

Data processing agreement

This Data Processing Agreement (“the DPA”) is entered into between:

1. PA FINANCE HOLDINGS LTD,
incorporated and registered in England and Wales with company number 14059331, whose registered office is at 80 Coleman Street, London, England, EC2R 5BJ (“the Controller” or “PAYALLY”); and
2. The Introducer,
who has entered into an Engagement Letter (“the Letter”) and agreed to the Introduction Terms and Conditions (“the Terms”) (together, “the Engagement Documents”) governing its relationship with the Introducer,

(each a “Party” and together “the Parties”).

This DPA forms an integral part of the Engagement Documents and sets out the terms and conditions under which the Introducer, when acting as a data processor, may process personal data on behalf of the Introducer in accordance with applicable data protection legislation, including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and where applicable, the EU General Data Protection Regulation (EU GDPR) and other data protection laws (collectively, “the Data Protection Laws”).

Terms and conditions

1. Definitions and interpretation

1.1. The definitions of the Data Protection Laws (as defined below) apply to this Agreement. In addition, the following definitions shall be applicable:

Authorised Persons

the persons that the Introducer authorises to give to the Controller the Personal Data processing instructions pursuant to clause 2.1.

Business Purposes

legitimate interest of the Controller, namely: a) to enable the Introducer to introduce prospective clients to the Controller and/or members of its group; b) to assess the suitability of referred contacts for the Controller’s services and conduct initial eligibility and risk assessments; c) to contact the referred individuals for the purposes of offering, explaining, or confirming interest in the financial services provided by the Controller; d) to provide financial services (such as multi-currency payments, safeguarded accounts, and related support) to referred clients after a Relevant Contract is entered into; e) to fulfill the Controller’s obligations under applicable laws, including anti-money laundering (AML), know-your-customer (KYC), and financial services regulations; f) to maintain records of introductions, client interactions, and commissions payable, and for audit or regulatory reporting; g) to track successful introductions and calculate commissions due to the Introducer.

Data Protection Legislation

all applicable privacy and data protection laws, including the UK GDPR, the Data Protection Act 2018, EU GDPR and any applicable national implementing laws, regulations and secondary legislation relating to the processing of the Personal Data.

Data Subject

An individual associated with a prospective or actual end customer of the Controller, whose Personal Data is disclosed to or processed by the Introducer in the course of providing introduction services, and whose Personal Data is processed under this Agreement.

End Customer

a legal entity that purchases or otherwise acquires the product or service of the Introducer for its own internal use and not for resale, redistribution, or further sublicensing.

GDPR

the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC.

Group

a group of affiliated companies with PAYALLY engaged in providing financial services to clients. The Group’s activities and services include the offering of comprehensive financial services, including multi-currency payments, safeguarded accounts, and dedicated support.

Personal Data

means any information relating to an identified or identifiable natural person which is processed as a result of, or in connection with, the provision of the access to the System; an identifiable natural person is the one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing, processes and process

any activity or set of activities which is performed on the Personal Data or on sets of the Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, viewing, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Personal Data Breach

a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to or use of, the Personal Data transmitted, stored or otherwise processed.

Data processing agreement

Services

the services provided by PAYALLY and the Group, including, among others, activities conducted under the Financial Conduct Authority (FCA) license 944721, which is held by PAYALLY Limited with company number 10600055.

Subprocessor

any person appointed by or on behalf of Processor to process Personal Data on behalf of the Introducer in connection with the Agreement.

System

an internal system of the Party used for the Party's operational activity and providing End Customer Services.

UK GDPR

the General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019.

1.2. Any Annexes to this Agreement form a part of this Agreement and will have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes Annexes.

2. Personal Data processing

2.1. The Introducer and the Controller acknowledge and agree that for the purpose of the Data Protection Legislation:

1. The Parties acknowledge and agree that, for the purposes of the Data Protection Legislation, the Introducer acts as a data controller in respect of the Personal Data it collects from individuals ("Data Subjects") and subsequently provides to the Controller. The Controller shall act as a separate and independent controller and process such Personal Data strictly for the Business Purposes and in accordance with this Agreement.
2. The Introducer confirms that it has obtained all necessary consents, authorisations, and/or other legal bases required under the Data Protection Legislation from the Data Subjects to lawfully disclose and transfer their Personal Data to the Controller for the Business Purposes set out in this Agreement.
3. The scope of any access to Personal Data and the manner of processing may only be extended or amended upon prior written agreement between the Parties, and subject to compliance with applicable Data Protection Legislation.
4. The processing of Personal Data shall be carried out within the United Kingdom, unless otherwise permitted by law and agreed by the Parties in writing, subject to adequate safeguards being in place in accordance with the Data Protection Legislation.

