HR Forte Data Processing Addendum

This Data Processing Addendum (**"DPA"**) supplements the HR Forte Terms and Conditions, subscription terms, order form, master subscription agreement, or other agreement between Customer and HR Forte governing Customer's access to and use of the HR Forte native SaaS HR and payroll platform, as updated from time to time in accordance with that agreement (**"Agreement"**). This DPA applies to the processing of Customer Personal Data by HR Forte in connection with the Platform.

This DPA is entered into between **[HR Forte legal entity name]** (**"HR Forte," "HRF," "we," "us," or "our"**) and the entity or person that accepts the Agreement or uses the Platform on behalf of itself or another organisation (**"Customer," "you," or "your"**). Customer may be an employer using the Platform for its own workforce, or a consultant, payroll bureau, accountant, HR service provider, corporate service provider, reseller, implementation partner, or other intermediary using the Platform for its own end clients.

For Customer Personal Data processed through the Platform, HR Forte generally acts as a processor or sub-processor, as applicable. Customer is responsible for determining its own role under Applicable Data Protection Laws and for ensuring that it has the necessary authority, notices, consents, contractual rights, and lawful basis to submit, manage, and process Customer Personal Data through the Platform. HR Forte does not manage, control, own, validate, approve, correct, or administer Customer Personal Data. Customer manages and controls Customer Personal Data through the Platform.

Unless otherwise defined in this DPA or in the Agreement, capitalised terms used in this DPA have the meanings given to them in the definitions section of this DPA.

Term	Meaning
Applicable Data Protection Laws	All data protection, privacy, cybersecurity, breach notification, employment data, payroll data, and personal data laws applicable to the processing of Customer Personal Data under the Agreement, including, where applicable, the EU GDPR, UK GDPR, Singapore PDPA, Malaysia PDPA, Vietnam personal data protection regulations, Thailand PDPA, Philippines Data Privacy Act, Hong Kong PDPO, Cambodia personal data rules, and any successor or implementing regulations.
Controller	The party that determines the purposes and means of processing Customer Personal Data. For Customer Personal Data processed through the HR Forte platform, Customer is generally the Controller.
Customer Personal Data	Personal Data submitted to, uploaded to, stored in, accessed through, generated in, or otherwise processed by HR Forte on behalf of Customer in connection with the Services.
Data Breach	A confirmed accidental, unlawful, or unauthorised destruction, loss, alteration, disclosure of, or access to Customer Personal Data processed by HR Forte under this DPA.
Data Subject	An identified or identifiable natural person to whom Customer Personal Data relates.
Personal Data	Any information relating to an identified or identifiable natural person, including any equivalent definition under Applicable Data Protection Laws.
Processing	Any operation performed on Personal Data, including collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, transmission, disclosure, alignment, restriction, erasure, or destruction.
Processor	The party that processes Personal Data on behalf of the Controller. For Customer Personal Data processed through the HR Forte platform, HR Forte is generally the Processor.
Services	The HR Forte SaaS platform and related services, including HR management, payroll, leave, claims, employee self-service, document management, time and attendance, support, implementation, maintenance, integrations, and other modules subscribed to by Customer.
Sensitive	Personal Data that is treated as sensitive, special category, or higher-

Personal Data	risk data under Applicable Data Protection Laws, including identification numbers, payroll and compensation data, bank account data, tax data, health-related data, biometric data if enabled, union membership data where processed, disciplinary data, criminal records where lawfully processed, and other legally protected categories.
Sub-processor	Any third party engaged by HR Forte to process Customer Personal Data on behalf of Customer in connection with the Services.

1. Definitions

In this DPA, the following terms have the meanings set out below. Capitalised terms not defined in this DPA have the meanings given in the Agreement.

2. Roles of the parties

Customer is the Controller of Customer Personal Data and is responsible for determining the purposes and lawful basis for processing Customer Personal Data. Customer is also responsible for the accuracy, quality, legality, and relevance of Customer Personal Data uploaded to or processed through the Services.

HR Forte is the Processor of Customer Personal Data and will process Customer Personal Data only on Customer's documented instructions, including the Agreement, this DPA, Customer's configuration of the Services, Customer's use of platform features, Customer's support requests, and any other written instructions agreed between the parties.

