security measures in its environment, including access control, encryption, backups, patching, network segregation and incident monitoring.

5. Subprocessors and transfers

For authorised On-Premise support, HarmonyHR will not appoint a subprocessor that accesses Customer Personal Data without Customer's prior written authorisation. For SaaS, HarmonyHR will identify applicable subprocessors before activation and obtain Customer's required authorisation. HarmonyHR will impose materially equivalent data-protection obligations on each authorised subprocessor and remains responsible for its performance to the extent required by law.

HarmonyHR will not transfer Customer Personal Data internationally except on Customer's documented instruction, where necessary to provide the authorised service, or where required by law. Where EU or UK data-protection law applies and a transfer mechanism is required, the Parties will use the applicable standard contractual clauses or other lawful safeguard before the transfer.

6. Rights, assistance and breach notification

Taking account of the nature of processing and information available, HarmonyHR will reasonably assist Customer with requests from data subjects, security of processing, personal-data breach response, data-protection impact assessments and regulatory consultations. HarmonyHR will notify Customer as set out in section 8. Customer remains responsible for determining whether notification to a regulator or individual is required.

7. Audit and information rights

Once per calendar year, and no more than once in any 12-month period unless a material incident occurs, Customer may request reasonable information necessary to demonstrate HarmonyHR's compliance with this Schedule. If that information is insufficient, Customer may conduct a remote audit or appoint an independent auditor on at least 30 days' written notice, during normal business hours, subject to confidentiality, security and non-disruption safeguards. Customer bears its audit costs unless the audit identifies a material breach by HarmonyHR.

8. Return and deletion

For On-Premise, HarmonyHR does not hold Customer Data except authorised support material and will delete it as stated in section 12. For SaaS, HarmonyHR will provide an export method during the subscription and delete or return Customer Personal Data at Customer's choice after termination, unless law requires retention. Backups may be retained only for the limited secure rotation period in Schedule 2 and will not be restored except for disaster recovery.

9. Applicable law

This Schedule is intended to meet processor-contract requirements of applicable data-protection law, including Article 28 GDPR and the corresponding provisions of the UK GDPR, to the extent those laws apply. It does not remove either Party's obligations under law applicable to that Party.

10. Priority

If Schedule 1 conflicts with another provision of the Agreement on the processing of Personal Data, Schedule 1 prevails to the extent of that conflict. Nothing in Schedule 1 requires HarmonyHR to process Personal Data that it has not received or does not control.

Schedule 2. SaaS Service Terms

1. Activation and service details

Schedule 2 applies only to a SaaS subscription expressly confirmed by HarmonyHR. Before activation, HarmonyHR will provide Customer with the selected data region, the applicable subprocessor list, the support channel, backup and recovery description, service-maintenance arrangements, export method, and the lawful transfer safeguard if Customer Personal Data is transferred internationally. If Customer does not accept a material service detail, SaaS will not be activated and no SaaS fee will be due.

2. Availability and maintenance

HarmonyHR targets monthly SaaS availability of 99.5 percent, excluding planned maintenance, emergency maintenance, Customer systems, Customer internet connectivity, force majeure, misuse, suspension permitted by the Agreement, and third-party systems outside HarmonyHR's reasonable control. Planned maintenance will normally be announced at least 48 hours in advance where practicable. Emergency maintenance may occur without advance notice where needed to protect the service or data. This target does not create service credits unless separately agreed in a signed writing.

3. Hosting, security and backups

HarmonyHR will host the SaaS service in the data region disclosed before activation and use reasonable safeguards for its production environment, including access management, encryption in transit, logical segregation, monitoring, vulnerability and patch management, and backup controls appropriate to the service. HarmonyHR will maintain encrypted or access-controlled backups under a documented rotation process. A backup is for disaster recovery and is not a substitute for Customer's own export and retention obligations.

4. Access, support and changes

HarmonyHR may update the SaaS service to maintain security, correct defects, improve performance or add functionality. It will not materially reduce the core functionality of Customer's purchased modules during the paid term, except where required by law, needed to address a security risk, or agreed by Customer. Customer may export Customer Data using available functionality or request reasonable assistance, which may be chargeable if outside standard support.

5. Subprocessors and Customer choices

HarmonyHR may use only the subprocessors disclosed before activation or subsequently notified to Customer. HarmonyHR will give reasonable advance notice of a material new subprocessor and provide Customer an opportunity to object on reasonable data-protection grounds. If the Parties cannot resolve a justified objection, Customer may terminate the affected SaaS service and receive a pro-rata refund of prepaid unused fees for that service.

