HRLOCKER DATA PROCESSING AGREEMENT (DPA)

Date of Agreement: [Insert Date]

Parties:

- HR Interventions Ltd (trading as HRLocker), registered at 5th Floor, Connaught House, One Burlington Road, Dublin 4, D04 C5Y6, acting as Data Processor
- [Customer Name], acting as Data Controller

1. DEFINITIONS
As per Article 4 GDPR:

- Personal Data: Information relating to an identified/identifiable person.
- Processing: Any operation performed on Personal Data.
- Data Controller: Entity determining purposes and means of processing.
- Data Processor: Entity processing on behalf of Controller.
- Sub-Processor: Third party engaged by Processor to process Personal Data.
- Data Breach: Unauthorised or unlawful destruction, loss, or access.
- Special Category Data: As per Article 9 GDPR.
- Criminal Conviction Data: As per Article 10 GDPR.

2. PURPOSE & SCOPE OF PROCESSING

- HRLocker processes Personal Data strictly per Controller instructions.
- Processing purposes include employee management, recruitment, and legal compliance.
- No other processing will occur without written authorisation from the Controller.

3. CONTROLLER RESPONSIBILITIES
The Controller is responsible for:

- Ensuring all data is lawfully collected (Article 6 GDPR).
- Managing access levels within the HRLocker platform.
- Handling Data Subject Access Requests (DSARs); HRLocker will assist but not respond directly.
- Determining and enforcing data retention policies.

4. HRLOCKER OBLIGATIONS

HRLocker shall:

- Only process data per documented Controller instructions.
- Implement technical and organisational measures as required by Article 32 GDPR.
- Ensure all authorised personnel are subject to confidentiality.
- Maintain records of processing under Article 30 GDPR.
- Assist with DPIAs and supervisory authority consultations where applicable.

5. SUB-PROCESSORS

- Sub-Processors used by HRLocker are listed on the HRLocker Security Hub.
- HRLocker shall notify the Controller at least 30 days prior to engaging a new Sub-Processor.
- Controllers may object in writing within that period. Continued use after the notice period constitutes acceptance.
- HRLocker ensures all Sub-Processors provide GDPR - equivalent protection.

6. DATA TRANSFERS

No Personal Data will be transferred outside the EEA or UK unless:

- Standard Contractual Clauses (SCCs) or UK Addendum are in place.
- Data subjects have enforceable rights and effective legal remedies.

Regulatory Adaptation:
The Parties agree that where changes to applicable data protection legislation or international data transfer frameworks (such as the adoption of the EU-U.S. Data Privacy Framework or revisions to SCCs) necessitate updates to this Agreement, such changes may be implemented through an addendum or written notice without requiring full renegotiation of the DPA. HRLocker shall notify the Controller of such updates and provide reasonable opportunity for review.

7. SECURITY & BREACH NOTIFICATION

HRLocker implements appropriate security measures as per Article 32.
In the event of a Data Breach, HRLocker shall:

- Notify the Controller within 72 hours.
- Provide breach details and mitigation steps.

8. SPECIAL CATEGORY & CRIMINAL CONVICTION DATA

- Controllers are solely responsible for ensuring lawful grounds for processing sensitive data (Articles 9 and 10 GDPR).
- HRLocker provides a designated module to process such data. Use of this module is mandatory for legal compliance.
- HRLocker is not liable for misuse by the Controller.

9. DATA RETENTION & TERMINATION

The Controller retains full responsibility for data retention during the contract.
Upon termination:

- HRLocker will permanently delete all Customer Data (including backups) on the day of termination unless otherwise agreed or legally required to retain it.
- Customers can export their data at any time before termination through the HRLocker portal.
- A deletion confirmation will be provided upon request.

10. AUDIT RIGHTS

HRLocker shall make available documentation reasonably required to demonstrate compliance with this DPA.

Onsite or thirdparty audits are permitted only:

- Upon 30 days' written notice.
- No more than once per year unless required by law.
- At the Controller's expense and subject to HRLocker's confidentiality and security obligations.

11. LIABILITY & INDEMNITY

HRLocker shall indemnify the Controller only for direct losses or fines due to proven GDPR violations.
HRLocker is not liable for:

- Indirect or consequential losses
- Controller's misuse or unlawful data processing.
- Sub-Processor actions where appropriate due diligence was conducted.
- Total liability is capped at the contract value.

12. GOVERNING LAW & DISPUTE RESOLUTION

- This Agreement is governed by Irish law.
- Disputes will be resolved by mediation within 30 days.
- If mediation fails, parties may refer disputes to the Irish courts.

SIGNED FOR AND ON BEHALF OF [Customer Name]
By: _____
Name: _____
Date: _____

SIGNED FOR AND ON BEHALF OF HR INTERVENTIONS LTD ("HRLocker")

By: Crystel Rynne
Date: 01/12/2024

Additional Provisions for GDPR Alignment
International Transfers

Where required, HRLocker and the Controller shall execute the latest version of the EU Standard Contractual Clauses (2021) and, where applicable, the UK International Data Transfer Addendum (IDTA), to ensure continued lawful transfer. These measures comply with GDPR Articles 45 to 49.

