DATA PROCESSING ADDENDUM

HarmonyATS

Effective Date: 05.12.2025

Processor / Service Provider	HarmonyHR LTD, incorporated and operating under the laws of Kyrgiz Republic, Register № 309328-3301-OOO, having its registered office at Imeni Baltagulova st., 27, Bishkek, Kyrgiz Republic.
Privacy Contact	info@harmonyats.org

This Data Processing Addendum ("DPA") forms part of, and is incorporated into, the applicable Master Subscription Agreement, Customer Terms of Service, Order Form, or other written or electronic agreement governing the Customer's access to and use of HarmonyATS (collectively, the "Agreement") between HarmonyHR LTD ("HarmonyHR", "Processor", or "Service Provider") and the customer entity that is a party to the Agreement ("Customer", "Controller", or, where applicable, "Business"). This DPA applies where and to the extent HarmonyHR Processes Customer Personal Data on behalf of Customer in connection with the provision of HarmonyATS, a cloud software-as-a-service applicant tracking system.

1. Scope and Order of Precedence

1.1 This DPA governs HarmonyHR's Processing of Customer Personal Data in connection with the Services and sets out the rights and obligations of the parties with respect to such Processing.

1.2 In the event of a conflict between this DPA and the Agreement, this DPA controls solely with respect to the subject matter of data protection and Processing of Customer Personal Data. In the event of a conflict between this DPA and any annex to this DPA, the body of this DPA controls unless the relevant annex expressly states otherwise.

1.3 This DPA does not apply to Processing activities for which HarmonyHR acts as an independent controller, including its own corporate administration, billing, fraud prevention, collections, sanctions screening, compliance, legal claims, internal security operations, business analytics based on Service Data, or processing described in HarmonyHR's public Privacy Policy for controller-side activities.

2. Definitions

"Applicable Data Protection Laws" means all laws, regulations, regulatory requirements, and binding guidance applicable to the Processing of Customer Personal Data under the Agreement, including, where applicable, the GDPR, the UK GDPR, the Data Protection Act 2018, and other privacy or data protection laws that apply to the parties in connection with the Services.

"Controller" means the entity that determines the purposes and means of the Processing of personal data, including any equivalent concept such as "business" under applicable privacy law.

"Customer Personal Data" means any personal data processed by HarmonyHR on behalf of Customer through or in connection with the Services.

"Data Subject" means an identified or identifiable natural person to whom Customer Personal Data relates.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data processed by HarmonyHR under this DPA.

"Process", "Processed", or "Processing" means any operation or set of operations performed on personal data, whether or not by automated means, and will be interpreted in accordance with Applicable Data Protection Laws.

"Processor" means the entity that Processes personal data on behalf of the Controller, including any equivalent concept such as "service provider" or "contractor" under applicable privacy law where relevant.

"Restricted Transfer" means a transfer of personal data that is subject to a transfer mechanism requirement under Applicable Data Protection Laws.

"Subprocessor" means any third party, including any HarmonyHR Affiliate, engaged by HarmonyHR to Process Customer Personal Data on behalf of Customer in connection with the Services.

Capitalized terms not defined in this DPA have the meanings given in the Agreement.

3. Roles of the Parties and Processing Details

3.1 Customer appoints HarmonyHR as a Processor or Service Provider, as applicable, to Process Customer Personal Data on Customer's behalf for the limited purpose of providing, securing, supporting, maintaining, improving, and administering the Services in accordance with the Agreement, this DPA, and Customer's documented instructions.

3.2 As between the parties, Customer is responsible for determining whether its collection and use of Customer Personal Data is lawful, including providing appropriate notices, obtaining any required consents, establishing and documenting a valid legal basis, determining applicable retention periods, and responding to Data Subject requests, except to the extent HarmonyHR is expressly required to assist under Applicable Data Protection Laws and this DPA.

3.3 If Customer acts as a Processor on behalf of another controller, Customer represents and warrants that Customer is duly authorized to instruct HarmonyHR and to grant the permissions set out in the Agreement and this DPA.