6. SaaS exit

During the subscription and for 30 calendar days after SaaS termination, Customer may export Customer Data using the standard export method, unless the Parties agree a longer period in writing. After that period, HarmonyHR will delete or irreversibly anonymise Customer Data from active systems, except where retention is required by law. Backups will be overwritten under the regular secure rotation process and will not be made available for ordinary access after the export period.

Schedule 3. Security and Resilience Terms

1. Scope and allocation of responsibility

This Schedule describes the baseline security commitments applicable to the HRIS. It applies to HarmonyHR systems and personnel only to the extent HarmonyHR controls them. For On-Premise, Customer remains responsible for the Customer environment and must evaluate whether its controls meet its regulatory, employment-law, information-security and internal-policy requirements. For SaaS, HarmonyHR is responsible for the production service controls described below; Customer remains responsible for its users, configurations, integrations, data classification and lawful use.

2. Security management

HarmonyHR will maintain security procedures appropriate to the nature of its services and periodically assess material security risks affecting systems under its control. HarmonyHR will restrict access to systems and Customer Data to authorised personnel with a legitimate service need, apply confidentiality obligations, and revoke access when it is no longer required. HarmonyHR will use reasonable administrative, technical and physical safeguards for its systems and facilities.

3. Identity, access and authentication

HarmonyHR will use access controls designed to enforce least privilege for its internal systems and, for SaaS, will make role-based access controls available in the HRIS. Customer is responsible for choosing and reviewing roles, authorising administrators, protecting credentials and ensuring that Authorised Users are appropriately trained. Where a SaaS feature supports multi-factor authentication, Customer should enable it for privileged accounts and other accounts identified by Customer's risk assessment.

4. Secure development, changes and vulnerabilities

HarmonyHR will use reasonable development and change-management practices for software it controls, including access restriction for source repositories, review appropriate to the change, and testing before production release where practicable. HarmonyHR will assess reported vulnerabilities, prioritise remediation according to risk, and may deploy urgent security changes without prior notice. Customer must promptly apply supported On-Premise security releases or accept the associated risk and possible support restrictions.

5. Encryption, logging and monitoring

For SaaS, HarmonyHR will use encryption in transit for supported external connections and will maintain controls intended to protect Customer Data at rest in the production environment. HarmonyHR will maintain service and security logs appropriate to operating and protecting the SaaS service. Customer is responsible for encryption, log retention and monitoring in an On-Premise environment. Neither Party is required to retain logs for a particular period unless a purchase document or applicable law expressly requires it.

6. Business continuity and disaster recovery

For SaaS, HarmonyHR will maintain business-continuity and recovery procedures proportionate to the service, including backups and recovery processes. HarmonyHR will periodically review those procedures. Recovery objectives depend on the incident, data region, scope of loss and service configuration; no specific recovery time or recovery point objective applies unless the Parties agree it in writing. For On-Premise, Customer is solely responsible for continuity, backup and recovery of its environment and Customer Data.

7. Security evidence and assessments

On reasonable written request and subject to confidentiality, HarmonyHR will provide available high-level information about controls relevant to the purchased service. Customer may use the audit rights in Schedule 1. HarmonyHR may use internal or independent assessments, vulnerability scanning and penetration testing for its systems, but does not promise a particular certification, assessment frequency or report unless expressly stated in a signed purchase document.

8. Security incident cooperation

The Parties will cooperate in good faith to investigate a security incident that materially affects the HRIS or Customer Data. Each Party will preserve reasonably relevant evidence, avoid actions that unnecessarily worsen the incident, and share information reasonably necessary for containment and remediation, subject to law, privilege, security and confidentiality. Neither Party may make a public statement identifying the other Party in connection with an incident without prior written approval, except where required by law.

Schedule 4. Implementation, Support and Change Management

1. Implementation and acceptance

Where implementation is purchased, HarmonyHR will perform the agreed implementation tasks using reasonable skill and care. Customer will provide timely decisions, suitably qualified personnel, accurate source information, required access and a reasonably safe working environment. Customer must review a delivered implementation milestone within 10 business days after notice of completion. A milestone is accepted when Customer confirms acceptance, uses it in production, or does not give a written notice describing material non-conformities within that period. HarmonyHR will reasonably correct verified material non-conformities.

2. Change requests

Either Party may request a change to scope, timeline, configuration, integration or professional services. A requested change is not binding unless the Parties agree in writing on its description, fees, timetable, dependencies and effect on the Agreement. HarmonyHR may reject a change that is technically infeasible, insecure, unlawful or incompatible with the product roadmap.