HR Forte may act as an independent Controller for limited Personal Data that it processes for its own business purposes, such as billing records, account administration contacts, product security logs, marketing contacts, customer relationship management, legal compliance, fraud prevention, and aggregated or anonymised product analytics. Such processing is governed by HR Forte's privacy policy and not by this DPA, unless the parties expressly agree otherwise.

3. Scope and purpose of processing

HR Forte will process Customer Personal Data only to provide, secure, maintain, support, improve, and administer the Services in accordance with the Agreement and this DPA. The subject matter, nature, purpose, duration, categories of Personal Data, categories of Data Subjects, and retention approach are described in **Schedule 1**.

HR Forte will not sell, rent, lease, or commercially disclose Customer Personal Data to third parties. HR Forte will not use Customer Personal Data for unrelated advertising, profiling, or data brokerage. HR Forte may use aggregated, de-identified, or anonymised information for service improvement, analytics, benchmarking, security monitoring, and product development, provided such information does not identify Customer, Customer's employees, or any Data Subject.

4. Customer instructions

Customer instructs HR Forte to process Customer Personal Data as necessary to provide the Services, comply with the Agreement, provide support requested by Customer, maintain platform security, troubleshoot issues, generate reports requested by Customer, process payroll and HR workflows configured by Customer, and comply with applicable legal obligations.

If HR Forte believes that an instruction from Customer infringes Applicable Data Protection Laws, HR Forte will inform Customer without undue delay, unless prohibited by law. HR Forte is not required to provide legal advice to Customer and may suspend execution of an instruction where HR Forte reasonably believes the instruction creates a material security, legal, or privacy risk.

5. Customer responsibilities

Customer is responsible for ensuring that it has all required notices, consents, employment law basis, contractual basis, statutory basis, legitimate interests, or other lawful grounds required to collect, upload, configure, and process Customer Personal Data through the Services. Customer is also responsible for ensuring that its authorised users use the Services lawfully and that user permissions are granted based on business need.

Customer must not upload Personal Data that is unnecessary for the subscribed Services or prohibited by the Agreement. Customer must use reasonable administrative controls, including role-based access, strong authentication, timely removal of terminated users, and careful configuration of employee access rights.

6. Confidentiality

HR Forte will ensure that personnel authorised to process Customer Personal Data are subject to confidentiality obligations or professional duties of confidentiality. HR Forte will limit access to Customer Personal Data to personnel who need such access to provide, secure, maintain, or support the Services.

Customer must ensure that its authorised users keep login credentials confidential and do not share administrator access with unauthorised persons. Customer is responsible for activity performed through Customer-controlled accounts, except to the extent caused by HR Forte’s breach of this DPA or the Agreement.

7. Security measures

HR Forte will implement and maintain appropriate technical and organisational measures designed to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or unauthorised access. These measures will be appropriate to the nature of HR and payroll data, the risks of processing, the state of the art, and the cost of implementation.

The current baseline security measures are described in **Schedule 2**. HR Forte may update its security measures from time to time, provided such updates do not materially reduce the overall protection of Customer Personal Data.

8. Sub-processors

Customer provides general authorisation for HR Forte to engage Sub-processors as necessary to provide the Services, including hosting, cloud infrastructure, communications, customer support, security monitoring, backup, analytics, and other operational services.

HR Forte hosts the Platform and Customer Personal Data on cloud infrastructure provided by Amazon Web Services, Inc. and/or its relevant affiliates (**AWS**). AWS acts as a material Sub-processor for infrastructure hosting, database hosting, storage, backup, security, availability, and related cloud operations. HR Forte will maintain a list of material Sub-processors in **Schedule 3**. HR Forte may update the list from time to time by written notice, customer notification, or publication on a legal, privacy, or trust page made available by HR Forte.

HR Forte remains responsible for the performance of its Sub-processors to the extent they process Customer Personal Data on HR Forte's behalf. HR Forte will provide Customer with notice of any intended addition or replacement of a material Sub-processor by email, platform notice, account notice, or update to the Sub-processor list. Customer may object on reasonable data protection grounds within **30 days** of notice. If the parties cannot resolve the objection, Customer may terminate the affected Services in accordance with the Agreement.

