Payhawk

Version 1.0
07.09.2023

DATA PROCESSING ADDENDUM

1. BACKGROUND

This Data Processing Addendum (hereinafter "DPA") is an integral part of and applicable together with the Payhawk Terms of Use (available at: https://payhawk.com/terms/, hereinafter the "Platform Agreement").

By clicking "I accept" using our Services, You agree to all terms and conditions of this DPA and the Terms of Use. This DPA applies to **You** (the "Client" or "Controller") and Payhawk Limited (the "Processor" or "Payhawk").

Both the Controller and the Processor shall be collectively referred to as the **Parties**, and each individual as the **Party**.

The purpose of this DPA is to lay down the rights and obligations of the Parties with regards to the processing of Personal Data for the provision of the Services under the Platform Agreement.

2. DEFINITIONS

Other capitalised notions used in the Agreement shall have the following meaning:

"**Data Controller**", "**Data Processor**", **Data Subject**", "**Processing**", "**Process**" and "**Processed**" each have the meaning set out in the Data Protection Legislation.

"Data Protection Legislation" means: all applicable data privacy, data protection laws, and regulations to which the Personal Data under this Privacy Policy is subject to. Data Protection Legislation shall include, but not be limited to the EU General Data Protection Regulation 2016/679 ("**EU GDPR**"), the Data Protection Act 2018 ("**UK-GDPR**"), the California Consumer Privacy Act of 2018 ("**CCPA**") and the Swiss Federal Data Protection Act and its implementing regulations ("**Swiss DPA**") in each case as may be amended, superseded or replaced from time to time, as well as the local data protection legislative acts of the countries where Payhawk operates**.**

"Personal Data" means any information relating to an identified or identifiable natural person that is Processed in connection with the Services and includes "Personal Data" and "personal information" as defined under applicable Data Protection Legislation.

"Sub-Processor(s)" means any entity (including the third parties or the persons associated with the Processor) appointed by the Processor or the person associated with the Processor for processing of Personal Data on behalf of the Controller for the provision of the Services under the Platform Agreement.

"Technical and Organizational measures" means the technical and organisational measures for the security of the Personal Data in scope of the processing, agreed between the parties, taking into account Article 32 of the GDPR and other Data Protecion Legislation, as applicable.

"Payhawk Platform" means the Payhawk Software-as-a-service (SaaS) solution that allows the Client to use the Services throughout the term of the Platform Agreement.

Other notions are understood as defined in the Data Protection Legislation and the Platform Agreement.

Payhawk Limited, 1 Waterhouse Square, London, EC1N 2ST United Kingdom, registered in London, UK with UIC 11747263 and VAT GB358714764

phone: +44 20 3868 8704
email: support@payhawk.com
website: www.payhawk.com

3. PROCESSOR'S OBLIGATIONS

3.1. The Processor undertakes:

(a) to ensure that the processing of Personal Data in scope of the present DPA is done in compliance with the the Data Protection Legislation and recommendations of the supervisory authorities;

(b) to implement appropriate Technical and Organisational Measures to ensure an appropriate level of security of the Personal Data processed on behalf of the Controller. Such measures must at least ensure the protection of the Personal Data against destruction, alteration and dissemination;

(c) to process the Personal Data in scope of the present DPA only on the documented instructions (including electronically) from the Controller, including with regard to transfers of Personal Data to a third country or an international organisation. The Parties aknowledge and agree that the use of the Payhawk Platform by the Client's Users constitutes the Client's documented instructions to Payhawk regarding the processing of the Personal Data in scope;

(d) to assist the Controller in fulfilling its obligations arising out of the Data Protection Legislation;

(e) to ensure confidentiality of the Personal Data processed by Payhawk as well as other information pertaining to the processing of Personal Data;

(f) to notify the Controller without undue delay of any situations where the Processor must disclose the Personal Data processed on behalf of the Controller in breach of the obligations stipulated in the Data Protection Legislation. If the Processor is obligated to disclose the Personal Data to comply with its statutory obligations or a regulatory request, the Processor shall also adhere to the following rules: (i) disclose as minimum Personal Data as possible, i.e. only the amount of Personal Data and the Personal Data of the nature which is mandatory to disclose when complying with the statutory obligation or regulatory request; and (ii) disclose the Personal Data only to those third parties a disclosure to which is mandatory when complying with the statutory duty; and (iii) the Processor shall demand from such third parties (each of them) to keep the Personal Data confidential;

4. SUB-PROCESSORS

4.1. The Controller hereby grants the Processor a general authorization to engage Sub-Processors for the provision of the Services under the Platform Agreement, pursuant to the terms for engaging Sub-Processers as provided and agreed hereunder.

