# HarmonyHR Privacy Policy

Effective date: 12 May 2025

## 1. Purpose, scope and relationship with the HRIS Terms

This Privacy Policy explains how HarmonyHR LLC handles Personal Data when it acts as an independent controller. It applies to the HarmonyHR website, business enquiries, demonstrations, business contacts, suppliers, contracting, invoicing, payment administration and our own support and security records.

This Policy does not make HarmonyHR the controller of Personal Data that a Customer stores in its HRIS environment. The default HRIS deployment is On-Premise: the Customer selects and controls its hosting environment and decides why and how employee information is used. If HarmonyHR processes Customer Personal Data during authorised support, an authorised diagnostic extract, or a SaaS deployment, it acts as a processor for Customer under Schedule 1 of the HarmonyHR HRIS Terms of Service (the HRIS Terms), not under this Policy.

This Policy concerns HRIS only. It does not apply to separate HarmonyHR products or services that have their own privacy notice. A Customer is responsible for providing its own employee-facing privacy notices and internal policies for its HRIS use.

## 2. Who we are and how to contact us

Controller. 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, we, us).

For privacy enquiries or to exercise a privacy right, contact us at info@harmonyhr.org or write to the address above. HarmonyHR has not appointed a data protection officer. This contact point is not a representation that a statutory DPO, EU representative or UK representative has been appointed. If applicable law later requires such an appointment, we will update this Policy and provide the relevant contact details.

For contractual notices, use the notice channel stated in the HRIS Terms or the applicable purchase document. A privacy request does not itself amend a contract, and a contractual notice does not itself constitute a privacy-rights request.

## 3. Roles in the HRIS

### 3.1 On-Premise - the normal model

In an On-Premise deployment, Customer selects, controls and operates the hosting environment. HarmonyHR has no standing remote access and does not routinely receive, host, monitor, analyse, sell, mine or otherwise use Customer Data. Customer is normally the controller, holder or owner of HRIS Customer Data; it determines the purposes, data categories, retention, access rights and hosting location.

If you are an employee, contractor, former employee, emergency contact or another person whose information is stored in a Customer HRIS, please contact the Customer - usually your employer - first. HarmonyHR generally cannot access, amend, export or erase that information and cannot make employment, payroll, benefits or other HR decisions for Customer.

### 3.2 Exceptional support access

HarmonyHR acts as Customer's processor only if Customer specifically authorises remote support access or provides an authorised diagnostic extract that contains Personal Data. Such processing is narrow in scope and limited to the approved support, implementation, diagnosis, remediation or maintenance activity. The Customer remains responsible for its HRIS environment, lawful basis, notices, access permissions and decisions about the data.

Remote access requires the Customer's prior written authorisation for the specified purpose, systems and period. The Customer may require its own NDA, access process, multi-factor authentication, supervision or logging. HarmonyHR records the authorisation and closure of the session and deletes support material as stated in the HRIS Terms, unless law requires retention or Customer gives another written instruction.

### 3.3 Future SaaS deployment

A provider-hosted deployment is not activated merely because the HRIS Terms mention SaaS. It exists only where an accepted purchase document expressly identifies SaaS. Before activation, HarmonyHR will provide the Customer with the applicable data region, subprocessor information, security measures, support channel, export method, backup and recovery description, and any required international-transfer safeguard. The data-processing, security, audit, export and deletion terms in Schedules 1 to 3 of the HRIS Terms then apply.

## 4. Personal Data HarmonyHR processes as an independent controller

We process only the data reasonably necessary for the relevant business purpose. The following table describes our ordinary controller processing. It does not describe Customer Data stored in an On-Premise HRIS.

| Activity | Typical Personal Data | Purpose and legal basis where GDPR/UK GDPR applies | Usual retention |
|---|---|---|---|
| Website operation, cookies and analytics | IP address, cookie or online identifier, browser/device information, approximate location derived from IP, referral source, pages viewed, interactions, server and security logs, essential-preference information | Operate, secure and troubleshoot the website; understand aggregate traffic and improve website content; legitimate interests and, for non-essential technologies where required, consent | For the session or a limited period proportionate to security, cookie settings and operational needs |
| Enquiries and demonstrations | Name, work email, telephone number or WhatsApp/Telegram contact, organisation, country, role, company-size range, message, meeting details and optionally a promotion code | Respond, arrange a demonstration and take requested pre-contractual steps; legitimate interests and/or steps at your request before a contract | Up to 24 months after last meaningful contact unless a contract or legal need requires longer retention |
| Customer, supplier and partner relationship | Contact details, role, correspondence, signature and authority information | Negotiate, enter into, perform and administer a business relationship; contract and legitimate interests | Relationship period plus applicable accounting, tax, limitation and legal retention periods |
| Invoicing and payments | Invoice recipient, authorised contact, billing address, tax and payment-administration information, payment references | Issue and reconcile invoices, prevent fraud, comply with accounting, tax and financial-institution requests; contract, legal obligation and legitimate interests | For the period required by applicable accounting, tax, anti-fraud and legal obligations |
| Support relationship and access records | Business contact details, support ticket content, authorised-access record, limited diagnostic information | Authenticate a request, provide support, protect the HRIS and document the support activity; contract and legitimate interests | Support record for a limited period; Personal Data in support material is deleted under the HRIS Terms |
| Rights requests, complaints and legal matters | Identity-verification information, request content, correspondence and relevant records | Verify identity, answer a request, meet legal obligations, establish, exercise or defend claims | Usually up to 24 months for the request record, or longer where law or a claim requires it |