9. International transfers

Customer acknowledges that HR Forte may process Customer Personal Data in countries where HR Forte, its affiliates, support personnel, infrastructure providers, or Sub-processors operate, subject to Applicable Data Protection Laws and this DPA.

Where Customer Personal Data is transferred from a jurisdiction that requires transfer safeguards to a jurisdiction that has not been recognised as providing an adequate level of protection, HR Forte will implement appropriate transfer mechanisms required by Applicable Data Protection Laws. These may include standard contractual clauses, recognised regional transfer terms, customer consent where lawful, transfer impact assessments, contractual safeguards, technical safeguards, organisational safeguards, or other lawful transfer mechanisms.

For transfers governed by the EU GDPR, the parties agree that the European Commission's Standard Contractual Clauses may apply as set out in **Schedule 4**, where required. For UK transfers, the parties may use the UK International Data Transfer Addendum or other lawful UK transfer mechanism. For Singapore transfers, Customer remains responsible for ensuring that any transfer instructions comply with the Singapore PDPA, while HR Forte will provide reasonable cooperation and contractual safeguards for transfers performed by HR Forte.

10. Data subject requests

HR Forte will provide reasonable assistance to Customer, taking into account the nature of the processing and the functionality of the Services, to enable Customer to respond to Data Subject requests. Such requests may include access, correction, deletion, portability, restriction, objection, withdrawal, or other rights available under Applicable Data Protection Laws.

If HR Forte receives a Data Subject request directly concerning Customer Personal Data, HR Forte will, unless legally prohibited, either direct the Data Subject to Customer or notify Customer. HR Forte will not respond substantively to such request unless instructed by Customer or required by law.

11. Assistance with compliance

Taking into account the nature of processing and information available to HR Forte, HR Forte will provide reasonable assistance to Customer in meeting Customer's obligations relating to data protection impact assessments, prior consultations with regulators, security obligations, breach notification obligations, and regulatory enquiries, to the extent such obligations relate to HR Forte's processing of Customer Personal Data.

HR Forte may charge reasonable fees for assistance that is outside the standard functionality of the Services or outside routine support, unless the assistance is required because of HR Forte's breach of this DPA.

12. Data Breach notification

HR Forte will notify Customer without undue delay after confirming a Data Breach affecting Customer Personal Data. The notification will be sent to Customer's designated security, privacy, legal, or account contact, or through another agreed communication channel.

The notification will include, to the extent known and legally permitted, a description of the nature of the Data Breach, categories and approximate number of affected Data Subjects and records, likely consequences, measures taken or proposed to address the Data Breach, and contact point for further information. HR Forte may provide this information in phases as it becomes available.

Customer is responsible for determining whether notification to regulators, employees, or other third parties is required, unless Applicable Data Protection Laws impose a direct notification obligation on HR Forte. HR Forte will reasonably cooperate with Customer's investigation and notification process.

13. Return and deletion of Customer Personal Data

During the subscription term, Customer may access, export, correct, or delete Customer Personal Data using available platform functionality, subject to the subscribed modules and technical limitations of the Services.

Upon termination or expiry of the Agreement, HR Forte will return or delete Customer Personal Data in accordance with the Agreement, Customer's written instruction, and **Schedule 5**. HR Forte may retain limited copies where required by law, audit obligations, dispute resolution, backup integrity, security logs, tax or accounting obligations, or legitimate business recordkeeping, provided such retained data remains protected under this DPA and is not used for any unrelated purpose.

14. Audit and compliance evidence

HR Forte will make available information reasonably necessary to demonstrate compliance with this DPA. This may include security summaries, certifications, audit reports, penetration test summaries,

policy attestations, data flow summaries, sub-processor lists, incident response summaries, and other relevant documentation, subject to confidentiality, security, and third-party restrictions.

Customer may request an audit no more than once per calendar year, unless required by a regulator or following a confirmed Data Breach caused by HR Forte. Audits must be reasonable, proportionate, conducted during normal business hours, subject to prior written notice of at least 30 days, and performed in a manner that does not compromise the security, confidentiality, availability, or privacy of HR Forte, other customers, or third-party systems. HR Forte may satisfy audit requests through independent third-party reports or written responses where appropriate for a multi-tenant SaaS environment.