3. Controller's obligations

3.1. The Controller as the Processor shall:

- i. process the Personal Data only to the extent and in such a manner as is strictly necessary for the Business Purposes and this Agreement. The Controller shall also process Personal Data in accordance with the Introducer's written instructions from Authorised Persons, if applicable. The Controller shall not process the Personal Data for any other purpose or in a way that does not comply with this Agreement, the Data Protection Legislation or the Business Purposes;
- ii. promptly comply with any of the Introducer's requests or instructions from the Authorised Persons requiring the Controller to rectify, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing. The Controller must promptly notify the Introducer if the Introducer's instruction would not comply with Data Protection Legislation;
- iii. maintain the confidentiality of all Personal Data and shall not disclose the Personal Data to any third party unless the Introducer or this Agreement generally authorises the disclosure or as required by the applicable law. If a law, court, regulator or supervisory authority requires the Controller to process or disclose the Personal Data, the Controller shall first inform the Introducer of the legal or regulatory requirement and give the Introducer an opportunity to object or challenge the requirement unless the applicable law or the Data Protection Legislation prohibits such notice; and
- iv. reasonably assist the Introducer with meeting the Introducer's compliance obligations under Data Protection Legislation, taking into account the nature of the Controller's processing and the information available to the Controller, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with supervisory authorities under the Data Protection Legislation.

4. Controller's personnel

4.1. The Controller shall ensure that all of its personnel

- i. are informed of the confidential nature of the Personal Data kept in the System and are bound by confidentiality obligations and use restrictions in respect of the Personal Data set out in this Agreement;
- ii. have undertaken training on the Data Protection Legislation relating to handling Personal Data and how it applies to their particular duties; and
- iii. are aware of both Controller's duties and their personal duties and obligations under the Data Protection Legislation and this Agreement.

4.2. The Controller shall take reasonable steps to ensure the reliability, integrity and trustworthiness of and conduct background checks consistent with applicable law on all of Controller's personnel with access to the Personal Data.

Data processing agreement

5. Data Protection and Security

- 5.1. The Controller must at all times implement appropriate technical and organisational measures against unauthorised or unlawful processing, access, use, disclosure, copying, modification, storage, reproduction, display or distribution of the Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data as required by the Data Protection Legislation.
- 5.2. The Controller shall keep detailed, accurate and up-to-date records on actions committed by the Introducer and the Controller personnel in order to ensure records of compliance with obligations under this Agreement and the Controller shall provide the Introducer with copies of the Records upon request.

6. Personal Data Breach

- 6.1. The Controller shall promptly and without undue delay notify the Introducer if any Personal Data is lost or destroyed or becomes damaged, corrupted, or unusable. The Controller will restore such Personal Data at its own expense.
- 6.2. The Controller shall immediately and without undue delay notify the Introducer if it becomes aware of
- i. any accidental, unauthorised or unlawful processing of the Personal Data; or
 - ii. any Personal Data Breach.
- 6.3. Where the Controller becomes aware of (1) and/or (2) above, it shall, without undue delay, also provide the Introducer with the following information:
- i. description of the nature of (1) and/or (2), including the categories and an approximate number of both Data Subjects and Personal Data records concerned; ii. the likely consequences; and
 - ii. description of the measures taken or proposed to be taken to address (1) and/or (2), including measures to mitigate its possible adverse effects.
- 6.4. Immediately following any unauthorised or unlawful Personal Data processing or Personal Data Breach, the Parties shall coordinate with each other to investigate the matter. The Controller shall reasonably cooperate with the Introducer in the Introducer's handling of the matter, including
- i. assisting with any investigation;
 - ii. providing the Introducer with physical access to any facilities and operations affected;
 - iii. facilitating interviews with the Controller's employees, former employees and others involved in the matter;
 - iv. making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by the Introducer; and
 - v. taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or unlawful Personal Data processing.
- 6.5. The Controller shall not inform any third party of any Personal Data Breach without first obtaining the Introducer's prior written consent, except when required to do so by the applicable law.
- 6.6. The Controller agrees that the Introducer has the sole right to determine:
- i. whether to provide notice of the Personal Data Breach to any Data Subjects, supervisory authorities, regulators, law enforcement agencies or others, as required by law or regulation or in the Introducer's discretion, including the contents and delivery method of the notice; and
 - ii. whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