Please do not send employee records, passwords, identity documents, bank details, health information or other sensitive Personal Data through a general website form or ordinary email unless we request it through an approved secure channel.

## 5. Customer Data: categories and boundaries

The HRIS may be configured by Customer to contain identity and business-contact data; job and organisation information; leave and absence data; survey and performance-review information; compensation, payroll and bank-account information; employment documents; DMS membership or benefit eligibility; and system access or audit data. HarmonyHR does not routinely receive this information in the On-Premise model.

The HRIS is not designed for applicant tracking, CV processing, recruitment workflows, biometric identification or medical-record management. Customer must not use it for payment-card data subject to PCI DSS, HIPAA protected health information, biometric data, medical records or other specialised regulated data unless HarmonyHR separately agrees in writing and the Parties implement the necessary safeguards.

HarmonyHR does not sell Customer Data, use it for behavioural advertising, use it to train artificial-intelligence models, data mine it, or publish Customer-identifying benchmarks. Limited technical Service Telemetry may be used only to

operate, secure, support and improve the HRIS as described in the HRIS Terms. If that telemetry contains Personal Data, it remains Customer Data and the processor terms apply.

## 6. Sources of controller Personal Data and whether it is required

We normally receive controller Personal Data directly from you, your employer or organisation, a website demo or contact form, correspondence, a contract discussion, a purchase document or a payment. We may receive business-contact information from a referral, publicly available professional source or a service provider acting for the relevant organisation. We do not purchase consumer marketing lists for HRIS Customer Data.

Providing contact information is voluntary, but we may be unable to answer an enquiry or arrange a demonstration without it. Information required for contracting, billing, tax, payment verification or security may be necessary to enter into or perform the relevant business relationship or comply with law. We will not require more data than reasonably necessary for that purpose.

## 7. How we use controller Personal Data

We use controller Personal Data to:

- respond to enquiries, arrange demonstrations and communicate with prospective and current business customers;
- negotiate, enter into, perform, support and administer contracts and professional services;
- issue invoices, reconcile payments and maintain accounting and contract records;
- verify authority, prevent fraud, satisfy reasonable bank, payment-provider, regulator, tax or legal requests, and protect our rights;
- operate, secure, measure, troubleshoot and improve the website and systems under our control; and
- establish, exercise or defend legal claims, comply with law and protect people, systems and property.

Where GDPR or UK GDPR applies, we rely on one or more of: performance of a contract; steps taken at your request before entering into a contract; compliance with a legal obligation; and legitimate interests in operating a secure B2B business, maintaining relationships, preventing fraud and defending rights. We rely on consent where applicable law requires it, such as for non-essential cookies or direct marketing. You may withdraw consent at any time; this does not affect processing before withdrawal.

HarmonyHR does not make decisions about individuals based solely on automated processing of controller Personal Data that produce legal or similarly significant effects. Customer may configure HRIS workflows, reports and access rules in its own environment. Customer, not HarmonyHR, is responsible for assessing the lawfulness and fairness of those configurations and for its employment or other decisions.

## 8. Cookies, Google analytics, marketing and online events

### 8.1 Technologies currently used

HarmonyHR uses Google Analytics 4 and Google Tag Manager on the HarmonyHR website. At the effective date, the public website is configured with Google Analytics measurement ID G-WS8XLQGN1W and Google Tag Manager container GTM-MTQTZGWM. These technologies may use cookies or comparable identifiers and process information about a visit, including online identifiers, IP-derived technical information, browser and device characteristics, referral source, pages and content viewed, interactions and approximate location derived from IP. We use this information to measure website traffic and performance, understand how visitors use the website, protect the website and improve its content and conversion paths.

Google Analytics and Google Tag Manager are not necessary for the basic delivery of the website and are treated as non-essential analytics technologies. We may also use strictly necessary cookies or comparable local-storage technologies for website operation, security, fraud prevention and selected preferences. Essential technologies are not used to create advertising profiles.