3.4 The subject matter, duration, nature, purpose, categories of Data Subjects, and categories of Customer Personal Data are described in Annex 1.

4. Customer Instructions

4.1 HarmonyHR will Process Customer Personal Data only on documented instructions from Customer, unless otherwise required by applicable law to which HarmonyHR is subject. The Agreement, this DPA, Customer's configuration and use of the Services, Customer's documented administrator settings, and Customer's written directions given through agreed support, administrative, or account channels constitute Customer's complete and documented instructions as of the Effective Date.

4.2 Customer instructs HarmonyHR to Process Customer Personal Data as reasonably necessary to provide the Services; to authenticate users; to host, store, back up, retrieve, display, transmit, organize, index, search, export, and delete Customer Personal Data; to provide support, troubleshooting, maintenance, and security monitoring; to prevent, detect, and remediate fraud, misuse, or security incidents; to comply with applicable law; and to engage approved Subprocessors in accordance with this DPA.

4.3 HarmonyHR will inform Customer if, in HarmonyHR's reasonable opinion and taking into account the nature of the Processing, a documented instruction infringes Applicable Data Protection Laws; provided, however, HarmonyHR is not required to provide legal advice to Customer.

4.4 HarmonyHR may refuse to follow an instruction that is unlawful, technically infeasible, insecure, outside the scope of the Agreement, inconsistent with the nature or Documentation of the Services, or would materially interfere with the integrity, confidentiality, availability, or security of the Services. Where legally permitted, HarmonyHR will explain the basis for the refusal.

5. Customer Compliance Responsibilities

5.1 Customer represents, warrants, and covenants that it has provided, and will continue to provide, all notices and obtain and maintain all rights, permissions, and lawful bases necessary for HarmonyHR to Process Customer Personal Data in accordance with the Agreement and this DPA.

5.2 Customer is solely responsible for the accuracy, quality, legality, reliability, and appropriateness of Customer Personal Data and for the means by which Customer acquired Customer Personal Data.

5.3 Customer will not submit to the Services, and will not instruct HarmonyHR to Process, Customer Personal Data in a manner that violates Applicable Data Protection Laws, employment laws, anti-discrimination laws, export control or sanctions laws, or other applicable law, or that would expose HarmonyHR to obligations materially inconsistent with the Agreement, the Documentation, or this DPA.

5.4 Unless expressly supported by the Services and lawful for Customer's use case, Customer should not upload unnecessary special category data, government-issued identification numbers, biometric data, financial account credentials, or other highly sensitive data. If Customer chooses to Process such data through the Services, Customer remains solely responsible for the lawfulness and suitability of doing so and for implementing any additional controls required by law.

6. Confidentiality

6.1 HarmonyHR will ensure that persons authorized to Process Customer Personal Data are subject to appropriate obligations of confidentiality, whether by contract, policy, or applicable law, and are given access to Customer Personal Data only on a need-to-know basis.

6.2 HarmonyHR will require such personnel to respect the confidentiality and security of Customer Personal Data during and after their engagement, in accordance with applicable law and HarmonyHR's internal policies.

7. Security Measures

7.1 Taking into account the state of the art, the costs of implementation, the nature, scope, context, and purposes of Processing, and the risks to individuals, HarmonyHR will implement and maintain appropriate technical and organizational measures designed to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or unauthorized access.

7.2 The technical and organizational measures maintained by HarmonyHR as of the Effective Date are described in Annex 2. HarmonyHR may update or modify such measures from time to time, provided that any such update or modification does not materially diminish the overall security of the Services.

7.3 Customer acknowledges that no security measure can guarantee absolute security and that HarmonyHR's obligations under this Section are obligations of reasonable care and ongoing maintenance, not a guarantee that the Services will be free from security incidents.

8. Use of Subprocessors

8.1 Customer provides a general authorization for HarmonyHR to engage Subprocessors to Process Customer Personal Data on Customer's behalf in connection with the Services.

8.2 HarmonyHR will impose data protection obligations on each Subprocessor that are no less protective in all material respects than the obligations imposed on HarmonyHR under this DPA, to the extent applicable to the nature of the services provided by the Subprocessor.