7. Subprocessors

The Controller may not authorise a subprocessor to process the Personal Data.

8. Recipients

The Parties agree that any transfer of the Personal Data from the Controller to a third party will be possible only if required by the applicable law.

9. Complaints, Data Subject Requests and Third-Party Rights

- 9.1. The Controller shall, at no additional cost, take such technical and organisational measures as may be appropriate and promptly provide such information to the Introducer as the Introducer may reasonably require to enable the Controller to comply with:
- i. the rights of Data Subjects under the Data Protection Legislation, including subject access and portability rights, the rights to rectify and erase the Personal Data, object to the processing and automated processing of the Personal Data, and restrict the processing of the Personal Data; and
 - ii. information or assessment notices served on the Introducer by any supervisory authority under the Data Protection Legislation.
- 9.2. The Controller shall notify the Introducer immediately if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either Party's compliance with the Data Protection Legislation.

Data processing agreement

9.3. The Controller shall give the Introducer its full cooperation and assistance in responding to any complaint, notice, communication or the Data Subject request.

9.4. The Controller shall not disclose the Personal Data to any Data Subject or to a third party other than at the Introducer's request or instruction, as provided for in this Agreement or as required by the applicable law.

10. Term and termination

10.1. This Agreement will remain in full force and effect until it is terminated by the Parties in accordance with this clause.

10.2. Any provision of this Agreement that expressly should come into or continue in force on or after the termination of this Agreement in order to protect Personal Data will remain in full force and effect.

10.3. The Introducer may terminate this Agreement immediately at its own discretion on written notice to the Controller without further liability or obligation.

10.4. If a change in any Data Protection Legislation prevents either Party from fulfilling all or part of its obligations under this Agreement, the Parties will suspend the processing of Personal Data until that processing complies with the new requirements. If the Parties are unable to bring the Personal Data processing into compliance with the Data Protection Legislation within 1 (one) month, they may terminate this Agreement on 30 (thirty) days prior written notice to the other Party.

11. Data Return and Destruction

11.1. At the Introducer's request, the Controller shall give the Introducer a copy of internal document, confirming access to all or part of the Introducer's and/or End Customers Personal Data in its possession or control in the format and on the media reasonably specified by the Introducer.

11.2. The Controller shall cease any processing and delete and/or return if requested in writing by the Introducer, all or any Personal Data related to this Agreement upon instruction from the Introducer or expiry of the term of this Agreement.

11.3. If any law, regulation, or government or regulatory body requires the Controller to retain any documents or materials that the Controller would otherwise be required to return or destroy, it will notify the Introducer in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends.

11.4. Where the Introducer has instructed that any Personal Data be deleted, the Controller will certify in writing that it has destroyed the Personal Data within 3 (three) calendar days after it completes the destruction.

12. Audit rights

Subject to this section, the Controller shall make available to the Introducer on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Introducer or an auditor mandated by the Introducer in relation to the Processing of the Introducer's and/or End Customers' Personal Data by the Sub-processors.

13. Breach Notification

13.1. If a Personal Data Breach occurs or is occurring, or the Controller becomes aware of a breach of any of its obligations under this Agreement or any Data Protection Legislation, Controller shall:

- i. promptly conduct its own audit to determine the cause;
- ii. produce a written report that includes detailed plans to remedy any deficiencies identified by the audit;
- iii. provide the Introducer with a copy of the written audit report; and
- iv. promptly remedy any deficiencies identified by the audit.