3. Support priorities

HarmonyHR will use reasonable efforts to classify requests as follows: a critical issue materially prevents all or a substantial part of production use with no reasonable workaround; a high issue materially impairs a core function for multiple users; a normal issue impairs a non-critical function or has a reasonable workaround; and a low issue is a question, request for information or enhancement. The response target in section 5 applies to all priorities. HarmonyHR will use commercially reasonable efforts to address critical and high issues first, but does not guarantee a resolution time.

4. Exclusions and customer cooperation

Support does not include development of unpurchased features, training, third-party products, Customer infrastructure, unsupported versions, Customer modifications, data correction, or issues caused by Customer's failure to meet the Agreement or technical requirements. HarmonyHR may require reproducible information, relevant logs, a test case, version details and Customer cooperation before diagnosing an issue. If a request is outside standard support, HarmonyHR may offer it as chargeable professional services.

5. Product changes and end of support

HarmonyHR may change, discontinue or replace a feature where reasonably necessary for security, law, technical compatibility or product evolution. It will not materially reduce the core purchased functionality during the paid term except as permitted by the Agreement. HarmonyHR will give reasonable notice before ending support for a version where practicable. Customer remains responsible for planning upgrades and testing integrations.

6. Remote-support record

For exceptional On-Premise remote access, HarmonyHR will keep a reasonable support record identifying the Customer authorisation, date, purpose, personnel involved and closure of the access session. On Customer's written request, HarmonyHR will provide a confirmation that the authorised access was closed and that any authorised diagnostic material was handled in accordance with section 12 and Schedule 1. This record does not require HarmonyHR to retain Customer Data or Customer credentials.

Schedule 5. Commercial Payment and Compliance Terms

1. Commercial purpose and payment trail

The Parties enter into the Agreement for the genuine commercial purpose of licensing, implementing, supporting or, where expressly agreed, hosting the HRIS. The applicable quotation, invoice, acceptance record, payment record and agreed correspondence are intended to evidence that commercial purpose, the scope supplied and the consideration paid. An electronic acceptance, email confirmation or equivalent electronic record is valid evidence of acceptance to the extent permitted by applicable law.

2. Payments and third-party payers

Customer must pay the invoiced amount from an account held in Customer's legal name. A payment by an affiliate, group treasury company, financing provider or other third party is permitted only with HarmonyHR's prior written approval and information reasonably sufficient to identify the payer, its relationship to Customer, the invoice being settled and the legitimate commercial purpose of the payment. HarmonyHR may return, hold or decline to apply a payment where required by law or where the information reasonably necessary to identify the payer or payment purpose is not provided.

3. Compliance information

Each Party will comply with applicable anti-money laundering, counter-terrorist-financing, sanctions, anti-bribery, tax and export-control laws in connection with the Agreement. HarmonyHR may request reasonable corporate, ownership, authority, tax-residency, payment-source or sanctions-compliance information from Customer where required by law, a financial institution, a payment provider or a reasonable risk assessment. Customer may make a corresponding request of HarmonyHR. Each Party will provide accurate information and promptly update information that becomes materially inaccurate.

HarmonyHR may defer performance, suspend the affected subscription or decline to apply a payment only to the extent reasonably necessary while a legally required or risk-based compliance review is pending, where the required information is not provided, or where performance or payment would breach applicable law or a binding direction of a competent authority. Where lawful and practicable, HarmonyHR will explain the information reasonably required and will restore performance once the issue is resolved. Nothing in this Schedule requires either Party to disclose information protected by law, legal privilege or another person's confidentiality rights.

4. Delivery and acceptance evidence

For an On-Premise delivery, the purchase document and implementation acceptance process in Schedule 4 establish the licensed scope and completion evidence. For SaaS, activation of the authorised Customer tenant and the first available use of the subscribed modules establish service commencement, subject to the agreed purchase document. On reasonable request, HarmonyHR will provide Customer or its bank with a factual confirmation of the Agreement, applicable invoice, payment status, deployment model and supplied scope, provided that the request is lawful and does not require disclosure of another customer's Confidential Information.

5. Records and retention

HarmonyHR may retain the Agreement, purchase documents, invoices, payment correspondence, acceptance records, support records and compliance information for the period required by applicable law or reasonably necessary to establish, exercise or defend legal claims, complete an audit, respond to a bank or regulator, or prevent fraud. Each Party remains responsible for retaining its own accounting, tax and payment records.