8.3 HarmonyHR remains responsible for the acts and omissions of its Subprocessors to the extent HarmonyHR would be responsible if performing the relevant Processing directly, subject always to the exclusions and limitations of liability in the Agreement and this DPA.

8.4 HarmonyHR is not required to maintain or publish a separate public Subprocessor List. HarmonyHR may make information about the categories or identities of Subprocessors available by reasonable means, including through contractual materials, account communications, support channels, or upon reasonable written request, in each case subject to confidentiality, security, legal, and third-party restrictions. HarmonyHR may add, replace, or remove Subprocessors from time to time in the ordinary course of business.

8.5 To the extent, and only to the extent, Applicable Data Protection Laws require Customer to have a right to object to a new Subprocessor, Customer may object only on reasonable, documented data protection grounds that are specific to the proposed Subprocessor and cannot be resolved by commercially reasonable measures. Customer must notify HarmonyHR in writing within ten (10) business days after the relevant notice or disclosure. The parties will discuss the concern in good faith. If HarmonyHR, in its sole but reasonable discretion, cannot implement a commercially reasonable measure to address the objection and continued use of the affected Processing would likely cause Customer to violate Applicable Data Protection Laws, either party may terminate only the affected portion of the Services on written notice. Unless required by applicable law or expressly provided in the Agreement, such termination will not create any refund, credit, or other payment obligation. This Section states Customer's sole and exclusive remedy for an objection to a new Subprocessor.

9. Assistance with Data Subject Requests, DPIAs, and Regulator Inquiries

9.1 Taking into account the nature of the Processing, HarmonyHR will provide Customer with reasonable assistance, through appropriate technical and organizational measures and subject to the nature of the Services, to enable Customer to respond to requests from Data Subjects to exercise their rights under Applicable Data Protection Laws.

9.2 If HarmonyHR receives a request directly from a Data Subject relating to Customer Personal Data, HarmonyHR will, to the extent legally permitted, direct the requester to Customer or notify Customer so that Customer may respond. HarmonyHR is not responsible for responding to such requests except as required by Applicable Data Protection Laws.

9.3 Taking into account the nature of the Processing and the information available to HarmonyHR, HarmonyHR will provide reasonable assistance to Customer with data protection impact assessments, prior consultations with supervisory authorities, and responses to lawful regulator inquiries relating to Customer's use of the Services, where such assistance is required by Applicable Data Protection Laws and Customer cannot reasonably fulfill the requirement without HarmonyHR's assistance.

9.4 HarmonyHR may charge reasonable fees at its then-current professional services rates for assistance provided under this Section to the extent such assistance is not required due to HarmonyHR's breach of this DPA or Applicable Data Protection Laws and requires material time, effort, customization, or external cost.

10. Personal Data Breach

10.1 HarmonyHR will notify Customer without undue delay after becoming aware of a confirmed Personal Data Breach affecting Customer Personal Data.

10.2 Such notification will include, to the extent reasonably available at the time, information reasonably necessary for Customer to understand the nature of the Personal Data Breach, assess its likely impact, and comply with Customer's notification obligations under Applicable Data Protection Laws. HarmonyHR may provide information in phases as it becomes available.

10.3 HarmonyHR will take commercially reasonable steps to investigate, contain, mitigate, and remediate the effects of a Personal Data Breach affecting Customer Personal Data.

10.4 HarmonyHR's notification of or response to a Personal Data Breach is not, and will not be construed as, an acknowledgment of fault or liability.

11. Deletion and Return of Customer Personal Data

11.1 Upon expiration or termination of the Agreement, and except to the extent applicable law requires continued retention, HarmonyHR will delete or return Customer Personal Data in accordance with the Agreement, this DPA, the functionality of the Services, and HarmonyHR's standard processes.

11.2 Subject to Customer's full payment of all amounts due and continued compliance with the Agreement, Customer may request export or return of Customer Personal Data using the Services' standard export functionality or through reasonable transition assistance, if agreed in writing, for up to thirty (30) days following the effective date of expiration or termination.