Data Retention on Termination

Upon termination of the contract, HRLocker will delete all Customer Data, including backups, on the same day unless otherwise required by law. No retention buffer period applies. A deletion confirmation will be provided upon request.

Fees for Compliance Support

HRLocker reserves the right to charge reasonable professional fees for assistance related to Data Protection Impact Assessments (DPIAs), Data Subject Access Requests (DSARs), or detailed audit documentation, beyond standard support. Fees will be applied at HRLocker's prevailing rates.

Support with Data Subject Rights

HRLocker shall, to the extent technically feasible, assist the Controller in responding to requests from Data Subjects under GDPR Articles 12–23. This includes access to system logs, exports, and deletions as necessary to fulfil lawful rights requests. HRLocker will not respond directly to Data Subjects without express written instruction from the Controller.

Annex I – Details of Processing

Field	Description
Subject Matter	HR management and applicant tracking via the HRLocker platform
Duration	For the duration of the customer contract or as required by law
Nature and Purpose	Provision of HRIS and ATS services including time tracking, document management, onboarding, leave management, employee records, recruitment, and compliance reporting
Types of Personal Data	Names, email addresses, phone numbers, job titles, employment history, work schedules, salary and benefits data, ID numbers, IP addresses, and other employment-related data. Special category data may be processed if input by the controller.
Categories of Data Subjects	Employees, job applicants, contractors, and internal HR representatives of the customer
Processing Activities	Hosting, storing, transmitting, displaying, deleting, modifying, and analysing data within the scope of platform functionality
Special Categories of Data	Only processed if explicitly input and managed by the Controller. Includes health/disability info, ethnicity, trade union membership, etc., if applicable
Sub-Processors	Listed at https://security.hrlocker.com with 30-day advance notice of changes

Annex II – Technical and Organisational Measures

At HRLocker, protecting your data is our priority. We are committed to maintaining the highest standards of data protection and information security. Our practices are designed to comply with the General Data Protection Regulation (GDPR) and align with ISO 27001 standards. Below is an overview of the Technical and Organisational Measures (TOMs) we implement to safeguard personal and business data.

1. Access Control

- Role-based access controls ensure only authorised personnel can access systems and data.
- Multi-factor authentication (MFA) adds an extra layer of protection.
- Access rights are regularly reviewed and monitored.

2. Data Encryption

- All sensitive data is encrypted at rest and in transit using industry-standard methods.
- Backups are securely stored in EU-based data centres.

3. Network and Systems Security

- Firewalls and intrusion detection systems are in place to protect our network.
- Anti-malware tools are deployed and updated regularly.
- Regular vulnerability scans and system updates are conducted.

4. Data Minimisation and Retention

- We only collect data that is necessary for specific business purposes.
- Data is securely deleted after it is no longer required, in line with retention policies.

5. Physical Security

- Restricted access to secure locations such as server rooms and offices.
- Surveillance systems monitor access to physical premises.

6. Data Breach Response

- Incident response plans are in place to detect, contain, and mitigate breaches.
- Breaches are escalated internally to the Incident Response Team, which assesses the impact and implements corrective actions.
- Affected parties and regulators are notified within 72 hours, as required by GDPR.

7. Data Breach Communication

- Notifications to affected parties include:
- Nature of the breach.
- Types of data affected.
- Mitigation steps taken.
- Contact details for further inquiries.
- Notifications are sent via email or phone, depending on the urgency and impact of the breach.

8. Employee Awareness and Training

- Employees receive regular training on GDPR, data privacy, and security best practices.
- Confidentiality agreements are signed by all staff.

9. Subprocessor Management

- We use trusted partners like Microsoft Azure (EU data centres) and HubSpot, ensuring their compliance with GDPR.
- Subprocessor practices are regularly audited.

10. Monitoring and Audit

- Continuous monitoring of systems and activity logs ensures proactive risk management.
- Internal and external audits are conducted in line with ISO 27001 standards.

11. Data Protection Impact Assessments (DPIAs)

- DPIAs are conducted for high-risk processing activities to identify and mitigate risks.

12. Business Continuity and Disaster Recovery

- Comprehensive backup and disaster recovery plans are tested regularly.
- Systems include redundancy and failover mechanisms to ensure availability.

Commitment to Data Protection

HRLocker ensures all subprocessors comply with GDPR and other relevant data protection laws. We continuously review our partnerships to maintain the highest standards of security and privacy. These measures are continuously reviewed and improved to adapt to evolving security challenges and regulations.

For more information, please contact support@hrlocker.com or our Data Protection Officer at DPO@enable-iso.com **.**

Annex III – Sub-Processors

A full and current list of Sub-Processors is available at https://www.hrlocker.com/security-centre/.

HRLocker shall notify the Controller of any intended changes at least 30 days in advance.

Annex IV – Data Protection Contact Points

Data Protection Officer: Phil Byrne

To ensure that independence is maintained with regard to the protection of organisational data, Phil Byrne can be contacted directly and in confidence, by sending your query to DPO@enable-iso.com.

Customer Data Protection Contact:
To be designated by the Customer in the Order Form or primary contract document.