### 8.2 Consent and choices

Where applicable law requires prior consent for non-essential cookies or comparable technologies, HarmonyHR will obtain that consent through the website's cookie interface before enabling Google Analytics, Google Tag Manager tags that set or read non-essential identifiers, or other non-essential technologies. The cookie interface must offer a real choice to accept, reject and later withdraw or change consent. Refusal of non-essential technologies must not prevent access to the basic website.

You can also manage or delete cookies through browser settings. Blocking essential technologies may affect website functionality. A browser setting does not necessarily remove data already received by a third party; use the available cookie choices and the relevant provider's controls where appropriate.

### 8.3 Forms, marketing and future tools

The website allows a visitor to request a product demonstration or contact HarmonyHR. A form may request first and last name, company name, country, number-of-employees range, business email, mobile number or WhatsApp/Telegram contact, and an optional promotion code. We use submitted information to answer the request, arrange a demonstration, assess the business enquiry, prevent abuse and maintain the related business record. Do not enter employee records, passwords, bank details or other sensitive information in a general website form.

At the effective date, HarmonyHR does not use HubSpot, advertising pixels, marketing automation, newsletters or webinar platforms. We do not use Google Analytics data to send direct marketing communications. If we introduce Google advertising, another analytics provider, a marketing cookie, newsletter, webinar platform or other non-essential tool, we will update this Policy and the cookie interface before use and obtain consent where required. You may opt out of direct marketing at any time using the unsubscribe method in a communication or by contacting us.

### 8.4 Analytics safeguards and tag-management controls

HarmonyHR does not intentionally configure Google Analytics or Google Tag Manager to send direct identifiers from a website form, including a person's name, email address, telephone number, WhatsApp/Telegram contact, message content, password, employee record, bank detail or another sensitive data element. The website form and its submission process are separate from analytics reporting. If HarmonyHR identifies that Personal Data has been sent to an analytics tool, we will take reasonable steps to stop the transmission, remove or request removal where available, and assess whether additional action is required.

Access to Google Analytics and Google Tag Manager should be limited to personnel and service providers with a legitimate business need. HarmonyHR will use Google Tag Manager only for approved tags and will review material tag changes before publication. We will not enable a new advertising, remarketing, session-recording, heatmap or comparable tracking technology through Google Tag Manager unless it is disclosed through the updated cookie interface and this Policy, and consent is obtained where required.

Analytics data is reviewed in aggregate where possible. We retain Google Analytics information according to the retention controls selected in the relevant Google account and only for as long as reasonably necessary for the stated measurement, security and improvement purposes. Aggregated reports that do not identify an individual may be retained longer for business analysis.

### 8.5 Website-processing summary

| Website component | Data that may be processed | Purpose | Your control or choice |
|---|---|---|---|
| Essential website and security technologies | Technical request data, security logs, selected preferences and limited identifiers necessary for operation | Deliver, secure, troubleshoot and prevent abuse of the website | Browser settings may affect these technologies and website functionality |
| Google Analytics 4 and Google Tag Manager | Cookie or online identifiers, browser/device data, IP-derived technical information, traffic source, page views and interaction events | Measure traffic, understand website use, improve content and conversion paths | Consent before non-essential use where required; change or withdraw choice in the cookie interface |
| Demo and contact forms | Name, company, country, employee-number range, business email, phone or messenger contact, promotion code and message content if provided | Respond to the request, arrange a demonstration, assess the B2B enquiry and prevent abuse | Do not submit sensitive information; contact us to update or request deletion of controller data where applicable |
| Direct marketing, advertising and online events | No current deployment as of the effective date | Not applicable unless HarmonyHR introduces a disclosed tool or activity | A future tool will be disclosed and consent obtained where applicable |

The cookie interface is the current operational source for granular cookie choices. If this Policy and the interface differ regarding a particular cookie or tag, HarmonyHR will correct the discrepancy without undue delay and, where required, disable the non-essential technology until the information and consent mechanism are aligned.

## 9. Recipients, disclosures and international transfers

We disclose controller Personal Data only where necessary and proportionate. Recipients may include:

- banks, payment providers, accountants, tax advisers, auditors, insurers and professional advisers;
- Google group entities and their service providers that deliver Google Analytics 4 and Google Tag Manager, to the extent those technologies are enabled and subject to the applicable Google service terms;
- website, email, security, hosting, communications or document-management service providers that support HarmonyHR's own business systems;
- regulators, tax authorities, courts, law-enforcement bodies or other authorities where disclosure is required or permitted by law; and
- a buyer, investor, successor or adviser in connection with a genuine merger, financing, reorganisation, sale of assets or similar corporate transaction, subject to confidentiality and applicable law.