11.3 After the applicable post-termination retrieval period, HarmonyHR may delete or render inaccessible Customer Personal Data in accordance with its standard deletion and retention processes. HarmonyHR is not obligated to maintain Customer Personal Data beyond that period except as required by applicable law, in routine backup, archival, or disaster recovery systems, or as otherwise permitted under the Agreement and this DPA.

11.4 Notwithstanding the foregoing, HarmonyHR may retain Customer Personal Data to the extent required by applicable law or as retained in routine backup systems, archival systems, evidentiary records, or disaster recovery systems, provided that in each case such retained Customer Personal Data will remain protected in accordance with this DPA and will not be actively Processed except as required by law or for legitimate backup, security, business continuity, evidentiary, or compliance purposes.

12. Audit and Information Rights

12.1 HarmonyHR will make available to Customer information reasonably necessary to demonstrate HarmonyHR's compliance with this DPA, which may include accurate summaries of relevant security and privacy practices, responses to reasonable written questionnaires, and, where available and appropriate, third-party assessments or audit summaries, in each case subject to confidentiality, security, privilege, and access restrictions.

12.2 To the extent Applicable Data Protection Laws require an audit right that cannot reasonably be satisfied by the information described in Section 12.1, Customer may request an audit of HarmonyHR's relevant Processing activities no more than once in any twelve (12) month period, except where a confirmed Personal Data Breach affecting Customer Personal Data or a binding instruction from a competent supervisory authority requires additional review.

12.3 Any audit under this Section must: (a) be limited to matters directly relevant to HarmonyHR's Processing of Customer Personal Data; (b) be conducted on at least thirty (30) days' prior written notice; (c) occur during normal business hours; (d) avoid unreasonable disruption to HarmonyHR's business, systems, personnel, and other customers; (e) be subject to strict confidentiality obligations; (f) be conducted by Customer or an independent third-party auditor that is not a competitor of HarmonyHR and is reasonably acceptable to HarmonyHR; and (g) not include access to source code, algorithms, penetration-test results, raw vulnerability data, facilities housing other customers' data, or systems unrelated to the Services.

12.4 HarmonyHR may satisfy any audit obligation through a combination of remote review, documentation review, interviews, walkthroughs, or other reasonably equivalent means where appropriate to protect the security of the Services and the confidentiality obligations owed to other customers and third parties. On-site access will be permitted only where legally required and only to the minimum extent necessary.

12.5 Customer will bear its own audit costs and reimburse HarmonyHR for reasonable costs incurred in supporting an audit under this Section, except to the extent applicable law prohibits such reimbursement. Information and materials disclosed under this Section are HarmonyHR Confidential Information.

13. International Transfers

13.1 Customer authorizes HarmonyHR and its Subprocessors to make Restricted Transfers of Customer Personal Data as reasonably necessary to provide the Services, subject to compliance with Applicable Data Protection Laws.

13.2 Where a Restricted Transfer requires a specific transfer mechanism, the parties agree that the European Commission's Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, Commission Implementing Decision (EU) 2021/914 (the "EU SCCs"), are incorporated by reference into this DPA and apply as follows: (a) Module Two (Controller to Processor) applies where Customer is a controller and HarmonyHR is a processor; (b) Module Three (Processor to Processor) applies where Customer is a processor and HarmonyHR is a subprocessor; (c) in each case, the optional docking clause is deemed included; and (d) the annexes to the EU SCCs are deemed completed with the information set out in the Agreement, this DPA, Annex 1, Annex 2, and any other information reasonably made available by HarmonyHR in writing where required to complete or support the applicable transfer mechanism.

13.3 Where UK GDPR applies to a Restricted Transfer and a lawful UK transfer mechanism is required, the parties agree that the UK International Data Transfer Addendum to the EU SCCs is incorporated by reference into this DPA, with the EU SCCs as modified by the mandatory terms of the UK Addendum. Where Swiss data protection law applies and a Swiss transfer mechanism is required, the EU SCCs will apply with the modifications necessary for Swiss law.