4.2. The Processor undertakes to engage only Sub-Processors, which offer an adequate level of technical and organizational measures so that the Personal Data processing complies with the requirements of the GDPR/UK-GDPR, the Data Protection Legislation, and ensures safeguarding of the rights of the data subjects.

4.3. It remains understood between the Parties that the Processor shall remain fully liable for the actions of its Sub-Processors and shall ensure that each Sub-Processor complies with the requirements of the Data Protection Legislation and the provisions of the present DPA.

5. PERSONAL DATA BREACHES

5.1. If the Processor (or any Sub-Processor) becomes aware of a Personal Data breach (incident) which affects or may affect the Personal Data, processed on behalf of the Controller, the Processor must notify the Controller thereof without undue delay and at least within 24

Payhawk Limited, 1 Waterhouse Square, London, EC1N 2ST United Kingdom, registered in London, UK with UIC 11747263 and VAT GB358714764

phone: +44 20 3868 8704
email: support@payhawk.com
website: www.payhawk.com

(twenty-four) hours of the acknowledgement of such breach, and provide the Controller with comprehensive information enabling the latter to fulfil its obligations of notifying the supervisory authority and/or data subjects of the Personal Data breach in accordance with the requirements of the Data Protection Legislation.

5.2. The Processor shall document all Personal Data breaches, comprising the facts relating to the Personal Data breach, its effects and the remedial actions taken. At the Controller's request, the Processor shall make such documents available (especially when such documents are requested by the supervisory authority).

5.3. The Processor shall actively cooperate with the Controller and take commercially reasonable steps which would (i) contribute to investigating the actual or potential Personal Data breach, (ii) assist in mitigating and otherwise remedying the consequences caused by such Personal Data breach, and (iii) help to prevent occurrence of Personal Data breaches of identical or similar nature in the future.

6. RETURN AND DELETION OF PERSONAL DATA

6.1. Within ninety (90) days from the expiry, termination or cancellation of the present DPA, the Processor undertakes to destroy or return the Personal Data received from the Controller on the basis of the Platform Agreement and the present DPA. The Processor shall ensure that its Sub-Processor(s) shall also destroy or return the received Personal Data, within thirty (90) days from the expiry, termination or cancellation of the present DPA.

6.2. The Processor shall be entitled to keep the Personal Data received from the Controller to the extent the Personal Data is necessary for compliance with the requirements of the applicable legal acts, while ensuring the protection and confidentiality of the Personal Data.

7. AUDIT

7.1. Subject to the Controller's written request, made at least thirty (30) days in advance ("Audit Request"), the Processor shall allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller. Such Audit Request shall include at least the scope and duration of the audit and shall not be conducted more than once per year. The audit must also be conducted during regular business hours, so that it does not undermine the ordinary activities of the Processor.

7.2. Subject to the Controller's written request at least thirty (30) days in advance, the Processor shall provide the Controller with all information necessary to demonstrate compliance with the obligations laid down in the GDPR/UK-GDPR, the Data Protection Legislation and the provisions of the present DPA.

7.3. The Processor undertakes to notify the Controller without undue delay of any changes in the technical or organizational measures which may affect the data processing operations carried out when performing the Platform Agreement and this DPA.

7.4. All audits, inspections and information requests, under this DPA, shall be limited strictly to the purposes of Payhawk's compliance with the Data Protection Legislation as a Processor and the provisions of this DPA.

8. TRANSFER OF PERSONAL DATA

8.1. If it is necessary for the performance of the Platform Agreement and/or fulfilment of the requirements of applicable legal acts, the Processor or its Sub-Processor(s) may transfer the

Payhawk Limited, 1 Waterhouse Square, London, EC1N 2ST United Kingdom, registered in London, UK with UIC 11747263 and VAT GB358714764

phone: +44 20 3868 8704
email: support@payhawk.com
website: www.payhawk.com

Personal Data outside the EEA and/or the UK to a specific data recipient only by duly complying with the provisions of Chapter V of the GDPR/UK-GDPR (in such case the Processor shall remain liable for adequate compliance with the Data Protection Legislation when transferring the data outside the EEA or UK).

9. LIABILITY AND INDEMNITY

9.1. Each Party defaulting on its performance or inadequately performing its obligations assumed under the DPA shall indemnify for the direct damages of the other Party sustained as a result.

9.2. The Processor's liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Platform Agreement.

9.3. In the event the Processor does not perform its obligations set forth in the DPA, the Controller's written instructions (including those transmitted electronically), and/or the requirements of the Data Protection Legislation, the Controller shall have the right: (i) to terminate the Platform Agreement unilaterally with a notice given to the Processor at least thirty (30) calendar days in advance, if the corresponding infringements have not been eliminated by the Processor within the specified time limit, and/or (ii) to prohibit the Processor, without delay and without any prior notice, from further processing of the Personal Data.