14. Warranties

14.1. The Controller warrants and represents that:

1. its employees, subcontractors, agents and any other person or persons accessing Personal Data on its behalf are reliable and trustworthy and have received the required training on the Data Protection Legislation relating to the Personal Data;
2. it and anyone operating on its behalf will process the Personal Data in compliance with the Data Protection Legislation and other laws, enactments, regulations, orders, standards and other similar instruments; and
3. considering the current technology environment and implementation costs, it will take appropriate technical and organisational measures to prevent the unauthorised or unlawful processing of the Personal Data and the accidental loss or destruction of, or damage to, the Personal Data, and ensure a level of security appropriate to:
 - i. the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage; ii. the nature of the Personal Data protected; and
 - ii. comply with all applicable Data Protection Legislation and its information and security policies.

Data processing agreement

15. Indemnification and Liability

15.1. Each Party (“Indemnifying Party”) shall indemnify, defend and hold harmless the other Party (“Indemnified Party”) from and against any and all direct losses, liabilities, damages, claims, costs, or expenses (including reasonable legal fees) arising out of or in connection with any breach of this Agreement or the Data Protection Legislation caused by the Indemnifying Party, its employees, agents or subcontractors, to the extent such breach results in a claim, fine, or other regulatory action against the Indemnified Party.

15.2. Liability for Damages.

Each Party shall be liable for damages caused by it, its employees, or authorised agents in connection with the performance of this Agreement, including but not limited to unauthorised or unlawful processing, loss or destruction of Personal Data, where such damage is due to negligence, breach of contract, or wilful misconduct.

15.3. Limitation of Liability.

Subject to clause 15.4 below, the total liability of either Party to the other, whether in contract, tort (including negligence), breach of statutory duty or otherwise, arising under or in connection with this Agreement shall be limited to £2,000,000 (two million pounds sterling) in aggregate.

15.4. Exclusions from Limitation.

Nothing in this Agreement shall limit or exclude either Party’s liability for:

- A. death or personal injury caused by its negligence;
- B. fraud or fraudulent misrepresentation;
- C. breach of confidentiality or data protection obligations under this Agreement where such breach results in regulatory fines, enforcement actions, or claims by data subjects; or
- D. any other liability which cannot be limited or excluded under applicable law.

16. Notice and the DPO

Any notice or other communication given to the Introducer under or in connection with this Agreement must be in writing and delivered to: legal@payally.com.

17. Governing Law and Dispute Resolution

This Agreement shall be governed by the laws of the England and Wales. Disputes arising from this Agreement shall be resolved exclusively in the courts of the England and Wales.

18. Miscellaneous Provisions

18.1. Neither Party shall assign its rights or obligations under this Agreement.

18.2. Any amendments to this Agreement must be in writing and signed by both Parties.

18.3. Any notice under this Agreement shall be in writing and delivered by hand, sent by registered mail, registered courier or transmitted by email.

Data Protection Officer of the Controller (Name, Contact Details):	data.protection@payally.com
The Introducer's email address to be used by Data Subjects to submit any requests they may have in line with the Applicable Laws shall be:	As stipulated in the Introducere’s application to PAYALLY

The Introducer agrees that the Controller may provide this email to Data Subjects without prior notice.

Data processing agreement

Annex A - Details of Processing the Personal Data

The Parties agreed that the foregoing is not intended to be an exhaustive list of applicable parameters.

1. Scope

The subject matter of the Processing of Introducer's Personal Data pertains to the Business Purposes.

2. The categories of Data Subjects whose Personal Data will be Processed by the Controller:

- 2.1. the Introduced Clients of the Introducer
- 2.2. the Introducer's employees

3. The types of Data Subjects whose Personal Data will be Processed by the Controller:

- 3.1. Data provided by the Introducer:
full name, date of birth, geolocation, address, email, phone number, position, name, payment information.
- 3.2. Technical data:
IP address, UTM parameters, geolocation, device type, browser type, cookies, and session ID.
- 3.3. For the purposes of this clause
 - A. full name includes name, parental name and surname
 - B. contact details include phone, address and email
 - C. payment information includes bank details, bank card details, bank ID.
 - D. session ID includes interaction with the site, the name of the site from which the user went to our site, the functions used, the pages viewed on our site, the way of usage of our site, and the actions taken if such actions are present.

4. Processing operations

The Personal Data will be subject to the following basic processing activities: viewing, compliance, records keeping