13.4 HarmonyHR will implement supplementary measures where required by Applicable Data Protection Laws and reasonably appropriate in light of the nature of the transfer, the Services, and the technical and organizational measures described in Annex 2.

14. Non-EU / Non-UK Privacy Law Concepts

14.1 To the extent a privacy law outside the European Union or United Kingdom applies to Customer Personal Data and uses concepts such as "service provider," "contractor," or "processor," HarmonyHR will Process Customer Personal Data solely for the business purposes of providing the Services and as otherwise permitted by the Agreement and applicable law.

14.2 HarmonyHR will not sell or share Customer Personal Data, and will not retain, use, or disclose Customer Personal Data for any purpose other than the specific business purposes set out in the Agreement and this DPA, including as necessary to provide, secure, maintain, support, troubleshoot, and improve the Services as permitted by applicable law.

14.3 Nothing in this DPA restricts HarmonyHR from using Service Data and from using de-identified, aggregated, or anonymized information that does not identify Customer, any Data Subject, or Customer Personal Data, to the extent permitted by applicable law and the Agreement.

15. Liability

15.1 Each party's liability arising out of or relating to this DPA will be subject to the exclusions and limitations of liability set out in the Agreement, except to the extent prohibited by Applicable Data Protection Laws.

15.2 This DPA does not expand either party's liability beyond what is stated in the Agreement, and no party may recover under both this DPA and the Agreement for the same loss.

16. Term and Termination

16.1 This DPA takes effect on the Effective Date and remains in force for as long as HarmonyHR Processes Customer Personal Data on behalf of Customer under the Agreement.

16.2 Any obligation in this DPA that by its nature is intended to survive termination or expiration, including obligations concerning confidentiality, liability, international transfers, deletion and return, retained data, and audit confidentiality, will survive for so long as HarmonyHR retains Customer Personal Data.

17. General

17.1 Except as expressly amended by this DPA, the Agreement remains in full force and effect.

17.2 If any provision of this DPA is held unenforceable, the remainder will remain in effect, and the unenforceable provision will be replaced by a valid provision that most closely reflects the parties' original intent and the requirements of Applicable Data Protection Laws.

17.3 This DPA may be accepted electronically in connection with the Services, and such electronic acceptance will have the same force and effect as a signed original.

17.4 Notices under this DPA may be delivered in accordance with the notice provisions of the Agreement. For privacy-specific communications relating to this DPA, HarmonyHR may be contacted at info@harmonyats.org.

17.5 Governing law and jurisdiction for this DPA will be the governing law and jurisdiction specified in the Agreement.

Annex 1 – Details of Processing

This Annex 1 forms part of the DPA and describes the Processing carried out by HarmonyHR on behalf of Customer in connection with HarmonyATS.

Item	Description
Controller	Customer identified in the Agreement, acting as the controller, employer, business, or equivalent responsible party for applicant, candidate,

Item	Description
	employee, contractor, referee, and related workforce data uploaded to HarmonyATS.
Processor / Service Provider	HarmonyHR LTD, acting as processor or service provider on behalf of Customer when providing HarmonyATS.
Subject matter	Processing of Customer Personal Data necessary to provide, secure, support, maintain, and administer the HarmonyATS cloud software-as-a-service applicant tracking system under the Agreement.
Duration	For the term of the Agreement and any applicable post-termination retrieval, deletion, backup, archival, or legal retention period described in the Agreement, this DPA, or required by law.
Nature of Processing	Collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure by transmission, alignment, restriction, deletion, and other processing operations necessary to provide the Services and related support.
Purpose of Processing	Providing applicant tracking, recruiting workflow management, candidate relationship and communication functions, permissions and user administration, reporting, support, implementation, troubleshooting, security, and related service operations for Customer.
Categories of Data Subjects	Job applicants, candidates, prospective candidates, referees and references, Customer's recruiters, hiring managers, interviewers, administrators, employees, contractors, and other individuals whose data Customer or its Authorized Users upload or otherwise submit to HarmonyATS.
Categories of Personal Data	Depending on Customer's use of the Services, categories may include identification data, contact data, professional and employment information, recruitment materials, interview feedback, assessment results, communications data, account and user profile data, scheduling information, job application history, notes and records created by Customer users, and any other personal data submitted to the Services by or on behalf of Customer.
Special categories / sensitive data	Not required for the ordinary operation of the Services unless Customer chooses to upload such data or applicable law requires it for