10. GENERAL PROVISIONS

10.1. The present Agreement shall come into effect and remain valid for the term of the Platform Agreement and shall be effective for an additional period after the expiry of the Platform Agreement as long as necessary to duly fulfil the obligations relating to the Personal Data processing outstanding after the expiry of the Platform Agreement (or for a longer period if it is provided for in applicable legal acts).

10.2. Clause, Schedule and paragraph headings shall not affect the interpretation of this DPA.

10.3. The Schedules form part of this DPA and shall have effect as if set out in full in the body of this DPA. Any reference to this DPA includes the Schedules.

10.4. Unless the context otherwise requires, words in the singular shall include the plural and in the plural shall include the singular, and a reference to one gender shall include a reference to the other genders.

10.5. A reference to a statute or statutory provision is a reference to it as amended, extended or re-enacted from time to time and shall include all subordinate legislation made from time to time under that statute or statutory provision.

10.6. Any words following the terms including, include, in particular or for example or any similar phrase shall be construed as illustrative and shall not limit the generality of the related general words.

10.7. In the case of conflict or ambiguity between any of the provisions of this DPA and the provisions of the Terms of Use, the provisions of this DPA shall prevail.

10.8. A reference to writing or written includes faxes and email.

11. GOVERNING LAW

11.1. The present Agreement shall be governed by the law applicable to the Platform Agreement.

12. JURISDICTION

12.1. In case of any dispute in relation with this DPA, the courts stipulated in the "Jurisdiction" section under the Platform Agreement shall have exclusive

Payhawk Limited, 1 Waterhouse Square, London, EC1N 2ST United Kingdom, registered in London, UK with UIC 11747263 and VAT GB358714764

phone: +44 20 3868 8704
email: support@payhawk.com
website: www.payhawk.com

jurisdiction. This is without limitation of the right of either Party to seek the mediation of competent mediation services with a view to settling the dispute amicably.

13. FINAL PROVISIONS

13.1. Each Party shall assume the obligation to inform, in an adequate manner complying with the provisions of the Data Protection Legislation, all natural persons (Parties' employees, authorized persons and other representatives) engaged for the performance of the Platform Agreement and the DPA where the Personal Data of such persons are or may be shared with the other Party as a result (e.g., in the process of electronic communication among the Parties' employees, etc.) or for the purposes and on the basis of proper performance of this DPA and the Platform Agreement.

Payhawk Limited, 1 Waterhouse Square, London, EC1N 2ST United Kingdom, registered in London, UK with UIC 11747263 and VAT GB358714764

phone: +44 20 3868 8704
email: support@payhawk.com
website: www.payhawk.com

SCHEDULE 1 – Description of the Processing of Personal Data

Subject Matter	**Processing of Personal Data on behalf of the Controller for the provision of the Services under the Platform Agreement.**
Categories of Data Subjects	**Individuals, authorized to use the Payhawk Platform on behalf of the Controller.**
Categories of Personal Data	**Personal Data uploaded on behalf of the Controller to the Payhawk Platform.**
Special Categories of Personal Data	**N/A**
Duration of the Processing	**For the duration of the Platform Agreement.**
Processing operations	**Personal Data cloud storage.**
Contact details for Payhawk	**Mihail Yanev, Data Protection Officer (DPO): dpo@payhawk.com**

SCHEDULE 2 – List of Sub-Processors

Sub-Processor	***Service***	***Country***
Amazon Web Services EMEA SARL (AWS)	**Cloud data storage**	**Luxembourg**
Google Cloud EMEA Limited	**Cloud data storage**	**Ireland**
Payhawk Subsidiaries: Payhawk EOOD Payhawk GmbH Payhawk S.L. Payhawk SAS Payhawk B.V.	**Payhawk Group operations**	**Bulgaria, Germany, Spain, Netherlands, France**

SCHEDULE 3 – Technical and Organizational Measures

1. Third-party security certifications

At the time of this DPA, Payhawk is certified under the following information security standards:

- **PSI-DSS (The Payment Card Industry Data Security Standard)**
- **SOC 2, type 2**
- **SOC 1, type 1**
- **ISO 27001:2017**
- **UK Cyber Essentials**

2. Technical and Organizational measures

The following Schedule sets out the particular Technical and Organizational Measures (TOMs) that Payhawk applies to the Processing of Personal Data under this DPA, which offer sufficient guarantees for the purposes of Data Protection Legislation.