We require service providers to protect controller Personal Data under appropriate confidentiality and security obligations and to use it only for the relevant service. We do not disclose Customer Data from an On-Premise environment because we do not routinely hold it. If HarmonyHR processes Customer Data during authorised support or SaaS, the subprocessor and disclosure rules in the HRIS Terms apply.

HarmonyHR is established in the Kyrgyz Republic and may process controller Personal Data there or in another country where a lawful recipient or service provider is located. If EU or UK data-protection law applies and a transfer requires a safeguard, we will use an applicable lawful mechanism, such as an adequacy decision, standard contractual clauses or another permitted transfer tool, before the transfer. You may contact us for information about the relevant mechanism, subject to confidentiality and security restrictions.

## 10. Retention, deletion and business records

We retain controller Personal Data only for as long as necessary for the stated purpose, the relevant business relationship, legal obligations, a security investigation, fraud prevention or the establishment, exercise or defence of claims. When retention is no longer required, we delete, anonymise or securely isolate information in accordance with our procedures, unless law requires otherwise.

Retention of Customer Data is determined by Customer in an On-Premise deployment. HarmonyHR does not have a general copy of that data. For authorised support material, the deletion rule in the HRIS Terms applies. For SaaS,

Customer receives the export and deletion rights in Schedule 2 of the HRIS Terms; backups may remain only for the limited secure rotation period stated there and are not made available for ordinary use after the export period.

We may retain a minimal record of a customer relationship, invoice, payment, agreement, acceptance, support authorisation and completed deletion for the period required by applicable law or reasonably necessary for accounting, bank or regulator enquiries, audit, fraud prevention or legal claims. This is not a right to retain operational HRIS Customer Data beyond the applicable agreement.

## 11. Your rights and how to exercise them

Depending on the law that applies to you and the relevant processing, you may have rights to request information, access, correction, deletion, restriction, objection, portability and withdrawal of consent. You may also have the right to complain to the competent data-protection authority or a court.

To make a request, email info@harmonyhr.org and state the organisation, contact details, request and the data or activity concerned. We may request information reasonably necessary to verify your identity and authority, protect others' information and understand the request. We respond within the period required by applicable law. We may refuse, limit or charge for a request only where that law permits.

If your request concerns HRIS Customer Data, we will normally direct you to the relevant Customer because it is the controller and determines how the information is used. We will reasonably assist the Customer where the HRIS Terms or applicable law requires it. Under Kyrgyz law, personal-data holders and processors must protect Personal Data and data subjects have rights to information about processing. Where applicable, you may contact the State Agency for Personal Data Protection under the Cabinet of Ministers of the Kyrgyz Republic or the competent authority in your country of residence.

## 12. Security and security boundaries

HarmonyHR applies organisational and technical safeguards appropriate to the risk for systems, personnel and processing under its control. These include access restrictions, confidentiality obligations, security procedures and measures described in the HRIS Terms. No transmission or storage method is completely secure; use an approved secure channel if we ask you to provide sensitive information.

For On-Premise, Customer controls the HRIS hosting environment, servers or cloud tenancy, administrator accounts, endpoint devices, corporate email, network, integrations, logging and backup systems. Customer is responsible for choosing security controls appropriate to its processing, including roles, access reviews, encryption, patching, monitoring, backups and recovery testing. HarmonyHR is not responsible for an incident, outage or data loss caused by the Customer environment, configuration, users, integrations or a third-party service, except to the extent directly caused by HarmonyHR's breach of the HRIS Terms.

If a Personal Data breach in systems or activities under HarmonyHR's control affects Customer Data, HarmonyHR will notify Customer and cooperate as stated in the HRIS Terms. Customer remains responsible for deciding whether notice to a supervisory authority or individuals is required, unless applicable law requires otherwise.

## 13. Children, third-party services and external links

The HRIS is designed for workplace administration and is not directed to children. Customer is responsible for determining whether it may lawfully enter information relating to minors or dependants in its HRIS and for providing the necessary notices or safeguards.

If you follow a link to or use a Third-Party Service, that provider's terms and privacy notice apply to its processing. Where Customer connects a Third-Party Service to the HRIS, Customer decides which information is shared and is responsible for evaluating that provider. HarmonyHR is not responsible for a Third-Party Service that Customer selects or controls, except to the extent directly caused by HarmonyHR's breach of the HRIS Terms.

## 14. Changes to this Policy

We may update this Policy to reflect changes in law, our processing or our services. The updated version will show a new effective date. For material changes, we will publish the updated Policy and, where required by law, provide additional notice or obtain consent before using Personal Data for a materially different purpose. The version in effect when we collected Personal Data continues to apply to that earlier collection unless a lawful change is made.