Item	Description
	Customer's recruiting activities. Any Processing of special categories of personal data or similarly sensitive data will be only as instructed by Customer and subject to appropriate safeguards under Applicable Data Protection Laws.
Frequency of Processing	Continuous or as initiated by Customer or its Authorized Users during the subscription term.
Storage / hosting region	In the jurisdictions in which HarmonyHR or its Subprocessors operate infrastructure, support, backup, disaster recovery, or service-delivery functions, as reasonably necessary to provide the Services, subject to Section 13 of this DPA and any disclosures or safeguards required by Applicable Data Protection Laws.
Transfer mechanism	As applicable under Section 13 of this DPA, including the incorporated EU SCCs, the UK Addendum, or another lawful transfer mechanism recognized under Applicable Data Protection Laws.

Customer remains solely responsible for determining which categories of personal data it uploads to the Services and for ensuring that such Processing is lawful.

Annex 2 – Technical and Organizational Measures

HarmonyHR maintains technical and organizational measures designed to protect Customer Personal Data, taking into account the nature of the Services and the risks presented by the Processing. The measures may be updated from time to time so long as the overall security of the Services is not materially diminished.

- Information security governance. HarmonyHR maintains internal policies and procedures addressing information security, confidentiality, access management, incident response, business continuity, and data handling practices appropriate to the Services.
- Access controls. HarmonyHR uses account authentication and authorization controls designed to limit access to Customer Personal Data to authorized personnel and authorized Customer users on a need-to-know basis, including role-based access where appropriate.
- Credential and account security. HarmonyHR maintains measures designed to help protect credentials and administrative access, such as password management controls and, where implemented, multifactor authentication for relevant accounts or administrative environments.
- Encryption and transmission security. HarmonyHR maintains measures designed to protect Customer Personal Data in transit and, where implemented for relevant systems, at rest, using industry-accepted cryptographic methods appropriate to the Services.
- System monitoring and logging. HarmonyHR maintains logging, monitoring, and alerting practices intended to support security operations, troubleshooting, misuse detection, and incident investigation.
- Network and endpoint protection. HarmonyHR maintains measures such as network segmentation, firewalling, malware protection, patching, and vulnerability management practices reasonably appropriate to the Services.

• Change management and development practices. HarmonyHR uses processes intended to manage changes to production systems and application code, including testing and review practices reasonably appropriate to the Services.

• Availability, backup, and recovery. HarmonyHR maintains backup, restoration, resilience, and disaster recovery measures reasonably appropriate to the Services, subject to the architecture and operational design of the Services.

• Personnel security and training. HarmonyHR requires relevant personnel to be bound by confidentiality obligations and provides training or awareness measures regarding privacy, security, and data handling responsibilities.

• Vendor management. HarmonyHR uses a review process for Subprocessors and vendors that may have access to Customer Personal Data, with contractual protections reasonably appropriate to the services they provide.

• Incident response. HarmonyHR maintains procedures for identifying, responding to, containing, investigating, mitigating, and documenting security incidents affecting systems used to provide the Services.

• Data minimization and deletion controls. HarmonyHR maintains operational processes designed to limit retention and support deletion or return of Customer Personal Data in accordance with the Agreement, this DPA, and applicable law.

• Physical security. To the extent HarmonyHR or its hosting providers operate facilities that store or process Customer Personal Data, physical access to such facilities is subject to reasonable access controls and environmental safeguards appropriate to the Services.

Execution

This DPA is deemed accepted and effective as of the Effective Date when incorporated into, referenced by, or accepted under the Agreement. No separate signature blocks, customer-side schedules, or additional placeholders are required for this DPA to be effective.