15. Government, regulator, and legal requests

If HR Forte receives a legally binding request from a court, regulator, law enforcement authority, government agency, or other public authority for disclosure of Customer Personal Data, HR Forte will notify Customer before disclosure where legally permitted. HR Forte will disclose only the minimum Customer Personal Data required by the request and will reasonably cooperate with Customer if Customer seeks to challenge or limit the request.

16. Records and accountability

HR Forte will maintain appropriate records of processing activities relating to Customer Personal Data as required by Applicable Data Protection Laws. HR Forte will also maintain policies and procedures designed to support confidentiality, access control, incident management, business continuity, vendor management, and data retention.

Customer is responsible for maintaining its own records of processing, employee notices, consent records where applicable, payroll processing basis, statutory reporting basis, data retention rules, internal role permissions, and Data Subject request logs.

17. Sensitive Personal Data and HR/payroll data

Customer acknowledges that HR and payroll processing may involve Sensitive Personal Data or higher-risk employment data. Customer must configure the Services and upload data in a manner consistent with Applicable Data Protection Laws and employment laws.

HR Forte will process Sensitive Personal Data only as necessary to provide the Services, comply with Customer’s documented instructions, provide support, secure the platform, or comply with legal obligations. HR Forte will apply the security measures in **Schedule 2** and any additional controls agreed in an Order Form or enterprise security addendum.

18. Artificial intelligence and automated processing

If HR Forte provides AI-enabled features, compliance assistance, chatbot functionality, workflow recommendations, analytics, or automated decision-support tools, HR Forte will process Customer Personal Data for those features only as described in the Agreement, product documentation, or Customer’s configuration.

Unless expressly agreed in writing, HR Forte will not use Customer Personal Data to train public or third-party foundation models. Customer remains responsible for reviewing AI-generated outputs before using them for employment, payroll, disciplinary, performance, hiring, termination, or statutory compliance decisions. HR Forte's AI-enabled features are decision-support tools and should not be treated as a substitute for Customer's legal, HR, tax, or payroll judgment.

19. Integrations and customer-enabled third parties

Customer may choose to connect the Services with third-party systems, applications, vendors, or APIs. Where Customer enables such integrations, Customer instructs HR Forte to exchange Customer Personal Data with those third parties as necessary for the integration.

HR Forte is not responsible for third-party systems selected, authorised, or configured by Customer, except to the extent HR Forte acts as a Sub-processor or otherwise expressly agrees in writing. Customer is responsible for assessing the privacy, security, and legal suitability of customer-enabled third-party integrations.

20. Limitation of liability

The liability of each party under this DPA is subject to the limitations and exclusions of liability in the Agreement, unless prohibited by Applicable Data Protection Laws. Nothing in this DPA limits liability that cannot be limited under applicable law.

21. Term and termination

This DPA begins on the effective date of the Agreement or the date HR Forte first processes Customer Personal Data on behalf of Customer, whichever is earlier. This DPA continues for as long as HR Forte processes Customer Personal Data on behalf of Customer.

The termination or expiry of the Agreement will not relieve either party of obligations that by their nature should survive, including confidentiality, data deletion, retained records, audit cooperation, liability, and legal compliance obligations.

22. Order of precedence

If there is a conflict between this DPA and the Agreement regarding Customer Personal Data, this DPA prevails. If Standard Contractual Clauses or other mandatory transfer clauses apply, those clauses prevail over this DPA to the extent of any conflict concerning the restricted transfer.

Schedule 1: Details of processing

---

1. Subject matter

HR Forte processes Customer Personal Data to provide HR, payroll, workforce management,

employee self-service, claims, leave, document, reporting, time and attendance, compliance, integration, implementation, maintenance, and support services through the HR Forte SaaS platform.

2. Duration

Processing continues for the term of the Agreement and for any post-termination retention, backup, deletion, legal hold, or transition period described in the Agreement, this DPA, or Customer's written instructions.