Task	***Current Security Measures***	***Responsibility***	***Policy***
Training & Awareness	Conducting regular training to all employees and new joiners regarding data protection and information security.	Information Security and Data Protection teams	Security Awareness Program/Data Protection Awareness Program
Third Party Processors	Conducting data protection compliance due diligence and information security audit before entering into any relationship which includes processing of Personal Data	Information Security and Data Protection teams	Vendor Management Policy
Third-Party Penetration Tests	Third-party penetration tests are conducted against the application and supporting infrastructure at least annually. Any findings as a result of tests are tracked to remediation. Reports are available on request with an appropriate NDA in place.	Information Security team	Information Security Policy
Data Centers Infrastructure Security	Our cloud service providers employ robust controls to secure the availability and security of our servers. This includes measures such as backup power, fire detection and suppression equipment, secure device destruction amongst others.	Information Security team	Information Security Policy

Payhawk Limited, 1 Waterhouse Square, London, EC1N 2ST United Kingdom, registered in London, UK with UIC 11747263 and VAT GB358714764

phone: +44 20 3868 8704
email: support@payhawk.com
website: www.payhawk.com

Data Centers Onsite Security	Our cloud service providers implement layered physical security controls to ensure on-site security including vetted security guards, fencing, video monitoring, intrusion detection technology, and more.	Information Security team	Information Security Policy
Access Control	Access is limited by following the least privilege model required for our staff to carry out their jobs. This is subject to frequent internal audits and technical enforcement and monitoring to ensure compliance. 2FA is required for all production systems.	Information Security team	Access Control Policy
Threat Detection	Payhawk leverages threat detection services within AWS to continuously monitor for malicious and unauthorized activity.	Information Security team	Information Security Policy
Vulnerability Scanning	We perform regular internal scans for vulnerability scanning of infrastructure and applications. Where issues are identified these are tracked until remediation.	Information Security team	Information Security Policy
DoS Mitigation	Payhawk uses a number of DDoS protection strategies and tools layered to mitigate DDoS threats. We utilize AWS Shield's sophisticated CDN with built-in DDoS protection as well as native AWS tools and application-specific mitigation techniques.	Information Security team	Information Security Policy
Encryption (in transit)	Communication with Payhawk is encrypted with TLS 1.2 or higher over public networks. We monitor community testing & research in this area and continue to adopt best practices in terms of cipher adoption and TLS configuration.	Information Security team	Information Security Policy
Encryption (at rest)	Payhawk data is encrypted at rest with industry-standard AES-256 encryption. By default, we encrypt at the asset or object level.	Information Security team	Information Security Policy
Disaster Recovery	In the event of a major region outage, Payhawk has the ability to deploy our application to a new hosting region. Our Disaster	Information Security team	Business Recovery Policy and Business

Payhawk Limited, 1 Waterhouse Square, London, EC1N 2ST United Kingdom, registered in London, UK with UIC 11747263 and VAT GB358714764

phone: +44 20 3868 8704
email: support@payhawk.com
website: www.payhawk.com

	Recovery plan ensures the availability of services and ease of recovery in the event of such a disaster. This plan is regularly tested and reviewed for areas of improvement or automation.		Continuity Policy
Quality Assurance	Payhawk's Quality Assurance process reviews and tests the codebase. The security team has resources to investigate and recommend remediation of security vulnerabilities within code. Regular syncs, training, and security resources are provided to the QA team.	Information Security and Quality Assurance teams	Information Security Policy
Environment Segregation	Testing, staging, and production environments are separated from one another. No customer data is used in any non-production environment.	Information Security team	Information Security Policy
Security Champions	Payhawk runs a Security Champions program with involvement and contributions from each of the development teams.	Information Security team	Security Champions Program
Laptops (Remote Access)	Password protected – complex user ID passwords, authorized user access only, device hard drive encryption; Anti-virus/Anti malware software installed and functional on all workstations, software to prohibit high risk malware sites, security software messages, virus definition files automatically updated daily, virus logs gathered to central location and reviewed regularly by I.T.	IT management team	IT Management Policy

Payhawk Limited, 1 Waterhouse Square, London, EC1N 2ST United Kingdom, registered in London, UK with UIC 11747263 and VAT GB358714764

phone: +44 20 3868 8704
email: support@payhawk.com
website: www.payhawk.com

Firewalls & Internet Gateways	Well configured software-based firewall is installed and functional, annual Firewall rule validation, no access to untrustworthy sites, warning messages, intrusion detection, authorized user only - access and management security devices such as routers, switches, firewalls, intrusion detection system, intrusion prevention system, content filtering solution, anti-spam devices.	IT management team	IT Management Policy
Patch Management & Software Update	Regular computer equipment and software maintenance, virus definition files automatically updated daily.	IT management team	IT Management Policy

Payhawk Limited, 1 Waterhouse Square, London, EC1N 2ST United Kingdom, registered in London, UK with UIC 11747263 and VAT GB358714764

phone: +44 20 3868 8704
email: support@payhawk.com
website: www.payhawk.com