3. Nature and purpose of processing

Processing activity	Purpose
Collection and upload	Customer uploads or enters employee, payroll, HR, and workforce data into the platform.
Storage and hosting	HR Forte stores Customer Personal Data in cloud or hosted environments to operate the Services.
Payroll and HR processing	HR Forte processes data to calculate payroll, manage leave, claims, attendance, employee records, documents, statutory data, reports, and workflows as configured by Customer.
User access and administration	HR Forte enables authorised users to access, manage, approve, export, or report on data based on permissions.
Support and troubleshooting	HR Forte may access Customer Personal Data where required to resolve support issues or maintain the platform.
Security and audit logging	HR Forte processes logs, metadata, access records, and security events to protect the Services.
Integrations	HR Forte exchanges data with customer-enabled systems and authorised third-party services where configured by Customer.
Backup and disaster recovery	HR Forte maintains backups and recovery processes to protect availability and integrity.
Compliance and legal obligations	HR Forte may process limited records where required by law, regulator, court order, audit, or dispute resolution.

4. Categories of Data Subjects

Customer Personal Data may relate to Customer's employees, former employees, workers, contractors, consultants, interns, temporary staff, job applicants if enabled, dependants,

beneficiaries, emergency contacts, customer administrators, authorised users, approvers, managers, payroll contacts, HR personnel, finance personnel, and other individuals whose data Customer submits to the Services.

5. Categories of Personal Data

Data category	Examples
Identity data	Name, employee ID, national ID, passport details, date of birth, gender, nationality, marital status, photograph where uploaded.
Contact data	Home address, phone number, email address, emergency contact details.
Employment data	Job title, department, location, manager, grade, employment status, start date, end date, contract details, work permit data where applicable.
Payroll and compensation data	Salary, allowances, deductions, bonuses, benefits, payroll history, tax data, statutory contributions, payslips, payroll reports.
Banking and payment data	Bank name, account number, payment instructions, reimbursement payment details.
Leave and attendance data	Leave balances, leave requests, approvals, attendance records, shift schedules, timesheets, GPS clock-in data where enabled.
Claims and expense data	Claim records, receipts, reimbursement details, approval comments.
Compliance and statutory data	Tax identifiers, social security numbers, statutory filings, immigration or work authorisation information where applicable.
Health or sensitive data	Medical certificates, disability information, sick leave records, insurance or benefits data, only where Customer uploads or configures such processing.
Documents	Employment contracts, policy acknowledgements, forms, letters, signed documents, uploaded supporting documents.
System and support data	User credentials, access logs, IP addresses, device details, audit trails, support tickets, error logs, configuration records.

6. Frequency of processing

Processing occurs continuously during Customer’s use of the Services and as otherwise necessary for support, maintenance, backup, reporting, security, and compliance purposes.

Schedule 2: Technical and organisational measures

Control area	Customer-facing commitment
Information security governance	HR Forte maintains security policies, assigns responsibility for information security, reviews risks, and operates controls appropriate to HR and payroll SaaS.
Access control	HR Forte applies role-based access controls, least privilege, account provisioning and de-provisioning processes, and administrative access controls.
Authentication	HR Forte supports secure authentication controls and may support multi-factor authentication depending on plan, configuration, or enterprise requirement.
Encryption	HR Forte uses encryption or equivalent safeguards for Customer Personal Data in transit and applies encryption or appropriate protection for data at rest where supported by infrastructure and service design.
Network and infrastructure security	HR Forte uses appropriate network segmentation, firewalls, secure configuration, vulnerability management, patching, and infrastructure monitoring.
Application security	HR Forte follows secure development practices, change control, code review, testing, and vulnerability remediation processes appropriate to the risk.
Logging and monitoring	HR Forte maintains security logs, access logs, and monitoring processes to detect, investigate, and respond to suspicious activity.
Support access	HR Forte restricts support access to authorised personnel and uses access controls, logging, and confidentiality obligations.
Backup and recovery	HR Forte maintains backup and recovery procedures designed to restore availability and access to Customer Personal Data in a timely manner after physical or technical incidents.
Incident management	HR Forte maintains an incident response process for identifying, investigating, mitigating, documenting, and communicating security incidents.
Personnel security	HR Forte personnel with access to Customer Personal Data are subject to confidentiality obligations and receive appropriate privacy or security

	awareness.
Vendor management	HR Forte assesses and manages material Sub-processors and requires contractual safeguards for Customer Personal Data.
Physical security	HR Forte relies on secure cloud or data centre facilities and applies appropriate office and device security controls for personnel environments.
Data segregation	HR Forte applies logical segregation and access controls appropriate to a multi-tenant SaaS environment.
Retention and deletion	HR Forte maintains retention, deletion, backup, and legal hold processes as described in this DPA and the Agreement.
Business continuity	HR Forte maintains business continuity and disaster recovery arrangements proportionate to the Services and customer subscription terms.
Testing and review	HR Forte periodically tests, assesses, or reviews security controls, including vulnerability assessments or penetration testing where appropriate.

Schedule 3: Sub-processors

Sub-processor	Purpose	Data processed
Amazon Web Services, Inc. and relevant affiliates	Cloud infrastructure, hosting, database hosting, storage, backup, security, availability, and related platform operations	Customer Personal Data hosted in the HR Forte platform, system logs, backup data, metadata
Scrut	Threat detection, vulnerability monitoring, audit logs, error monitoring, uptime monitoring, and incident response support.	Technical data, log data, security events, IP addresses, and usage metadata.
Hubspot	Support case management, user assistance, onboarding, issue tracking, and customer communications. Product analytics, website analytics, error analysis, performance measurement, and feature improvement.	Contact data, support tickets, communications data, screenshots or attachments submitted by users. Website data, usage data, technical data, and aggregated or pseudonymised metrics where possible.
Google Workspace and Microsoft 365	Account notifications, authentication messages, operational alerts, product communications, and user messaging.	Contact data, message metadata, and communication content where applicable.
Stripe & ZOHO Billings	Invoicing support, payment processing, account reconciliation, and billing administration.	Billing contact data, customer account details, invoice information, and payment-related references.
OpenWebUi	AskGenie and other AI-assisted functionality, where enabled and subject to customer configuration and contractual controls.	Prompts, outputs, usage metrics, and limited contextual data required to provide the feature.

Schedule 4: International transfer terms

1. EU and EEA transfers

Where the EU GDPR applies and Customer Personal Data is transferred from the European Economic Area to a country not recognised as adequate, the parties agree that the European Commission Standard Contractual Clauses, Module Two Controller-to-Processor, will apply unless another lawful transfer mechanism is available.

For purposes of the Standard Contractual Clauses, Customer is the **data exporter** and HR Forte is the **data importer**, unless the factual transfer arrangement requires a different designation. The details of processing in Schedule 1 and the security measures in Schedule 2 are incorporated into the applicable annexes.

2. UK transfers

Where the UK GDPR applies and Customer Personal Data is transferred from the United Kingdom to a country not recognised as adequate, the parties will use the UK International Data Transfer Addendum or another lawful UK transfer mechanism.

3. Singapore and Asia-Pacific transfers

Where the Singapore PDPA or other Asia-Pacific data protection laws require transfer safeguards, HR Forte will provide reasonable contractual, technical, and organisational safeguards for transfers performed by HR Forte. Customer remains responsible for ensuring that its use of the Services, transfer instructions, employee notices, and internal approvals satisfy Applicable Data Protection Laws.

4. Transfer impact and supplementary measures

Where required by Applicable Data Protection Laws, the parties will reasonably cooperate to assess transfer risks and identify supplementary measures. Such measures may include encryption, access controls, data minimisation, regional hosting options where available, contractual commitments, transparency reporting, or limits on support access.

Schedule 5: Retention, return, and deletion

Stage	Recommended HRF position
During subscription	Customer can access, correct, export, and delete data using available platform functions, subject to role permissions and module functionality.
Termination effective date	Customer should export required data before termination or request transition assistance in writing.
Standard post-termination period	HR Forte may retain Customer Personal Data for 180 days after termination to allow export, transition, dispute handling, or reactivation, unless a different period is stated in the Agreement.
Deletion from production systems	HR Forte deletes or de-identifies Customer Personal Data from production systems after the post-termination period, unless legally required to retain it.
Backup retention	Customer Personal Data may remain in encrypted or protected backups until overwritten according to HR Forte's normal backup cycle, typically **daily**.
Legal retention	HR Forte may retain limited records required for legal, tax, accounting, security, audit, regulatory, or dispute purposes.
Certification of deletion	Upon written request, HR Forte may provide written confirmation of deletion or de-identification, subject to backup and legal retention limitations.